Matrix Methods for Formula Size Lower Bounds

Troy Lee

LRI, Université Paris-Sud
Circuit Complexity

- A million dollar question: Show an explicit function (in NP) which requires superpolynomial size circuits!

- For functions in NP the best circuit lower bound we know is $5n - o(n)$ [LR01, IM02]

- The smallest complexity class we know to contain a function requiring superpolynomial size circuits is MAEXP! [BFT98]
Formula Size

• Weakening of the circuit model—a formula is a binary tree with internal nodes labelled by AND, OR and leaves labelled by literals. The size of a formula is its number of leaves.

• PARITY has formula size $\theta(n^2)$ [Khr71].

• Showing superpolynomial formula size lower bounds for a function in NP would imply NP $\neq$ NC$^1$.

• The best lower bound for a function in NP is $n^{3-o(1)}$ [Hås98].
A New Technique

- We devise a new lower bound technique based on matrix rank.

- We exactly determine the formula size of PARITY: if $n = 2^\ell + k$ then

  $$L(\text{PARITY}) = 2^\ell(2^\ell + 3k) = n^2 + k2^\ell - k^2.$$ 

- The formula size of many other basic functions remains unresolved:

  $$\frac{n^2}{4} \leq L(\text{MAJORITY}) \leq n^{4.57}$$
A Hierarchy of Techniques

Formula size

Rectangle bound

Linear programming bound
  [KKN95]

(Adversary method)$^2$
  [LLS05]

$s(f)^2$

Koutsoupias

Håstad

Khrapchenko
Karchmer–Wigderson Game [KW88]

- Elegant characterization of formula size in terms of a communication game.

- For a Boolean function $f$, let $X = f^{-1}(0), Y = f^{-1}(1)$ and
  $$R_f = \{(x, y, i) : x \in X, y \in Y, x_i \neq y_i\}$$

- The game is then the following: Alice is given $x \in X$, Bob is given $y \in Y$ and they wish to find $i$ such that $(x, y, i) \in R_f$.

- Karchmer–Wigderson Thm: The number of leaves in a best communication protocol for $R_f$ equals the formula size of $f$. 
Communication complexity of relations

\[ R \subseteq X \times Y \times Z \]

Communication protocol is a binary tree:

Alice’s nodes labelled by a function:

\[ a_v : X \to \{0, 1\} \]

Similarly, Bob’s nodes labelled

\[ b_v : Y \to \{0, 1\} \]

Leaves labelled by elements \( z \in Z \).

Denote by \( C^P(R) \) the number of leaves in a best protocol for \( R \).
Proof by picture: $C^P(R_f) \leq L(f)$.

General idea: Alice speaks at AND nodes and Bob speaks at OR nodes.

Initially, $f(x) \neq f(y)$ and we maintain this disagreement on subformulas as we move down the tree.
Proof by picture: $C^P(R_f) \leq L(f)$.

First we define Alice’s action at the top node:

If $x$ does not satisfy the left subformula, then Alice sends the bit 0;
otherwise she sends the bit 1.
Proof by picture: $C^P(R_f) \leq L(f)$.

Say that $x$ does not satisfy the left subformula.
Proof by picture: \( C^P(R_f) \leq L(f) \).

Now Bob speaks at the OR gate:

If \( y \) satisfies the left subformula, Bob says 0. Otherwise, he says 1.
Proof by picture: \( C^P(R_f) \leq \mathbb{L}(f) \).

Now Bob speaks at the OR gate:

If \( y \) satisfies the left subformula, Bob says 0.
Otherwise, he says 1.
Proof by picture: \( C^P(R_f) \leq L(f) \).

We continue down the tree in a similar fashion, maintaining the property that \( x \) and \( y \) take different values on subformulas.

Eventually, we reach a literal \( \ell_i \) such that \( \ell_i(x) \neq \ell_i(y) \) and so \( x \) and \( y \) differ on bit \( i \).
Communication Complexity and the Rectangle

Bound

\[ R \subseteq X \times Y \times Z \]
Communication Complexity and the Rectangle

Bound
\[ R \subseteq X \times Y \times Z \]
Communication Complexity and the Rectangle

Bound
\[ R \subseteq X \times Y \times Z \]
Communication Complexity and the Rectangle

Bound

\[ R \subseteq X \times Y \times Z \]
Communication Complexity and the Rectangle

Bound

\[ R \subseteq X \times Y \times Z \]

A rectangle \( S \) is monochromatic if there exists \( z \) such that \((x, y, z) \in S\) for all \((x, y) \in S\).

A successful protocol partitions \( X \times Y \) into monochromatic rectangles.
Communication Complexity and the Rectangle

Bound
\[ R \subseteq X \times Y \times Z \]
Rectangle Bound

- We denote by $C^D(R)$ the size of a smallest partition of $X \times Y$ into monochromatic (with respect to $R$) rectangles. By the argument above, $C^D(R) \leq C^P(R)$.

- The rectangle bound is a purely combinatorial quantity.

- We can still hope to prove larger lower bounds by focusing on the rectangle bound:

  $$C^D(R) \leq C^P(R) \leq 2^{(\log C^D(R))^2}$$

- Major drawback—it is NP hard to compute.
Rectangles and Rank

• Rank is one of the most successful ways to prove lower bounds on communication complexity of functions

• Let $M[x, y] = f(x, y)$. A monochromatic 1-rectangle has rank one, thus $\text{rk}(M) \leq C^D(f)$.

• It has been difficult to adapt the rank technique to communication complexity of relations.
Rank for relations

- The key idea is a selection function $S : X \times Y \rightarrow Z$.

- A selection function turns a relation into a function, by selecting one output.

- Let $R|_S = \{(x, y, z) : S(x, y) = z\}$. Then
  \[
  C^P(R) = \min_S C^P(R|_S).
  \]
Rank for relations

• With the help of selection functions, we can now apply the rank method as before.

• Let $S_z$ be a matrix where $S_z[x, y] = 1$ if $S(x, y) = z$ and 0 otherwise.

$$\min_S \sum_{z \in Z} \text{rk}(S_z) \leq C^D(R)$$
Approximating Rank

• In general this bound seems difficult to use because of the minimization over all selection functions

• We get around this by the following lower bound on rank:

\[
\left\lceil \frac{\| M \|_{tr}^2}{\| M \|_F^2} \right\rceil \leq \text{rk}(M)
\]

where

- \( \| M \|_{tr} = \sum_i \lambda_i(M) \)

- \( \| M \|_F^2 = \sum_i \lambda_i^2(M) \)
Application to Parity

• Selection function: $S : 2^{n-1} \times 2^{n-1} \rightarrow [n]$.

• For every $i \in [n]$, there are $2^{n-1}$ pairs where behavior of selection function is determined—the sensitive pairs.

• If selection function $S$ only output $i$ where forced to, then $\text{rk}(S_i) = 2^{n-1}$. Thus $S$ must output $i$ in more places to bring down rank.
Application to Parity

- Because of sensitive pairs $\|S_i\|_{tr} \geq 2^{n-1}$ for every $i$.

- Also, $\|S_i\|_F^2$ is simply number of ones in $S_i$.

- Putting these observations together:

$$\min_{s_i} \sum_i \left\lceil \frac{(2^{n-1})^2}{s_i} \right\rceil \leq L(\text{PARITY})$$

where $\sum_i s_i = (2^{n-1})^2$. 
Application to Parity

We have

\[
\min_{s_i} \sum_i \left\lceil \frac{(2^n-1)^2}{s_i} \right\rceil \leq L(PARITY)
\]

where \(\sum_i s_i = (2^{n-1})^2\).

- Ignoring the ceilings, Jensen’s inequality says minimum attained when all \(s_i\) equal, \(s_i = (2^{n-1})^2/n\). This is not possible when \(n\) is not a power of two.

- If \(n = 2^\ell + k\), best thing to do, take each \(s_i\) a power of two, as evenly as possible:

\[
L(PARITY) = 2^\ell (2^\ell + 3k) = n^2 + k2^\ell - k^2
\]
Open problems

• Application to threshold functions?

\[ \frac{n^2}{4} \leq L(\text{MAJORITY}) \leq n^{4.57} \]

• More subtle lower bound on rank? Use not just number of ones in each \( S_i \) but also their placement.