1 This Issues Column!

This issue’s Open Problem Column is by William Gasarch and is Wanted: A Communication Complexity Proof for Circuit Lower Bounds on PARITY.

2 Request for Columns!

I invite any reader who has knowledge of some area to contact me and arrange to write a column about open problems in that area. That area can be (1) broad or narrow or anywhere inbetween, and (2) really important or really unimportant or anywhere inbetween.

Wanted: A Communication Complexity Proof for Circuit Lower Bounds on PARITY

By William Gasarch

Disclaimer: I believe this is a known open problem that was devised by several people independently. I am one of them.

3 Notation

We will use the following notations throughout this paper.

Notation 3.1 As usual the term circuit means family of circuits. All circuits will alternate AND and OR gates. There will be no NOT gates; however, both inputs and their negations are available. The depth of a circuit is the longest path from input to output. The fan-in of a circuit is the most number of inputs to a gate. The size of a circuits is the number of gates. A \((d, f, s)-circuit\) is a circuit of depth \(d\), fan-in \(f\), and size \(s\). It is clear what it means for a circuit to compute a function \(g : \{0, 1\}^n \to \{0, 1\}^k\).

Notation 3.2 As usual the term protocol means family of protocols. All protocols alternate who sends a message. The number of rounds in a protocol is the number of times someone sends a message. The bandwidth of a protocol is the max number of bits in a message. A \((d, b)-protocol\) is a protocol with \(d\) rounds and bandwidth \(b\). A protocol computes a relation \(R \subseteq \{0, 1\}^n \times \{0, 1\}^n \times I\) if whenever Alice gets \(x\) and Bob gets \(y\): (1) if there exists some \(i \in I\) such that \((x, y, i) \in R\) then they agree on one such \(i\), (2) if there is no such \(i\) then the protocol can do anything.

4 \(\text{PARITY}_n\)

Def 4.1 \(\text{PARITY}_n\) is the function that, on input \((x_1, \ldots, x_n) \in \{0, 1\}^n\) outputs \(\sum_{i=1}^{n} x_i \pmod{2}\).

How big a circuit do you need to computer \(\text{PARITY}_n\)? The following are known:
There is an \((O(n), 2, O(n))\) circuit for \(\text{PARITY}_n\) (easy).

There is a \((O(1), 2^O(n), 2^O(n))\) circuit for \(\text{PARITY}_n\) (easy).

For all constants \(d\) there is a \((d, O(n^{(d-1)/(d-1)2^{n^1/(d-1)}}), O(n^{(d-1)/(d-2)2^{n^1/(d-1)}}))\) circuit for \(\text{PARITY}_n\) (The only reference I have found for this is Hastad [4, 5, 6].)

Furst, Saxe, Sipser [3] (henceforth FSS) and Ajtai [1] showed that, for all constants \(d\), for all polynomials \(s(n)\), \(\text{PARITY}_n\) cannot be computed by a \((d, s(n), s(n))\) circuit. The proof went as follows: For \(d = 2\) this is easy to show. Assume there is a \((d, s(n), s(n))\) circuit where \(s(n)\) is polynomial. Place a random restriction on the inputs where some inputs are set to 0, some are set to 1, and \(n\) are left alone. With high probability the first two levels, say an AND of OR’s, can be rewritten with only polynomial more gates as an OR of AND’s. This new circuit collapses to get a depth \((d - 1, s'(n'), s'(n'))\). This is impossible inductively. This kind of proof, where a random restriction leads to being able to write an AND or ORs as and OR of ANDS (without too much increase in size) is a Switching Lemma.

Yao [10] proved that for all constants \(d\) \(\text{PARITY}_n\) cannot be computed by a \((d, O(2^{n^1/4d}), O(2^{n^1/4d}))\) circuit. Hastad [4, 5, 6] obtained the optimal result: \(\text{PARITY}_n\) cannot be computed by a \((d, O(2^{n^1/(d-1)}), O(2^{n^1/(d-1)})\) circuit. (There are some polynomial terms I am omitting.) Hastad obtained this result by refining the FSS’s Switching Lemma. His version has been widely used in many contexts and, when The Switching Lemma is referred to, it means Hastad’s. Razborov [8] has a simpler proof of the Switching Lemma. Fortnow and Laplante [2] have a proof of the switching lemma that uses Kolmogorov Complexity.

The proofs of FSS, Yao, and Hastad are all probabilistic. Smolensky [9] had a completely different proof. He showed that \(\text{PARITY}_n\) could not be approximated by a low degree polynomial, and that anything computed by a constant depth, small circuit could be. We’ll call this type of proof algebraic.

5 Lower Bounds on Circuits via Communication Complexity

Karchmer [7] devised an approach to lower bounds via communication complexity. We present his theorem that links the two.

Def 5.1 Let \(g: \{0, 1\}^n \rightarrow \{0, 1\}\). Let \(R_g \subseteq \{0, 1\}^n \times \{0, 1\}^n \times [n]\) be the set

\[
\{(x, y, i) : f(x) = 0 \land f(y) = 1 \land x_i \neq y_i\}.
\]

Theorem 5.2 Let \(f: \{0, 1\}^n \rightarrow \{0, 1\}\). There is a \((d, 2, s)\) circuit for \(f\) iff there is a \((d, 1)\) protocol for \(R_g\). (The \(s\) plays no role.)

Proof:

1) Assume there is a \((d, 2, s)\) circuit for \(f\). We use this to create a \((d, 1)\)-protocol for \(D(R_g)\).

1. Alice takes \(x\) and runs the circuit on it. We assume she gets 0. Bob takes \(y\) and runs the circuit on it. We assume he gets 1. Note that Alice and Bob “disagree” on what the final output is.
2. We assume the top gate is an AND (if its an OR the proof is similar). Alice sees that the output when the circuit run on $x$ is 0. Hence either the left or the right or both inputs to the top gate are 0. She sends Bob 0 if the left input is 0, 1 if the right input is 0. Note that Alice and Bob “disagree” on what the output of that OR gate is.

3. They keep going in this matter until they find the original input they disagree on.

Note that the number of rounds is exactly the depth of the circuit. Also note that the bandwidth of the protocol is 1.

2) Assume there is a $(d, 1)$ protocol for $R_g$. Show there is a depth $d$, fan-in 2, size $s$ circuit for $f$.

Take the protocol for $R_g$. Formally it is a binary decision tree (since its a $(d, 1)$ protocol). We’ll assume Alice sends first. The top node tells Alice that on inputs BLAH she sends a 0 and on inputs BLAHBLAH she sends 1. When we convert this protocol into a circuit we will NOT be concerned with BLAH or BLAHBLAH.

Take the decision tree and do the following to form a circuit:

1. Look at a node representing Alice sending a bit. In the protocol the node is thought of as
   *Alice knows her input and knows what Bob has send her and based on that sends a 0 or a 1.*
   As such it is a node with two edges coming out of it (going to Bob-nodes). We reverse that: we make this node into an AND gate and the edges are now the inputs.

2. Similarly, replace every Bob-node with an OR gate.

3. Let $L$ be a leaf of the protocol. Associated to $L$ is $i \in [n]$ such that, if the protocol gets to that leaf then Alice and Bob agree that $x_i \neq y_i$. One can also show that either (1) every ordered pair that goes to $L$ has $x_i = 1$ and $y_i = 0$, or (2) every ordered pair that goes to $L$ has $x_i = 0$ and $y_i = 1$. In Case 1 replace $L$ by input $z_i$, in Case 2 replace $L$ by input $\overline{z_i}$.

We omit the proof that the circuit so created computes $g$. □

Before this result the following thoughts had currency:

- We’ve made very little progress in proving lower bounds on circuits.
- We’ve made a lot of progress in proving lower bounds on communication protocols.

So the hope was that Theorem 5.2 would allow progress on lower bounds on circuits. Did it? Yes and mostly No. There were many results about *monotone circuits* that used this framework. But alas, very few on general circuits.

6 What about Known Circuit Results?

Could there be a communication complexity proof that any constant depth, unbounded fan-in circuit for PARITY requires exponential size? (Note that while we say *unbounded* it really is bounded by the size $s$ of the circuit.) Theorem 5.2 is about fan-in 2 circuits. The following modification is folklore but I do not think has ever been written down.

**Theorem 6.1** Let $g : \{0, 1\}^n \rightarrow \{0, 1\}$. There is a $(d, s, s)$ circuit for $f$ iff there is a $(d, \lceil \log(s) \rceil)$ protocol for $R_g$. 

3
Proof:

All \( \log(s) \) in this proof are really \( \lceil \log(s) \rceil \).

1) Assume there is a depth \( d \), fan-in \( s \), size \( s \) circuit for \( f \). We show a \( d \) rounds, \( \log(s) \) bandwidth protocol for \( R_g \).

1. Alice takes \( x \) and runs the circuit on it. We assume she gets 0. Bob takes \( y \) and runs the circuit on it. We assume he gets 1. Note that Alice and Bob “disagree” on the output.

2. We assume the top gate is an AND (if its an OR the proof is similar). Alice sees that the output of the top gate is a 0. Hence one of the \( s \) inputs is a 0. Alice tells Bob which one with \( \log(s) \) bits. Note that Alice and Bob “disagree” on the output of this OR gate.

3. They keep going in this manner until they find the original input they disagree on.

Note that the number of rounds is \( d \) and the bandwidth is \( \log(s) \).

2) Assume there is a \((d, \log(s))\) protocol for \( R_g \). Show there is a depth \( d \), fan-in \( f \), size \( s \) circuit for \( g \). This proof is similar to the proof of Theorem 5.2.2.

7 Open Problem

Theorem 6.1 points to a possible alternative method to get lower bounds on the size of constant depth circuits for \( \text{PARITY}_n \):

**Conjecture 7.1** Fix \( d \), a constant. If there is a \((d, b)\) protocol for \( R_{\text{PARITY}_n} \) then \( b \) is \( \Omega(n^{1/(d-1)}) \).

There is one thing wrong with this conjecture. It is already known to be true! Just use Theorem 6.1.2 and use the known lower bounds on \( \text{PARITY}_n \). So what am I really looking for?

**Open Problem:** Give a communication complexity proof for any of the following. Fix \( d \), a constant.

1. If there is a \((d, b)\) protocol for \( R_{\text{PARITY}_n} \) then \( b \) is superpolynomial.

2. If there is a \((d, b)\) protocol for \( R_{\text{PARITY}_n} \) then \( b \) is \( \Omega(2^{n^{1/(d-1)}}) \) (or replace \( 2^{n^{1/(d-1)}} \) with a smaller superpolynomial function).

Such a proof would give another way to obtain lower bounds on \( \text{PARITY}_n \) and foster a link between communication complexity and lower bounds on circuits.

References


