Evasiveness of Subgraph Containment and Related Properties ⋆

Amit Chakrabarti, Subhash Khot, and Yaoyun Shi

Department of Computer Science, Princeton University, Princeton NJ 08544, USA
{amitc,khot,shiyy}@cs.princeton.edu

Abstract. We prove new results on evasiveness of monotone graph properties by extending the techniques of Kahn, Saks and Sturtevant [4]. For the property of containing a subgraph isomorphic to a fixed graph, and a fairly large class of related n-vertex graph properties, we show evasiveness for an arithmetic progression of values of n. This implies a $\frac{1}{2}n^2 - O(n)$ lower bound on the decision tree complexity of these properties.

We prove that properties that are preserved under taking graph minors are evasive for all sufficiently large n. This greatly generalizes the evasiveness result for planarity [1]. We prove a similar result for bipartite subgraph containment.

Keywords: Decision Tree Complexity, Monotone Graph Properties, Evasiveness, Graph Property Testing.

1 Introduction

Suppose we have an input graph G and are required to decide whether or not it has a certain (isomorphism invariant) property P. The graph is given by an oracle which answers queries of the form "is (x, y) an edge of G?" A *decision tree algorithm* for P is a strategy that specifies a sequence of such queries to the oracle, where each query may depend upon the outcomes of the previous ones, terminating when sufficient information about G has been obtained to decide whether or not P holds for G. The *cost* of such a decision tree algorithm is the worst case number of queries that it makes. The *decision tree complexity* of P is the minimum cost of any decision tree algorithm for P.

Since an n-vertex graph has $\frac{1}{2}n(n-1)$ vertex pairs each of which could either be an edge or not, it is clear that any property of n-vertex graphs has complexity at most $\frac{1}{2}n(n-1)$. If a property happens to have complexity *exactly* $\frac{1}{2}n(n-1)$ then it is said to be *evasive*.[1]

A property of n-vertex graphs is said to be *monotone* if, starting with a graph which has the property, the addition of edges does not destroy the property. It

⋆ This work was supported in part by NSF Grant CCR-96-23768, NSF Grant CCR-98-20855 and ARO Grant DAAH04-96-1-0181.

[1] Some authors call such properties "elusive" instead of evasive.

is said to be *nontrivial* if there exists an n-vertex graph which has the property and one which does not. Connectedness, non-planarity, non-k-colorability and the property of containing a perfect matching are all examples of nontrivial monotone properties (for sufficiently large n). Rosenberg [7] attributes to Karp the following conjecture which, remarkably, remains open even today.

Karp Conjecture: Every nontrivial monotone graph property is evasive.

As a first step towards a resolution of this conjecture, Rivest and Vuillemin [6] proved that such properties have complexity at least $n^2/16$, thereby settling the Aanderaa-Rosenberg conjecture [7] of an $\Omega(n^2)$ complexity lower bound. The next big advance was the work of Kahn, Saks and Sturtevant [4] where an interesting *topological approach* was used to prove that the Karp Conjecture holds whenever n is a prime power. Triesch [8] used this approach, together with a complicated construction, to prove the evasiveness of some special classes of properties. Similar topological ideas were used by Yao [9] to prove a related result: namely, that nontrivial monotone *bipartite* graph properties are always evasive. Prior to the work of Kahn et.al., adversarial strategies had been devised to prove the evasiveness of certain specific graph properties for all n in [5], [1] and [3]. These strategies worked for the properties of acyclicity, connectedness, 2-connectedness, planarity and simple variants on these. The most sophisticated of these adversarial strategies was one used by Bollobás [2] to prove the evasiveness of the property of containing a k-clique, for any $k,\ 2 \leq k \leq n$.

Let H be any fixed graph. For n-vertex graphs, let Q_n^H denote the property of containing H as a subgraph (not necessarily as an induced subgraph). From the work of Bollobás [2] we know that Q_n^H is evasive for all n in the special case when H is a complete graph. This raises the natural question: what can we say about general H?

In this paper, we study this question and some related ones, extending, for the first time, the topological approach of [4] to a fairly general class of graph properties. For each of these properties, we draw stronger inferences than [4]. Our Main Theorem is stated below.

Theorem 1.1 (Main Theorem). *For any fixed graph H there exists an integer r_0 with the following property. Suppose $n = \sum_{i=1}^{r} q^{\alpha_i}$ where q is a prime power, $q \geq |H|$, each $\alpha_i \geq 1$ and $r \equiv 1 \pmod{r_0}$. Then Q_n^H is evasive.*

In order to understand the significance and strength of this theorem, consider the following statements (proven in this paper). Each of these statements follows either from the Main Theorem or from the techniques used in proving it.

- For any graph H, there is an *arithmetic progression* such that Q_n^H is evasive for all n in the progression. Note that this is a much stronger inference than can be drawn by applying the results of [4].
- The decision tree complexity of Q_n^H is $\frac{1}{2}n^2 - O(n)$. This bound does not follow from the results of [4].
- If the graph H is *bipartite*, then Q_n^H is evasive for large enough n.

- Any n-vertex nontrivial graph property that is preserved under taking graph minors is evasive for large enough n. This includes lots of very natural graph properties such as embeddability on any surface, outerplanarity, linkless embeddability in $\mathbf{R}^3$, the property of being a series-parallel graph, etc. Thus, our result generalizes a result of Best et.al. [1] who show that planarity is evasive.
- Any monotone boolean combination of the properties Q_n^H for several different graphs H still satisfies our Main Theorem. Thus, for example, if H_1, H_2 and H_3 are fixed graphs, then the property of containing as subgraph either H_1 or both of H_2 and H_3 is still evasive for those n which satisfy the conditions of the Main Theorem.

The remainder of the paper is organized as follows. In Section 2 we review the basics of the topological approach of Kahn et.al.[4], establishing a connection between proving evasiveness of monotone properties and computing Euler characteristics of abstract complexes. Then in Section 3 we define a certain auxiliary property of graphs and prove a technical result (called the Main Lemma) about this property. This result is then used in Section 4 to prove our main theorem. In Section 5, we provide proofs for the additional results itemized above. We end with some concluding remarks in Section 6.

Notations, terminology and conventions: We call a graph *trivial* if it has no edges. Throughout this paper, all graphs will be assumed to be nontrivial, have no loops and no parallel edges. For a graph G, $|G|$ will denote the number of vertices in G, also called the *size* of G, $V(G)$ will denote its vertex set, $E(G)$ its edge set, $\mathrm{chr}(G)$ its chromatic number and $\mathrm{clq}(G)$ the size of its largest clique. Graphs which occur as "input graphs" on which boolean properties are to be tested are assumed to be always vertex-labeled. All other graphs are assumed to be unlabeled, unless otherwise specified. When we speak of an "edge" in an input graph, we really mean an unordered vertex pair which may or may not be an edge.

2 Review of the Topological Approach

A property of m boolean variables $x_1, \ldots, x_m$ is a function $P : \{0,1\}^m \to \{0,1\}$; we say that the m-tuple $(x_1, \ldots, x_m)$ has (or satisfies) property P if $P(x_1, \ldots, x_m) = 1$. We say that P is *monotone* if for every m-tuple $(x_1, \ldots, x_m)$ that satisfies P, increasing any x_i from 0 to 1 yields an m-tuple that also satisfies P. We say that P is *evasive* if any decision tree algorithm for P has cost m. In our study of graph properties, the variables will be unordered pairs of vertices (i.e., potential edges of the graph) and P will be required to be invariant under relabelings of the graph.

Let $[m]$ denote the set $\{1, 2, \ldots, m\}$ and consider the collection of subsets $S \subseteq [m]$ with the following property: setting the variables indexed by S to 1 and those indexed by $[m] \setminus S$ to 0 yields an m-tuple which *does not satisfy* P. Since P is monotone, this collection of sets is downward closed under set inclusion. Recall that such a downward closed collection of sets is called an *abstract complex*, and that the sets in this collection are called the *faces* of the complex. This observation motivates

Definition 2.1. *If P is monotone, then the abstract complex associated with P, denoted $\Delta(P)$, is defined as follows:*

$$\Delta(P) = \{S \subseteq [m] \,:\, \text{If } x_i = 1 \Longleftrightarrow i \in S, \text{ then } (x_1, \ldots, x_m) \text{ does not satisfy } P\}.$$

Associated with an abstract complex Δ is a topologically important number called its *Euler characteristic* which is denoted $\chi(\Delta)$ and is defined as follows:

$$\chi(\Delta) = \sum_{\emptyset \neq F \in \Delta} (-1)^{|F|-1}. \tag{1}$$

Kahn et.al.[4] showed that non-evasiveness of P has topological consequences for $\Delta(P)$. The following theorem is implicit in their work:

Theorem 2.2 (Kahn et.al. [4]). *If the monotone property P is not evasive, then $\chi(\Delta(P)) = 1$.* □

For our result, we shall need to use a stronger theorem which can also be found in [4]. Let Δ be an abstract complex defined on $[m]$ and let Γ be a finite group which acts on the set $[m]$, preserving the faces of Δ. The action partitions $[m]$ into orbits, say $A_1, \ldots, A_k$. We use the action of Γ to define another abstract complex Δ_Γ on $[k]$ as follows:

$$\Delta_\Gamma = \{S \subseteq [k] \,:\, \bigcup_{i \in S} A_i \in \Delta\} \tag{2}$$

Sometimes, as is the case with our work, it is not easy to say much about $\Delta(P)$ for a monotone property P. But it is possible to find some group Γ such that its action produces a more understandable abstract complex $(\Delta(P))_\Gamma$. The next theorem, the most important tool in [4], says that if Γ has certain rather restrictive properties, then non-evasiveness of P has a topological consequence on this new complex.

Theorem 2.3 (Kahn et.al. [4]). *Suppose Γ has a normal subgroup Γ_1 which is such that $|\Gamma_1|$ is a prime power and the quotient group Γ/Γ_1 is cyclic. Then if P is not evasive, we have $\chi((\Delta(P))_\Gamma) = 1$.* □

An application of this result leads to the following theorem which is the main result of [4].

Theorem 2.4 (Kahn et.al. [4]). *Let P_n be a nontrivial monotone property of n-vertex graphs. If n is a prime power, then P_n is evasive.* □

In order to derive Theorem 2.4 from Theorem 2.3, Kahn et.al. construct a group which acts on the vertices of the input graph and thus, indirectly, on the edges. The number theoretic constraint on n is a consequence of the fact that this action depends crucially on being able to view the vertices of the graph as elements of a finite field. Our approach to proving evasiveness for more general n will be to devise a more sophisticated group action. Before we do so, we will need an auxiliary result which we shall establish in the next section.

3 The Main Lemma

Consider the following operation on a graph G. Let the vertices of G be colored, using *all* the colors in some set C, so that no two adjacent vertices get the same color. Let G' be a graph with vertex set C where two distinct vertices $c_1, c_2 \in C$ are adjacent iff the coloring assigns colors c_1 and c_2 to the end-points of some edge in G. We shall call G' a *compression of graph G induced by coloring C*. If there exists a C which induces a compression G' of G, we shall write $G' \lhd G$.

Definition 3.1. *A family $\mathcal{F}$ of graphs is said to be closed under compression if for graphs G, H such that $G \in \mathcal{F}$ and $H \lhd G$ we have $H \in \mathcal{F}$.*

Let $\mathcal{F}$ be a nonempty finite family of (nontrivial) graphs that is closed under compression. The property $P_n^{\mathcal{F}}$ that an input graph G on n vertices contains some member of $\mathcal{F}$ as a subgraph is clearly nontrivial, for n large enough, and monotone. Let $\Delta_n^{\mathcal{F}}$ be the abstract complex associated with this property and let $\chi_n = \chi(\Delta_n^{\mathcal{F}})$ be the Euler characteristic of this complex.

The purpose of this section is to establish that for any such family $\mathcal{F}$, we have $\chi_n \neq 1$ infinitely often. Let us set

$$T = 2^{2^t}, \text{ where } t \text{ is the smallest integer such that } T \geq \min_{F \in \mathcal{F}} |F|. \tag{3}$$

We shall prove

Lemma 3.2 (Main Lemma). *If $n \equiv 1 \pmod{T-1}$ then $\chi_n \equiv 0 \pmod 2$.*

Since we only care about $\chi_n \bmod 2$, we can use the fact that addition and subtraction are equivalent mod 2 in (1) to get[2]

$$\chi_n \;\equiv\; \#\{G : G \text{ is nontrivial and does not satisfy } P_n^{\mathcal{F}}\} \pmod 2. \tag{4}$$

Consider n-vertex input graphs with vertices labeled with integers from 0 to $n-1$. For $n > T$, let us define a group action on such graphs as follows. For $a, b \in \{0, 1, 2, \ldots, T-1\}$ and a odd, let permutation $\phi_{a,b}$ be defined by mapping vertex i to vertex $(ai + b) \bmod T$ for $i \in \{0, 1, \ldots, T-1\}$. The other $n - T$ vertices are left fixed. It is routine to check that the set of all these permutations forms a group Φ under composition, thereby defining a group action on the labeled vertices. This action induces an action on graphs in the obvious manner, thereby partitioning the set of all labeled n-vertex graphs into orbits. Since the order $|\Phi|$ of the group is $T^2/2$, a power of 2, each orbit has size a power of 2. Therefore, (4) can be modified to

$$\chi_n \;\equiv\; \#\left\{G : \begin{array}{c} G \text{ is nontrivial, invariant under} \\ \Phi \text{ and does not satisfy } P_n^{\mathcal{F}} \end{array}\right\} \pmod 2. \tag{5}$$

The action of Φ on the vertices also induces an action on edges (or rather, on unordered pairs of distinct vertices, each of which may or may not be an edge),

[2] Note that we are counting not graphs, but labeled graphs.

not to be confused with the action on labeled graphs mentioned above. Therefore the set of edges amongst vertices $0, 1, \ldots, T-1$ is partitioned into orbits. Since any odd integer is invertible mod T, we get 2^t orbits $E_0, E_1, \ldots, E_{2^t-1}$, where

$$E_i = \{(x, y) : 0 \leq x < y < T, \quad y - x = 2^i k \text{ for some odd number } k\} . \quad (6)$$

Let G be an invariant graph. From now on, let us refer to the vertices $0, 1, \ldots, T-1$ as *left vertices* and the rest as *right vertices*. Let G_{left} and G_{right} denote the subgraphs of G induced by the left and right vertices, respectively. By invariance of G, the set of right vertices adjacent to any left vertex is the same for each left vertex; let $\mathcal{R}(G)$ denote this set. Also, the set of edges $E(G_{\text{left}})$ is the union of a certain number of the orbits E_i; let $\text{orb}(G)$ denote this number. We shall show that whether or not G has the property $P_n^{\mathcal{F}}$ is completely determined once $G_{\text{right}}, \mathcal{R}(G)$ and this number $\text{orb}(G)$ are fixed; the specific G_{left} does not matter.

Lemma 3.3. *For any invariant G, we have* $\text{chr}(G_{\text{left}}) = \text{clq}(G_{\text{left}}) = 2^{\text{orb}(G)}$.

Proof. Let $I \subseteq \{0, 1, \ldots, 2^t - 1\}$ be such that $E(G_{\text{left}}) = \bigcup_{i \in I} E_i$; then we have $|I| = \text{orb}(G)$. Consider two vertices x, y of G_{left}. If their binary representations agree on the bit positions indexed by I, then $x - y = \sum_{i \in I'} \pm 2^i$ for some set I' disjoint from I. By (6), this implies $(x, y) \notin E(G_{\text{left}})$. Therefore, the vertices of G_{left} can be partitioned into $2^{|I|}$ independent sets; thus $\text{chr}(G_{\text{left}}) \leq 2^{\text{orb}(G)}$. On the other hand, if x, y are such that the bits in positions outside I are all zero, then $x - y = \sum_{i \in I''} \pm 2^i$ for some $I'' \subseteq I$, which by (6) implies that $(x, y) \in E(G_{\text{left}})$. Therefore, G_{left} has a clique of size $2^{|I|} = 2^{\text{orb}(G)}$. The lemma follows. ◻

Lemma 3.4. *Let G_1, G_2 be two invariant n-vertex labeled graphs with $G_{1,\text{right}} = G_{2,\text{right}}$, $\mathcal{R}(G_1) = \mathcal{R}(G_2)$ and $\text{orb}(G_1) = \text{orb}(G_2)$. Then G_1 has property $P_n^{\mathcal{F}}$ if and only if G_2 does.*

Proof. Suppose G_1 has property $P_n^{\mathcal{F}}$; we shall show that G_2 does too. Suppose G_1 contains $F \in \mathcal{F}$ as a subgraph. We fix a particular occurrence of F within G_1 so that we can talk about $F_{\text{left}}, F_{\text{right}}$ and $\mathcal{R}(F) := \mathcal{R}(G_1) \cap V(F)$.

Using Lemma 3.3 and the hypothesis, we obtain $\text{chr}(F_{\text{left}}) \leq \text{chr}(G_{1,\text{left}}) = \text{clq}(G_{2,\text{left}})$. Let $h = \text{chr}(F_{\text{left}})$; from the above inequality it is clear that $G_{2,\text{left}}$ contains K_h as a subgraph. Fix a particular occurrence of K_h and, starting with the graph F_{right}, connect each of the h left vertices in this occurrence to each vertex in $\mathcal{R}(F)$. Let F' be the resulting graph. Since $\mathcal{R}(F) \subseteq \mathcal{R}(G_1) = \mathcal{R}(G_2)$ and since F_{right} is a subgraph of $G_{1,\text{right}} = G_{2,\text{right}}$, it follows that F' is a subgraph of G_2.

Consider the following coloring of the graph F: we use h colors for its left vertices and color each right vertex with a distinct color, never using any of these h colors. Let $F'' \lhd F$ be the compression of F induced by this coloring. It is not hard to see that F'' is a subgraph of F' and therefore of G_2. Since $\mathcal{F}$ is closed under compression, $F'' \in \mathcal{F}$. Therefore G_2 has property $P_n^{\mathcal{F}}$. ◻

Lemma 3.5. *For $n \geq T = 2^{2^t}$, we have $\chi_n \equiv \chi_{n-T+1} \pmod 2$.*

Proof. Let k be a fixed integer with $0 \leq k \leq 2^t$. Recall that the group action induced on the edges creates 2^t orbits. Consider the family of all n-vertex invariant graphs G with $\mathcal{R}(G)$ and G_{right} fixed, and $\text{orb}(G) = k$. By Lemma 3.4, either all graphs in this family have property $P_n^{\mathcal{F}}$ or none of them does. The size of this family is $\binom{2^t}{k}$ which is even if $k \neq 0$ and $k \neq 2^t$. If $k = 2^t$, G_{left} is a complete graph, and so G contains a clique of size T. From (3), we see that G has property $P_n^{\mathcal{F}}$. Therefore, by (5),

$$\chi_n \;\equiv\; \#\left\{G : \begin{array}{c}\text{orb}(G) = 0 \text{ and } G \text{ is nontrivial,}\\ \text{invariant and doesn't satisfy } P_n^{\mathcal{F}}\end{array}\right\} \pmod 2 \;. \tag{7}$$

Suppose we take such a G with $\text{orb}(G) = 0$ and collapse all its left vertices into one vertex which we connect to every vertex in $\mathcal{R}(G)$ and to no others, thereby yielding a graph $\hat{G}$. This gives a bijection from n-vertex invariant graphs G with $\text{orb}(G) = 0$ to $(n - T + 1)$-vertex graphs.

It is clear that if $\hat{G}$ has property $P_{n-T+1}^{\mathcal{F}}$, then G has property $P_n^{\mathcal{F}}$. Now suppose G has property $P_n^{\mathcal{F}}$ and let $F \in \mathcal{F}$ be a subgraph of G. Since $\text{orb}(G) = 0$, the vertices in F_{left} form an independent set; thus we may color them all with one color and then color each remaining vertex of F with a distinct color different from the one just used. This coloring produces a compression $\hat{F} \lhd F$ which clearly is a subgraph of $\hat{G}$. Since $\mathcal{F}$ is closed under compression, we have $\hat{F} \in \mathcal{F}$ and so $\hat{G}$ has property $P_{n-T+1}^{\mathcal{F}}$. Thus our bijection respects the relevant property and this completes the proof. ◻

We now have all the pieces needed for the

Proof. **(of Lemma 3.2)** Set $n = T = 2^{2^t}$. The only way for an n-vertex graph to have $\text{orb}(G) = 0$ is for it to have no edges. Using (7), this implies $\chi_T \equiv 0 \pmod 2$. Invoking Lemma 3.5 completes the proof. ◻

4 Proof of the Main Theorem

We now return to proving Theorem 1.1. According to the theorem's hypotheses

$$n = \sum_{i=1}^{r} q^{\alpha_i} \tag{8}$$

where q is a prime power, $q \geq |H|$, each $\alpha_i \geq 1$ and $r \equiv 1 \pmod{r_0}$. Our goal is to show that Q_n^H is evasive under these hypotheses for some choice of r_0.

The chief difficulty in applying the topological approach outlined in Section 2 lies in having to construct a group action natural enough for the property under consideration and satisfying the stringent conditions on the underlying group necessary for Theorem 2.3 to apply. In this section we shall come up with a group action that allows us to "merge together" big clusters of vertices in our graph, in the process changing the property under consideration from Q_n^H to $P_r^{\mathcal{F}}$ for some family $\mathcal{F}$ of graphs, r being as in (8).

We partition vertex set of our n-vertex graph into clusters $V_1, \ldots, V_r$, with $|V_i| = q^{\alpha_i}$ and identify vertices in V_i with elements of the finite field $\mathbb{F}_{q^{\alpha_i}}$. Define a permutation group Γ on the vertices as follows:

$$\Gamma = \{\langle a, b_1, b_2, \ldots, b_r\rangle \;:\; a \in \mathbb{F}_q^*,\; b_i \in \mathbb{F}_{q^{\alpha_i}}\} \;, \tag{9}$$

where $\langle a, b_1, b_2, \ldots, b_r\rangle$ denotes a permutation which sends $x \in V_i = \mathbb{F}_{q^{\alpha_i}}$ to $ax + b_i \in V_i$. Let $\Gamma_1 = \{\langle 1, b_1, \ldots, b_r\rangle \;:\; b_i \in \mathbb{F}_{q^{\alpha_i}}\}$. It is easy to check that Γ_1 is a normal subgroup of Γ, $|\Gamma_1| = q^{\alpha_1 + \cdots + \alpha_r}$, a prime power, and $\Gamma/\Gamma_1 \cong \mathbb{F}_q^*$, a cyclic group. Thus Γ satisfies the hypotheses of Theorem 2.3.

As in Section 3, the action of Γ induces a group action on the edges and thus partitions the edges into orbits. Let $\mathcal{A}$ denote the set of these orbits and let $\Delta = \Delta(Q_n^H)$ denote the abstract complex associated with property Q_n^H. Define a complex Δ_Γ on $\mathcal{A}$ as in (2):

$$\Delta_\Gamma = \{\mathcal{D} \subseteq \mathcal{A} \;:\; \bigcup_{A \in \mathcal{D}} A \;\in \Delta\} \;. \tag{10}$$

Our intention is to show that the Euler characteristic $\chi(\Delta_\Gamma) \neq 1$. By Theorem 2.3, evasiveness of Q_n^H will follow. To this end, let us investigate what the faces of Δ_Γ look like. Call an edge an *intracluster edge* if both its end points lie in the same V_i for some i; call the edge an *intercluster edge* otherwise.

Lemma 4.1. *An orbit containing an intracluster edge is not contained in any face of Δ_Γ.*

Proof. Let $A \in \mathcal{A}$ be the orbit of the intracluster edge (u, v), $u, v \in V_i$. Then $A = \{(au + b, av + b) \;:\; b \in \mathbb{F}_{q^{\alpha_i}},\; a \in \mathbb{F}_q^*\}$. Set $w = v - u$. Then $(0, w) \in A$. Consider the set of vertices $X = \{wz \;:\; z \in \mathbb{F}_q\}$. For $0 \neq x \in X$ we clearly have $(0, x) \in A$. Thus for any pair of distinct vertices $x_1, x_2 \in X$, we have $(0, x_2 - x_1) \in A$, whence $(x_1, x_2) \in A$. So A contains all edges among vertices in X. Since $|X| = q \geq |H|$, the orbit A contains H as a subgraph. By definition, Δ cannot contain a face that includes A and so no face of Δ_Γ can contain A. □

If $u \in V_i, v \in V_j, i < j$, then the orbit of the intercluster edge (u, v) is the set E_{ij} of all edges between V_i and V_j. Let $\mathcal{E} = \{E_{ij} |\; i < j\} \subseteq \mathcal{A}$. From the preceding lemma and (10) it is clear that

$$\Delta_\Gamma = \{\mathcal{D} \subseteq \mathcal{E} \;:\; \bigcup_{A \in \mathcal{D}} A \;\in \Delta\} \;. \tag{11}$$

Let $\mathcal{D}$ be any subset of $\mathcal{E}$. Then $G_\mathcal{D} = \bigcup_{A \in \mathcal{D}} A$ is a graph on n vertices with no intracluster edges and such that if $i \neq j$, the edges between V_i and V_j are either all present or all absent. Define a graph $\hat{G}_\mathcal{D}$ on r vertices $v_1, \ldots, v_r$ such that (v_i, v_j) is an edge iff all edges between V_i, V_j are present in $G_\mathcal{D}$.

Let $\mathcal{T}_H$ denote the family of all graphs $\hat{H}$ such that $\hat{H} \lhd H$. It is easy to check that $\mathcal{T}_H$ is closed under compression (refer to Definition 3.1). The following lemma is simple to prove and connects this section with Section 3.

Lemma 4.2. *H is a subgraph of $G_{\mathcal{D}}$ if and only if there is a $\hat{H} \in \mathcal{T}_H$ such that $\hat{H}$ is a subgraph of $\hat{G}_{\mathcal{D}}$. In other words, $G_{\mathcal{D}}$ satisfies Q_n^H iff $\hat{G}_{\mathcal{D}}$ satisfies $P_r^{\mathcal{T}_H}$.*

Proof. Suppose H is a subgraph of $G_{\mathcal{D}}$. Consider the following coloring of $G_{\mathcal{D}}$: all vertices in a cluster are colored the same and no two clusters use the same color. This is a valid coloring since each cluster of vertices is an independent set. This coloring induces a coloring of H which in turn induces a compression $\hat{H} \lhd H$. Clearly this $\hat{H}$ is a subgraph of $\hat{G}_{\mathcal{D}}$.

Now suppose $\hat{H} \lhd H$ is a subgraph of $\hat{G}_{\mathcal{D}}$. Consider the graph H_1 with vertices in $\cup_{i=1}^{r} V_i$ formed by taking all edges in E_{ij} whenever v_i and v_j are adjacent in $\hat{H}$. Since each $|V_i| \geq q \geq |H|$, it follows that H is a subgraph of H_1, and therefore of $G_{\mathcal{D}}$. □

We are ready to prove our Main Theorem.

Proof. **(of Theorem 1.1)** Suppose Q_n^H is not evasive. From Theorem 2.3, we have $\chi(\Delta_\Gamma) = 1$. If $r = 1$, there is only one cluster, so by Lemma 4.1 we have $\Delta_\Gamma = \{\emptyset\}$, whence $\chi(\Delta_\Gamma) = 0$, a contradiction. Therefore $r > 1$. Equation (11) and Lemma 4.2 imply that there is a one-to-one correspondence between faces of Δ_Γ and nontrivial r-vertex graphs not satisfying property $P_r^{\mathcal{T}_H}$. Hence the abstract complex Δ_Γ is same as the abstract complex $\Delta_r^{\mathcal{T}_H}$ defined in Section 3. It follows from the definition of compression that $\mathcal{T}_H$ contains the complete graph on $\mathrm{chr}(H)$ vertices and contains no smaller graph. Therefore, (3) yields $t = \lceil \lg \lg \mathrm{chr}(H) \rceil$. Setting $r_0 = 2^{2^t} - 1$ and applying Lemma 3.2 we have $\chi(\Delta_r^{\mathcal{T}_H}) \neq 1$ and so $\chi(\Delta_\Gamma) \neq 1$, a contradiction. □

5 Consequences and Extensions

Our techniques enable us to prove certain results with "cleaner" statements than our Main Theorem 1.1; we prove four such results below. The first two are simple corollaries of Theorem 1.1 while the other two can be easily proved using the machinery of its proof. Finally, we present an interesting generalization of our Main Theorem.

Theorem 5.1. *For any graph H there exist infinitely many primes p with the following property: for all sufficiently large n divisible by p, the property Q_n^H is evasive.*

Remark: Note that this establishes the evasiveness of Q_n^H for an arithmetic progression of values of n.

Proof. Choose an integer t such that $T = 2^{2^t}$ is at least $|H|$. By Dirichlet's Theorem there exist infinitely many primes p such that $p \equiv 2 \pmod{T-1}$. Fix one such $p \geq T$ and pick any $n \geq p^2(T-1)$ divisible by p. Now $p-1$ is relatively prime to $T-1$, therefore there is an integer x such that $x(p-1) \equiv$

$n/p-1 \pmod{T-1}$ and $0 \leq x < T-1$. From the lower bound on n we have $n/p - px > 0$. Therefore we can write

$$n = \sum_{i=1}^{x} p^2 + \sum_{i=1}^{n/p-px} p$$

which is an expression of n as a sum of powers of p. The number of summands in this expression is $x + n/p - px \equiv 1 \pmod{T-1}$. Since $p \geq T \geq |H|$, we can apply Theorem 1.1 to conclude that Q_n^H is evasive. □

Corollary 5.2. *For any graph H there exists a constant $c = c(H)$ such that for all sufficiently large n, the decision tree complexity of Q_n^H is at least $\frac{1}{2}n^2 - cn$.* □

Theorem 5.3. *If the graph H is bipartite, then Q_n^H is evasive for all sufficiently large n.*

Proof. Since $\mathrm{chr}(H) = 2$, in the proof of Theorem 1.1, using the notation of that proof, we may take $t = 0$ which gives $r_0 = 1$. The condition $r \equiv 1 \pmod{r_0}$ is now trivially satisfied. The condition on n becomes a simple requirement that n be divisible by a prime power $q \geq |H|$. But if n is sufficiently large then it clearly satisfies this condition. □

Theorem 5.4. *Let $\mathcal{M}$ be an infinite minor-closed family of graphs that does not include all graphs. For n-vertex graphs, let $R_n^{\mathcal{M}}$ be the property of being in $\mathcal{M}$. Then $R_n^{\mathcal{M}}$ is evasive for all sufficiently large n.*

Remark: Planarity was already known to be evasive. This result is a major generalization.

Proof. Let H be a graph not in $\mathcal{M}$ with minimum size, and let $h = |H|$. Then H is a minor of both the complete graph K_h and the complete bipartite graph $K_{h,h}$; therefore no graph in $\mathcal{M}$ can contain either K_h or $K_{h,h}$ as a subgraph.

Suppose n is divisible by a prime power $q \geq h$, a condition that always holds if n is sufficiently large. Following the argument of Section 4 we divide the labeled vertices of the candidate graph G into clusters of size q and consider the orbits of the edges created by the action of the group Γ described there. Let Δ be the abstract complex associated *with the negation*[3] *of* $R_n^{\mathcal{M}}$. An orbit containing an intracluster edge cannot be included in a face of Δ_Γ because its edges, if present, would create a K_q subgraph. An orbit containing an intercluster edge cannot be included either because its edges, if present, would create a $K_{q,q}$ subgraph. Thus, $\Delta_\Gamma = \{\emptyset\}$ and so $\chi(\Delta_\Gamma) = 0 \neq 1$. By Theorem 2.3, the negation of $R_n^{\mathcal{M}}$ is evasive and therefore so is $R_n^{\mathcal{M}}$. □

The next theorem generalizes our Main Theorem and can be proved essentially using the same argument as that for the Main Theorem.

[3] Notice that the property $R_n^{\mathcal{M}}$ is not monotone. However, its negation is monotone. Clearly a property is evasive if its negation is.

Theorem 5.5. *Let $f : \{0,1\}^k \to \{0,1\}$ be a nontrivial monotone boolean function and let $H_1, \ldots, H_k$ be arbitrary graphs. Define the composite property $Q_n = f(Q_n^{H_1}, \ldots, Q_n^{H_k})$. Then there exists an integer r_0 with the following property. Suppose $n = \sum_{i=1}^{r} q^{\alpha_i}$ where q is a prime power, $q \geq \max_{1 \leq i \leq k} |H_i|$, each $\alpha_i \geq 1$ and $r \equiv 1 \pmod{r_0}$. Then Q_n is evasive.* □

Remark: This theorem shows, for instance, that properties like "G either contains H_1 as a subgraph or else contains both H_2 and H_3 as subgraphs" are evasive for several values of n. This theorem has corollaries similar to Theorem 5.1 and Corollary 5.2.

6 Concluding Remarks

The major open question in the area of decision tree complexity of graph properties is to settle the Karp Conjecture. The pioneering work of Kahn et.al. [4] has given us a possible direction to follow in attempting to settle this conjecture. Since the publication of that work, our work is the first which extends their topological approach for a fairly general class of graph properties.

An obvious open question raised by our work is: how far can one enlarge the set of values of n for which our results hold? We conjecture that in the notation of Section 3, we have $\chi_n \neq 1$ for large enough n. If proved true, this conjecture would remove all number theoretic restrictions in the Main Theorem.

7 Acknowledgments

We would like to express our sincere thanks to Professors Sanjeev Arora, Bernard Chazelle and Andrew Yao for their valuable comments and suggestions. We are grateful to the referees for their comments and for pointing out a simplification in the proof of Lemma 3.3.

References

1. Best, M.R., van Emde Boas, P., Lenstra, H.W., Jr. *A sharpened version of the Aanderaa-Rosenberg Conjecture*, Report ZW 30/74, Mathematisch Centrum Amsterdam, 1974.
2. Bollobás, B. *Complete subgraphs are elusive*, J. Combinatorial Th. (B), **21** (1976), 1–7.
3. Bollobás, B. *Extremal Graph Theory*, Academic Press, 1978, Chapter 8.
4. Kahn, J., Saks, M., Sturtevant, D. *A topological approach to evasiveness*, Combinatorica, **4** (1984), 297–306.
5. Milner, E.C., Welsh, D.J.A. *On the computational complexity of graph theoretical properties*, Proc. 5th British Columbia Conf. on Combinatorics (C.St.J.A. Nash-Williams and J. Sheehan, Eds.), 1975, 471–487.
6. Rivest, R.L., Vuillemin, J. *On recognizing graph properties from adjacency matrices*, Theoret. Comput. Sci., **3** (1976), 371–384.

7. Rosenberg, A.L. *On the time required to recognize properties of graphs: A problem*, SIGACT News, **5** (1973), 15–16.
8. Triesch, E. *Some results on elusive graph properties*, SIAM J. Comput., **23** (1994), 247–254.
9. Yao, A.C. *Monotone bipartite graph properties are evasive*, SIAM J. Comput., **17** (1988), 517–520.