Mystery of Negations

S Jukna

CS6840 presentation by
Amit Roy

Department of Computer Science & Engineering
Indian Institute of Technology - Madras

Negations

Lower Bounds and Negations

No non-linear lower bounds are known for circuits using *NOT* gates and the effect of such gates on a circuit size remains to a large extent a mystery.

Minimum Negations

What is the minimum number of NOT gates required in a circuit computing f?

Minimum Negations

What is the minimum number of *NOT* gates required in a circuit computing f?

$\Rightarrow \lceil \log(n+1) \rceil$ *NEGATIONS*

Theorem [Markov 1957]

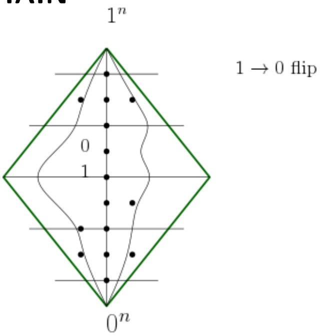
For every function f , the minimum number of NOT gates contained in a circuit computing f is precisely
$M(f) := \lceil log(d(f)+1) \rceil$

PRELIMINARIES

MONOTONOCITY

- $x, y \in \{0,1\}^n$ we say $x \leq y$ if $\forall i \; x_i \leq y_i$
- A function f is monotone if $x \leq y$ implies $f(x) \leq f(y)$

CHAIN



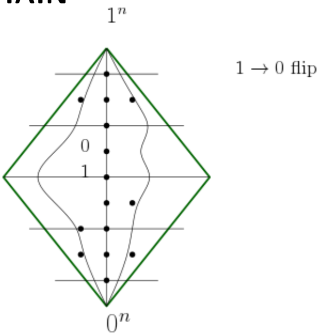
- A Chain is an increasing sequence $y^1 < y^2 \ldots < y^k$ in the boolean hypercube.

Preliminaries

MONOTONOCITY

- $x, y \in \{0,1\}^n$ we say $x \leq y$ if $\forall i \; x_i \leq y_i$
- A function f is monotone if $x \leq y$ implies $f(x) \leq f(y)$

CHAIN



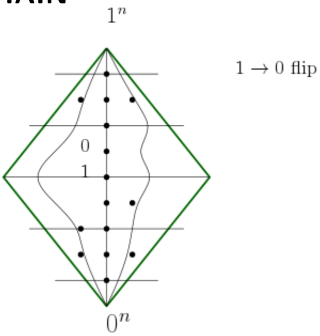
- A Chain is an increasing sequence $y^1 < y^2 \ldots < y^k$ in the boolean hypercube.
- *Decrease* $d_Y(f)$ on a chain Y is no of indices i s.t. $f(y^i) > f(y^{i+1})$.

Preliminaries

MONOTONOCITY

- $x, y \in \{0,1\}^n$ we say $x \leq y$ if $\forall i\ x_i \leq y_i$
- A function f is monotone if $x \leq y$ implies $f(x) \leq f(y)$

CHAIN



- A Chain is an increasing sequence $y^1 < y^2 \ldots < y^k$ in the boolean hypercube.
- *Decrease* $d_Y(f)$ on a chain Y is no of indices i s.t. $f(y^i) > f(y^{i+1})$.
- *Decrease* $d(f)$ of f is maximum of $d_Y(f)$ over all chains Y

Theorem[Markov 1957]

For every function f , the minimum number of NOT gates contained in a circuit computing f is precisely
$M(f) := \lceil log(d(f) + 1) \rceil$

Proof

Lower Bound

Let $neg(f)$ be the number of negation gates in the circuit computing f. We will first show that $neg(f) \geq \lceil \log(d(f)+1) \rceil$

Proof

Lower Bound

Let $neg(f)$ be the number of negation gates in the circuit computing f. We will first show that $neg(f) \geq \lceil \log(d(f)+1) \rceil$

- Fix a chain $Y = \{y^1 < y^2 < \dots y^k\}$ for which $d_Y(f) = d(f)$
- $I(f) = \{i \mid f(y^i) > f(y^{i+1})\}$

Proof

Lower Bound

Let $neg(f)$ be the number of negation gates in the circuit computing f. We will first show that $neg(f) \geq \lceil \log(d(f)+1) \rceil$

- Fix a chain $Y = \{y^1 < y^2 < \dots y^k\}$ for which $d_Y(f) = d(f)$
- $I(f) = \{i \mid f(y^i) > f(y^{i+1})\}$
  Clearly $|I(f)| = d(f)$
- Let g be fn computed on output of first negation

Proof

Lower Bound

Let $neg(f)$ be the number of negation gates in the circuit computing f. We will first show that $neg(f) \geq \lceil \log(d(f)+1) \rceil$

- Fix a chain $Y = \{y^1 < y^2 < \dots y^k\}$ for which $d_Y(f) = d(f)$
- $I(f) = \{i \mid f(y^i) > f(y^{i+1})\}$
  Clearly $|I(f)| = d(f)$
- Let g be fn computed on output of first negation
- $d_Y(g) \leq 1$

Proof

- If $d_Y(g) = 0$ the $g \equiv 0$ or $g \equiv 1$. Replace by constant 0 or 1.
- Otherwise, $\exists$ an i_0 s.t. $g(y^i) = 1$ for all $i \in I_1 = \{1, \ldots i_0\}$ and $g(y_i) = 0$ for all $i \in I_0 = \{i_0 + 1, \ldots, k\}$
- Depending $|I_1 \cap I(f)| \geq |I(f)|/2$ or not, replace the gate g by constant 0 or 1
- In both cases , the new fn f_1 has one fewer *NOT* gate and $d_Y(f_1) \geq |I(f)|/2$
- Do this for $r \leq \lceil \log(|I(f)| + 1) \rceil - 1$ steps and we will have contradiction.

Proof

Upper Bound

Let $f : \{0,1\}^n \rightarrow \{0,1\}$ and $neg(f)$ be the number of negation gates in the circuit computing f.

To show

$$neg(f) \leq \lceil \log (d(f) + 1) \rceil$$

Proof by Induction on

$$M(f) := \lceil \log (d(f) + 1) \rceil$$

Base Case

$M(f) = 0 \Rightarrow d(f) = 0,$ so f is monotone and $neg(f) = 0$

Induction Step

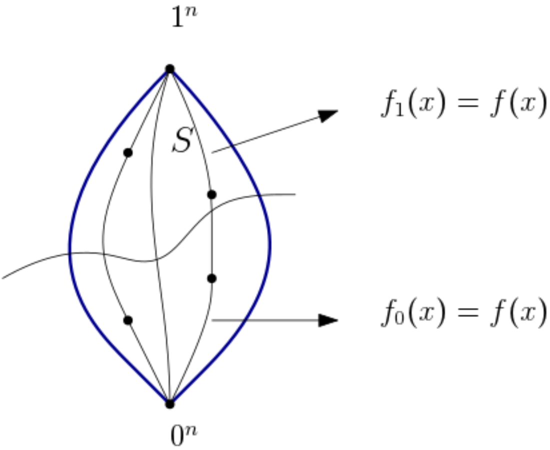
$neg(f') \leq M(f')$ for all boolean functions f' s.t. $M(f') \leq M(f) - 1$

Let S be set of all vectors $x \in \{0,1\}^n$ s.t. *for every chain* Y *starting with* x we have

$$d_Y(f) < 2^{M(f)-1} \tag{1}$$

We can also show that *every chain* Y *ending in a vector outside the set* S we have

$$d_Y(f) < 2^{M(f)-1} \tag{2}$$


1^n
S
$f_1(x) = f(x)$
$f_0(x) = f(x)$
0^n

Consider these 2 functions f_0 and f_1 as follows :-

$$f_1(x) = \begin{cases} f(x) & , if \ \ x \in S \\ 0 & , if \ \ x \notin S \end{cases}$$

and

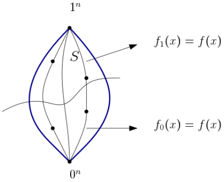
$$f_0(x) = \begin{cases} 1 & , if \ \ x \in S \\ f(x) & , if \ \ x \notin S \end{cases}$$

From (1) *and* (2) we have ,

$$d(f_1) \leq 2^{M(f)-1} - 1$$

$$d(f_0) \leq 2^{M(f)-1} - 1$$

f_1 : Upper part , all $f(x)$ and below the line all $0's$
f_0 : Lower part , all $f(x)$ and upper part has all $1's$



Hence by Induction Hypothesis,

$$M(f_1) = \lceil \log \left(d(f_1) + 1 \right) \rceil \leq M(f) - 1$$

$$M(f_0) = \lceil \log \left(d(f_0) + 1 \right) \rceil \leq M(f) - 1$$

Therefore remains to show

$$neg(f) \leq 1 + max\{neg(f_0), neg(f_1)\} \leq M(f)$$

Connector Function

Let $\mu(y, y', x)$ be a boolean function in $n+2$ variables $y, y', x_1 \dots x_n$. We say μ is a connector of two boolean functions $f_0(x)$ and $f_1(x)$ if for $i = 0, 1$

$$\mu(i, \neg i, x) = f_i(x)$$

that is, $\mu(0, 1, x) = f_0(x)$ and $\mu(1, 0, x) = f_1(x)$

Claim

Every pair of functions $f_0(x)$ and $f_1(x)$ has a connector μ such that $neg(\mu) \leq max\{neg(f_0), neg(f_1)\}$

Proof: Assume for now . . .

Let $s(x)$ be the characteristic function of S i.e.

$$s(x) = \begin{cases} 1 & , x \in S \\ 0 & , x \notin S \end{cases}$$

Note: $s(x)$ is monotone !!

Let μ be a connector of f_0 and f_1. Then

$$f(x) = \mu(s(x), \neg s(x), x)$$

$$f(x) = \mu(s(x), \neg s(x), x)$$

$$neg(f) \leq 1 + neg(\mu) = 1 + max\{neg(f_0), neg(f_1)\}$$
$$\Rightarrow neg(f) \leq M(f)$$

□

Why ??

$$x \in S \Rightarrow s(x) = 1$$

$$\Rightarrow \mu(1, 0, x) = f_1(x) = f(x)$$

and

$$x \notin S \Rightarrow s(x) = 0$$

$$\Rightarrow \mu(0, 1, x) = f_0(x) = f(x)$$

Hence ,

$$f(x) = \mu(s(x), \neg s(x), x)$$

Proof of Claim

Every pair of functions $f_0(x)$ and $f_1(x)$ has a connector μ such that $neg(\mu) \leq max\{neg(f_0), neg(f_1)\}$

Proof: Proof by Induction on $r = max\{neg(f_0), neg(f_1)\}$

Proof of Claim

Every pair of functions $f_0(x)$ and $f_1(x)$ has a connector μ such that $neg(\mu) \leq max\{neg(f_0), neg(f_1)\}$

Proof: Proof by Induction on $r = max\{neg(f_0), neg(f_1)\}$

- Base Case $r = 0 \Rightarrow f_i$ are monotone and hence
  $\mu(y, y', x) = (y \wedge f_1) \vee (y' \wedge f_0)$ **[0 negations !!!]**

Proof of Claim

Every pair of functions $f_0(x)$ and $f_1(x)$ has a connector μ such that $neg(\mu) \leq max\{neg(f_0), neg(f_1)\}$

Proof: Proof by Induction on $r = max\{neg(f_0), neg(f_1)\}$

- Base Case $r = 0 \Rightarrow f_i$ are monotone and hence
  $\mu(y, y', x) = (y \wedge f_1) \vee (y' \wedge f_0)$ **[0 negations !!!]**
- Induction Step
  $C_i(x)$ be the circuit with $neg(f_i)$ negations and computing $f_i(x)$
  - Replace first NOT gate in C_i by a var z, obtaining new circuit $C_i'(z, x)$ on $n + 1$ variables and computing $f_i'(z, x)$
  - $C_i'(z, x)$ has one NOT gate fewer
  - $neg(f_i') \leq r - 1$

Proof Contd

- Define $h_i(x)$ as monotone function computed before the first *NOT* gate. We have

$$f_i(x) = f_i'(\neg h_i(x), x)$$

- By Induction Hypothesis , $\exists$ connector boolean function $\mu'(y, y', z, x)$ (connector for pair f_0', f_1') s.t. $neg(\mu') \leq max\{neg(f_0'), neg(f_1')\} \leq r - 1$
- Replace var z with the function $Z(y, y', x) = \neg((y \wedge h_1(x)) \vee (y' \wedge h_0(x)))$ to obtain a new connector boolean function $\mu(y, y', x)$
  - $Z(0, 1, x) = \neg h_0(x)$ and $Z(1, 0, x) = \neg h_1(x)$
- $\mu(y, y', x)$ is a connector for f_0, f_1

Proof Contd

- Note that h_0 and h_1 are monotone
- $neg(\mu) \leq 1 + neg(\mu') \leq r$ [As Required]

  Remember $r = max\{neg(f_0), neg(f_1)\}$

Hence $neg(\mu) \leq max\{neg(f_0), neg(f_1)\}$ □

Theorem[Fischer's 1974]

If a function on n variables can be computed by a circuit of size of t, then it can be computed by a circuit of size at most $2t + \mathcal{O}(n^2 \log^2 n)$ using atmost $M(n) := \lceil \log(n+1) \rceil$ *NOT* gates

Proof:

Theorem[Fischer's 1974]

If a function on n variables can be computed by a circuit of size of t, then it can be computed by a circuit of size at most $2t + \mathcal{O}(n^2 \log^2 n)$ using atmost $M(n) := \lceil \log(n+1) \rceil$ *NOT* gates

Proof:

- Push all the negations to the inputs (with care !!) [Size= 2t]
- $NEG(x_1, x_2, \ldots x_n) = (\neg x_1, \ldots \neg x_n)$ using just $M(n)$ negations and size $\mathcal{O}(n^2 \log^2 n)$
- $$\neg x_i = \bigwedge_{k=0}^{n} (\neg T_k^n(x) \vee T_{k,i}^n(x))$$

Proof Contd

- T_k^n is Threshold function and $T_{k,i}^n(x_1, \dots x_n) := T_k^{n-1}(x_1, \dots x_{i-1}, x_{i+1}, \dots x_n)$
- Remains to compute $\neg T(x) := (\neg T_1^n(x), \neg T_2^n(x), \dots \neg T_n^n(x))$ using atmost $\lceil \log(n+1) \rceil$ negations
- Hint:- $T(x) := (T_1^n(x), T_2^n(x), \dots T_n^n(x))$ can be computed by monotone circuits

Rest left as an exercise!

Motivation from Markov's

To what extend can we decrease the number of *NOT* gates in a circuit without a substantial increase in its size?

Motivation from Markov's

To what extend can we decrease the number of *NOT* gates in a circuit without a substantial increase in its size?

Suppose a function f in n variables can be computed by a circuit of size polynomial in n , but for every circuit with $M(f)$ negations computing f requires superpolynomial size $(n^{\log n})$. What is then minimal number $R(f)$ of negations sufficient to compute f in polynomial size?

$R(f)$: Minimum no of negations sufficient to compute f in polynomial size

Fischer's result only implies that

$$M(f) - - - - - - R(f) - - - - - - \lceil \log(n+1) \rceil$$

where, $M(f) = \lceil \log(d(f)+1) \rceil$

Improvement to Fischer's Simulation

- Berkowitz and Valiant have shown that for *slice* functions, negations are almost useless i.e. can't lead to any superpolynomial savings

Will there be any superpolynomial savings at all using NOT gates?

Will there be any superpolynomial savings at all using NOT gates?

YES !!

Will there be any superpolynomial savings at all using NOT gates?

YES !!

Razborov resolved this (long standing) problem.

1. There exist explicit monotone boolean function f s.t. $R(f) > 0$. The function is characteristic function of bipartite graphs containing a perfect matching.

Will there be any superpolynomial savings at all using NOT gates?

YES !!

Razborov resolved this (long standing) problem.

1. There exist explicit monotone boolean function f s.t. $R(f) > 0$. The function is characteristic function of bipartite graphs containing a perfect matching.
2. **Tardos Function** Non-monotone circuit (poly sized $m^{O(1)}$) and monotone circuit (size $2^{\Omega(m^{\frac{1}{8}})}$)

Related Results

Under additional restrictions following are the results by different authors.

Related Results

Under additional restrictions following are the results by different authors.

1. Okolnishnikova(1982) and Ajtai and Gurevich (1987)
   There exists monotone boolean function that can be computed with poly size , constant depth , unbounded fan in but can not be computed with monotone poly size constant depth circuits.

Related Results

Under additional restrictions following are the results by different authors.

1. Okolnishnikova(1982) and Ajtai and Gurevich (1987) There exists monotone boolean function that can be computed with poly size , constant depth , unbounded fan in but can not be computed with monotone poly size constant depth circuits.
2. Santha and Wilson(1993) In the class of constant-depth circuits, we need much more than $\lceil \log(n+1) \rceil$ negations . A multi output function that cannot be computed by constant depth using $o(\frac{n}{\log^{1+\epsilon} n})$

How many negations are enough to prove $P \neq NP$?

Markov-Fischer

To show that $P \neq NP$, it is enough to show a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ which is in NP and cannot be computed by any polynomial size circuit. By the results of Markov and Fischer it would be enough to prove a "weaker" result. Namely, let

$P^{(r)}$ = class of all functions $f : \{0,1\}^n \rightarrow \{0,1\}^n$ computable by poly-size circuits with atmost r NOT gates.

CLIQUE

Let *CLIQUE* be the monotone boolean function of $\binom{n}{2}$ variables which accepts a given input graph on n vertices iff it contains a clique on $n/2$ vertices . Since, $P \neq NP$ if $CLIQUE \notin P$, Markov-Fischer results imply that :

If $CLIQUE \notin P^{(r)}$ for $r = \lceil \log(n+1) \rceil$, then $P \neq NP$

Razborov's 1985

$$CLIQUE \notin P^{(r)} \text{ for } r = 0$$

Amano and Maruoka (2005) have shown a stronger result :

$$CLIQUE \notin P^{(r)} \text{ even for } r = \frac{1}{6} \log \log n$$

By results of Markov and Fischer, for any f we have

$$0 \leq R(f) \leq \lceil \log(n+1) \rceil$$

By results of Markov and Fischer, for any f we have

$$0 \leq R(f) \leq \lceil \log(n+1) \rceil$$

- If it were the case that $R(f) \leq \frac{1}{6} \log \log n$ for every monotone function f then we would already have the $CLIQUE \notin P$ and hence $\mathbf{P} \neq \mathbf{NP}$!!!.

By results of Markov and Fischer, for any f we have

$$0 \leq R(f) \leq \lceil \log(n+1) \rceil$$

- If it were the case that $R(f) \leq \frac{1}{6} \log \log n$ for every monotone function f then we would already have the $CLIQUE \notin P$ and hence $\mathbf{P} \neq \mathbf{NP}$!!!.
- Unfortunately, Jukna(2004) showed that there are monotone functions $f \in P$ for which $R(f)$ is near to Markov's $\log n$ border.

Theorem [Jukna 2004]

There exists explicit feasible monotone functions $f_n : \{0,1\}^n \to \{0,1\}^n$ such that $R(f_n) \geq \log n - 9 \log\log n$

Thoughts and Questions

Thanks