DIMACS Technical Report 2004-51
October 2004

A $O(n^2)$ lower bound for swaping the order of n input bits in planar boolean circuit

by

Bin Tian[1]
Department of Computer Science
Rutgers University
Piscataway, NJ 08854

[1]This research is supported in part by DIMACS Summer Award 2004.

ABSTRACT

When confined to a 2 dimensional world, many regular tasks become supprisingly hard. One example is to swap the order of n input bits in a planar boolean circuit. Mario Szegedy conjectured that $O(n^2)$ gates are necessary. This paper gives a short proof.

1 Introduction

A boolean circuit is a circuit where all gates except input/output gates are boolean functions. A boolean circuit can be drawn as a directed acyclic graph, where each vertex corresponds to a gate (including input/output gates), each edge corresponds to a link between gates. If the graph can be drawn on a plane with no crossing edges, then we say the circuit is planar.

There is one problem with this definition: we treat input and output gates no different than internal gates, therefore their location can be arbitrary. However in a real circuit the input and output gates are most likely fixed. Given a map

$$\sigma : \{0,1\}^m \rightarrow \{0,1\}^n$$

the problem of designing a boolean circuit of smallest size is under the following restrictions:

1. A circuit board is a rectangular shaped box.
2. On one side of the box there are m input gates, $x_0, x_1, \ldots, x_{m-1}$.
3. On the opposite side there are n output gates, $y_0, y_1, \ldots, y_{n-1}$.
4. All intermediate gates must stay inside the box.
5. No crossing edges.

Under the above restriction, let's look at the circuit size for computing the function

$$\sigma(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_{n-1}, \ldots, x_0).$$

Notice that σ simply swap the order of input bits.

Mario Szegedy conjected that at least $O(n^2)$ gates are needed. I will show that his conjecture is correct.

2 The Proof

Let C be our circuit and $E(C)$ be the set of directed links between gates. For every gate v define its level $l(v)$:

- If v is a input gate, $l(v) = 0$.
- Otherwise, $l(v) = \min\{l(u) + 1 | (u, v) \in E(C)\}$.

In other words, $l(v)$ is the shortest distance from some input gate to v.

Define $LEVEL(i) = \{v | l(v) = i, v \in V(G)\}$ be the set of all gates on level i. Apparently

$$LEVEL(i) \bigcap LEVEL(j) = \Phi \qquad \forall i \neq j.$$

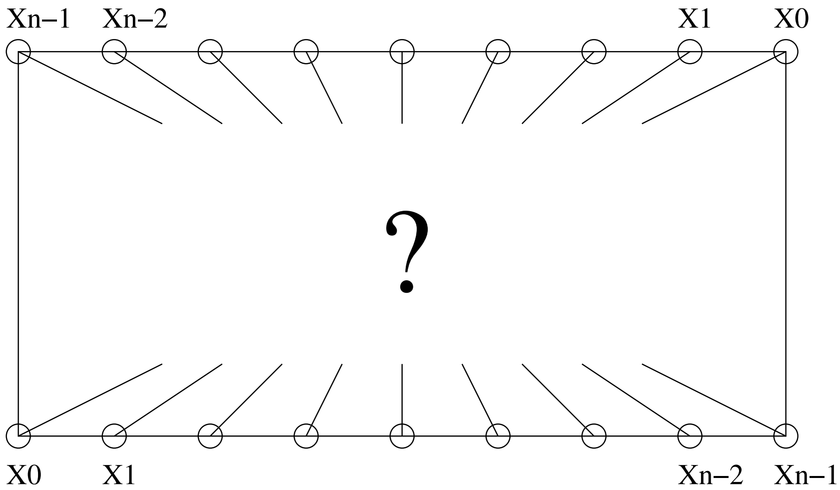

Figure 1: How many gates are needed to swap the order of input bits?

In order to show the circuit has size $O(n^2)$, it is enough to show that $\forall\ 0 \le i \le \lfloor n/2 \rfloor$ $|LEVEL(i)| \ge n - 2i - 1$. This is because then the circuit have size at least

$$\sum_{0 \le i \le \lfloor n/2 \rfloor} n - 2i - 1 = O(n^2)$$

.

For easy description of this proof, let's label, from left to right, input gates $I_0 \dots I_{n-1}$, output gates $O_0 \dots O_{n-1}$. Define $d(i) = \min\{i, n-i-1\}$.

Definition: A set of gates S is said to *separate* output gate O_i if and only if every path from input gate I_{n-i} to O_i pass through some gates of S. Define $D(S)$ to be the set of output gates separated by S.

Lemma 1 $|S| \ge |D(S)|$.

Proof: Output gates in $D(S)$ are completely determined by gates in S. $\diamond$

Lemma 2 $l(O_i) \ge d(i)\ \forall\ 0 \le i \le n-1$.

Proof: Let p be one of the possibly many shortest paths from arbitrary input I_j to O_i. Apparently p is a cut. $|p| = l(O_i)$. If $j \le n - i$ (shown in figure 3), then p separate $O_0, O_1, \dots, O_{i-1}$. By Lemma 1, $l(O_i) = |p| \ge i$. If $j > n - i$, then p separate $O_{i+1}, O_{i+2}, \dots, O_{n-1}$, $l(O_i) = |p| \ge n - i - 1$. So $l(O_i) \ge \min\{n - i - 1, i\} = d(i)$. $\diamond$

Corollary 1 $LEVEL(i) \ne \emptyset\ \forall\ 0 \le i \le \lfloor n/2 \rfloor$.

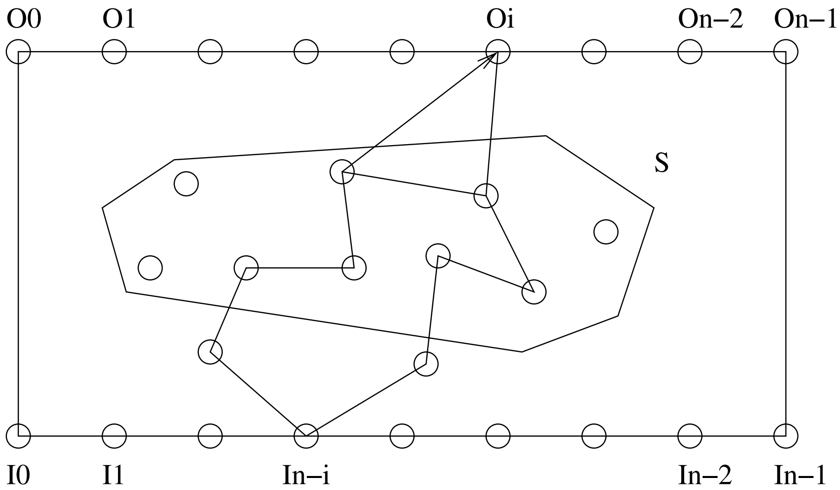

Figure 2: S separates O_i

Proof: $l(O_{\lfloor n/2 \rfloor}) \geq d(\lfloor n/2 \rfloor) = \min\{\lfloor n/2 \rfloor, n - \lfloor n/2 \rfloor\} \geq \lfloor n/2 \rfloor$. So $LEVEL(l(O_{\lfloor n/2 \rfloor})) \neq \emptyset$. By definition, all lower levels are also non-empty. $\diamond$

Now let's consider $D(LEVEL(k))$, the set of output gates separated by $LEVEL(k)$. If an output gate O_i has $l(O_i) \geq k$, then $LEVEL(k)$ must separate O_i, because any path from input vertex to O_i must pass through level k before it can reach level $l(O_j) \geq k$.

So how many output gates have level greater than or equal to k? For any $k < i < n - k$, $l(O_i) \geq d(O_i) \geq k$. So $|D(LEVEL(k))| \geq n - 2k - 1$. By Lemma 1, $|LEVEL(k)| \geq |D(LEVEL(K))| \geq n - 2k - 1$. $\diamond$

3 Conclusion

Notice that in the proof we never assume anything about the fan-in or fan-out of the gates. The $O(n)$ lower bounds applys for arbitrary fan-in fan-out.

A natural extension is that almost all permutations on n boolean bits require $O(n^2)$ gates in planar boolean circuit.