Decision Tree Complexity, Solvable Groups, and the Distribution of Prime Numbers

Joint Work 2010

László Babai

Raghav Kulkarni (speaker)

Vipul Naik
University of Chicago, Chicago, IL, USA

Anandam Banerjee
Northeastern University, Boston, MA, USA

Decision Tree Complexity

Decision Tree Model aka Query Model

boolean function $f : \{0,1\}^N \to \{0,1\}$

- <u>Input:</u> $x = (x_1, \ldots, x_N) \in \{0,1\}^N$
- <u>Access:</u> (adaptive) queries $x_i \stackrel{?}{=} 1$
- <u>Cost:</u> #queries
- <u>Goal</u>: determine $f(x)$

<u>Decision Tree Complexity</u>

D(f) := #queries on **worst** input

Evasiveness

$f \in \{0,1\}^N \to \{0,1\}$ is <u>evasive</u>, if

$$D(f) = N$$

A sequence P_n of boolean functions is said to be <u>eventually</u> evasive if P_n is evasive for all sufficiently large n

Note: n and N may be **different**

Graph Properties

Graph Properties as Boolean Functions

Graph Property P_n: collection of n-vertex labeled graphs invariant under relabeling

$$N = \binom{n}{2}$$

n-vertex graph $\longleftrightarrow$ string in $\{0,1\}^N$
graph property $\longleftrightarrow$ $f : \{0,1\}^N \to \{0,1\}$
invariant under relabeling of $[n]$

Examples: planarity, 3-colorability,
complete graphs, connectedness,
Eulerian graphs, perfect graphs

Trivial Graph Properties: all graphs or no graphs

Monotone Graph Properties

- Monotone (Decreasing) Graph Property: closed under edge deletion.

- Examples: planarity, 3-colorability, {empty graph}, trivial graph properties

- Non-monotone Examples: perfect graphs, Eulerian graphs, cycles

Forbidden Subgraph Property
H - a fixed graph

$Q_n^H :=$ the class of all n-vertex graphs that **do not contain** H as a (not necessarily induced) subgraph.

Q_n^H is monotone (decreasing)

Evasiveness Conjecture

Evasiveness Conjecture
aka Aanderaa-Rosenberg-Karp Conjecture for Monotone Graph Properties

For any n, any non-trivial monotone property P_n of n-vertex graphs must be *evasive*, *i.e.*, $D(P_n) = \binom{n}{2}$.

- Aanderaa - Rosenberg Conjecture 1973:
  $D(P_n) = \Omega(n^2)$.

- (Theorem) Rivest and Vuillemin 1978:
  $D(P_n) \geq n^2/16$

- Kahn, Saks, and Sturtevant 1984:
  (KSS Theorem)
  $D(P_n) = \binom{n}{2}$ when n is a prime power
  (conceptual breakthrough: **topological** approach)

KSS Approach

- monotone property : simplicial complex
- group actions on simplicial complex
- Oliver's Theorem:
  group actions $\rightarrow$ fixed points
- fixed point $\rightarrow$ invariant subgraph

Results via KSS topological approach

- Yao 1988: evasiveness in bipartite graphs with fixed partition

- Triesch 1996: bipartite properties (among all graphs)

- Chakrabarti, Khot, and Shi 2002:
  - more tools for Forbidden Subgraph
  - $D(Q_n^H) = \binom{n}{2} - O(n)$
  - forbidden minor : eventually evasive

Our Results

Our Results

- Conditional Results: We confirm under widely accepted number theoretic hypotheses, the eventual evasiveness of
  (a) every forbidden subgraph property
  (b) any monotone property of sparse graphs
  . sparse: $\leq n^{3/2-\epsilon}$ edges

- Unconditional Results
  (a) forbidden sub: $D(Q_n^H) = \binom{n}{2} - O(1)$
  . improves CKS bound: $\binom{n}{2} - O(n)$
  (b) any monotone property of sparse graphs
  . sparse: $\leq cn \log n$

- Unconditional Corollary: forbidden topological subgraph eventually evasive (generalizes CKS: forbidden minor)

Number Theoretic Dependencies

<u>Chowla's Conjecture 1944:</u>
on smallest Dirichlet Prime

$$(\exists p < d^{1+o(1)})(p \equiv a \mod d)$$

<u>Generalized Riemann Hypothesis 1884:</u>
for Dirichlet L-functions

$$(\exists p < d^{2+o(1)})(p \equiv a \mod d)$$

<u>Vinogradov's Theorem 1937:</u>
odd Goldbach Conjecture

$$k \text{ odd} \Rightarrow k = p_1 + p_2 + p_3$$

<u>Haselgrove's Strengthening 1954:</u>
of Vinogradov's Theorem

$$p_1 \approx p_2 \approx p_3$$

<u>Weil's Character Sum Estimates 1941:</u>
for characters of finite field

pseudorandomness of d^{th} power residues

Our Methods

- use KSS topological approach
- use full power of Oliver's Theorem
- new group actions
  via number theory (results/conjectures)
- invariant graphs analysed
  via Weil's character sum estimates
- forbidden subgraph: use CKS reduction of
  Euler characteristic

Some Preliminaries

Abstract Simplicial Complex.

Let $X = \{x_1, \ldots, x_m\}$.
Let $\Delta \subseteq 2^X$ such that:

$$(f \in \Delta)(f' \subseteq f) \Rightarrow f' \in \Delta.$$

Δ : <u>abstract simplicial complex</u>
$f \in \Delta$: <u>face</u> of Δ.

(Dimension) $\dim(\Delta) := \max\{(|f| - 1) \ : \ f \in \Delta\}$.

(Euler Characteristic)

$$\chi(\Delta) := \sum_{f \in \Delta, f \neq \emptyset} (-1)^{|f|-1}.$$

Monotone Property and Abstract Complex

$$[n] := \{1, 2, \ldots, n\}.$$

$$\binom{[n]}{2} := \{\{i, j\} \ : \ (i \neq j \in [n])\}.$$

$\mathcal{G}_n$ - n-vertex (labeled) graphs.

$$G \in \mathcal{G}_n \Rightarrow E(G) \subseteq \binom{[n]}{2}.$$

P_n - monotone (decreasing) graph property

$$\Delta^{P_n} := \{E(G) \ : \ G \in P_n\}$$

$$\dim(P_n) := \dim(\Delta^{P_n})$$

dim = maximum possible #edges - 1

Oliver's Fixed Point Theorem 1976

<u>Oliver's Condition on Group Γ:</u>

$$(\exists\ \Gamma_2, \Gamma_1)(\Gamma_2 \lhd \Gamma_1 \lhd \Gamma)$$

$\exists$ primes p, q such that

- $|\Gamma/\Gamma_1| = q^\beta$

- Γ_1/Γ_2 is cyclic

- $|\Gamma_2| = p^\alpha$

all such groups are <u>solvable</u>; $p = q$ permitted

<u>Oliver's Theorem 1976:</u>
Δ - contractible, non-empty
Γ - satisfies Oliver's Condition
$\Rightarrow$ Γ action on Δ must have
a non-empty <u>Γ-invariant face</u>

Kahn, Saks, and Sturtevant's Approach

$\boxed{\text{Evasiveness} \leftarrow \text{Topology} + \text{Group Actions}}$

- P_n <u>not evasive</u> $\Rightarrow \Delta^{P_n}$ <u>contractible</u>
  $(\Rightarrow \chi(P_n) = 1)$

- <u>Graph Property:</u> $\Gamma \leq S_n \Rightarrow \Gamma$ acts on Δ^{P_n}.

- use Oliver's Fixed Point Theorem

KSS Theorem

Theorem (KSS 1984): If $n = p^\alpha$, then any non-evasive monotone graph property P_n satisfied by at least one graph is satisfied by K_n, and hence by all graphs.

Key use of prime power: There exists a group $\Gamma \leq S_n$ such that:

(a) Γ satisfies Oliver's Condition

(b) Γ is transitive on $\binom{[n]}{2}$

Γ acts on the non-empty contractible simplicial complex Δ^{P_n} and via Oliver, Δ^{P_n} has a non-empty Γ-invariant face

Since Γ is transitive on $\binom{[n]}{2}$, this Γ-invariant face must be K_n. Thus, $K_n \in \Delta^{P_n}$

KSS Group Construction for $n = p^\alpha$
$\Gamma := \mathbb{F}_{p^\alpha}^{+} \rtimes \mathbb{F}_{p^\alpha}^{\times}$: affine group over $\mathbb{F}_{p^\alpha}$
Explicitly

- identify $[n]$ with $\mathbb{F}_{p^\alpha}$
- $\Gamma := \{\gamma : x \mapsto ax + b \mid a \in \mathbb{F}_{p^\alpha}^{\times} \ \& \ b \in \mathbb{F}_{p^\alpha}^{+}\}$
- Γ - cyclic extension of a p-group
  (thus Γ satisfies Oliver's Condition)
- Γ - transitive on $\binom{[n]}{2}$

Our Approach to Sparse Graphs

Evasiveness and Dimension

A Restatement of Evasiveness Conjecture:

$(P_n \neq \emptyset)(P_n$ not evasive$) \Rightarrow \mathrm{dim}(P_n) = \binom{n}{2} - 1.$

Our Sparse Graph Results:
$(P_n \neq \emptyset)(P_n$ not evasive$) \Rightarrow \mathrm{dim}(P_n) \geq m(n)$

in other words ...
any non-trivial monotone property of graphs with at most $m(n)$ edges is evasive
stronger number theory $\Rightarrow$ larger $m(n)$

Dimension Lower Bound

trivial bound via KSS : $\Omega(n)$

We show

- $\Omega(n \log n)$ <u>unconditionally</u>

- $\Omega(n^{5/4-\epsilon})$ <u>under GRH</u>

- $\Omega(n^{3/2-\epsilon})$ <u>under Chowla's Conjecture</u>

still far from quadratic

This translates to ...

property of graphs with at most m edges $\equiv$ property fails for any graph having $> m$ edges

any non-trivial monotone property of graphs with at most m edges is eventually evasive where

- $m = cn \log n$ unconditionally
- $m = n^{5/4-\epsilon}$ under GRH
- $m = n^{3/2-\epsilon}$ under Chowla's Conjecture

Our Approach to Sparse Graphs:

Construct $\Gamma \leq S_n$ such that:

- Γ satisfies <u>Oliver's Condition</u>

- size of the <u>orbit of any edge</u> under Γ is as <u>large</u> as possible

<u>KSS 84</u>

$\boxed{\text{Evasiveness} \leftarrow \text{Topology} + \boxed{\text{Group Actions}}}$

<u>Our new component</u>

$\boxed{\boxed{\text{Group Actions}} \leftarrow \text{Analytic Number Theory}}$

Forbidden Subrgraph

CKS Approach to Forbidden Subgraph
Chakrabarti, Khot, and Shi 2002:

- use KSS + Oliver

- construct new group actions
  specific to Forbidden Subgraph

- invariant graph trivially contains
  a large clique

Our New Components to CKS Approach

- metabelian group actions
  to force large clique non-trivially

- Paley graphs

- Weil's character sum estimates

- use distribution of prime numbers
  (known/conjectured) to glue the pieces

Paley-type Graphs & Metabelian Groups
Construction of Graph $P(q, d)$

- $V = \mathbb{F}_q$ $\quad$ q odd prime power
  d even $\quad$ $d \mid q - 1$

- $i \sim j \iff (i - j)^d = 1$ (over $\mathbb{F}_q$)

$\Gamma(q, d) :=$ order qd subgroup of $\mathbb{F}_q^+ \rtimes \mathbb{F}_q^\times$

Main Observations

- orbit of any (unordered) pair $\{i, j\} \in \binom{[q]}{2}$ under $\Gamma(q, d)$ action is isomorphic to $P(q, d)$

- if $\frac{q-1}{d} \leq q^{1/2h}$ then $P(q, d)$ contains a clique on h vertices

Paley-type graphs **pseudorandom**

proof goes via standard application of Weil's Character Sum Estimates

More Details : Sparse Graphs

(mostly skipping ...)

A Prime-Partition of k.

Goldbach Conjecture:
k - even integer $\Rightarrow k = p_1 + p_2$
p_i prime.

Vinogradov's **Theorem**:
k - large odd integers
$\Rightarrow k = p_1 + p_2 + p_3$

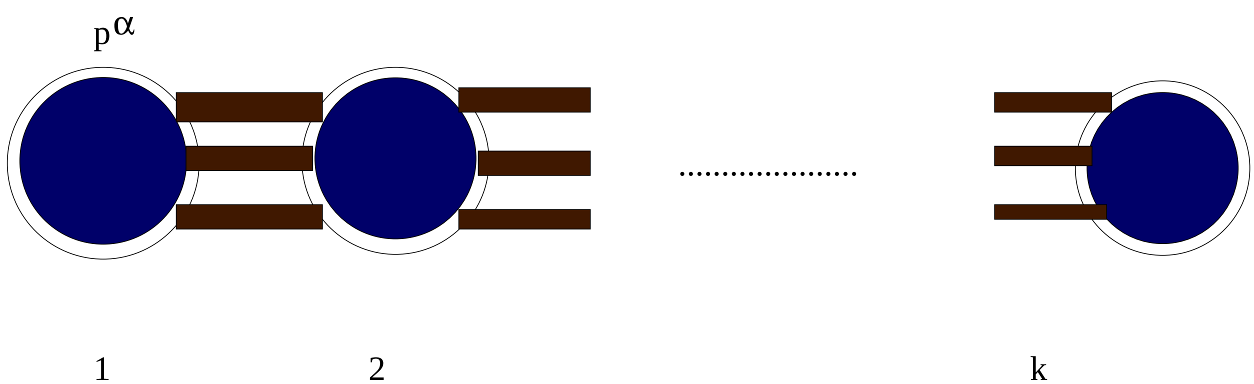
Haselgrove's Strengthening: $\boxed{p_i = \Omega(k)}$

Corollary: k large even integer
$\Rightarrow k = p_1 + p_2 + p_3 + p_4$,
$\boxed{p_i = \Omega(k)}$

Partition of $\{1, 2, \ldots, n\}$

Let $n = p^{\alpha}k \qquad p$ prime

$|S| = n.$



$$[n] = \underbrace{\mathbb{F}_{p^{\alpha}} \dot{\cup} \ldots \dot{\cup} \mathbb{F}_{p^{\alpha}}}_{k}$$

Our Basic Group Construction

Γ acts on $[n]$ such that

- within each block Γ simulates action of affine group over $\mathbb{F}_{p^\alpha}$: $x \mapsto ax + b$

- $k = p_1 + p_2 + p_3$ where $p_i \approx p_j$ (Vinogradov + Haselgrove)

$$H := \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_3}$$

- Γ permutes blocks according to $H \leq S_k$

$$\overbrace{\underbrace{00\ldots0}_{p_1}\underbrace{00\ldots0}_{p_2}\underbrace{00\ldots0}_{p_3}}^{k}$$

- Γ satisfies Oliver's Condition (not obvious)

Description of Γ

$$n = p^\alpha k \qquad H \leq S_k$$

$$\Gamma := (\underbrace{\mathbb{F}_{p^\alpha}^{+} \times \cdots \times \mathbb{F}_{p^\alpha}^{+}}_{k}) \rtimes (\mathbb{F}_{p^\alpha}^{\times} \times H)$$

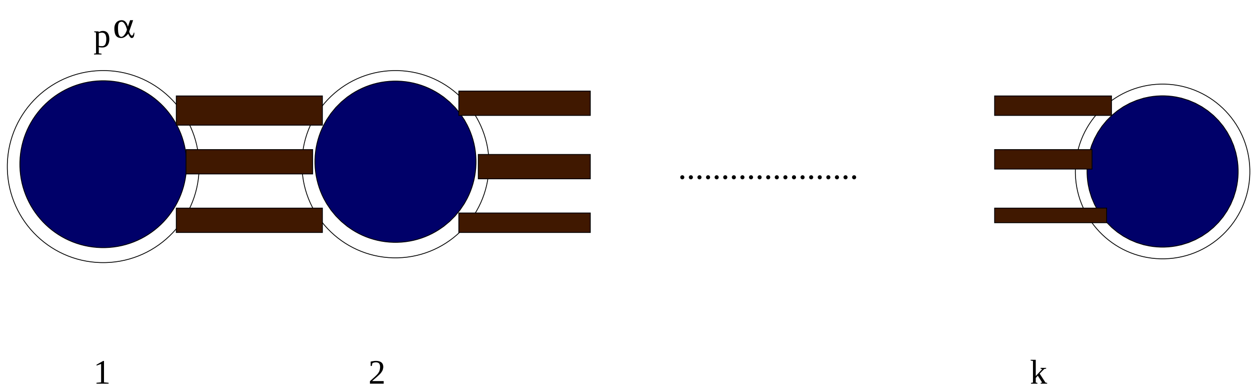
Orbit of an Edge

Two types of edges

- <u>intra-cluster</u> : orbit K_{p^α}

- <u>inter-cluster</u> : orbit K_{p^α, p^α}

intra-cluster edge orbits $\leftrightarrow$ H-orbits on $[k]$ inter-cluster edge orbits $\leftrightarrow$ H-orbits on $\binom{[k]}{2}$



Orbit Size Lower Bounds

$k = p_1 + p_2 + p_3 \quad p_i \approx p_j \quad p_1 \leq p_2 \leq p_3$

- intra-cluster edge -

$$|\text{intra-cluster orbit}| \geq \binom{p^\alpha}{2} \times p_1$$

- inter-cluster edge -

$$|\text{inter-cluster orbit}| \geq (p^\alpha)^2 \times p_1$$

- any edge -

$$|\text{any orbit}| = \Omega(p^\alpha \times p^\alpha \times p_1)$$

Choice of p^α

$$p^\alpha := \text{largest prime power dividing } n$$

- $p^\alpha = \Omega(\log n)$
- $n \sim 3p^\alpha p_1$
- $|\text{any orbit}| = \Omega(n \log n)$

(thanks to Vinogradov's **Theorem**)
this proves **unconditionally** ...

there exists a constant c such that any monotone property of graphs with $\leq cn \log n$ edges is evasive

Another Partition of n

We want to write

$$n = pk + r$$

such that

$$p,\ r\ prime.$$

$$p = \Theta(n^{1/4})$$

$$\frac{n}{4} \le r \le \frac{n}{2}$$

$$(\exists q)(q\ prime)(q \mid r - 1)(q = \Theta(n^{1/4-\epsilon}))$$

GRH and Dirichlet Primes

For a fixed D and a such that gcd$(a, D) = 1$ there are infinitely many primes of the form $p \equiv a$ mod D.

Under GRH:
If $D = O(n^{1/2-\epsilon})$, then
for any a such that $gcd(a, D) = 1$,
there exists a prime $p \equiv a$ mod D
such that $\frac{n}{2} \leq p \leq n$.

GRH $\Rightarrow$ desired partition

Choose some prime $p = \Theta(n^{1/4})$.
Choose another prime $q = \Theta(n^{1/4-\epsilon})$.
We need to find a prime r such that

$$r \equiv n \bmod p \ \& \ r \equiv 1 \bmod q$$

Equivalently,
for some a such that $gcd(a, pq) = 1$
we want to find $\frac{n}{4} \leq r \leq \frac{n}{2}$ such that

$$r \equiv a \bmod pq.$$

Since $pq = O(n^{1/2-\epsilon})$,
GRH $\Rightarrow$ such r exists.

Choosing Γ

$$\Gamma := \Gamma_{[pk]} \times \Gamma_r$$

where

$$\Gamma_r := \mathbb{F}_r^+ \rtimes \mathbb{Z}_q$$

$\Gamma_{[pk]}$ - as constructed previously using prime partition of k.

With this delicate choice of parameters, Γ satisfies Oliver's Condition and one can show:

$(P_n \neq \emptyset)(P_n$ not evasive$) \Rightarrow \dim(P_n) = \Omega(n^{5/4-\epsilon})$

Possible Directions

- first try to resolve the following:
  (under number theoretic conjectures)

  $(P_n \neq \emptyset)(P_n \text{ not evasive}) \Rightarrow \dim(P_n) = \Omega(n^2)$

- prove evasivenes conjecture or
  strong dimension lower bounds
  on sets of positive density

- unconditional result for Forbidden Subgraph

Thanks !