Symposium on Theoretical Aspects of Computer Science 2010 (Nancy, France), pp. 71-82
www.stacs-conf.org

EVASIVENESS AND THE DISTRIBUTION OF PRIME NUMBERS

LÁSZLÓ BABAI [1,2] AND ANANDAM BANERJEE [3] AND RAGHAV KULKARNI [1] AND VIPUL NAIK [1]

[1] University of Chicago, Chicago, IL, USA.

[3] Northeastern University, Boston, MA, USA.

Abstract. A Boolean function on N variables is called *evasive* if its decision-tree complexity is N. A sequence B_n of Boolean functions is *eventually evasive* if B_n is evasive for all sufficiently large n.

We confirm the eventual evasiveness of several classes of monotone graph properties under widely accepted number theoretic hypotheses. In particular we show that Chowla's conjecture on Dirichlet primes implies that (a) for any graph H, "forbidden subgraph H" is eventually evasive and (b) all nontrivial monotone properties of graphs with $\leq n^{3/2-\epsilon}$ edges are eventually evasive. (n is the number of vertices.)

While Chowla's conjecture is not known to follow from the Extended Riemann Hypothesis (ERH, the Riemann Hypothesis for Dirichlet's L functions), we show (b) with the bound $O(n^{5/4-\epsilon})$ under ERH.

We also prove unconditional results: (a′) for any graph H, the query complexity of "forbidden subgraph H" is $\binom{n}{2}-O(1)$; (b′) for some constant $c > 0$, all nontrivial monotone properties of graphs with $\leq cn \log n + O(1)$ edges are eventually evasive.

Even these weaker, unconditional results rely on deep results from number theory such as Vinogradov's theorem on the Goldbach conjecture.

Our technical contribution consists in connecting the topological framework of Kahn, Saks, and Sturtevant (1984), as further developed by Chakrabarti, Khot, and Shi (2002), with a deeper analysis of the orbital structure of permutation groups and their connection to the distribution of prime numbers. Our unconditional results include stronger versions and generalizations of some result of Chakrabarti et al.

1. Introduction

1.1. The framework

A *graph property* P_n of n-vertex graphs is a collection of graphs on the vertex set $[n] = \{1, \ldots, n\}$ that is invariant under relabeling of the vertices. A property P_n is called *monotone* (decreasing) if it is preserved under the deletion of edges. The trivial graph properties are the empty set and the set of all graphs. A class of examples are the *forbidden*

1998 ACM Subject Classification: F.2.2, F.1.1, F.1.3.

Key words and phrases: Decision tree complexity, evasiveness, graph property, group action, Dirichlet primes, Extended Riemann Hypothesis.

[2]Partially supported by NSF Grant CCF-0830370.

27th Symposium on Theoretical Aspects of Computer Science, Nancy, 2010
Editors: Jean-Yves Marion, Thomas Schwentick
Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany
Digital Object Identifier: 10.4230/LIPIcs.STACS.2010.2445

subgraph properties: for a fixed graph H, let Q_n^H denote the class of n-vertex graphs that do not contain a (not necessarily induced) subgraph isomorphic to H.

We view a set of labeled graphs on n vertices as a Boolean function on the $N = \binom{n}{2}$ variables describing adjacency. A Boolean function on N variables is *evasive* if its deterministic query (decision-tree) complexity is N.

The long-standing Aanderaa-Rosenberg-Karp conjecture asserts that *every nontrivial monotone graph property is evasive.* The problem remains open even for important special classes of monotone properties, such as the forbidden subgraph properties.

1.2. History

In this note, n always denotes the number of vertices of the graphs under consideration.

Aanderaa and Rosenberg (1973) [17] conjectured a lower bound of $\Omega(n^2)$ on the query complexity of monotone graph properties. Rivest and Vuillemin (1976) [19] verified this conjecture, proving an $n^2/16$ lower bound. Kleitman and Kwiatkowski (1980) [10] improved this to $n^2/9$. Karp conjectured that nontrivial monotone graph properties were in fact evasive. We refer to this statement as the Aanderaa-Rosenberg-Karp (ARK) conjecture.

In their seminal paper, Kahn, Saks, and Sturtevant [11] observe that non-evasiveness of monotone Boolean functions has strong topological consequences (contracibility of the associated simplicial complex). They then use results of R. Oliver about fixed points of group actions on such complexes to verify the ARK conjecture when n is a prime-power. As a by-product, they improve the lower bound for general n to $n^2/4$.

Since then, the topological approach of [11] has been influential in solving various interesting special cases of the ARK conjecture. Yao (1988) [25] proves that non-trivial monotone properties of bipartite graphs with a given partition (U, V) are evasive (require $|U||V|$ queries). Triesch (1996) [22] shows (in the original model) that any monotone property of bipartite graphs (all the graphs satisfying the property are bipartite) is evasive. Chakrabarti, Khot, and Shi (2002) [3] introduce important new techniques which we use; we improve over several of their results (see Section 1.4).

1.3. Prime numbers in arithmetic progressions

Dirichlet's Theorem (1837) (cf. [5]) asserts that if $\gcd(a, m) = 1$ then there exist infinitely many primes $p \equiv a \pmod m$. Let $p(m, a)$ denote the smallest such prime p. Let $p(m) = \max\{p(m, a) \mid \gcd(a, m) = 1\}$. Linnik's celebrated theorem (1947) asserts that $p(m) = O(m^L)$ for some absolute constant L (cf. [16, Chap. V.]). Heath-Brown [9] shows that $L \leq 5.5$. Chowla [4] observes that under the Extended Riemann Hypothesis (ERH) we have $L \leq 2 + \epsilon$ for all $\epsilon > 0$ and conjectures that $L \leq 1 + \epsilon$ suffices:

Conjecture 1.1 (S. Chowla [4])**.** For every $\epsilon > 0$ and every m we have $p(m) = O(m^{1+\epsilon})$.

This conjecture is widely believed; in fact, number theorists suggest as plausible the stronger form $p(m) = O(m(\log m)^2)$ [8]. Turán [23] proves the tantalizing result that for almost all a we have $p(m, a) = O(m \log m)$.

Let us call a prime p an *ϵ-near Fermat prime* if there exists an $s \geq 0$ such that $2^s \mid p-1$ and $\frac{p-1}{2^s} \leq p^\epsilon$.

We need the following weak form of Chowla's conjecture:

Conjecture 1.2 (Weak Chowla Conjecture)**.** For every $\epsilon > 0$ there exist infinitely many ϵ-near Fermat primes.

In other words, the weak conjecture says that for every ϵ, for infinitely many values of s we have $p(2^s, 1) < (2^s)^{1+\epsilon}$.

1.4. Main results

For a graph property P we use P_n to denote the set of graphs on vertex set $[n]$ with property P. We say that P is *eventually evasive* if P_n is evasive for all sufficiently large n.

Our first set of results states that the "forbidden subgraph" property is "almost evasive" under three different interpretations of this phrase.

Theorem 1.3 (Forbidden subgraphs)**.** *For all graphs H, the forbidden subgraph property Q_n^H (a) is eventually evasive, assuming the Weak Chowla Conjecture; (b) is evasive for almost all n (unconditionally); and (c) has query complexity $\binom{n}{2} - O(1)$ for all n (unconditionally).*

Part (b) says the asymptotic density of values of n for which the problem is not evasive is zero. Part (c) improves the bound $\binom{n}{2} - O(n)$ given in [3]. Parts (a) and (c) will be proved in Section 3. We defer the proof of part (b) to the journal version.

The term "monotone property of graphs with $\leq m$ edges" describes a monotone property that fails for all graphs with more than m edges.

Theorem 1.4 (Sparse graphs)**.** *All nontrivial monotone properties of graphs with at most $f(n)$ edges are eventually evasive, where (a) under Chowla's Conjecture, $f(n) = n^{3/2-\epsilon}$ for any $\epsilon > 0$; (b) under ERH, $f(n) = n^{5/4-\epsilon}$; and (c) unconditionally, $f(n) = cn \log n$ for some constant $c > 0$. (d) Unconditionally, all nontrivial monotone properties of graphs with no cycle of length greater than $(n/4)(1-\epsilon)$ are eventually evasive (for all $\epsilon > 0$).*

Part (c) of Theorem 1.4 will be proved in Section 4. Parts (a) and (b) follow in Section 5. The proof of part (d) follows along the lines of part (c); we defer the details to the journal version of this paper.

We note that the proofs of the unconditional results (c) and (d) in Theorem 1.4 rely on Haselgrove's version [7] of Vinogradov's Theorem on Goldbach's Conjecture (cf. Sec. 4.2).

Recall that a *topological subgraph* of a graph G is obtained by taking a subgraph and replacing any induced path $u - \cdots - v$ in the subgraph by an edge $\{u, v\}$ (repeatedly) and deleting parallel edges. A *minor* of a graph is obtained by taking a subgraph and contracting edges (repeatedly). If a class of graphs is closed under taking minors then it is also closed under taking topological subgraphs but not conversely; for instance, graphs with maximum degree ≤ 3 are closed under taking toopological subgraphs but every graph is a minor of a regular graph of degree 3.

Corollary 1.5 (Excluded topological subgraphs)**.** *Let P be a nontrivial class of graphs closed under taking topological subgraphs. Then P is eventually evasive.*

This unconditional result extends one of the results of Chakrabarti et al. [3], namely, that nontrival classes of graphs closed under taking minors is eventually evasive.

Corollary 1.5 follows from part (c) of Theorem 1.4 in the light of Mader's Theorem which states that if the average degree of a graph G is greater than $2^{\binom{k+1}{2}}$ then it contains a topological K_k [13, 14].

Theorem 1.4 suggests a new stratification of the ARK Conjecture. For a monotone (decreasing) graph property P_n, let

$$\dim(P_n) := \max\{|E(G)| - 1 \mid G \in P_n\}.$$

We can now restate the ARK Conjecture:

Conjecture 1.6. If P_n is a non-evasive, non-empty, monotone decreasing graph property then $\dim(P_n) = \binom{n}{2} - 1$.

2. Preliminaries

2.1. Group action

For the basics of group theory we refer to [18]. All groups in this paper are finite. For groups Γ_1, Γ_2 we use $\Gamma_1 \leq \Gamma_2$ to denote that Γ_1 is a subgroup; and $\Gamma_1 \lhd \Gamma_2$ to denote that Γ_1 is a (not necessarily proper) normal subgroup. We say that Γ is a p-group if $|\Gamma|$ is a power of the prime p.

For a set Ω called the "permutation domain," let $\mathrm{Sym}(\Omega)$ denote the *symmetric group* on Ω, consisting of the $|\Omega|!$ permutations of Ω. For $\Omega = [n] = \{1, \ldots, n\}$, we set $\Sigma_n = \mathrm{Sym}([n])$. For a group Γ, a homomorphism $\varphi : \Gamma \to \mathrm{Sym}(\Omega)$ is called a Γ-*action* on Ω. The action is *faithful* if $\ker(\varphi) = \{1\}$. For $x \in \Omega$ and $\gamma \in \Gamma$ we denote by x^γ the image of x under $\varphi(\gamma)$. For $x \in \Omega$ we write $x^\Gamma = \{x^\gamma : \gamma \in \Gamma\}$ and call it the *orbit* of x under the Γ-action. The orbits partition Ω.

Let $\binom{\Omega}{t}$ denote the set of t-subsets of Ω. There is a natural induced action $\mathrm{Sym}(\Omega) \to \mathrm{Sym}(\binom{\Omega}{t})$ which also defines a natural Γ-action on $\binom{\Omega}{t}$. We denote this action by $\Gamma^{(t)}$. Similarly, there is a natural induced Γ-action on $\Omega \times \Omega$. The orbits of this action are called the *orbitals* of Γ. We shall need the undirected version of this concept; we shall call the orbits of the Γ-action on $\binom{\Omega}{2}$ the *u-orbitals* (undirected orbitals) of the Γ-action.

By an action of the group Γ on a structure $\mathfrak{X}$ such as a group or a graph or a simplicial complex we mean a homomorphism $\Gamma \to \mathrm{Aut}(\mathfrak{X})$ where $\mathrm{Aut}(\mathfrak{X})$ denotes the automorphism group of $\mathfrak{X}$.

Let Γ and Δ be groups and let $\psi : \Delta \to \mathrm{Aut}(\Gamma)$ be a Δ-action on Γ. These data uniquely define a group $\Theta = \Gamma \rtimes \Delta$, the *semidirect product* of Γ and Δ with respect to ψ. This group has order $|\Theta| = |\Gamma||\Delta|$ and has the following properites: Θ has two subgroups $\Gamma^* \cong \Gamma$ and $\Delta^* \cong \Delta$ such that $\Gamma^* \lhd \Theta$; $\Gamma^* \cap \Delta^* = \{1\}$; and $\Theta = \Gamma^*\Delta^* = \{\gamma\delta \mid \gamma \in \Gamma^*, \delta \in \Delta^*\}$. Moreover, identifying Γ with Γ^* and Δ with Δ^*, for all $\gamma \in \Gamma$ and $\delta \in \Delta$ we have $\gamma^{\psi(\delta)} = \delta^{-1}\gamma\delta$.

Θ can be defined as the set $\Delta \times \Gamma$ under the group operation

$$(\delta_1, \gamma_1)(\delta_2, \gamma_2) = (\delta_1\delta_2, \gamma_1^{\psi(\delta_2)}\gamma_2) \qquad (\delta_i \in \Delta, \gamma_i \in \Gamma).$$

For more on semidirect products, which we use extensively, see [18, Chap. 7].

The group $\mathrm{AGL}(1, q)$ of affine transformations $x \mapsto ax + b$ of $\mathbb{F}_q$ ($a \in \mathbb{F}_q^\times$, $b \in \mathbb{F}_q$) acts on $\mathbb{F}_q$. For each $d \mid q - 1$, $\mathrm{AGL}(1, q)$ has a unique subgroup of order qd; we call this subgroup $\Gamma(q, d)$. We note that $\mathbb{F}_q^+ \lhd \Gamma(q, d)$ and $\Gamma(q, d)/\mathbb{F}_q^+$ is cyclic of order d and is isomorphic to a subgroup Δ of $\mathrm{AGL}(1, q)$; $\Gamma(q, d)$ can be described as a *semidirect product* $(\mathbb{F}_q^+) \rtimes \Delta$.

2.2. Simplicial complexes and monotone graph properties

An *abstract simplicial complex* $\mathcal{K}$ on the set Ω is a subset of the power-set of Ω, closed under subsets: if $B \subset A \in \mathcal{K}$ then $B \in \mathcal{K}$. The elements of $\mathcal{K}$ are called its *faces*. The *dimension* of $A \in \mathcal{K}$ is $\dim(A) = |A| - 1$; the dimension of $\mathcal{K}$ is $\dim(\mathcal{K}) = \max\{\dim(A) \mid A \in \mathcal{K}\}$. The *Euler characteristic* of $\mathcal{K}$ is defined as

$$\chi(\mathcal{K}) := \sum_{A \in \mathcal{K}, A \neq \emptyset} (-1)^{\dim(A)}.$$

Let $[n] := \{1, 2, \ldots, n\}$ and $\Omega = \binom{[n]}{2}$. Let P_n be a subset of the power-set of Ω, i. e., a set of graphs on the vertex set $[n]$. We call P_n a *graph property* if it is invariant under the induced action $\Sigma_n^{(2)}$. We call this graph property *monotone decreasing* if it is closed under subgraphs, i. e., it is a simplicial complex. We shall omit the adjective "decreasing."

2.3. Oliver's Fixed Point Theorem

Let $\mathcal{K} \subseteq 2^\Omega$ be an abstract simplicial complex with a Γ-action. The *fixed point complex* $\mathcal{K}_\Gamma$ action is defined as follows. Let $\Omega_1, \ldots, \Omega_k$ be the Γ-orbits on Ω. Set

$$\mathcal{K}_\Gamma := \{S \subseteq [k] \mid \bigcup_{i \in S} \Omega_i \in \mathcal{K}\}.$$

We say that a group Γ satisfies **Oliver's condition** if there exist (not necessarily distinct) primes p, q such that Γ has a (not necessarily proper) chain of subgroups $\Gamma_2 \lhd \Gamma_1 \lhd \Gamma$ such that Γ_2 is a p-group, Γ_1/Γ_2 is cyclic, and Γ/Γ_1 is a q-group.

Theorem 2.1 (Oliver [15])**.** *Assume the group Γ satisfies Oliver's condition. If Γ acts on a nonempty contractible simplicial complex $\mathcal{K}$ then*

$$\chi(\mathcal{K}_\Gamma) \equiv 1 \pmod{q}. \tag{2.1}$$

In particular, such an action must always have a nonempty invariant face.

2.4. The KSS approach and the general strategy

The topological approach to evasiveness, initiated by Kahn, Saks, and Sturtevant, is based on the following key observation.

Lemma 2.2 (Kahn-Saks-Sturtevant [11])**.** *If P_n is a non-evasive graph property then P_n is contractible.*

Kahn, Saks, and Sturtevant recognized that Lemma 2.2 brought Oliver's Theorem to bear on evasiveness. The combination of Lemma 2.2 and Theorem 2.1 suggests the following general strategy, used by all authors in the area who have employed the topological method, including this paper: We find primes p, q, a group Γ satisfying Oliver's condition with these primes, and a Γ-action on P_n, such that $\chi(P_n) \equiv 0 \pmod{q}$. By Oliver's Theorem and the KSS Lemma this implies that P_n is evasive. The novelty is in finding the right Γ.

KSS [11] made the assumption that n is a prime power and used as $\Gamma = \mathrm{AGL}(1, n)$, the group of affine transformations $x \mapsto ax + b$ over the field of order n. While we use subgroups of such groups as our building blocks, the attempt to combine these leads to hard problems on the distribution of prime numbers.

Regarding the "forbidden subgraph" property, Chakrabarti, Khot, and Shi [3] built considerable machinery which we use. Our conclusions are considerably stronger than theirs; the additional techniques involved include a study of the orbitals of certain metacyclic groups, a universality property of cyclotomic graphs derivable using Weil's character sum estimates, plus the number theoretic reductions indicated.

For the "sparse graphs" result (Theorem 1.4) we need Γ such that all u-orbitals of Γ are large and therefore $(P_n)_\Gamma = \{\emptyset\}$.

In both cases, we are forced to use rather large building blocks of size q, say, where q is a prime such that $q-1$ has a large divisor which is a prime for Theorem 1.4 and a power of 2 for Theorem 1.3.

3. Forbidden subgraphs

In this section we prove parts (a) and (c) of Theorem 1.3.

3.1. The CKS condition

A *homomorphism* of a graph H to a graph H' is a map $f : V(H) \to V(H')$ such that $(\forall x, y \in V(H))(\{x, y\} \in E(H) \Rightarrow \{f(x), f(y)\} \in E(H'))$. (In particular, $f^{-1}(x')$ is an independent set in H for all $x' \in V(H')$.) Let $Q_r^{[[H]]}$ be the set of those H' with $V(H') = [r]$ that do not admit an $H \to H'$ homomorphism. Let further $T_H := \min\{2^{2^t} - 1 \mid 2^{2^t} \geq h\}$ where h denotes the number of vertices of H. The following is the main lemma of Chakrabarti, Khot, and Shi [3].

Lemma 3.1 (Chakrabarti et al. [3])**.** *If* $r \equiv 1 \pmod{T_H}$ *then* $\chi(Q_r^{[[H]]}) \equiv 0 \pmod 2$.

3.2. Cliques in generalized Paley graphs

Let q be an odd prime power and d an even divisor of $q-1$. Consider the graph $P(q, d)$ whose vertex set is $\mathbb{F}_q$ and the adjacency between the vertices is defined as follows: $i \sim j \iff (i-j)^d = 1$. $P(q, d)$ is called a *generalized Paley graph*.

Lemma 3.2. *If* $(q-1)/d \leq q^{1/(2h)}$ *then* $P(q, d)$ *contains a clique on* h *vertices.*

This follows from the following lemma which in turn can be proved by a routine application of Weil's character sum estimates (cf. [1]).

Lemma 3.3. *Let* $a_1, \ldots, a_t$ *be distinct elements of the finite field* $\mathbb{F}_q$*. Assume* $\ell \mid q-1$*. Then the number of solutions* $x \in \mathbb{F}_q$ *to the system of equations* $(a_i + x)^{(q-1)/\ell} = 1$ *is* $\frac{q}{\ell^t} \pm t\sqrt{q}$. ∎

Let $\Gamma(q, d)$ be the subgroup of order qd of $\mathrm{AGL}(1, q)$ defined in Section 2.1.

Observation 3.4. Each u-orbital of $\Gamma(q, d)$ is isomorphic to $P(q, d)$. ∎

Corollary 3.5. *If* $\frac{q-1}{d} \le q^{1/(2h)}$ *then each u-orbital of* $\Gamma(q,d)$ *contains a clique of size* h.

3.3. ϵ-near-Fermat primes

The numbers in the title were defined in Section 1.3. In this section we prove Theorem 1.3, part (a).

Theorem 3.6. *Let* H *be a graph on* h *vertices. If there are infinitely many* $\frac{1}{2h}$*-near-Fermat primes then* Q_n^H *is eventually evasive.*

Proof. Fix an odd prime $p \equiv 2 \pmod{T_H}$ such that $p \ge |H|$. If there are infinitely many $\frac{1}{2h}$-near-Fermat primes then infinitely many of them belong to the same residue class mod p, say $a + \mathbb{Z}p$. Let q_i be the i-th $\frac{1}{2h}$-near-Fermat prime such that $q_i \ge p$ and $q_i \equiv a \pmod{p}$. Let $r' = na^{-1} \pmod{p}$ and $k' = \sum_{i=1}^{r'} q_i$. Then $k' \equiv n \pmod{p}$ and therefore $n = pk + k'$ for some k.

Now in order to use Lemma 3.1, we need to write n as a sum of r terms where $r \equiv 1 \pmod{T_H}$. We already have r' of these terms; we shall choose each of the remaining $r - r'$ terms to be p or p^2. If there are t terms equal to p^2 then this gives us a total of $r = t + (k - tp) + r'$ terms, so we need $t(p-1) \equiv k + r' \pmod{T_H}$. By assumption, $p - 1 \equiv 1 \pmod{T_H}$; therefore such a t exists; for large enough n, it will also satisfy the constraints $0 \le t \le k/p$,

Let now

$$\Lambda_1 := \left((\mathbb{F}_{p^2}^+)^t \times (\mathbb{F}_p^+)^{k-tp} \right) \rtimes \mathbb{F}_{p^2}^\times$$

acting on $[pk]$ with t orbits of size p^2 and $k - pt$ orbits of size p as follows: on an orbit of size p^i $(i = 1, 2)$ the action is $\mathrm{AGL}(1, p^i)$. The additive groups act independently, with a single multiplicative action on top. $\mathbb{F}_{p^2}^\times$ acts on $\mathbb{F}_p^+$ through the group homomorphism $\mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$ defined by the map $x \mapsto x^{p-1}$. Let B_j denote an orbit of Λ_1 on $[kp]$. Now the orbit of any pair $\{u, v\} \in \binom{B_j}{2}$ is a clique of size $|B_j| \ge p \ge h$, therefore a Λ_1-invariant graph cannot contain an intra-cluster edge.

Let d_i be the largest power of 2 that divides $q_i - 1$. Let C_i be the subgroup of $\mathbb{F}_{q_i}^\times$ of order d_i. Let $\Lambda_2 := \prod_{i=1}^{r'} \Gamma(q_i, d_i)$, acting on $[k']$ with r' orbits of sizes $q_1, \ldots, q_{r'}$ in the obvious manner.

From Lemma 3.2 we know that the orbit of any $\{u, v\} \in \binom{[q_i]}{2}$ must contain a clique of size h. Hence, an invariant graph cannot contain any intra-cluster edge.

Overall, let $\Gamma := \Lambda_1 \times \Lambda_2$, acting on $[n]$. Since $q_i \ge p$, we have $\gcd(q_i, p^2 - 1) = 1$. Thus, Γ is a "2-group extension of a cyclic extension of a p-group" and therefore satisfies Oliver's Condition (stated before Theorem 2.1). Hence, assuming Q_n^H is non-evasive, Lemma 2.2 and Theorem 2.1 imply

$$\chi((Q_n^H)_\Gamma) \equiv 1 \pmod{2}.$$

On the other hand, we claim that the fixed-point complex $(Q_n^H)_\Gamma$ is isomorphic to $Q_r^{[[H]]}$. The (simple) proof goes along the lines of Lemma 4.2 of [3]. Thus, by Lemma 3.1 we have $\chi(Q_r^{[[H]]}) \equiv 0 \pmod{2}$, a contradiction. ∎

3.4. Unconditionally, Q_n^H is only $O(1)$ away from being evasive

In this section, we prove part (c) of Theorem 1.3.

Theorem 3.7. *For every graph H there exists a number C_H such that the query complexity of Q_n^H is $\geq \binom{n}{2} - C_H$.*

Proof. Let h be the number of vertices of H. Let p be the smallest prime such that $p \geq h$ and $p \equiv 2 \pmod{T_H}$. So $p < f(H)$ for some function f by Dirichlet's Theorem (we don't need any specific estimates here). Since $p - 1 \equiv 1 \pmod{T_H}$, we have $\gcd(p-1, T_H) = 1$ and therefore $\gcd(p-1, pT_H) = 1$. Now, by the Chinese Remainder Theorem, select the smallest positive integer k' satisfying $k' \equiv n \pmod{pT_H}$ and $k' \equiv 1 \pmod{p-1}$. Note that $k' < p^2 T_H$. Let $k = (n - k')/(pT_H)$; so we have $n = kpT_H + k'$.

Let $N' = \binom{n}{2} - \binom{k'}{2}$. Consider the following Boolean function B_n^H on N' variables. Consider graphs X on the vertex set $[n]$ with the property that they have no edges among their last k' vertices. These graphs can be viewed as Boolean functions of the remaining N' variables. Now we say that such a graph has property B_n^H if it does not contain H as a subgraph.

Claim. The function B_n^H is evasive.

The Claim immediately implies that the query complexity of Q_n^H is at least N', proving the Theorem with $C_H = \binom{k'}{2} < p^4 T_H^2 < f(H)^4 T_H^2$.

To prove the Claim, consider the groups $\Lambda := (\mathbb{F}_p^+)^{kT_H} \rtimes \mathbb{F}_p^\times$ and $\Gamma := \Lambda \times \mathbb{Z}_{k'}$. Here Λ acts on $[pkT_H]$ in the obvious way: we divide $[pkT_H]$ into kT_H blocks of size p; $\mathbb{F}_p^+$ acts on each block independently and $\mathbb{F}_p^\times$ acts on the blocks simultaneously (diagonal action) so on each block they combine to an $\mathrm{AGL}(1,p)$-action. $\mathbb{Z}_{k'}$ acts as a k'-cycle on the remaining k' vertices. So Γ is a cyclic extension of a p-group (because $\gcd(p-1, k') = 1$).

If B_n^H is not evasive then from Theorem 2.1 and Lemma 2.2, we have $\chi\left((B_n^H)_\Gamma\right) = 1$.

On the other hand we claim that, $(B_n^H)_\Gamma \cong Q_r^{[[H]]}$, where $r = kT_H + 1$. The proof of this claim is exactly the same as the proof of Lemma 4.2 of [3]. Thus, from Lemma 3.1, we conclude that $\chi(Q_r^{[[H]]})$ is even. This contradicts the previous conclusion that $\chi(Q_r^{[[H]]}) = 1$. ∎

Remark 3.8. Specific estimates on the smallest Dirichlet prime can be used to estimate C_H. Linnik's theorem implies $C_H < h^{O(1)}$, extending Theorem 3.7 to strong lower bounds for variable H up to $h = n^c$ for some positive constant c.

4. Sparse graphs: unconditional results

We prove part (c) of Theorem 1.4.

Theorem 4.1. *If the non-empty monotone graph property P_n is not evasive then*

$$\dim(P_n) = \Omega(n \log n).$$

4.1. The basic group construction

Assume in this section that $n = p^\alpha k$ where p is prime. Let $\Delta_k \leq \Sigma_k$. We construct the group $\Gamma_0(p^\alpha, \Delta_k)$ acting on $[n]$.

Let $\Delta = (\mathbb{F}_{p^\alpha}^\times \times \Delta_k)$. Let $\Gamma_0(p^\alpha, \Delta_k)$ be the semidirect product $(\mathbb{F}_{p^\alpha}^+)^k \rtimes \Delta$ with respect to the Δ-action on $(\mathbb{F}_{p^\alpha}^+)^k$ defined by

$$(a, \sigma) : (b_1, \ldots, b_k) \mapsto (ab_{\sigma^{-1}(1)}, \ldots, ab_{\sigma^{-1}(k)}).$$

We describe the action of $\Gamma_0(p^\alpha, \Delta_k)$ on $[n]$. Partition $[n]$ into k clusters of size p^α each. Identify each cluster with the field of order p^α, i.e., as a set, $[n] = [k] \times \mathbb{F}_{p^\alpha}$. The action of $\gamma = (b_1, \ldots, b_k, a, \sigma)$ is described by

$$\gamma : (x, y) \mapsto (\sigma(x), ay + b_{\sigma(x)}).$$

An unordered pair $(i, j) \in [n]$ is termed an *intra-cluster edge* if both i and j are in the same cluster, otherwise it is termed an *inter-cluster edge.* Note that every u-orbital under Γ has only intra-cluster edges or only inter-cluster edges. Denote by m_{intra} and m_{inter} the minimum sizes of u-orbitals of intra-cluster and inter-cluster edges respectively.

We denote by m'_k the minimum size of an orbit in $[k]$ under Δ_k and by m''_k the minimum size of a u-orbital in $[k]$. We then have:

$$m_{\text{intra}} \geq \binom{p^\alpha}{2} \times m'_k, \qquad m_{\text{inter}} \geq (p^\alpha)^2 \times m''_k$$

Let $m_k{}' := \min\{m'_k, m''_k\}$ and define m^* as the minimum size of a u-orbital in $[n]$. Then

$$m^* = \min\{m_{\text{intra}}, m_{\text{inter}}\} = \Omega(p^{2\alpha} m_k) \tag{4.1}$$

4.2. Vinogradov's Theorem

The Goldbach Conjecture asserts that every even integer can be written as the sum of two primes. Vinogradov's Theorem [24] says that every sufficiently large odd integer k is the sum of three primes $k = p_1 + p_2 + p_3$. We use here Haselgrove's version [7] of Vinogradov's theorem which states that we can require the primes to be roughly equal: $p_i \sim k/3$. This can be combined with the Prime Number Theorem to conclude that every sufficiently large even integer k is a sum of four roughly equal primes.

4.3. Construction of the group

Let $n = p^\alpha k$ where p is prime. Assume k is not bounded. Write k as a sum of $t \leq 4$ roughly equal primes p_i. Let $\Delta_k := \prod_i \mathbb{Z}_{p_i}$ where $\mathbb{Z}_{p_i}$ denotes the cyclic group of order p_i and the direct product is taken over the *distinct* p_i.

Δ_k acts on $[k]$ as follows: partition k into parts of sizes $p_1, \ldots, p_t$ and call these parts $[p_i]$. The group $\mathbb{Z}_{p_i}$ acts as a cyclic group on the part $[p_i]$. In case of repetitions, the same factor $\mathbb{Z}_{p_i}$ acts on all the parts of size p_i.

We follow the notation of Section 4.1 and consider the group $\Gamma_0(p^\alpha, \Delta_k)$ with our specific Δ_k. We have $m_k = \Omega(k)$ and hence we get, from equation (4.1):

Lemma 4.2. *Let $n = p^\alpha k$ where p is a prime. For the group $\Gamma_0(p^\alpha, \Delta_k)$, we have $m^* = \Omega(p^{2\alpha} k) = \Omega(p^\alpha n)$, where m^* denotes the minimum size of a u-orbital.*

4.4. Proof for the superlinear bound

Let $n = p^\alpha k$ where p^α is the largest prime power dividing n; so $p^\alpha = \Omega(\log n)$; this will be a lower bound on the size of u-orbitals. Our group Γ will be of the general form discussed in Section 4.1.

Case 1. $p^\alpha = \Omega(n^{2/3})$.

Let $\Gamma = \Gamma_0(p^\alpha, \{1\})$. Following the notation of Section 4.1, we get $m'_k = m''_k = 1$, and this yields that $m^* = \Omega((p^\alpha)^2) = \Omega(n^{4/3}) = \Omega(n \log n)$. Oliver's condition is easily verified for Γ.

Case 2. $k = \Omega(n^{1/3})$.

Consider the $\Gamma := \Gamma_0(p^\alpha, \Delta_k)$ acting on $[n]$ where Δ_k is as described in Section 4.3. The minimum possible size m^* of a u-orbital is $\Omega(np^\alpha)$ by Lemma 4.2. Finally, since $p^\alpha = \Omega(\log n)$, we obtain $m^* = \Omega(n \log n)$.

If all p_i are co-prime to $p^\alpha - 1$ then $\mathbb{F}_{p^\alpha}^\times \times \Delta_k$ becomes a cyclic group and Γ becomes a cyclic extension of a p-group.

Since $p_i = \Omega(k) = \Omega(n^{1/3})$ for all i and $p^\alpha = O(n^{2/3})$, size considerations yield that at most one p_i divides $p^\alpha - 1$ and p_i^2 does not. Suppose, without loss of generality, p_1 divides $p^\alpha - 1$. Let $p^\alpha - 1 = p_1 d$, then d must be co-prime to each p_i. Thus, $\Delta = (\mathbb{Z}_{p_1} \times \mathbb{Z}_d) \times (\mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_t}) = (\mathbb{Z}_d \times \mathbb{Z}_{p_2} \times \ldots \times \mathbb{Z}_{p_r}) \times (\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_1})$. Thus, Δ is a p_1-group extension of a cyclic group. Hence, Γ satisfies Oliver's Condition (cf. Theorem 2.1). ∎

Remark 4.3. For almost all n, our proof gives a better dimension lower bound of $\Omega(n^{1+\frac{1+o(1)}{\ln \ln n}})$.

5. Sparse graphs: conditional improvements

In this section we prove parts (a) and (b) of Theorem 1.4.

5.1. General Setup

Let $n = pk + r$, where p and r are prime numbers. Let q be a prime divisor of $(r-1)$. We partition $[n]$ into two parts of size pk and r, denoted by $[pk]$ and $[r]$ respectively. We now construct a group $\Gamma(p, q, r)$ acting on $[n]$ as a direct product of a group acting on $[pk]$ and a group acting on $[r]$, as follows:

$$\Gamma = \Gamma(p, q, r) := \Gamma_0(p, \Delta_k) \times \Gamma(r, q)$$

Here, $\Gamma_0(p, \Delta_k)$ acts on $[pk]$ and is as defined in Section 4.3, and involves choosing a partition of k into upto four primes that are all $\Omega(k)$.

$\Gamma(r, q)$ is defined as the semidirect product $\mathbb{F}_r^+ \rtimes C_q$, with C_q viewed as a subgroup of the group $\mathbb{F}_r^\times$. It acts on $[r]$ as follows: We identify $[r]$ with the field of size r. Let (b, a) be a typical element of Γ_r where $b \in \mathbb{F}_r$ and $a \in C_q$. Then, $(b, a) : x \mapsto ax + b$.

Thus, $\Gamma = \Gamma(p, q, r)$ acts on $[n]$. Let m^* be the minimum size of the orbit of any edge $(i, j) \in \binom{[n]}{2}$ under the action of Γ. One can show that

$$m^* = \Omega(\min\{p^2 k, pkr, qr\}). \tag{5.1}$$

We shall choose p, q, r carefully such that (a) the value of m^* is large, and (b) Oliver's condition holds for $\Gamma(p, q, r)$.

5.2. ERH and Dirichlet primes

The Extended Riemann Hypothesis (ERH) implies the following strong version of the Prime Number Theorem for arithmetic progressions. Let $\pi(n, D, a)$ denote the numer of primes $p \leq n$, $p \equiv a \pmod{D}$. Then for $D < n$ we have

$$\pi(n, D, a) = \frac{\mathrm{li}(n)}{\varphi(D)} + O(\sqrt{x} \ln x) \tag{5.2}$$

where $\mathrm{li}(n) = \int_2^n dt/t$ and the constant implied by the big-Oh notation is absolute (cf. [16, Ch. 7, eqn. (5.12)] or [2, Thm. 8.4.5]).

This result immediately implies "Bertrand's Postulate for Dirichlet primes:"

Lemma 5.1 (Bertrand's Postulate for Dirichlet primes)**.** *Assume ERH. Suppose the sequence D_n satisfies $D_n = o(\sqrt{n}/\log^2 n)$. Then for all sufficiently large n and for any a_n relatively prime to D_n there exists a prime $p \equiv a_n \pmod{D_n}$ such that $\frac{n}{2} \leq p \leq n$.*

5.3. With ERH but without Chowla

We want to write $n = pk + r$, where p and r are primes, and with q a prime divisor of $r - 1$, as described in Section 5.1. Specifically, we try for:

$$p = \Theta(n^{1/4}), \quad \frac{n}{4} \leq r \leq \frac{n}{2}, \quad q = \Theta(n^{1/4-\epsilon})$$

We claim that under ERH, such a partition of n is possible.

To see this, fix some $p = \Theta(n^{1/4})$ such that $\gcd(p, n) = 1$. Fix some $q = \Theta(n^{1/4-\epsilon})$. Now, $r \equiv 1 \pmod{q}$ and $r \equiv n \pmod{p}$ solves to $r \equiv a \pmod{pq}$ for some a such that $\gcd(a, pq) = 1$. Since $pq = \Theta(n^{1/2-\epsilon})$, we can conclude under ERH (using Lemma 5.1) that there exists a prime $r \equiv a \pmod{pq}$ such that $\frac{n}{4} \leq r \leq \frac{n}{2}$. This gives us the desired partition. One can verify that our Γ satisfies Oliver's Condition. Equation (5.1) gives $m^* = \Omega(n^{5/4-\epsilon})$. This completes the proof of part (b) of Theorem 1.4. ∎

5.4. Stronger bound using Chowla's conjecture

Let a and D be relatively prime. Let p be the first prime such that $p \equiv a \pmod{D}$. Chowla's conjecture tells us that $p = O(D^{1+\epsilon})$ for every $\epsilon > 0$. Using this, we show $m^* = \Omega(n^{3/2-\epsilon})$.

We can use Chowla's conjecture, along with the general setup of Section 5.1, to obtain a stronger lower bound on m^*. The new bounds we hope to achieve are:

$$p = \Theta(\sqrt{n}), \quad n^{1-2.5\delta} \leq r \leq n^{1-0.5\delta}, \quad q = \Theta(n^{1/2-\delta})$$

Such a partition is always possible assuming Chowla's conjecture. To see this, first fix $p = \Theta(n^{1/2})$, then fix $q = \Theta(n^{1/2-2\delta})$ and find the least solution for $r \equiv 1 \pmod{q}$ and $r \equiv n \pmod{p}$, which is equivalent to solving for $r \equiv a \pmod{pq}$ for some $a < pq$. The least solution will be greater than pq unless a happens to be a prime. In this case, we add another constraint, say $r \equiv a + 1 \pmod{3}$ and resolve to get the least solution greater than pq. Note that $n^{1-2.5\delta} \leq r \leq n^{1-0.5\delta}$. Now, from Equation (5.1), we get the lower bound of $m^* = \Omega(n^{3/2-4\delta})$. This completes the proof of part (a) of Theorem 1.4. ∎

Acknowledgment.

Raghav Kulkarni expresses his gratitude to Sasha Razborov for bringing the subject to his attention and for helpful initial discussions.

References

[1] Babai, L., Gál, A., Wigderson, A.: Superpolynomial lower bounds for monotone span programs. *Combinatorica* 19 (1999), 301–320.
[2] Bach, E., Shallit, J.: *Algorithmic Number Theory, Vol. 1.* The MIT Press 1996.
[3] Chakrabarti, A., Khot, S., Shi, Y.: Evasiveness of Subgraph Containment and Related Properties. *SIAM J. Comput.* 31(3) (2001), 866-875.
[4] Chowla, S. On the least prime in the arithmetical progression. *J. Indian Math. Soc.* 1(2) (1934), 1–3.
[5] Davenport, H.: *Multiplicative Number Theory.* (2nd Edn) Springer Verlag, New York, 1980.
[6] Granville, A., Pomerance, C.: On the least prime in certain arithmetic progressions. *J. London Math. Soc.* 41(2) (1990), 193–200.
[7] Haselgrove, C. B.: Some theorems on the analytic theory of numbers. *J. London Math. Soc.* 36 (1951) 273–277
[8] Heath-Brown, D. R.: Almost-primes in arithmetic progressions and short intervals. *Math. Proc. Cambr. Phil. Soc.* 83 (1978) 357–376.
[9] Heath-Brown, D. R.: Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc.* 64(3) (1992) 265–338.
[10] Kleitman, D. J., Kwiatkowski, D. J.: Further results on the Aanderaa-Rosenberg Conjecture *J. Comb. Th. B* 28 (1980), 85–90.
[11] Kahn, J., Saks, M., Sturtevant, D.: A topological approach to evasiveness. *Combinatorica* 4 (1984), 297–306.
[12] Lutz, F. H.: Examples of $\mathbb{Z}$-acyclic and contractible vertex-homogeneous simplicial complexes.. *Discrete Comput. Geom.* 27 (2002), No. 1, 137–154.
[13] Mader, W.: Homomorphieeigenschaften und mittlere Kantendichte von Graphen. *Math. Ann.* 174 (1967), 265–268.
[14] Mader, W.: Homomorphiesätze für Graphen. *Math. Ann.* **175** (1968), 154–168.
[15] Oliver, R.: Fixed-point sets of group actions on finite acyclic complexes. *Comment. Math. Helv.* 50 (1975), 155–177.
[16] Prachar, K.: *Primzahlverteilung.* Springer, 1957.
[17] Rosenberg A. L.: On the time required to recognize properties of graphs: A problem. *SIGACT News* 5 (4) (1973), 15–16.
[18] Rotman, J.: *An Introduction to the Theory of Groups.* Springer Verlag, 1994.
[19] Rivest, R.L., Vuillemin, J.: On recognizing graph properties from adjacency matrices. *Theoret. Comp. Sci.* 3 (1976), 371–384.
[20] Smith P. A.: Fixed point theorems for periodic transformations. *Amer. J. of Math.* 63 (1941), 1–8.
[21] Titchmarsh, E. C.: A divisor problem. *Rend. Circ. Mat. Palermo* 54 (1930), 419–429.
[22] Triesch, E.: On the recognition complexity of some graph properties. *Combinatorica* 16 (2) (1996) 259–268.
[23] Turán, P.: Über die Primzahlen der arithmetischen Progression. *Acta Sci. Math. (Szeged)* 8 (1936/37) 226–235.
[24] Vinogradov, I. M.: *The Method of Trigonometrical Sums in the Theory of Numbers (Russian).* Trav. Inst. Math. Stekloff 10, 1937.
[25] Yao, A. C.: Monotone bipartite properties are evasive. *SIAM J. Comput.* 17 (1988), 517–520.