Tight Lower Bounds for the Complexity of Multic Peace for the Complexity of Multicoloring∗†

Marthe Bonamy¹, Łukasz Kowalik², Michał Pilipczuk³, Arkadiusz Socała⁴, and Marcin Wrochna⁵

1 CNRS, LaBRI, Bordeaux, France
marthe.bonamy@labri.fr
2 University of Warsaw, Warsaw, Poland
kowalik@mimuw.edu.pl
3 University of Warsaw, Warsaw, Poland
michal.pilipczuk@mimuw.edu.pl
4 University of Warsaw, Warsaw, Poland
arkadiusz.socala@mimuw.edu.pl
5 University of Warsaw, Warsaw, Poland
m.wrochna@mimuw.edu.pl

Abstract

In the multicoloring problem, also known as \((a:b)\)-coloring or \(b\)-fold coloring, we are given a graph \(G\) and a set of \(a\) colors, and the task is to assign a subset of \(b\) colors to each vertex of \(G\) so that adjacent vertices receive disjoint color subsets. This natural generalization of the classic coloring problem (the \(b = 1\) case) is equivalent to finding a homomorphism to the Kneser graph \(KG_{a,b}\), and gives relaxations approaching the fractional chromatic number.

We study the complexity of determining whether a graph has an \((a:b)\)-coloring. Our main result is that this problem does not admit an algorithm with running time \(f(b) \cdot 2^{o\left(\log b\right)} \cdot n\), for any computable \(f(b)\), unless the Exponential Time Hypothesis (ETH) fails. A \((b + 1)^n \cdot \text{poly}(n)\)-time algorithm due to Nederlof [2008] shows that this is tight. A direct corollary of our result is that the graph homomorphism problem does not admit a \(2^{O(n + h)}\)-algorithm unless ETH fails, even if the target graph is required to be a Kneser graph. This refines the understanding given by the recent lower bound of Cygan et al. [SODA 2016].

The crucial ingredient in our hardness reduction is the usage of detecting matrices of Lindström [Canad. Math. Bull., 1965], which is a combinatorial tool that, to the best of our knowledge, has not yet been used for proving complexity lower bounds. As a side result, we prove that the running time of the algorithms of Abasi et al. [MFCS 2014] and of Gabizon et al. [ESA 2015] for the \(r\)-monomial detection problem are optimal under ETH.

1998 ACM Subject Classification G.2.2 Graph Theory, F.2.2 Nonnumerical Algorithms and Problems

Keywords and phrases multicoloring, Kneser graph homomorphism, ETH lower bound

Digital Object Identifier 10.4230/LIPIcs.ESA.2017.18

* A full version of the paper is available at https://arxiv.org/abs/1607.03432.
† Work supported by the National Science Centre of Poland, grants number 2013/11/D/ST6/03073 (MP, MW) and 2015/17/N/ST6/01224 (AS). The work of Ł. Kowalik is a part of the project TOTAL that has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement No 677651). Michał Pilipczuk is supported by the Foundation for Polish Science (FNP) via the START stipend programme.
Tight Lower Bounds for the Complexity of Multicoloring

1 Introduction

The complexity of determining the chromatic number of a graph is undoubtedly among the most intensively studied computational problems. Countless variants and generalizations of graph colorings have been introduced and investigated. Here, we focus on multicolorings, also known as \((a:b)\)-colorings. In this setting, we are given a graph \(G\), a palette of \(a\) colors, and a number \(b\leq a\). An \((a:b)\)-coloring of \(G\) is any assignment of \(b\) distinct colors to each vertex so that adjacent vertices receive disjoint subsets of colors. The \((a:b)\)-COLORING problem asks whether \(G\) admits an \((a:b)\)-coloring. For \(b=1\) we obtain the classic graph coloring problem. The smallest \(a\) for which an \((a:b)\)-coloring exists is called the \(b\)-fold chromatic number, denoted by \(\chi_b(G)\).

The motivation behind \((a:b)\)-colorings can be perhaps best explained by showing the connection with the fractional chromatic number. For a graph \(G\), it is denoted as \(\chi_f(G)\) and defined as the optimum value of the natural LP relaxation of the problem of computing the chromatic number of \(G\), expressed as finding a cover of the vertex set using the minimum possible number of independent sets. It can be easily seen that by relaxing the standard coloring problem by allowing \(b\) times more colors while requiring that every vertex receives \(b\) colors and adjacent vertices receive disjoint subsets, with increasing \(b\) we approximate \(\chi_f(G)\) better and better. Consequently, \(\lim_{b\to\infty} \chi_b(G)/b = \chi_f(G)\).

Another connection concerns Kneser graphs. Recall that for positive integers \(a, b\) with \(b < a/2\), the Kneser graph \(KG_{a,b}\) has all \(b\)-element subsets of \(\{1, 2, \ldots, a\}\) as vertices, and two subsets are considered adjacent if and only if they are disjoint. For instance, \(KG_{5,2}\) is the well-known Petersen graph (see Fig. 1, right). Thus, \((a:b)\)-coloring of a graph \(G\) can be interpreted as a homomorphism from \(G\) to the Kneser graph \(KG_{a,b}\) (see Fig. 1). Kneser graphs are well studied in the context of colorings, mostly due to the celebrated result of Lovász [28], who determined their chromatic number, initiating the field of topological combinatorics.

Multicolorings and \((a:b)\)-colorings have been studied both from combinatorial [6, 12, 26] and algorithmic [5, 18, 19, 24, 25, 29, 30, 33] points of view. The main real-life motivation comes from the problem of assigning frequencies to nodes in a cellular network so that adjacent nodes receive disjoint sets of frequencies on which they can operate. This makes (near-)planar and distributed settings particularly interesting for practical applications. We refer to the survey of Halldórsson and Kortsarz [17] for a broader discussion.
In this paper we focus on the paradigm of exact exponential time algorithms: given a graph \( G \) on \( n \) vertices and numbers \( a \geq b \), we would like to determine whether \( G \) is \((a:b)\)-colorable as quickly as possible. Since the problem is already NP-hard for \( a = 3 \) and \( b = 1 \), we do not expect it to be solvable in polynomial time, and hence look for an efficient exponential-time algorithm. A straightforward dynamic programming approach yields an algorithm with running time \( \mathcal{O}^*(2^n \cdot (b + 1)^n) \) as follows. For each function \( \eta: V(G) \rightarrow \{0, 1, \ldots, b\} \) and each \( k = 0, 1, \ldots, a \), we create one boolean entry \( D(\eta, k) \) denoting whether one can choose \( k \)-independent sets in \( G \) so that every vertex \( v \in V(G) \) is covered exactly \( \eta(v) \) times. Then value \( D(\eta, k) \) can be computed as a disjunction of values \( D(\eta', k - 1) \) over \( \eta' \) obtained from \( \eta \) by subtracting 1 on vertices from some independent set in \( G \).

This simple algorithm can be improved by finding an appropriate algebraic formula for the number of \((a:b)\)-colorings of the graph and using the inclusion-exclusion principle to compute it quickly, similarly as in the case of standard colorings [2]. Such an algebraic formula was given by Nederlof [32, Theorem 3.5] in the context of a more general Multi Set Cover problem. Nederlof also observed that in the case of \((a:b)\)-COLORING, a simple application of the inclusion-exclusion principle to compute the formula yields an \( \mathcal{O}^*((b + 1)^n) \)-time exponential-space algorithm. Hua et al. [21] noted that the formulation of Nederlof [32] for Multi Set Cover can be also used to obtain a polynomial-space algorithm for this problem. By taking all maximal independent sets to be the family in the Multi Set Cover problem, and applying the classic Moon-Moser upper bound on their number [31], we obtain an algorithm for \((a:b)\)-COLORING that runs in time \( \mathcal{O}^*(3^{n/3} \cdot (b + 1)^n) \) and uses polynomial space. Note that by plugging \( b = 1 \) to the results above, we obtain algorithms for the standard coloring problem using \( \mathcal{O}^*(2^n) \) time and exponential space, or using \( \mathcal{O}^*(2.8845^n) \) time and polynomial space, which almost matches the fastest known procedures [2].

The complexity of \((a:b)\)-COLORING becomes particularly interesting in context of the Graph Homomorphism problem: given graphs \( G \) and \( H \), with \( n \) and \( h \) vertices respectively, determine whether \( G \) admits a homomorphism to \( H \). By the celebrated result of Hell and Nešetřil [20] the problem is in \( P \) if \( H \) is bipartite and NP-complete otherwise. For quite a while it was open whether there is an algorithm for Graph Homomorphism running in time \( 2^{\mathcal{O}(n + h)} \). It was recently answered in the negative by Cygan et al. [9]; more precisely, they proved that an algorithm with running time \( 2^{\mathcal{O}(n \log h)} \) contradicts the Exponential Time Hypothesis (ETH) of Impagliazzo et al. [22]. However, Graph Homomorphism is a very general problem, hence researchers try to uncover a more fine-grained picture and identify families of graphs \( H \) such that the problem can be solved more efficiently whenever \( H \in \mathcal{H} \). For example, Fomin, Heggernes and Kratsch [13] showed that when \( H \) is of treewidth at most \( t \), then Graph Homomorphism can be solved in time \( \mathcal{O}^*((t + 3)^n) \). It was later extended to graphs of cliquewidth bounded by \( t \), with \( \mathcal{O}^*((2t + 1)^{\max(n,h) \log h}) \), time bound by Wahlström [35]. On the other hand, \( H \) needs not be sparse to admit efficient homomorphism testing: the family of cliques admits the \( \mathcal{O}^*(2^n) \) running time as shown by Björklund et al. [2]. As noted above, this generalizes to Kneser graphs \( KG_{a,b} \), by the \( \mathcal{O}^*((b + 1)^n) \)-time algorithm of Nederlof. In this context, the natural question is whether the appearance of \( b \) in the base of the exponent is necessary, or is there an algorithm running in time \( \mathcal{O}^*(c^n) \) for some universal constant \( c \) independent of \( b \).

**Our contribution.** We show that the algorithms for \((a:b)\)-COLORING mentioned above are essentially optimal under the Exponential Time Hypothesis. Specifically, we prove the following results:

---

1. The \( \mathcal{O}^*(\cdot) \) notation hides factors polynomial in the input size.
Theorem 1. If there is an algorithm for \((a:b)\)-coloring that runs in time \(f(b) \cdot 2^{o(\log b)} n\), for some computable function \(f(b)\), then ETH fails. This holds even if the algorithm is only required to work on instances where \(a = \Theta(b^2 \log b)\).

Corollary 2. If there is an algorithm for Graph Homomorphism that runs in time \(f(h) \cdot 2^{o(\log \log h)} n\), for some computable \(f(h)\), then ETH fails. This holds even if the algorithm is only required to work on instances where \(H\) is a Kneser graph \(KG_{a,b}\) with \(a = \Theta(b^2 \log b)\).

The bound for \((a:b)\)-coloring is tight, as the straightforward \(O^*(2^n \cdot (b+1)^n) = 2^{O(\log b)} n\) dynamic programming algorithm already shows. At first glance, one might have suspected that \((a:b)\)-coloring, as an interpolation between classical coloring and fractional coloring, both solvable in \(2^{O(n)}\) time [16], should be just as easy; Theorem 1 refutes this suspicion.

Corollary 2 in particular excludes any algorithm for testing homomorphisms into Kneser graphs with running time \(2^{O(n+h)}\). It cannot give a tight lower bound matching the result of Cygan et al. [9] for general homomorphisms, because \(h = |V(KG_{a,b})| = \binom{b}{a}\) is not polynomial in \(b\). On the other hand, it exhibits the first explicit family of graphs \(H\) for which the complexity of Graph Homomorphism increases with \(b\).

In our proof, we first show a lower bound for the list variant of the problem, where every vertex is given a list of colors that can be assigned to it (see Section 2 for formal definitions). The list version is reduced to the standard version by introducing a large Kneser graph \(KG_{a+b,5}\); we need \(a\) and \(b\) to be really small so that the size of this Kneser graph does not dwarf the size of the rest of the construction. However, this is not necessary for the list version, where we obtain lower bounds for a much wider range of functions \(b(n)\).

Theorem 3. If there is an algorithm for List \((a:b)\)-coloring that runs in time \(2^{o(\log b)} n\), then ETH fails. This holds even if the algorithm is only required to work on instances where \(a = \Theta(b^2 \log b)\) and \(b = \Theta(b(n))\) for an arbitrarily chosen polynomial-time computable function \(b(n)\) such that \(b(n) \in \omega(1)\) and \(b(n) = O(n/\log n)\).

The crucial ingredient in the proof of Theorem 3 is the usage of \(d\)-detecting matrices introduced by Lindström [27]. We choose to work with their combinatorial formulation, hence we shall talk about \(d\)-detecting families. Suppose we are given some universe \(U\) and there is an unknown function \(f: U \rightarrow \{0, 1, \ldots, d-1\}\), for some fixed positive integer \(d\). One may think of \(U\) as consisting of coins of unknown weights that are integers between 0 and \(d-1\). We would like to learn \(f\) (the weight of every coin) by asking a small number of queries about single coins, but it turns out that significantly fewer questions are needed: there is a \(d\)-detecting family of size \(O(|U|/\log |U|)\), for every fixed \(d\) [27]. The logarithmic factor in the denominator will be crucial for deriving our lower bound.

Let us now sketch how \(d\)-detecting families are used in the proof of Theorem 3. Given an instance \(\varphi\) of 3-SAT with \(n\) variables and \(O(n)\) clauses, and a number \(b \leq n/\log n\), we will construct an instance \(G\) of List \((a:b)\)-coloring for some \(a\). This instance will have a positive answer if and only if \(\varphi\) is satisfiable, and the constructed graph \(G\) will have \(O(n/\log b)\) vertices. It can be easily seen that this will yield the promised lower bound.

Partition the clause set \(C\) of \(\varphi\) into groups \(C_1, C_2, \ldots, C_p\), each of size roughly \(b\); thus \(p = O(n/b)\). Similarly, partition the variable set \(V\) of \(\varphi\) into groups \(V_1, \ldots, V_q\), each of size roughly \(\log_2 b\); thus \(q = O(n/\log b)\). In the output instance we create one vertex per each variable group—hence we have \(O(n/\log b)\) such vertices—and one block of vertices per each...
of $k$-monomial detection to concrete problems. For instance, $r$-SIMPLE $k$-PATH, the problem of finding a walk of length $k$ that visits every vertex at most $r$ times, can be solved in time $O^*(2^{O(k / \log k)})$. However, for $r$-SIMPLE $k$-PATH, as well as other problems that can be tackled using this technique, the best known lower bounds under ETH exclude only algorithms with running time $O^*(2^{n^{1/2}})$. Whether the log $r$ factor in the exponent is necessary was left open by Abasi et al. and Gabizon et al.

We observe that the LIST $(a:b)$-COLORING problem can be reduced to $(r, k)$-MONOMIAL TESTING over the field $GF(2)$ in such a way that an $O^*(2^{k \cdot (\frac{\log r}{\log \log r})})$-time algorithm for the latter would imply a $2^{\Omega(\log b)n}$-time algorithm for the former, which would contradict ETH. Thus, we show that the known algorithms for $(r, k)$-MONOMIAL TESTING most probably cannot be sped up in general; nevertheless, the question of lower bounds for specific applications remains open. However, going through LIST $(a:b)$-COLORING to establish a lower bound for $(r, k)$-MONOMIAL TESTING is actually quite a detour, because the latter problem has a much larger expressive power. Therefore, we also give a more straightforward reduction that starts from a convenient form of SUBSET SUM; this reduction also proves the lower bound for a wider range of $r$, expressed as a function of $k$.

**Outline.** In Section 2 we set up the notation as well as recall definitions and well-known facts. We also discuss $d$-detecting families, the main combinatorial tool used in our reduction. In Section 3 we prove the lower bound for the list version of the problem, i.e., Theorem 3, and sketch the few steps needed for the standard version, thereby proving Theorem 1. Section 4 is
devoted to deriving lower bounds for low-degree monomial testing. Due to space constraints, proofs of statements marked with (♠) are deferred to the full version [3] of this paper.

2 Preliminaries

Notation. We use standard graph notation, see e.g. [10, 11]. All graphs we consider in this paper are simple and undirected. For an integer $k$, we denote $[k] = \{0, \ldots, k-1\}$. By $\uplus$ we denote the disjoint union, i.e., by $A \uplus B$ we mean $A \cup B$ with the indication that $A$ and $B$ are disjoint. If $I$ and $J$ are instances of decision problems $P$ and $R$, respectively, then we say that $I$ and $J$ are equivalent if either both $I$ and $J$ are YES-instances, or both are NO-instances of the respective problems.

Exponential-Time Hypothesis. The Exponential Time Hypothesis (ETH) of Impagliazzo et al. [22] states that there exists a constant $c > 0$, such that there is no algorithm solving 3-SAT in time $O^*(2^{cn})$. During the recent years, ETH became the central conjecture used for proving tight bounds on the complexity of various problems. One of the most important results connected to ETH is the Sparsification Lemma [23], which essentially gives a reduction from an arbitrary instance of $k$-SAT to an instance where the number of clauses is linear in the number of variables. The following well-known corollary can be derived by combining ETH with the Sparsification Lemma.

Theorem 4 (see e.g. Theorem 14.4 in [10]). Unless ETH fails, there is no algorithm for 3-SAT that runs in time $2^{o(n+m)}$, on formulas with $n$ variables and $m$ clauses.

We need the following regularization result of Tovey [34]. Following Tovey, by (3,4)-SAT we call the variant of 3-SAT where each clause of the input formula contains exactly 3 different variables, and each variable occurs in at most 4 clauses.

Lemma 5 ([34]). Given a 3-SAT formula $\varphi$ with $n$ variables and $m$ clauses one can transform it in polynomial time into an equivalent (3,4)-SAT instance $\varphi'$ with $O(n+m)$ variables and clauses.

Corollary 6. Unless ETH fails, there is no algorithm for (3,4)-SAT that runs in time $2^{o(n)}$, where $n$ denotes the number of variables of the input formula.

List and nonuniform list $(a:b)$-coloring. For integers $a, b$ and a graph $G$ with a function $L: V(G) \to 2^a$ (assigning a list of colors to every vertex), an $L$-$(a:b)$-coloring of $G$ is an assignment of exactly $b$ colors from $L(v)$ to each vertex $v \in V(G)$, such that adjacent vertices get disjoint color sets. The List $(a:b)$-COLORING problem asks, given $(G, L)$, whether an $L$-$(a:b)$-coloring of $G$ exists.

As an intermediary step of our reduction, we use the following generalization of list colorings where the number of demanded colors varies with every vertex. For integers $a, b$, a graph $G$ with a function $L: V(G) \to 2^a$ and a demand function $\beta: V(G) \to \{1, \ldots, b\}$, an $L$-$(a;b)$-coloring of $G$ is an assignment of exactly $\beta(v)$ colors from $L(v)$ to each vertex $v \in V(G)$, such that adjacent vertices get disjoint color sets. Nonuniform List $(a:b)$-COLORING is then the problem in which given $(G, L, \beta)$ we ask if an $L$-$(a;b)$-coloring of $G$ exists.

d-detecting families. In our reductions the following notion plays a crucial role.
Definition 7. A $d$-detecting family for a finite set $U$ is a family $\mathcal{F} \subseteq 2^U$ of subsets of $U$ such that for every two functions $f, g : U \to \{0, \ldots, d - 1\}$, $f \neq g$, there is a set $S$ in the family such that $\sum_{x \in S} f(x) \neq \sum_{x \in S} g(x)$.

A deterministic construction of sublinear, $d$-detecting families was given by Lindström [27], together with a proof that even the constant factor 2 in the family size cannot be improved.

Theorem 8 ([27]). For every constant $d \in \mathbb{N}$ and finite set $U$, there is a $d$-detecting family $\mathcal{F}$ on $U$ of size $\frac{2|U|}{\log^2 |U|} \cdot (1 + o(1))$. Furthermore, $\mathcal{F}$ can be constructed in $\text{poly}(|U|)$ time.

Other constructions, generalizations, and discussion of similar results can be found in Grebinski and Kucherov [15], and in Bshouty [4]. Note that the expression $\sum_{x \in S} f(x)$ is just the product of $f$ as a vector in $[d]|U|$ with the characteristic vector of $S$. Hence, instead of subset families, Lindström speaks of detecting vectors, while later works see them as detecting matrices, that is, $(0,1)$-matrices with these vectors as rows (which define an injection on $[d]|U|$ despite having few rows). Similar definitions appear in the study of query complexity, e.g., as in the popular Mastermind game [7].

3 Hardness of List $(a:b)$-coloring

In this section we show our main technical contribution: an ETH-based lower bound for LIST $(a:b)$-COLORING. We begin with key part: reducing an $n$-variable instance 3-SAT to an instance of NONUNIFORM LIST $(a:b)$-COLORING with only $O\left( \frac{n}{\log n} \right)$ vertices. Next, it is rather easy to reduce NONUNIFORM LIST $(a:b)$-COLORING to LIST $(a:b)$-COLORING.

3.1 The nonuniform case

We prove the following theorem through the remaining part of this section.

Theorem 9. For any instance $\phi$ of $(3,4)$-SAT with $n$ variables and any integer $2 \leq b \leq n/\log_2 n$, there is an equivalent instance $(G, \beta, L)$ of NONUNIFORM LIST $(a:2b)$-COLORING such that $a = O(b^2 \log b)$, $|V(G)| = O\left( \frac{n}{\log n} \right)$ and $G$ is 3-colorable. Moreover, the instance $(G, \beta, L)$ and the 3-coloring of $G$ can be constructed in $\text{poly}(n)$ time.

Consider an instance $\phi$ of 3-SAT where each variable appears in at most four clauses. Let $V$ be the set of its variables and $C$ be the set of its clauses. Note that $\frac{1}{3} |V| \leq |C| \leq \frac{4}{3} |V|$. Let $a = 12b^2 \cdot \lfloor \log_2 b \rfloor$. We shall construct, for some integers $n_V = O\left( |V|/\log b \right)$ and $n_C = O\left( |C|/b \right)$:
- a partition $V = V_1 \uplus \ldots \uplus V_{n_V}$ of variables into groups of size at most $\lfloor \log_2 b \rfloor$,
- a partition $C = C_1 \uplus \ldots \uplus C_{n_C}$ of clauses into groups of size at most $b$,
- a function $\sigma : \{1, \ldots, n_V\} \to [12 \cdot b \cdot \lfloor \log_2 b \rfloor]$, such that the following condition holds:

  For any $j = 1, \ldots, n_C$, the variables occurring in clauses of $C_j$ are all different and they all belong to pairwise different variable groups. Moreover, the indices of these groups are mapped to pairwise different values by $\sigma$.

In other words, any two literals of clauses in $C_j$ have different variables, and if they belong to $V_i$ and $V_i'$ respectively, then $\sigma(i) \neq \sigma(i')$.

Lemma 10 (\textcircled{\textbullet}). Partitions $V = V_1 \uplus \ldots \uplus V_{n_V}$, $C = C_1 \uplus \ldots \uplus C_{n_C}$ and a function $\sigma$ satisfying (\textcircled{\textbullet}) can be found in time $O(n)$.  

ESA 2017
For every $1 \leq i \leq n_V$, the set $V_i$ of variables admits $2^{|V_i|} \leq b$ different assignments. We will therefore say that each assignment on $V_i$ is given by an integer $x \in [b]$, for example by interpreting the first $|V_i|$ bits of the binary representation of $x$ as truth values for variables in $V_i$. Note that when $|V_i| < \log_2 b$, different integers from $[b]$ may give the same assignment on $V_i$.

For $1 \leq j \leq n_C$, let $I_j \subseteq \{1, \ldots, n_V\}$ be the set of indices of variable groups that contain some variable occurring in the clauses of $C_j$. Since every clause contains exactly three literals, property (K) means that $|I_j| = 3|C_j|$ and that $\sigma$ is injective over each $I_j$. See Fig. 2.

For $1 \leq j \leq n_C$, let $\{C_{j,1}, \ldots, C_{j,n_F}\}$ be a 4-detecting family of subsets of $C_j$, for some $n_F = \Theta(\frac{b}{\log b})$ (we can assume $n_F$ does not depend on $j$ by adding arbitrary sets when $|C_j| < b$). For every $1 \leq k \leq n_F$, let $C_{j,n_F+k} = C_j \setminus C_{j,k}$.

We are now ready to build the graph $G$, the demand function $\beta : V(G) \to \{1, \ldots, 2b\}$, and the list assignment $L$ as follows.

1. For $1 \leq i \leq n_V$, create a vertex $v_i$ with $\beta(v_i) = b - 1$ and $L(v_i) = \{b \cdot \sigma(i) + x \mid x \in [b]\}$.
2. For $1 \leq j \leq n_C$ and $1 \leq k \leq 2n_F$, create a vertex $u_{j,k}$ adjacent to each $v_i$ for $i \in I_j$. Let $\beta(u_{j,k}) = |C_{j,k}|$ and
   \[
   L(u_{j,k}) = \{b \cdot \sigma(i) + x \mid 1 \leq i \leq n_V, x \in [2^{|V_i|}] \text{ such that } x \text{ gives an assignment of } V_i \text{ that satisfies some clause of } C_{j,k}\}.
   \]
3. For $1 \leq j \leq n_C$, create a vertex $w_j$, adjacent to each $v_i$ for $i \in I_j$ and to each $u_{j,k}$ ($1 \leq k \leq 2n_F$). Let $\beta(w_j) = 2|C_j|$ and $L(w_j) = \bigcup_{i \in I_j} \{b \cdot \sigma(i) + x \mid x \in [b]\}$.

Before giving a detailed proof of the correctness, let us describe the reduction in intuitive terms. Note that vertices of type $v_i$ get all but one color from their list; this missing color, say $b \cdot \sigma(i) + x_i$, for some $x_i \in [b]$, defines an assignment on $V_i$. For every $j = 1, \ldots, n_C$ the goal of the gadget consisting of $w_j$ and vertices $u_{j,k}$ is to express the constraint that every clause in $C_j$ has a literal satisfied by this assignment. Since $w_j, u_{j,k}$ are adjacent to all vertices in $\{v_i \mid i \in I_j\}$, they may only use the missing colors (of the form $b \cdot \sigma(i) + x_i$, where $i \in I_j$).

Since $|I_j| = 3|C_j|$, there are $3|C_j|$ such colors and $2|C_j|$ of them go to $w_j$. This leaves exactly $|C_j|$ colors for vertices of type $u_{j,k}$, corresponding to a choice of $|C_j|$ satisfied literals from the $3|C_j|$ literals in clauses of $C_j$. The lists and demands for vertices $u_{j,k}$ guarantee that...
exactly \(|C_{j,k}|\) chosen satisfied literals occur in clauses of \(C_{j,k}\). The properties of 4-detecting families will ensure that every clause has exactly one chosen, satisfied literal, and hence at least one satisfied literal. We proceed with formal proofs.

**Lemma 11.** If \(\phi\) is satisfiable then \(G\) is \(L-\langle a;\beta\rangle\)-colorable.

**Proof.** Consider a satisfying assignment \(\eta\) for \(\phi\). For \(1 \leq i \leq n_V\), let \(x_i \in [2^{|V_i|}]\) be an integer giving the same assignment on \(V_i\) as \(\eta\). For every clause \(c\) of \(\phi\), choose one literal satisfied by \(\eta\) in it, and let \(i_c\) be index of the group \(V_i\) containing the literal’s variable. Let \(\alpha : V(G) \rightarrow (\{0,1,2\})^{|I|}\) be the \(L-\langle a;\beta\rangle\)-coloring of \(G\) defined as follows, for \(1 \leq i \leq n_V\), \(1 \leq j \leq n_C\), \(1 \leq k \leq 2n_F\):

- \(\alpha(v_i) = L(v_i) \setminus \{b \cdot \sigma(i) + x_i\}\)
- \(\alpha(u_{j,k}) = \{b \cdot \sigma(i_c) + x_{i_c} | c \in C_{j,k}\}\)
- \(\alpha(w_j) = \{b \cdot \sigma(i) + x_i | i \in I_j \setminus \{i_c | c \in C_j\}\}\).

Let us first check that every vertex \(v\) gets colors from its list \(L(v)\) only. This is immediate for vertices \(v_i\) and \(w_j\), while for \(u_{j,k}\) it follows from the fact that \(x_{i_c}\) gives a partial assignment to \(V_i\) that satisfies some clause of \(C_{j,k}\).

Now let us check that for every vertex \(v\), the coloring \(\alpha\) assigns exactly \(\beta(v)\) colors to \(v\). For \(\alpha(v_i)\) this follows from the fact that \(|L(v_i)| = b\) and \(|x_i| < 2^{|V_i|} \leq b\). Since by property (\(\mathcal{G}\)), \(\sigma\) is injective on \(I_j\), and thus on \(\{i_c | c \in C_{j,k}\} \subseteq I_j\), we have \(|\alpha(u_{j,k})| = |C_{j,k}| = b(u_{j,k}).\)

Similarly, since \(\sigma\) is injective on \(I_j\) and \(|I_j \setminus \{i_c | c \in C_j\} | = 3|C_j| - |C_{j,k}| = 2|C_j|\), we get \(|\alpha(w_j)| = 2|C_j| = \beta(w_j)\).

It remains to argue that the sets assigned to any two adjacent vertices are disjoint. There are three types of edges in the graph, namely \(v_iu_{j,k}, v_iw_j\), and \(w_ju_{j,k}\). The disjointness of \(\alpha(w_j)\) and \(\alpha(u_{j,k})\) is immediate from the definition of \(\alpha\), since \(C_{j,k} \subseteq C_j\). Fix \(j = 1, \ldots, n_C\). Since \(\sigma\) is injective on \(I_j\), for any two different \(i, i' \in I_j\), we have \(b \cdot \sigma(i) + x_i \not\in L(v_i)\). Hence,

\[
\bigcup_{i \in I_j} \alpha(v_i) = \{b \cdot \sigma(i) + x | i \in I_j \text{ and } x \in [b]\} \setminus \{b \cdot \sigma(i) + x_i | i \in I_j\}.
\]

Since \(\alpha(u_{j,k}), \alpha(w_j) \subseteq \{b \cdot \sigma(i) + x_i | i \in I_j\}\), it follows that edges of types \(v_iu_{j,k}\) and \(v_iw_j\) received disjoint sets of colors on their endpoints, concluding the proof.

**Lemma 12.** If \(G\) is \(L-\langle a;\beta\rangle\)-colorable then \(\phi\) is satisfiable.

**Proof.** Assume that \(G\) is \(L-\langle a;\beta\rangle\)-colorable, and let \(a\) be the corresponding coloring.

For \(1 \leq i \leq n_V\), we have \(|L(v_i)| = b\) and \(|\alpha(v_i)| = b - 1\), so \(v_i\) misses exactly one color from its list. Let \(b \cdot \sigma(i) + x_i\), for some \(x_i \in [b]\), be the missing color. We want to argue that the assignment \(x\) for \(\phi\) given by \(x_i\) on each \(V_i\) satisfies \(\phi\).

Consider any clause group \(C_j\), for \(1 \leq j \leq n_C\). Every vertex in \(\{w_j\} \cup \{u_{j,k} | 1 \leq k \leq 2n_F\}\) contains \(\{v_i | i \in I_j\}\) in its neighborhood. Therefore, the sets \(\alpha(u_{j,k})\) and \(\alpha(w_j)\) are disjoint from \(\bigcup_{i \in I_j} \alpha(v_i)\). Since \(L(u_{j,k}), L(w_j) \subseteq \{b \cdot \sigma(i) + x' | i \in I_j, x' \in [b]\}\), we get that \(\alpha(u_{j,k})\) and \(\alpha(w_j)\) are contained in the set of missing colors \(\{b \cdot \sigma(i) + x_i | i \in I_j\}\) (corresponding to the chosen assignment). By property (\(\mathcal{F}\)), this set has exactly \(|I_j| = 3|C_j|\) different colors. Of these, exactly \(2|C_j|\) are contained in \(\alpha(w_j)\). Let the remaining \(|C_j|\) colors be \(\{b \cdot \sigma(i) + x_i | i \in I_j\}\), for some subset \(J_j \subseteq I_j\) of \(|C_j|\) indices.

Since \(\alpha(u_{j,k})\) is disjoint from \(\alpha(w_j)\), we have \(\alpha(u_{j,k}) \subseteq \{b \cdot \sigma(i) + x_i | i \in J_j\}\) for all \(k\).

By definition of \(I_j\), for every \(i \in J_j \subseteq I_j\) there is a variable in \(V_i\) that appears in some clause of \(C_j\). By property (\(\mathcal{F}\)), it can only occur in one such clause, so let \(l_i\) be the literal in the clause of \(C_j\) where it appears. For every color \(b \cdot \sigma(i) + x_i \in \alpha(u_{j,k})\), by definition of the lists...
for \( u_{j,k} \) we know that \( x_i \) gives a partial assignment to \( V_i \) that satisfies some clause of \( C_{j,k} \). This means \( x_i \) makes the literal \( l_i \) true and \( l_i \) occurs in a clause of \( C_{j,k} \). Therefore, for each \( k \), at least \(|\alpha(u_{j,k})| = |C_{j,k}|\) literals from the set \( \{l_i \mid i \in J_j\} \) occur in clauses of \( C_{j,k} \) and are made true by the assignment \( x \).

Let \( f : C_j \to \{0,1,2,3\} \) be the function assigning to each clause \( c \in C_j \) the number of literals of \( c \) in \( \{l_i \mid i \in J_j\} \). By the above, \( \sum_{c \in C_j} f(c) \geq |C_{j,k}| \) for \( 1 \leq k \leq 2n \). Since each literal in \( \{l_i \mid i \in J_j\} \) belongs to some clause of \( C_j \), we have \( \sum_{c \in C_j} f(c) = |J_j| = |C_j| \). Then,

\[
\sum_{c \in C_j} f(c) \leq |C_j| - |C_{j,n,\alpha}| = |C_{j,k}|.
\]

Hence \( \sum_{c \in C_j} f(c) = |C_{j,k}| \) for \( 1 \leq k \leq 2n \). Let \( g : C_j \to \{0,1,2,3\} \) be the constant function \( g \equiv 1 \). Note that

\[
\sum_{c \in C_j} g(c) = |C_{j,k}| = \sum_{c \in C_j} f(c).
\]

Since \( \{C_{j,1}, \ldots, C_{j,n} \} \) is a 4-detecting family, this implies that \( f \equiv 1 \). Thus, for every clause \( c \) of \( C_j \) we have \( f(c) = 1 \), meaning that there is a literal from the set \( \{l_i \mid i \in J_j\} \) in this clause. All these literals are made positive by the assignment \( \eta \), therefore all clauses of \( C_j \) are satisfied. Since \( j = 1, \ldots, n_C \) was arbitrary, this concludes the proof that \( \eta \) is a satisfying assignment for \( \phi \).

The construction can clearly be made in polynomial time and the total number of vertices is \( n_V + n_C \cdot \mathcal{O}\left(\frac{1}{\log b}\right) + n_C = \mathcal{O}\left(\frac{n}{\log b}\right) \). Moreover, we get a proper 3-coloring of \( G \), by coloring vertices of the type \( v_i \) by color 1, vertices of the type \( u_{j,k} \) by color 2, and vertices of the type \( w_j \) by color 3. By Lemmas 11 and 12, this concludes the proof of Theorem 9.

### 3.2 The uniform case

In this section we reduce the nonuniform case to the uniform one, and state the resulting lower bound on the complexity of \( \text{LIST} \ (a:b) \text{-COLORING} \).

**Lemma 13.** For any instance \( I = (G, \beta, L) \) of NONUNIFORM \( \text{LIST} \ (a:b) \text{-COLORING} \) where the graph \( G \) is \( t \)-colorable, there is an equivalent instance \( (G',L') \) of \( \text{LIST} \ ((a + b):b) \text{-COLORING} \). Moreover, given a \( t \)-coloring of \( G \) the instance \( (G',L') \) can be constructed in time polynomial in \(|I| + b \).

**Proof.** Let \( c : V(G) \to [t] \) be a \( t \)-coloring of \( G \). For every vertex \( v \), define a set of filling colors \( F(v) = \{a + c(v)b + i : i = 0, \ldots, b - |\beta(v)| - 1\} \) and put \( L'(v) = L(v) \cup F(v) \).

Let \( \alpha : V(G) \to 2[^{|a|}] \) be an \( L-(a:b) \)-coloring of \( G \). We define a coloring \( \alpha' : V(G) \to 2[^{|a|+tb}] \) by setting \( \alpha'(v) = \alpha(v) \cup F(v) \) for every vertex \( v \in V(G) \). Observe that \( \alpha'(v) \subseteq L'(v) \) and \(|\alpha'(v)| = |\alpha(v)| + (b - |\beta(v)|) = b \). Since \( \alpha \) was a proper \( L-(a:b) \)-coloring, adjacent vertices can only share the filling colors. However, the lists of adjacent vertices have disjoint subsets of filling colors, since these vertices are colored differently by \( c \). It follows that \( \alpha' \) is an \( L'-(a:b) \)-coloring of \( G \).

Conversely, let \( \alpha' : V(G) \to 2[^{|a|+tb}] \) be an \( L'-(a:b) \)-coloring of \( G \). For every vertex \( v \), we have \(|\alpha'(v) \cap [a]| = b - |\alpha'(v) \cap F(v)| \geq b - (b - |\beta(v)|) = |\beta(v)| \). Define \( \alpha(v) \) to be any cardinality \( \beta(v) \) subset of \( \alpha'(v) \cap [a] \). It is immediate that \( \alpha \) is an \( L-(a:b) \)-coloring of \( G \).  

We are now ready to prove one of our main results.
Theorem 3. If there is an algorithm for List (a:b)-coloring that runs in time $2^{o(\log b)n}$, then ETH fails. This holds even if the algorithm is only required to work on instances where $a = \Theta(b^2 \log b)$ and $b = \Theta(b(n))$ for an arbitrarily chosen polynomial-time computable function $b(n)$ such that $b(n) \in o(1)$ and $b(n) = O(n/\log n)$.

Proof. Let $b(n)$ be a function as in the statement. We can assume w.l.o.g. that $2 \leq b(n) \leq n/\log_2 n$ (otherwise, replace $b(n)$ with $b'(n) = 2 + \lfloor b(n)/c \rfloor$ in the reasoning below, for $c$ a big enough constant; clearly $b'(n) = \Theta(b(n))$). Fix a function $f(b) = o(\log b)$ and assume there is an algorithm $A$ for List (a:b)-coloring that runs in time $2^{f(b)n}$, whenever $b = \Theta(b(n))$.

Consider an instance of (3,4)-SAT with $n$ variables. Let $b = b(n)$. By Theorem 9 in poly(n) time we get an equivalent instance $(G,\beta,L)$ of NONUNIFORM List (a;(2b))-coloring such that $a = \Theta(b^2 \log b)$, $|V(G)| = O(\frac{n}{\log b})$, and a 3-coloring of $G$. Next, by Lemma 13 in poly(n) time we get an equivalent instance $(G,L')$ of List ((a + 6b):(2b))-coloring.

Finally, we solve the instance $(G,L')$ using algorithm $A$. Since $b(n) = \omega(1)$, we have $f(b(n)) = o(\log(b(n)))$, and $A$ runs in time $2^{o(\log b(n))}|V(G)| = 2^{o(\log b(n))} \geq 2^{o(n)}$. By Corollary 6, this contradicts ETH.

Finally, we reduce List (a:b)-coloring to (a:b)-coloring. This is done by increasing the number of colors by $b$, adding a Kneser graph $KG_{a+b,b}$ (which can be colored essentially only by assigning each $b$-set of colors to its corresponding vertex), and replacing the lists by edges to appropriate vertices of the Kneser graph.

Lemma 14. Given an instance of List (a:b)-coloring with $n$ vertices, an equivalent instance of (a + b : b)-coloring with $n + \left(\frac{a+b}{b}\right)$ vertices can be computed in poly(n, $\left(\frac{a+b}{b}\right)$)-time.

For $b \in o\left(\frac{\log n}{\log \log n}\right)$, $a = O(b^2 \log b)$, we show that $\left(\frac{a+b}{b}\right) = o(n)$, allowing us to compose our reductions with Lemma 14. An analysis similar to the one in Theorem 3 then concludes the proof of Theorem 1 and Corollary 2; we refer to the full version [3] for details.

4 Low-degree testing

In this section we derive lower bounds for (r, k)-MONOMIAL TESTING. In this problem, we are given an arithmetic circuit $C$ over some field $F$ (with input, constant, addition, and multiplication gates). One gate is designated to be the output gate, and it computes some polynomial $P$ of the variables $x_1, x_2, \ldots, x_n$ that appear in the input gates. We assume that $P$ is a homogenous polynomial of degree $k$, i.e., all its monomials have total degree $k$. The task is to verify whether $P$ contains an $r$-monomial, i.e., a monomial in which every variable has its individual degree bounded by $r$, for a given $r \leq k$. Abasi et al. [1] gave a very fast randomized algorithm for (r, k)-MONOMIAL TESTING.

Theorem 15 (Abasi et al. [1]). Fix integers $r, k$ with $2 \leq r \leq k$. Let $p \leq 2r^2 + 2r$ be a prime, and let $g \in GF(p)[x_1, \ldots, x_n]$ be a homogenous polynomial of degree $k$, computable by a circuit $C$. There is a randomized algorithm running in time $O(r^{2k/r}|C|(rn)^{O(1)})$ which:

- with probability at least 1/2 always answers YES when $g$ contains an $r$-monomial,
- always answers NO when $g$ contains no $r$-monomial.

This result was later derandomized by Gabizon et al. [14] under the assumption that the circuit is non-cancelling, that is, it contains only input, addition, and multiplication gates. Many concrete problems like $r$-SIMPLE k-PATH can be reduced to (r, k)-MONOMIAL
Testing by encoding the set of candidate objects as monomials of some large polynomial, so that “good” objects correspond to monomials with low individual degrees.

As we show in the full version [3] of this paper, this is also the case for LIST \((a:b)\)-COLORING. Namely, for an instance \((G, L)\) of LIST \((a:b)\)-COLORING we can construct a homogeneous polynomial \(p_G\) of degree \(k = 2m\) with \(n(a+1)\) variables, together with a circuit of size \(2^n \text{poly}(a, n)\) evaluating it, such that \(G\) admits a list \((a:b)\)-coloring iff \(p_G\) contains a \(b\)-monomial. Using Theorem 15 with \(r = b\), we get yet another polynomial-space algorithm for LIST \((a:b)\)-COLORING, running in time \(O(b^{Ω(n)} \text{poly}(n))\). Similarly, if the running time in Theorem 15 was improved to \(2^{o(\log r/r)} |C| \text{poly}(r, n)\), then we would get an algorithm for LIST \((a:b)\)-COLORING in time \(O(2^{o(\log r/r)} \text{poly}(n))\), which contradicts ETH by Theorem 3. However, a careful examination shows that this chain of reductions would only yield instances of \((r,k)\)-MONOMIAL TESTING with \(r = O(\sqrt{k}/\log k)\). Hence, this does not exclude the existence of a fast algorithm that works only for large \(r\). Below we show a more direct reduction, which excludes such algorithms for a wider spectrum of pairs \((r,k)\).

In the CARRY-LESS SUBSET SUM problem, we are given \(n + 1\) numbers \(s, a_1, \ldots, a_n\), each represented as \(n\) decimal digits. For any number \(x\), the \(j\)-th decimal digit of \(x\) is denoted by \(x^{(j)}\). It is assumed that \(\sum_{j=1}^{n} a_j^{(j)} < 10\), for every \(j = 1, \ldots, n\). The goal is to verify whether there is a sequence of indices \(1 \leq i_1 < \ldots < i_k \leq n\) such that \(\sum_{q=1}^{k} a_{i_q} = s\). Note that by the small sum assumption, this is equivalent to the statement that \(\sum_{q=1}^{k} a_{i_q}^{(j)} = s^{(j)}\), for every \(j = 1, \ldots, n\). The standard NP-hardness reduction from 3-SAT (see e.g. [8]) in fact gives instances of CARRY-LESS SUBSET SUM of linear size, yielding the following.

\textbf{Lemma 16 (♠).} Unless ETH fails, the CARRY-LESS SUBSET SUM problem cannot be solved in \(2^{o(n)}\) time.

We proceed with a sketch of the reduction from CARRY-LESS SUBSET SUM to \((r,k)\)-MONOMIAL TESTING; details can be found in the full version [3] of this paper. Let us choose a parameter \(t \in \{1, \ldots, n\}\). Assume w.l.o.g. that \(t\) divides \(n\) (otherwise, add zeroes at the end of every input number). Let \(q = n/t\). For an \(n\)-digit decimal number \(x\), for every \(j = 1, \ldots, t\), let \(x^{[j]}\) denote the \(q\)-digit number given by the \(j\)-th block of \(q\) digits in \(x\), i.e., \(x^{[j]} = (x^{(jq-1)}, \ldots, x^{((j-1)q)})_{10}\).

Let \(r = 10^t - 1\). Define the following polynomial over GF(2):

\[ q_S = \prod_{i=1}^{n} \left( y_i + z_i \cdot \prod_{j=1}^{t} x_j^{a_j^{(j)}} \right) . \prod_{j=1}^{t} x^{r-a_j^{(j)}} = \sum_{S \subseteq\{1, \ldots, n\}} \prod_{j=1}^{t} \prod_{i \in S} a_j^{(j)} \cdot \prod_{i \in S} y_i \prod_{i \in S} z_i. \]

Let \(p_S\) denote the polynomial obtained from \(q_S\) by filtering out all the monomials of degree different than \(k = tr + n\). The first expression defining \(q_S\) gives a circuit of size \(O(n)\), and thus with a standard construction, we show \(p_S\) can be evaluated by a circuit of size \(O(n t^2 + n^2 t)\). It is relatively easy to see that by construction, \((s, a_1, \ldots, a_n)\) is a YES-instance of CARRY-LESS SUBSET SUM iff \(q_S\) contains the monomial \(\prod_{j=1}^{t} x_j^{a_j^{(j)}} \prod_{i \in S} y_i \prod_{i \in S} z_i\), for some \(S \subseteq\{1, \ldots, n\}\) (the variables \(y_i\) and \(z_i\) guaranteeing that no pair of monomials cancels out). This in turn holds iff \(p_S\) contains an \(r\)-monomial (with exactly \(n\) variables \(y_i\) and \(z_i\), and hence degree exactly \(r\) for each \(x_i\) variable).

With this reduction, we obtain our main lower bound for \((r,k)\)-MONOMIAL TESTING. We state it in the most general, but technical form, and derive an exemplary corollary below.

\textbf{Theorem 17 (♠).} If there is an algorithm solving \((r,k)\)-MONOMIAL TESTING in time \(2^{o(k \log r/r)} |C|^{O(1)}\), then ETH fails. The statement remains true even if the algorithm works
only for instances where \( r = 2^{\Theta(n/t(n))} \) and \( k = t(n)2^{\Theta(n/t(n))} \), for an arbitrarily chosen function \( t : \mathbb{N} \to \mathbb{N} \) computable in \( 2^{o(n)} \) time, such that \( t(n) = \omega(1) \) and \( t(n) \leq n \) for every \( n \).

\[\textbf{Theorem 18 (♠).} \] Let \( \sigma \in [0,1) \). Then, unless ETH fails, there is no algorithm for \((r,k)\)-MONOMIAL TESTING that solves instances with \( r = \Theta(k^\sigma) \) in time \( 2^{o(k \log r \cdot |C|)} \). In particular, no algorithm solves \((r,k)\)-MONOMIAL TESTING in time \( 2^{o(k \log r \cdot |C|)} \) for all input values \( r \), unless ETH fails.

\textbf{Acknowledgements.} The authors thank Andreas Björklund and Matthias Mnich for sharing the problem considered in this paper.

\[\textbf{References}\]

Tight Lower Bounds for the Complexity of Multicoloring


