A Simple Lower Bound for Monotone Clique Using a Communication Game

Mikael Goldmann
Johan Håstad

Royal Institute of Technology
Stockholm, SWEDEN

Abstract

We give a simple proof that a monotone circuit for the k-clique problem in an n-vertex graph requires depth $\Omega\left(\sqrt{k}\right)$, when $k \leq \left(\sqrt[3]{n/2}\right)^2$. The proof is based on an equivalence between the depth of a Boolean circuit for a function and the number of rounds required to solve a related communication problem. This equivalence was shown by Karchmer and Wigderson.

Key words. computational complexity, theory of computation, circuit complexity, formula complexity, monotone circuits

1 Introduction

In complexity theory we are interested in the amount of resources that are required to compute a certain function. For a Turing machine the resources would typically be the number of transitions (time) and the number of tape squares used (space). For a Boolean circuit we would be interested in the number of gates (its size) and the maximal distance from an input to the output gate (its depth). These measures correspond to work and parallel time respectively.

Since it has been difficult to show non-trivial lower bounds for general Boolean circuits, one has chosen to study various restricted circuit models. A number of lower bounds have been shown for the size of Boolean circuits of constant depth [Ajt83, FSS84, Hås86, Raz87, Smo87, Yao85].

Another case studied is monotone circuits, i.e. we only allow $\wedge$-gates and $\vee$-gates, but no $\neg$-gates . Several interesting results for monotone circuits can be found in [And85, Raz85, AB87, KW88, RW89, RW90].

In what follows we will be looking at monotone circuits where each gate has fanin at most 2. In [KW88] Karchmer and Wigderson show that a monotone circuit for st-connectivity in an n-vertex graph has depth $\Theta\left(\log^2 n\right)$. As part of their proof they show that computing a function f with a Boolean circuit is connected to the following communication game:
We have two players, player 1 and player 2, and they are each given an n-bit string, x and y respectively, where $x \in f^{-1}(1)$ and

$y \in f^{-1}(0)$. The game proceeds in rounds. In each round player 1 can send player 2 a one bit message or vice versa. Their task is to find an index i so that $x_i \neq y_i$.

There is also a monotone version of the game where i should satisfy $x_i = 1$ and $y_i = 0$. Note that for a monotone f there is always such an i.

Karchmer and Wigderson [KW88] showed the following equivalence between circuit depth and the number of rounds needed in the game:

Theorem 1 (Karchmer and Wigderson) *For a function f and an input length n, the number of rounds needed in the communication game equals the required depth of a circuit computing f.*

This is true both in the monotone and the general case.

Our main result is a simple proof that a circuit for the k-clique problem in an n-vertex graph requires depth $\Omega\left(\sqrt{k}\right)$ when $k \leq \left(\sqrt[3]{n/2}\right)^2$. We use the above equivalence between circuit depth and communication complexity.

Raz and Wigderson have recently showed by a much more complicated method that the clique problem requires depth $\Omega(n)$ [RW90].

2 Notation

As mentioned in the introduction, we will be concerned with clique problem.

Definition 1 *We call the set of graphs on n vertices containing a k-clique $CLIQUE(n, k)$.*

We need to express subset size in the following way:

Definition 2 *For an arbitrary set B and $A \subseteq B$ we define*

$$\mu(A) = \frac{|A|}{|B|}.$$

Remark 1 *This definition is useful when we want to describe how much is known about some element x. Suppose that, but we know that $x \in A \subseteq B$. Suppose further that we know the structure of B, but that the structure of A is unknown, or very complicated. Then the amount of information we have about x is given by the structure of B and $\mu(A)$. The smaller $\mu(A)$ is, the more we know about x.*

For notational convenience we introduce the following shorthand:

Definition 3 *For an arbitrary set B and an integer k*

$$\binom{B}{k} = \{A \subseteq B \mid |A| = k\}.$$

3 Proof outline

We will show a lower bound on the depth of a circuit for $CLIQUE(n, k)$. The idea behind the proof is quite simple. By [KW88], what we need to do is to show that a protocol for the related monotone communication game must use many rounds.

The communication version of the clique problem would be as follows: Player 1 is given a graph, G_1 containing a k-clique and player 2 is given a graph, G_2, that does not have a k-clique. Their task is to find an edge that is present in G_1 but not in G_2.

We will modify this by only looking at certain graphs. We then bound the number of rounds needed for this restricted set of inputs. In particular, player 1, the clique player, receives a set q of k vertices, which corresponds to the graph that has a k-clique on the vertices in q, and no edges other than those in

the clique. Player 2, the color player, receives a $k-1$ coloring, c, of the vertices, corresponding to a complete $k-1$-partite graph. The task of finding the "faulty" edge in the clique now translates into finding two vertices $u, v \in q$ that have the same color. We call $\{u, v\}$ a monochromatic edge.

In a round the players are allowed to send one bit each rather than only one of them sending a bit. Since we are interested in the number of rounds rather than the number of bits transferred, this can only make life easier for them. Each bit that the clique/color player sends decreases the set of possible cliques/colorings. The adversary strategy that we will use is to makes sure that an edge that appears in some remaining clique is bichromatic in most remaining colorings, and the remaining colorings are $1-1$ on the vertices that appear in all remaining cliques.

When a vertex appears in many of the remaining cliques we "fix" it i.e. we restrict the set of remaining cliques to those that contain this vertex. We then restrict the remaining colorings to those that are $1-1$ on the "fixed" vertices.

If an edge $\{u, v\}$ is monochromatic in many of the remaining colorings, we restrict the set of remaining colorings to those colorings c that have $c(u) = c(v)$. Since $\{u, v\}$ was monochromatic, u and v cannot both be fixed vertices since all remaining colorings are $1-1$ on the fixed vertices. Assume that u is not fixed. We now restrict the cliques to those that do not contain u, so an edge that appears in some remaining clique is not monochromatic in many of the remaining colorings.

We continue this process for $\sqrt{k}/4$ rounds. From the remaining cliques and colorings we choose q and c. Since any edge, $\{u, v\}$, in q is not monochromatic for some of the possible choices for c, the clique player cannot know of an edge in q that must be monochromatic in c. Thus a protocol requires more than $\sqrt{k}/4$ rounds.

In section 4 we formally describe the adversary strategy that, given a protocol, finds a clique-coloring pair, (q, c), that requires many rounds. In section 5 we will prove that the pair (q, c) does indeed require many rounds.

4 An adversary strategy for a protocol

In the next section we give a lower bound for the depth of a monotone circuit for recognizing $CLIQUE(n,\ k)$. In this section we show how the pair of inputs that require the players to communicate for "many" rounds is chosen.

In our communication game the clique player is given a set q of k vertices which correspond to a clique. The color player is given a $k-1$-partition of the graph in the shape of a $k-1$ coloring c of the graph. Their task is to agree on a monochromatic edge , i.e. an edge $\{u, v\} \subset q$ such that $c(u) = c(v)$.

As the protocol proceeds we will look at the following sets:

$V = \{1, 2, \ldots n\}$ is the set of vertices in a graph,

Q_t is the set of cliques that remain after round t,

C_t is the set of colorings remaining after round t,

$M_t \subseteq V$ is a set of vertices that occur in every clique after round t,

$m_t = |M_t|$,

$L_t \subseteq V$ is a set of vertices that occur in no clique after round t,

$l_t = |L_t|$.

At the beginning we have

$$\begin{aligned} Q_0 &= \binom{V}{k}, \\ C_0 &= \{c : V \to [k-1]\}, \\ M_0 &= \phi, \\ L_0 &= \phi. \end{aligned}$$

We now describe how to handle the protocol. Recalling Remark 1, we consider Q and C to be subsets of the following sets:

$$\begin{aligned} Q &\subseteq \left\{ q \in \binom{V}{k} \mid M \subseteq q \right\}, \\ C &\subseteq \{c : V \setminus L \to [k-1]\}. \end{aligned}$$

Thus m_t together with $\mu(Q_t)$ tells us how much the color player knows about the clique players k-set after round t.

Similarly, l_t and $\mu(C_t)$ measure what the clique player knows about the color players coloring.

The protocol is handled in the following fashion. In each round we allow both players to send one bit each instead of just one of them sending a bit.

At round t the following happens:

1. The clique player sends bit b_1.

   $Q^0 \leftarrow \{q \in Q_{t-1} | b_1 = 0\}$

   $Q^1 \leftarrow \{q \in Q_{t-1} | b_1 = 1\}$

   $Q \leftarrow$ the larger of Q^0 and Q^1

   $M \leftarrow M_{t-1}$

2. Find $v \in V \setminus M$ so that

   $\mu(\{q \in Q \mid v \in q\}) \geq 2(k-m)\mu(Q)/(n-m)$

   i.e. at least twice as often as the average vertex.

   If such v exists

   $M \leftarrow M \cup \{v\}$

   $Q \leftarrow \{q \in Q \mid v \in q\}$

   Remark 2 *Thus, $\mu(Q)$ increases by at least a factor two since Q is now a subset of a smaller set.*

   We repeat this step until no such vertex v can be found.

3. $Q'_t \leftarrow Q$

   $C'_t \leftarrow \{c \in C_{t-1} \mid c \text{ is } 1-1 \text{ on } M\}$

   $M_t \leftarrow M$.

4. The color player sends bit b_2.

   $C^0 \leftarrow \{c \in C'_t | b_2 = 0\}$

   $C^1 \leftarrow \{c \in C'_t | b_2 = 1\}$

   $C \leftarrow$ the larger of C^0 and C^1

   $L \leftarrow L_{t-1}$

5. Find $u, v \in V \setminus L$ where $u \neq v$

   such that $\mu(\{c \in C \mid c(u) = c(v)\}) \geq 2\mu(C)/(k-1)$

   i.e. at least twice as often as average.

   If such u and v are found

   Since all $c \in C$ are $1-1$ on M_t we can without loss of generality assume $u \notin M_t$.

   $L \leftarrow L \cup \{u\}$

   $C \leftarrow \{c \in C \mid c(u) = c(v)\}$

   Remark 3 *When a c is restricted in this way on L it can be seen as a function $c : V \setminus L \to [k-1]$. Thus, $\mu(C)$ increases by at least a factor two.*

   We repeat this step until no such vertices u and v can be found.

6. $Q_t \leftarrow \{q \in Q \mid L \cap q = \phi\}$

   $C_t \leftarrow C$

   $L_t \leftarrow L$

5 The lower bound

We are now ready to prove a lower bound for the depth of a monotone circuit for *CLIQUE*$(n,\ k)$. If we handle the protocol as described the following is true.

Proposition 2 *Let t satisfy the following inequalities:*

$$t \leq \frac{\sqrt{k}}{4}, \quad (1)$$

$$t \leq \frac{n}{8k}. \quad (2)$$

Then the following inequalities hold:

$$\mu(Q_t) \geq 2^{m_t - 2t}, \quad (3)$$

$$\mu(C_t) \geq 2^{l_t - 2t}. \quad (4)$$

Assuming that this is correct, we get a lower bound on circuit depth by

Theorem 3 *For $k \leq \left(\sqrt[3]{n/2}\right)^2$ recognizing k-cliques in a graph with n vertices requires depth $\Omega\left(\sqrt{k}\right)$.*

Proof: For such values of k (2) will always be satisfied as long as (1) is. Run the protocol $T = \sqrt{k}/4$ rounds. We obtain Q_T, C_T, M_T and L_T. Give the players some input pair $(q, c) \in Q_T \times C_T$. We have $q \cap L_T = \phi$.

If T rounds were sufficient the clique player would now know an edge $\{x, y\} \subseteq q$ that is monochromatic edge in all $c \in C_T$. This implies $x \in L_T \vee y \in L_T$, i.e. $q \cap L_T \neq \phi$, and we have a contradiction.

The theorem now follows by the equivalence between circuit depth and communication complexity stated in Theorem 1. ∎

Remark 4 *This shows that a monotone circuit for CLIQUE$(n,\ (n/2)^{\frac{2}{3}})$ must have depth $\Omega\left(\sqrt[3]{n}\right)$. Alon and Boppana [AB87] have proved a lower bound for the size of a monotone circuit for CLIQUE$(n,\ k)$ that implies a $\Omega(\sqrt[3]{n/\log n})$ lower bound on the depth of such a circuit. Apart from the minor improvement, we feel that our proof is simpler.*

We will prove Proposition 2 by induction over t, the number of rounds used. Before we do so we need relationships between $\mu(C'_t)$ and $\mu(C_{t-1})$, and between $\mu(Q_t)$ and $\mu(Q'_t)$.

Lemma 4 *After step 3 we have*

$$\mu(C'_t) \geq \left(1 - \frac{(m_t+1)^2}{k-1}\right)\mu(C_{t-1}).$$

Proof: Let us use the following shorthand:

$$C_t^{(u,v)} = \{c \in C_t \mid c(u) = c(v)\}.$$

We observe that we always have for $t > 0$, different $u, v \in V \setminus L_{t-1}$

$$\mu\left(C_{t-1}^{(u,v)}\right) < \frac{2\mu(C_{t-1})}{k-1}.$$

This follows by our choice of C_0 and from step 5 in round $t-1$.

$$\begin{aligned}
\mu(C'_t) &= \mu\left(\{c \in C_{t-1} \mid c \text{ 1-1 on } M_t\}\right) \\
&= \mu(C_{t-1}) - \mu\left(\bigcup_{\substack{u,v \in M_t \\ u \neq v}} C_{t-1}^{(u,v)}\right) \\
&\geq \mu(C_{t-1}) - \sum_{\substack{u,v \in M_t \\ u \neq v}} \mu\left(C_{t-1}^{(u,v)}\right) \\
&\geq \left(1 - \binom{m_t}{2}\frac{2}{k-1}\right)\mu(C_{t-1}) \\
&> \left(1 - \frac{(m_t+1)^2}{k-1}\right)\mu(C_{t-1}).
\end{aligned}$$

∎

Lemma 5 *After step 6 we have*

$$\mu(Q_t) \geq \left(1 - \frac{2kl_t}{n}\right)\mu(Q'_t).$$

Proof: After step 2 we have for all $v \in V \setminus M_t$

$$\mu\left(\{q \in Q'_t \mid v \in q\}\right) < \frac{2(k-m_t)\mu(Q'_t)}{n-m_t}$$

Since $L_t \subseteq V \setminus M_t$ we have the same bound for $v \in L_t$.

$$\begin{aligned}
\mu(Q_t) &= \mu(Q'_t) - \mu\left(\bigcup_{v \in L_t} \{q \in Q'_t \mid v \in q\}\right) \\
&\geq \left(1 - \frac{2(k-m_t)l_t}{n-m_t}\right)\mu(Q'_t) \\
&\geq \left(1 - \frac{2kl_t}{n}\right)\mu(Q'_t).
\end{aligned}$$

■

Proof of Proposition 2: We wish to show that equations (3) and (4) hold for all t that satisfy (1) and (2).

Since we have $\mu(Q_0) = \mu(Col_0) = 1$ and $m_0 = l_0 = 0$ the proposition is true for $t = 0$.

Now assume that the proposition holds for the first $t-1$ rounds. First we use the induction hypothesis to give lower bounds for $\mu(Q'_t)$ and $\mu(C'_t)$. By Remark 2 we get:

$$\begin{aligned}
\mu(Q'_t) &\geq \frac{1}{2}2^{m_t - m_{t-1}}\mu(Q_{t-1}) \\
\text{by induction} &\geq 2^{m_t - 2t + 1}. \qquad (5)
\end{aligned}$$

Since $\mu(Q'_t) \leq 1$ we have that $m_t \leq 2t-1$. When we apply this to Lemma 4 we obtain:

$$\begin{aligned}
\mu(C'_t) &\geq \left(1 - \frac{(m_t+1)^2}{k-1}\right)\mu(C_{t-1}) \\
&\geq \left(1 - \frac{4t^2}{k-1}\right)\mu(C_{t-1}) \\
\text{using (1)} &\geq \left(1 - \frac{k}{4(k-1)}\right)\mu(C_{t-1}) \\
&\geq \frac{1}{2}\mu(C_{t-1}) \\
\text{by induction} &\geq 2^{l_{t-1} - 2t + 1}. \qquad (6)
\end{aligned}$$

We now go on to the second part of round t, where the color player sends one bit. The bounds established for $\mu(Q'_t)$ and $\mu(C'_t)$ allow us to finish the proof. We get by Remark 3:

$$\begin{aligned}
\mu(C_t) &\geq \frac{1}{2}2^{l_t - l_{t-1}}\mu(C'_t) \\
\text{using (6)} &\geq \frac{1}{2}2^{l_t - l_{t-1}}2^{l_{t-1} - 2t + 1} \\
&\geq 2^{l_t - 2t}.
\end{aligned}$$

This shows that (4) holds. Since $\mu(C_t) \leq 1$ we know that $l_t \leq 2t$. We apply this to Lemma 5:

$$\begin{aligned}
\mu(Q_t) &\geq \left(1 - \frac{2kl_t}{n}\right)\mu(Q'_t) \\
&\geq \left(1 - \frac{4kt}{n}\right)\mu(Q'_t) \\
\text{using (2)} &\geq \frac{1}{2}\mu(Q'_t) \\
\text{using (5)} &\geq \frac{1}{2}2^{m_t - 2t + 1} \\
&\geq 2^{m_t - 2t}.
\end{aligned}$$

This completes the proof of the proposition. ■

6 Acknowledgment

We are grateful to Mauricio Karchmer for his comments and suggestions on a draft of this article. We also thank Noga Alon for helpful discussions.

References

[AB87] N. Alon and R. B. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7:1–22, 1987.

[Ajt83] M. Ajtai. $\sum_1^1$-formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.

[And85] A. E. Andreev. On a method for obtaining lower bounds for the complexity of individual monotone functions. *Dokl. Ak. Nauk. SSSR 282*, pages 1033–1037, 1985. English translation in *Sov. Math. Dokl.*, 31:530–534, 1985.

[FSS84] M. Furst, J. Saxe, and M. Sipser. Parity, circuits, and the polynomial time hierarchy. *Math. System Theory*, 17:13–27, 1984.

[Hås86] J. Håstad. *Computational Limitations of Small-Depth Circuits*. MIT PRESS, 1986.

[KW88] M. Karchmer and A. Wigderson. Monotone circuits for connectivity require super-logarithmic depth. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, 1988.

[Raz85] A. A. Razborov. Lower bounds on monotone network complexity of the logical permanent. *Matem. Zam.*, 37(6):887–900, 1985. English translation in *Math. Notes of the Academy of Sciences of the USSR*, 37:485–493, 1985.

[Raz87] A. A. Razborov. Lower bounds on the size of bounded-depth networks over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):598–607, 1987. English translation in 41:4, pages 333-338.

[RW89] R. Raz and A. Wigderson. Probabilistic communication complexity of boolean relations. In *Proceedings of the 30th Annual IEEE Symposium on Foundation of computer science*, pages 562–567, 1989.

[RW90] R. Raz and A. Wigderson. Monotone circuits for matching require linear depth. *22nd annual ACM Symposium on Theory of Computing*, pages 287–292, 1990.

[Smo87] R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. *Proceedings of 19th Annual ACM Symposium on Theory of Computing*, pages 77–82, 1987.

[Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. *Proceedings 26th Annual IEEE Symposium on Foundations of Computer Science*, pages 1–10, 1985.