

Barriers Workshop
Princeton, 8/25/2009

AC^0 & Monotone Complexity of k-CLIQUE on Random Graphs

Benjamin Rossman

Massachusetts Institute of Technology

Outline of the Talk

k-CLIQUE has average-case complexity

$$n^{k/4+O(1)}$$

both in AC^0 and for monotone circuits

1. Background: circuits, random graphs
2. Monotone lower bound
3. AC^0 lower bound
4. Monotone AC^0 upper bound

Circuits

- AND, OR, NOT gates
- We consider **circuits taking graphs as inputs**:
($\binom{n}{2}$) variables representing potential edges in an n -vertex graph.
- **Circuit** = non-uniform sequence of circuits on n -vertex graphs for $n=1,2,3,\dots$

Circuits

- **Monotone** = only AND and OR gates (no NOT gates)
- **AC⁰** = {polynomial-size, constant depth, unbounded fan-in circuits}

k-CLIQUE

- **k-CLIQUE** is the problem of deciding whether a graph contains a **k-clique** (a set of k vertices with all possible edges among them).
- k is constant (not an input to the problem).
- Worst-case complexity is obviously $O(n^k)$.
In fact, can do $O(n^{(w/3)k + \text{constant}})$ where w is exponent of matrix multiplication.
- Lower bound of $n^{\Omega(k)}$ would imply $P \neq NP$.

Random Graphs

- $G(n,p)$ denotes the Erdos-Renyi random graph.
- Functions $p(n) \in \Theta(n^{-2/(k-1)})$ are precisely the threshold functions for the existence of k -cliques in $G(n,p)$.
- $p(n) \in o(n^{-2/(k-1)}) \Rightarrow G(n,p)$ almost surely has no k -clique.
- $p(n) \in \omega(n^{-2/(k-1)}) \Rightarrow G(n,p)$ almost surely contains a k -clique.

k-CLIQUE on Random Graphs

- For $p : \mathbb{N} \rightarrow [0,1]$, a boolean function f is said to **solve k-CLIQUE on $G(n,p)$** if

$$f(G) = 1 \text{ iff } G \text{ has a k-clique}$$

almost surely for $G = G(n,p)$.

- Trivial for subcritical $p(n) \in o(n^{-2/(k-1)})$ and supercritical $p(n) \in \omega(n^{-2/(k-1)})$.
- All the action is for *threshold functions* $p(n) \in \Theta(n^{-2/(k-1)})$.

k-CLIQUE on Random Graphs

- For $p : \mathbb{N} \rightarrow [0,1]$, a boolean function f is said to **solve k-CLIQUE on $G(n,p)$** if

$$f(G) = 1 \text{ iff } G \text{ has a k-clique}$$

almost surely for $G = G(n,p)$.

- f is said to **solve k-CLIQUE on random graphs** if it solves k-CLIQUE on $G(n,p)$ for *every* function $p : \mathbb{N} \rightarrow [0,1]$.

k-CLIQUE on Random Graphs

Theorem (R., STOC'08)

AC⁰ circuits which solve k-CLIQUE on random graphs have size $\Omega(n^{k/4})$.

Theorem (Kazuyuki Amano, CCC'09)

There exist AC⁰ circuits of size $O(n^{k/4 + \text{constant}})$ which solve k-CLIQUE on random graphs.

k-CLIQUE on Random Graphs

Theorem (R. '09)

Monotone circuits which solve k-CLIQUE on random graphs have size $\Omega(n^{k/4})$.

Theorem (R. '09, adapting Amano)

There exist monotone AC⁰ circuits of size $O(n^{k/4 + \text{constant}})$ which solve k-CLIQUE on random graphs.

k-CLIQUE on Random Graphs

CONJECTURE

General circuits which solve k-CLIQUE on random graphs have size $\Omega(n^{k/4})$.

Worst-Case Lower Bounds

- k -CLIQUE in AC^0 (depth d):

$$\Omega(n^{\sqrt{k}/d^{1.5}}) \quad \text{Lynch '86}$$

$$\Omega(n^{k/89d^2}) \quad \text{Beame '90}$$

- k -CLIQUE on monotone circuits:

$$\Omega(n^k/\text{polylog}(n)) \quad \text{Razborov '85}$$

Monotone Circuits

- Let C be a monotone circuit.
- Assume **AND** and **OR** gates have fan-in 2.
- For a node $x \in C$, let C_x denote the subcircuit at x .

Minterms

- For a monotone function $f : 2^X \rightarrow \{0,1\}$, a set $A \subseteq X$ is a **minterm** of f if

$$f(A) = 1 \text{ and } f(B) = 0 \text{ for all } B \subset A.$$

- $\text{Minterms}(f \vee g) \subseteq \text{Minterms}(f) \cup \text{Minterms}(g)$
- $\text{Minterms}(f \wedge g) \subseteq \{A \cup B : A \in \text{Minterms}(f), B \in \text{Minterms}(g)\}$

Some Observations

Observation 1.

Suppose C computes the **AND** of k variables.

Then there exists a node $x \in C$ such that C_x has a minterm of size $> k/3$ and $\leq 2k/3$.

- Minterms of input nodes have size 1.

Some Observations

Observation 1.

Suppose C computes the **AND** of k variables.

Then there exists a node $x \in C$ such that C_x has a minterm of size $> k/3$ and $\leq 2k/3$.

- If $f \wedge g$ has a minterm of size t , then f or g has a minterm of size $\geq t/2$.
- Every minterm of $f \wedge g$ is a minterm of f or g .

Some Observations

Observation 2.

Suppose C computes the k -THRESHOLD function of n variables.

Then for all $A \subseteq [n]$ of size k , there exists $x \in C$ such that C_x has a minterm within A of size $> k/3$ and $\leq 2k/3$.

- Let's call x a "witness" for A .

Some Observations

Observation 3.

Suppose C computes the k -THRESHOLD function of n variables.

Then there exist $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ minterms of size s .

- *Counting argument!*

Some Observations

Observation 3.

Suppose C computes the k -THRESHOLD function of n variables.

Then there exist $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ minterms of size s .

- For *contra*, assume $\forall x$ and s , C_x has $o(n^s/|C|)$ minterms of size s . Each of these minterms is contained in $O(n^{k-s})$ sets of size k . So only $o(n^k)$ sets A of size k can have "witnesses".

Some Observations

Observation 4.

~~Suppose C computes the k -THRESHOLD function of n variables.~~

Suppose C has $\Omega(n^k)$ minterms of size k .

Then there exist $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ minterms of size s .

Clq-Minterms

- Let F be a monotone function on graphs.
- For $A \subseteq [n]$, let K_A = clique supported on A .
- We say that A is a **clq-minterm** of F if
$$F(K_A) = 1 \text{ and } F(K_B) = 0 \text{ for all } B \subset A.$$
- Example. k -CLIQUE has all $\binom{n}{k}$ possible clq-minterms of size k .

Some Observations

Observation 5.

Suppose C is a monotone circuit on graphs with $\Omega(n^k)$ clq-minterms of size k .

Then there exist $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ clq-minterms of size s .

Monotone Lower Bound

- Fix $p(n) = n^{-2/(k-1) - \varepsilon}$ for sufficiently small $\varepsilon > 0$.
- $p(n)$ is subcritical for the existence of k -cliques, i.e. $G(n,p)$ almost surely has no k -clique.

Monotone Lower Bound

- We will sketch a proof of:

Theorem. Suppose monotone C satisfies:

$$E[C(\text{random } k\text{-clique})] \geq 1 - o(1),$$

$$E[C(G(n,p))] \leq o(1).$$

Then C has size $\Omega(n^{2k/9})$.

- Easy extension to:

Theorem. Monotone circuits which solve k -
CLIQUE on random graphs have size $\Omega(n^{2k/9})$.

Monotone Lower Bound

Assume (for *contra*): $|C| \leq o(n^{2k/9})$
 $E[C(\text{random } k\text{-clique})] \geq 1 - o(1),$
 $E[C(G(n,p))] \leq o(1).$

Monotone Lower Bound

Assume (for *contra*): $|C| \leq o(n^{2k/9})$
 $E[C(\text{random } k\text{-clique})] \geq 1 - o(1),$
 $E[C(G(n,p))] \leq o(1).$

STEP 1. *We may further assume:*

for all $x \in C$ and $A \subseteq [n]$ such that $|A| \leq 2k/3,$

if $E[C_x(G(n,p) \cup K_A)] \geq 1 - n^{-\lg(n)}$

then $C_x(K_A) = 1.$

Intuition for **STEP 1**

- Since C is poly-size, we can replace all nodes $x \in C$ such that

$$\mathbf{E}[C_x(G(n,p))] \geq 1 - n^{-\lg(n)}$$

with the constant function 1 and only increase $\mathbf{E}[C(G(n,p))]$ by a negligible amount.

Intuition for **STEP 1**

- For any $A \subseteq [n]$, we can replace all nodes $x \in C$ such that

$$E[C_x(G(n,p) \cup K_A)] \geq 1 - n^{-\lg(n)}$$

with $C_x \vee \text{Clique-Indicator}_A$ and only increase $E[C(G(n,p) \cup K_A)]$ by negligible amount.

- To get **STEP 1**, we carry out these node substitutions simultaneously for all A of size $\leq 2k/3$ (this is the rough idea).

Monotone Lower Bound

Assume (for *contra*): $|C| \leq o(n^{2k/9})$
 $E[C(\text{random } k\text{-clique})] \geq 1 - o(1),$
 $E[C(G(n,p))] \leq o(1).$

STEP 2.

Notice that C has $\Omega(n^k)$ clq-minterms of size k .

Monotone Lower Bound

STEP 2. There exists $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ clq-minterms of size s .

Because $|C| = O(n^{2k/9})$, C_x has $\Omega(p^{-(s \text{ choose } 2)(1+\epsilon)})$ clq-minterms of size s .

Monotone Lower Bound

STEP 2. There exists $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ clq-minterms of size s .

Because $|C| = O(n^{2k/9})$, C_x has $\Omega(p^{-(s \text{ choose } 2)(1+\epsilon)})$ clq-minterms of size s .

- What if these clq-minterms are disjoint?

Monotone Lower Bound

STEP 2. There exists $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ clq-minterms of size s .

Because $|C| = O(n^{2k/9})$, C_x has $\Omega(p^{-(s \text{ choose } 2)(1+\epsilon)})$ clq-minterms of size s .

- What if these clq-minterms are disjoint?
- Then $\mathbf{E}[C_x(G(n,p))] \geq 1 - \exp(-n^{\Omega(1)}) \geq 1 - n^{-\lg(n)}$.
- So by **STEP 1**, $C_x(\text{empty graph}) = 1$.
- **CONTRADICTION!**

Combinatorial Lemma

Combinatorial Lemma (1). Let H be an s -regular hypergraph of size $m^{s(1+\varepsilon)}$. There exists a set A properly contained in an hyperedge of H such that for $(1/m)$ -biased random set X of vertices,

$\Pr(X \cup A \text{ contains an hyperedge of } H)$

$$\geq 1 - \exp(-\Omega(m^\varepsilon)).$$

Combinatorial Lemma

Combinatorial Lemma (1). Let H be an s -regular hypergraph of size $m^{s(1+\varepsilon)}$. There exists a set A properly contained in an hyperedge of H such that for $(1/m)$ -biased random set X of vertices,

$$\Pr(X \cup A \text{ contains an hyperedge of } H) \geq 1 - \exp(-\Omega(m^\varepsilon)).$$

- Proof is easy if H is a sunflower! Indeed, under the stronger assumption that H has size $m^{s^2(1+\varepsilon)}$, we can find a large enough sunflower.

Combinatorial Lemma

Combinatorial Lemma (1). Let H be an s -regular hypergraph of size $m^{s(1+\epsilon)}$. There exists a set A properly contained in an hyperedge of H such that for $(1/m)$ -biased random set X of vertices,

$$\Pr(X \cup A \text{ contains an hyperedge of } H) \geq 1 - \exp(-\Omega(m^\epsilon)).$$

- To prove the lemma, we find an "approximate" sunflower in H (where petals - core don't overlap too much on average).

Combinatorial Lemma

Combinatorial Lemma (1). Let H be an s -regular hypergraph of size $m^{s(1+\varepsilon)}$. There exists a set A properly contained in an hyperedge of H such that for $(1/m)$ -biased random set X of vertices,

$$\Pr(X \cup A \text{ contains an hyperedge of } H) \geq 1 - \exp(-\Omega(m^\varepsilon)).$$

- CASE 1: Some set B of vertices of size $t \in \{1, \dots, s-1\}$ is contained in $m^{(s-t)(1+\varepsilon)}$ hyperedges. *Use induction!*

Combinatorial Lemma

Combinatorial Lemma (1). Let H be an s -regular hypergraph of size $m^{s(1+\epsilon)}$. There exists a set A properly contained in an hyperedge of H such that for $(1/m)$ -biased random set X of vertices,

$$\Pr(X \cup A \text{ contains an hyperedge of } H) \geq 1 - \exp(-\Omega(m^\epsilon)).$$

- CASE 2: No set $B \subseteq [n]$ of any size $t \in \{1, \dots, s-1\}$ is contained in $m^{(s-t)(1+\epsilon)}$ hyperedges. *Hyperedges don't intersect too much on average!*

Combinatorial Lemma

Combinatorial Lemma (1). Let H be an s -regular hypergraph of size $m^{s(1+\epsilon)}$. There exists a set A properly contained in an hyperedge of H such that for $(1/m)$ -biased random set X of vertices,

$$\Pr(X \cup A \text{ contains an hyperedge of } H) \geq 1 - \exp(-\Omega(m^\epsilon)).$$

- CASE 2: No set $B \subseteq [n]$ of any size $t \in \{1, \dots, s-1\}$ is contained in $m^{(s-t)(1+\epsilon)}$ hyperedges. *JANSON'S INEQUALITY implies lemma holds with $A = \emptyset$.*

Combinatorial Lemma

Combinatorial Lemma (1). Let H be an s -regular hypergraph of size $m^{s(1+\varepsilon)}$. There exists a set A properly contained in an hyperedge of H such that for $(1/m)$ -biased random set X of vertices,

$\Pr(X \cup A$ contains an *hyperedge* of H)

$$\geq 1 - \exp(-\Omega(m^\varepsilon)).$$

Combinatorial Lemma

Combinatorial Lemma (2). Let H be an s -regular hypergraph of size $m^{(s \text{ choose } 2)(1+\epsilon)}$. There exists a set A properly contained in a hyperedge such that for a random graph $G = G(n, 1/m)$

$\Pr(G \cup K_A$ contains a *clique supported on a hyperedge* of $H) \geq 1 - \exp(-\Omega(m^\epsilon))$.

Monotone Lower Bound

STEP 2. There exists $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ clq-minterms of size s .

Because $|C| = O(n^{2k/9})$, C_x has $\Omega(p^{-(s \text{ choose } 2)(1+\epsilon)})$ clq-minterms of size s .

Monotone Lower Bound

STEP 2. There exists $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ clq-minterms of size s .

Because $|C| = O(n^{2k/9})$, C_x has $\Omega(p^{-(s \text{ choose } 2)(1+\epsilon)})$ clq-minterms of size s .

- By the lemma (with $m = 1/p$ and $H = \{\text{clq-minterms of } C_x \text{ of size } s\}$), there exists A properly contained in a hyperedge such that

$$E[C_x(G(n,p) \cup K_A)] \geq 1 - \exp(-\Omega(n^{\epsilon'})) \geq 1 - n^{-\lg(n)}.$$

Monotone Lower Bound

STEP 2. There exists $x \in C$ and $s \in (k/3, 2k/3]$ such that C_x has $\Omega(n^s/|C|)$ clq-minterms of size s .

Because $|C| = O(n^{2k/9})$, C_x has $\Omega(p^{-(s \text{ choose } 2)(1+\epsilon)})$ clq-minterms of size s .

- By the lemma (with $m = 1/p$ and $H = \{\text{clq-minterms of } C_x \text{ of size } s\}$), there exists A properly contained in a hyperedge such that $E[C_x(G(n,p) \cup K_A)] \geq 1 - \exp(-\Omega(n^{\epsilon'})) \geq 1 - n^{-\lg(n)}$.
- By STEP 1, $C_x(K_A) = 1$. *CONTRADICTION!*

Monotone Lower Bound

- We have shown:

Theorem. Suppose monotone C satisfies:

$$E[C(\text{random } k\text{-clique})] \geq 1 - o(1),$$

$$E[C(G(n,p))] \leq o(1).$$

Then C has size $\Omega(n^{2k/9})$.

- Easy extension to:

Theorem. Monotone circuits which solve k -**CLIQUE** on random graphs have size $\Omega(n^{2k/9})$.

Monotone Lower Bound

- *Even stronger:*

Theorem. Suppose monotone C satisfies:

$$E[C(\text{random } k\text{-clique})] \geq \Omega(1),$$

$$E[C(G(n,p))] \leq 1 - \exp(-n^{o(1)}).$$

Then C has size $\Omega(n^{2k/9})$.

From $2k/9$ to $k/4$

- To improve this lower bound to $\Omega(n^{k/4})$, instead of *clq-minterms* (values on K_A), consider **double-clq-minterms**.
- This is analogous to what happens with the AC^0 lower bound.

AC⁰ Lower Bound

- **AC⁰** = {polynomial-size fan-in 2 circuits with a constant number of alternations}

Equivalently to: {polynomial-size, constant depth, unbounded fan-in circuits}

AC⁰ Lower Bound

- Suppose C is an AC⁰ circuit which solves k -CLIQUE *exactly*. We will show $|C| \geq \Omega(n^{2k/9})$.
- Let $G = G(n,p)$, same subcritical $p(n)$.
- Let $A =$ uniform random k -element subset of $[n]$.
- For $x \in C$, define $S_x \subseteq A$ by
$$S_x = \{a \in A : \exists B \subseteq A - \{a\}, C_x(G \cup K_B) \neq C_x(G \cup K_{B \cup \{a\}})\}$$
- Almost surely, $S_{\text{out}} = A$.

AC⁰ Lower Bound

Observation. If $S_{\text{out}} = A$, there exists $x \in C$ such that $k/3 < |S_x| \leq 2k/3$.

- $|S_x| \leq 2$ for input nodes x
- $S_{\neg x} = S_x$
- $S_{x \wedge y}, S_{x \vee y} \subseteq S_x \cup S_y$ for all siblings x, y

AC⁰ Lower Bound

Combinatorial Lemma. For all $x \in C$ (using only the fact that C_x is an AC⁰ circuit) and $t \in \{0, \dots, k\}$

$$\Pr(|S_x| = t) \leq n^{-t+o(1)} p^{-\binom{t}{2}}.$$

For $t \in (k/3, 2k/3]$,

$$\Pr(|S_x| = t) \leq n^{-2k/9 - \Omega(1)}.$$

- Proof uses **Hastad's Switching Lemma** (on the constant-depth version of C_x).

AC⁰ Lower Bound

Combinatorial Lemma. For $t \in (k/3, 2k/3]$,

$$\Pr(|S_x| = t) \leq n^{-2k/9 - \Omega(1)}.$$

- If we assume $|C| = O(n^{2k/9})$: by union bound, almost surely $|S_x| \notin (k/3, 2k/3]$ for all $x \in C$.

\Rightarrow almost surely $S_{\text{out}} \neq A$

CONTRADICTION!

AC⁰ Lower Bound

- This argument proves:

Theorem. AC⁰ circuits which solve k-CLIQUE *exactly* have size $\Omega(n^{2k/9})$.

- Easy extension to:

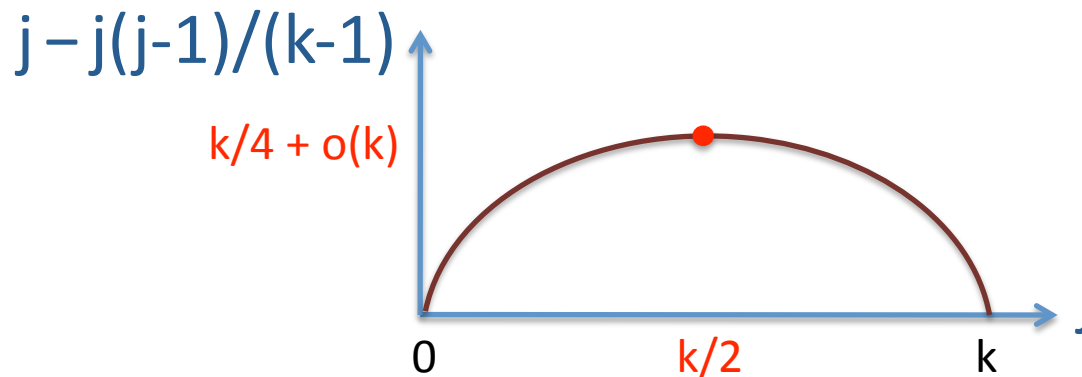
Theorem. AC⁰ circuits which solves k-CLIQUE on $G(n,q)$ at a single threshold $q(n) = \Theta(n^{-2/(k-1)})$ have size $\Omega(n^{2k/9})$.

- Can improve to $\Omega(n^{k/4})$.

Monotone AC⁰ Upper Bound

- Consider a threshold function $q(n) = \Theta(n^{-2/(k-1)})$.
- Expected # of j -cliques in $G(n,q)$ is

$$\binom{n}{j} q^{\binom{j}{2}} = \Theta(n^{j - j(j-1)/(k-1)}).$$



- $G(n,q)$ has only $n^{k/4 + o(k)}$ cliques in total.

Monotone AC^0 Upper Bound

- Amano's idea: Construct a circuit which keeps track of all j -cliques for $j = 1, 2, \dots, k$ in k layers. With clever book-keeping only need size $n^{k/4 + o(k)}$.
- Observation: Amano's AC^0 circuits can be made monotone (with a small extra trick).
- Easy extension to a circuit which solves k -CLIQUE on random graphs.

Thank you!