Lower Bounds for the Complexity of Reliable Boolean Circuits with Noisy Gates

Péter Gács, *Senior Member, IEEE* and Anna Gál

Abstract — We prove that the reliable computation of any Boolean function with sensitivity s requires $\Omega(s \log s)$ gates if the gates fail independently with a fixed positive probability. This theorem was stated by Dobrushin and Ortyukov in 1977, but their proof was found by Pippenger, Stamoulis and Tsitsiklis to contain some errors.

Index Terms — Reliable computation, noisy gates, Boolean functions.

1 Introduction

In this paper, we prove lower bounds on the number of gates needed to compute Boolean functions by circuits with noisy gates. We say that a gate fails if its output is incorrect. Let us fix a bound $\varepsilon \in (0, 1/2)$ on the failure probability of the gates and a bound $p \in (0, 1/2)$ on the probability that the value computed by the circuit is incorrect. These parameters which will be held constant throughout the paper, and dependence on them will not be explicitly indicated either in the defined concepts like redundancy, or in the $O()$ and $\Omega()$ notation.

A *noisy gate* fails with a probability bounded by ε. A *noisy circuit* has noisy gates that fail independently.

A noisy circuit is *reliable* if the value computed by the circuit on any given input is correct with probability $\geq 1 - p$. The size of a reliable noisy circuit has to be larger than the size needed for circuits using only correct gates. By the *noisy complexity* of a function we mean the minimum number of gates needed for the reliable computation of the function. Note that in this model the circuit cannot be more reliable than its last gate. For a given function, the ratio of its noisy and noiseless complexities is called the *redundancy* of the noisy computation of the function.

The following upper bounds are known for the noisy computation of Boolean functions. The results of von Neumann [9], Dobrushin and Ortyukov [3] and Pippenger [11] prove that if a function can be computed by a noiseless circuit of size L, then $O(L \log L)$ noisy gates are sufficient for the reliable computation of the function. Pippenger [11] proved that any function depending on n variables can be computed by $O(2^n/n)$ noisy gates. Since the noiseless computation of

[0]Péter Gács, Department of Computer Science, Boston University, Boston, MA 02215
Anna Gál, Department of Computer Science, The University of Chicago, Chicago, IL 60637
Péter Gács was supported in part by NSF Grant CCR-9002614.
Anna Gál was supported in part by NSF Grant CCR 8710078 and OTKA Grant 2581.
This work was presented in part at the 32-nd IEEE Symposium on the Foundations of Computer Science, San Juan, Puerto Rico, October 1991.

almost all Boolean functions requires $\Omega(2^n/n)$ gates (Shannon [15], Muller [8]), this means that for almost all functions the redundancy of their noisy computation is just a constant. Pippenger [11] also exhibited specific functions with constant redundancy. For the noisy computation of any function of n variables over a complete basis Φ, Uhlig [16] proved upper bounds arbitrarily close to $\rho(\Phi)2^n/n$ as $\varepsilon \to 0$, where $\rho(\Phi)$ is a constant depending on Φ, and $\rho(\Phi)2^n/n$ is the asymptotic bound for the noiseless complexity of almost all Boolean functions of n variables (Lupanov [7]).

These are rather surprising results. It is natural to ask whether there exist functions with nonconstant redundancy or whether the $O(L \log L)$ upper bound of [9],[3],[11] is tight for some functions. It is also desirable to exhibit such functions.

Dobrushin and Ortyukov in their 1977 paper [2] stated the following theorem providing answers to this important problem: The computation of any function with sensitivity s requires $\Omega(s \log s)$ gates if the gates of the circuit fail independently with a fixed probability $\varepsilon \in (0, 1/2)$, but the value computed by the circuit on any input is incorrect with probability not greater than $p \in (0, 1/3)$. Thus, in particular, the reliable computation of the parity or the "or" functions of n variables requires $\Omega(n \log n)$ noisy gates.

Unfortunately, as noticed by Pippenger, Stamoulis and Tsitsiklis [12], the proof in [2] is incorrect. Pippenger, Stamoulis and Tsitsiklis [12] pointed out the questionable arguments in the proof, and suggested that part of the strategy seemed hopelessly flawed. They gave in [12] an $\Omega(n \log n)$ lower bound for the parity function, keeping part of the approach of Dobrushin and Ortyukov, but replacing a significant part of their proof with entirely new arguments using specific properties of the parity function. The more general statement about any function with given sensitivity remained unproven.

In this paper we prove that functions with sensitivity s do indeed require $\Omega(s \log s)$ noisy gates for their reliable computation. We can prove the stronger $\Omega(b \log b)$ lower bound, where b is block sensitivity rather than sensitivity. (See Definition 6.1.) The results hold for circuits with arbitrary constant fan-in gates. Our proof uses the original Dobrushin-Ortyukov strategy, proving the correct probabilistic lemmas to carry it out. We give two different proofs. The first stays closer to the steps of Dobrushin and Ortyukov and works for circuits with error probability at most $p \in (0, 1/4)$. The second proof works for $p \in (0, 1/2)$, thus it gives a stronger result than the original theorem.

We note that these are the only known lower bounds proving nonconstant redundancy for functions other than the parity function, and they allow to prove maximal $\Omega(\log L)$ redundancy of noisy computation over arbitrary constant fan-in basis for a large class of functions, including all symmetric functions.

Recently we learned that the paper of Reischuk and Schmeltz [13] gives an independent proof of the $\Omega(s \log s)$ lower bound. A preliminary version of our paper appeared in [5].

2 The main theorem

Let f be a Boolean function of n variables. Let $x = (x_1, \ldots, x_n)$ be any input string. Denote by x^ℓ the input string which differs from x only in the ℓ-th bit, i.e. $x_i^\ell = x_i$ for each $i \neq \ell$ and $x_\ell^\ell = \neg x_\ell$.

Definition 2.1 The function f is *sensitive* to the ℓ-th bit on x if $f(x) \neq f(x^\ell)$. The *sensitivity of f on x* is the number of bits to which f is sensitive on x. The *sensitivity* of f is the maximum over all x of the sensitivity of f on x.

We consider Boolean circuits with gates having constant fan-in and computing functions from a finite set Φ. A complete basis is a set of functions such that any Boolean function can be represented by their composition. Φ may or may not be a complete basis. We assume only that any circuit C computing a particular function f uses constant fan-in gates computing functions from a finite set Φ_C, such that f can be represented by the composition of functions from Φ_C.

Let $n(\Phi_C)$ be the maximum fan-in of the gates computing functions from the set Φ_C. Let n_g denote the fan-in of gate g.

Definition 2.2 Let $z \in \{0,1\}^{n_g}$. Denote by $g(z)$ the value of the function that the gate g has to compute, on input z. We say that the gate g *fails*, if receiving input z it outputs a value different from $g(z)$.

The main theorem gives the lower bound for the case that the gates fail independently with a fixed probability $\varepsilon \in (0, 1/2)$. It has been argued (Pippenger [11]) that for proving lower bounds this is the best model to consider, as opposed to proving upper bounds, where the assumption that the gates fail independently with probability at most $\varepsilon \in (0, 1/2)$ is more appropriate.

Definition 2.3 Denote by $C(x)$ the random value computed by the circuit C on input x. We say that a circuit *computes f with error probability at most p* if the probability that $C(x) \neq f(x)$ is at most p for any input x.

In the whole following exposition, the notation $v = \Omega(w)$ means that there is a constant $c > 0$ depending on parameters p, ε, etc. but not on the Boolean function f to be computed, such that $v \geq cw$.

The main theorem is stated below:

Theorem 2.4 *Let ε and p be any constants so that $\varepsilon \in (0, 1/2)$, $p \in (0, 1/2)$. Let f be any Boolean function with sensitivity s. Suppose a circuit whose gates fail independently with fixed probability ε computes f with error probability at most p . Then the number of gates of the circuit is $\Omega(s \log s)$.*

Corollary 2.5 *The redundancy of the noisy computation by Boolean circuits of any function of n variables with $O(n)$ noiseless complexity and $\Omega(n)$ sensitivity is $\Omega(\log n)$.*

Corollary 2.5 applies to a large class of functions. In particular the following statement holds:

Corollary 2.6 *The redundancy of the noisy computation by Boolean circuits of any nonconstant symmetric function of n variables is $\Omega(\log n)$.*

We note that there is a difference between the redundancies of noisy computations by circuits and by decision trees. A similar model of noisy computation is considered by Feige et al. [4] for Boolean decision trees. The nodes of the tree are allowed to be independently faulty with some probability, and the result of the computation has to be correct with at least a fixed probability for every input. Feige et al. [4] give bounds for the depth of noisy decision trees computing symmetric functions. These bounds show that some nonconstant symmetric functions have constant redundancy of noisy computation by decision trees.

Corollary 2.7 *There exist Boolean functions of n variables with constant redundancy of noisy computation by decision trees and $\Omega(\log n)$ redundancy of noisy computation by circuits.*

3 Noisy wires

Following Dobrushin and Ortyukov, for the proof of the main theorem, we consider an equivalent problem.

Let C be a circuit satisfying the condition that if its gates fail independently with probability ε then the circuit computes f with error probability at most p.

As suggested in [2], consider the case when not only the gates but the wires of C may fail as well. We say that a wire fails when it transmits an incorrect value.

Let $\delta \in [0, \varepsilon/n(\Phi_C)]$ and suppose that the wires of C fail independently, each with probability δ. This means that the input $y \in \{0,1\}^{n_g}$ received by gate g may be different from the input $t \in \{0,1\}^{n_g}$ that the gate should have received.

The following statement is proved as Lemma 3.1 in [2]: Let $\varepsilon \in (0, 1/2)$, $\delta \in [0, \varepsilon/n(\Phi_C)]$. Then for any gate g of the circuit C there exist unique values $\eta_g(y, \delta) \in [0, 1]$ such that if the wires of C fail independently with probability δ and the gate g fails with probability $\eta_g(y, \delta)$ when receiving input y, then the probability that the output of g is different from $g(t)$ (where t is the input entering the input wires of the gate) is equal to ε.

Consider now the behavior of circuit C in two different failure modes. In the first mode the wires of the circuit are correct and the gates fail independently with probability $\varepsilon \in (0, 1/2)$. In the second mode, each wire fails independently with fixed probability $\delta \in [0, \varepsilon/n(\Phi_C)]$ and each gate fails independently with probability $\eta_g(y, \delta)$ when receiving y. Lemma 3.2 of [2] shows that these two failure modes are equivalent in the sense that the circuit C computes f with the same error probability: for any input x and any gate g, the output of g differs from the output computed by the same gate in an error-free computation of C on input x with the same probability in both modes. Thus to prove Theorem 2.4 it suffices to prove a lower bound for the size of C computing f with error probability at most p with errors occurring at both the wires and the gates. More precisely, we shall prove the following.

Theorem 3.1 *Let δ and p be any constants so that $\delta \in (0, 1/2)$, $p \in (0, 1/2)$. Let f be any function with sensitivity s. Let C be a circuit such that its wires fail independently with fixed probability δ and each gate g fails independently with probability $\eta_g(y, \delta)$ when receiving y. Suppose C computes f with error probability at most p. Then the number of gates of C is $\Omega(s \log s)$.*

4 Probabilistic lemmas

In this section we prove a few statements which we will need for the proof of the main theorem.

Lemma 4.1 *Let $H_1, \ldots, H_n$ be independent events, $\gamma \in (0,1)$ and $\Pr[\bigcup_{i=1}^n H_i] \le \gamma$. Then*

$$\Pr[\bigcup_{i=1}^n H_i] \ge (1-\gamma) \sum_{i=1}^n \Pr[H_i] \,.$$

Proof:

$$\begin{aligned}
\Pr[\bigcup_{i=1}^n H_i] &\ge \sum_{i=1}^n \Pr[H_i \cap (\neg \bigcup_{j \ne i} H_j)] \\
&\ge \sum_{i=1}^n \Pr[H_i]\,(1 - \Pr[\bigcup_{j=1}^n H_j]) \\
&\ge (1-\gamma) \sum_{i=1}^n \Pr[H_i] \,.
\end{aligned}$$

Lemma 4.2 *Let E be an event, p and c constants from $(0,1)$. Let H and G be independent events such that $\Pr[G] \ge c$ and $\Pr[E \mid H] \ge 1-p$. Then*

$$\Pr[E \mid H \cap G] \ge 1 - \frac{p}{c} \,.$$

Proof:

$$\Pr[E \mid H \cap G] = 1 - \Pr[\neg E \mid H \cap G] \,.$$

$$\begin{aligned}
\Pr[\neg E \mid H \cap G] &= \frac{\Pr[\neg E \cap H \cap G]}{\Pr[H \cap G]} \le \frac{\Pr[\neg E \cap H]}{\Pr[H \cap G]} \\
&= \frac{\Pr[\neg E \mid H]\Pr[H]}{\Pr[H]\Pr[G]} \le \frac{p}{c} \,.
\end{aligned}$$

Lemma 4.3 *Let E be an event and $p \in (0,1)$ a constant. Let $H_1, \ldots, H_n$ be independent events such that $\Pr[E \mid H_i] \ge 1-p$ for $\forall i$. Then*

$$\Pr[E \mid \bigcup_{i=1}^n H_i] \ge (1-\sqrt{p})^2 \,.$$

Proof:

We prove that if the conditions of the lemma hold then for any $c \in (0,1)$

$$\Pr[E \mid \bigcup_{i=1}^n H_i] \ge (1 - \frac{p}{c})(1-c) \,. \tag{1}$$

Taking $c = \sqrt{p}$ we get the statement of the lemma.

Let us use the notation $G_i = \neg(H_1 \cup \ldots \cup H_i)$. Then the events H_1, $H_2 \cap G_1$, …, $H_{k+1} \cap G_k$ do not intersect and

$$\bigcup_{i=1}^{n} H_i = H_1 \dot\cup (H_2 \cap G_1) \dot\cup (H_3 \cap G_2) \dot\cup \ldots \dot\cup (H_n \cap G_{n-1}) \,,$$

$$\Pr[G_1] \geq \Pr[G_2] \geq \ldots \geq \Pr[G_{n-1}] \,. \tag{2}$$

Fix any constant $c \in (0,1)$. Suppose $\Pr[G_k] \geq c$ for some k. Then since $H_{\ell+1}$ and G_ℓ are independent events, by Lemma 4.2 and (2) the following holds for each $1 \leq \ell \leq k$:

$$\Pr[E \mid H_{\ell+1} \cap G_\ell] \geq 1 - \frac{p}{c} \,.$$

Since $\bigcup_{i=1}^{k+1} H_i = H_1 \dot\cup (H_2 \cap G_1) \dot\cup \ldots \dot\cup (H_{k+1} \cap G_k)$ we get that

$$\text{if } \Pr[G_k] \geq c \text{ then } \Pr[E \mid \bigcup_{i=1}^{k+1} H_i] \geq 1 - \frac{p}{c} \,. \tag{3}$$

This proves (1) if $\Pr[G_{n-1}] \geq c$.

If $\Pr[G_{n-1}] < c$ and $\Pr[G_1] \geq c$ then consider the largest index k such that $\Pr[G_k] \geq c$. Thus $1 \leq k < n-1$ and

$$\Pr[G_k] \geq c \quad \text{but} \quad \Pr[G_{k+1}] < c \,.$$

By (3) $\Pr[E \mid \bigcup_{i=1}^{k+1} H_i] \geq 1 - (p/c)$, and

$$\Pr[\bigcup_{i=1}^{k+1} H_i] \geq 1 - c \ \text{ since } \bigcup_{i=1}^{k+1} H_i = \neg G_{k+1} \,.$$

We get

$$\begin{aligned} \Pr[E \mid \bigcup_{i=1}^{n} H_i] &\geq \Pr[E \mid \bigcup_{i=1}^{k+1} H_i] \Pr[\bigcup_{i=1}^{k+1} H_i] \\ &\geq (1 - \frac{p}{c})(1 - c) \,. \end{aligned}$$

If $\Pr[G_1] < c$ then $\Pr[H_1] \geq 1 - c$ and

$$\begin{aligned} \Pr[E \mid \bigcup_{i=1}^{n} H_i] &\geq \Pr[E \mid H_1] \Pr[H_1] \\ &\geq (1-p)(1-c) \\ &> (1 - \frac{p}{c})(1-c) \end{aligned}$$

which concludes the proof of Lemma 4.3.

Lemma 4.4 *Let E be an event and let H_i $(i = 1, 2, \ldots)$ be independent events, with* $\Pr[E] = p$, $\Pr[E \mid H_i] = \lambda_i$, $\Pr[H_i] = q_i > 0$. *Then*

$$\sum_i \frac{q_i}{1-q_i}(\lambda_i - p)^2 \le p.$$

This lemma says that if p is small and the λ_i are large then the q_i must be small. In particular, if we also have $\lambda_i \ge 1 - p > 1/2$ then simple substitution gives

$$\sum_i q_i \le \frac{p}{(1-2p)^2}.$$

Proof: Let $f_i(\omega)$ be the indicator function of the event H_i and g be the indicator function of the event E where ω runs through the elementary events of our probability space. For two functions $u(\omega), v(\omega)$, let (u, v) denote the expected value of $u(\omega)v(\omega)$. Let

$$h_i(\omega) = \frac{f_i(\omega) - q_i}{\sqrt{q_i(1-q_i)}}.$$

The independence of the events H_i implies that $(h_i, h_j) = 1$ if $i = j$ and 0 otherwise, i.e., that the h_i form an orthonormal set of vectors with respect to the scalar product (u, v). The length of the projection of g onto h_i is (g, h_i), therefore we have

$$\begin{aligned} p = (g, g) \ge \sum_i (g, h_i)^2 &= \sum_i \frac{((g, f_i) - pq_i)^2}{q_i(1-q_i)} \\ &= \sum_i (\lambda_i - p)^2 \frac{q_i}{1-q_i}. \end{aligned}$$

5 Proof of the main theorem

We prove the "noisy wires" version (Theorem 3.1).

Let z be an input such that f has maximum sensitivity on z. Let $S \subset \{1, \ldots, n\}$ be the set of indices so that $\ell \in S$ if and only if f is sensitive to the ℓ-th bit on input z. Then $|S| = s$, where s is the sensitivity of f.

For each $\ell \in S$ denote by B_ℓ the set of all wires originating from the ℓ-th input of the circuit. Let $m_\ell = |B_\ell|$.

For any set $\beta \subset B_\ell$, let $H(\beta)$ be the event that the wires belonging to β fail and the other wires of B_ℓ are correct.

Denote by β_ℓ the subset of B_ℓ where

$$\max_{\beta \subset B_\ell} \Pr[C(z^\ell) = f(z^\ell) \mid H(\beta)]$$

is obtained. Note that β_ℓ may or may not be the empty set.

By the conditions of the theorem, C computes f with error probability at most p, which means that $\Pr[C(z^\ell) = f(z^\ell)] \ge 1 - p$. Thus,

$$\Pr[C(z^\ell) = f(z^\ell) \mid H(\beta_\ell)] \ge 1 - p\,. \tag{4}$$

Denote by H_ℓ the event that the wires of B_ℓ not belonging to β_ℓ fail and the wires of β_ℓ are correct. In other words: $H_\ell = H(B_\ell \setminus \beta_\ell)$.

Since f is sensitive to the ℓ-th bit on z

$$\Pr[C(z) \neq f(z) \mid H_\ell] = \Pr[C(z^\ell) = f(z^\ell) \mid H(\beta_\ell)] \,.$$

By (4) this means that for each $\ell \in S$

$$\Pr[C(z) \neq f(z) \mid H_\ell] \geq 1 - p \,.$$

H_ℓ are independent events since the wires fail independently.

First we prove the theorem for the case $p \in (0, 1/4)$: We apply Lemma 4.3 and get

$$\Pr[C(z) \neq f(z) \mid \bigcup_{\ell \in S} H_\ell] \geq (1 - \sqrt{p})^2.$$

Using this inequality, from

$$\begin{aligned} p &\geq \Pr[C(z) \neq f(z)] \\ &\geq \Pr[C(z) \neq f(z) \mid \bigcup_{\ell \in S} H_\ell] \Pr[\bigcup_{\ell \in S} H_\ell] \end{aligned}$$

we conclude that

$$\Pr[\bigcup_{\ell \in S} H_\ell] \leq \frac{p}{(1 - \sqrt{p})^2} \,. \tag{5}$$

$p/(1 - \sqrt{p})^2 \in (0, 1)$ since $p \in (0, 1/4)$. Applying Lemma 4.1 we get

$$\Pr[\bigcup_{\ell \in S} H_\ell] \geq (1 - \frac{p}{(1 - \sqrt{p})^2}) \sum_{\ell \in S} \Pr[H_\ell] \,. \tag{6}$$

Using

$$\Pr[H_\ell] = (1 - \delta)^{|\beta_\ell|} \delta^{m_\ell - |\beta_\ell|} \geq \delta^{m_\ell} \tag{7}$$

where δ is the failure probability of the wires, from (5) and (6) follows

$$\frac{p}{1 - 2\sqrt{p}} \geq \sum_{\ell \in S} \delta^{m_\ell} \,.$$

Then

$$\frac{p}{1 - 2\sqrt{p}} \geq s(\prod_{\ell \in S} \delta^{m_\ell})^{1/s}$$

by the inequality between the arithmetic and geometric means. Taking the logarithm we conclude

$$\sum_{\ell \in S} m_\ell \geq \frac{s}{\log(1/\delta)} \log(s \, \frac{1 - 2\sqrt{p}}{p}) \,. \tag{8}$$

Since the maximum fan-in of the gates of the circuit $n(\Phi_C)$ is constant, (8) means that the number of gates in the circuit is $\Omega(s \log s)$, and this completes the proof of the theorem for $p \in (0, 1/4)$.

For proving the theorem for $p \in (0, 1/2)$ we apply Lemma 4.4, which gives

$$\frac{p}{(1-2p)^2} \geq \sum_{\ell \in S} \Pr[H_\ell] \, .$$

Using (7) this means

$$\frac{p}{(1-2p)^2} \geq \sum_{\ell \in S} \delta^{m_\ell} \, .$$

By the above arguments, this completes the proof of the theorem.

6 Block sensitivity

Let f be a Boolean function of n variables, $x = (x_1, \ldots, x_n)$ any input and S any subset of indices, $S \subset \{1, \ldots, n\}$. Denote by x^S the input obtained from x by complementing all bits with indices from S and keeping the other bits of x unchanged.

Definition 6.1 The function f is *sensitive to* S on input x if $f(x) \neq f(x^S)$. The *block sensitivity of* f *on* x is the largest number b such that there exist b disjoint sets $S_1, \ldots, S_b$ such that for all $1 \leq i \leq b$, f is sensitive to S_i on x. The *block sensitivity* of f is the maximum over all x of the block sensitivity of f on x.

This measure of complexity was introduced by Nisan in [10]. Clearly for any function

$$\text{block sensitivity} \geq \text{sensitivity} \, .$$

It is shown in [10] that for all monotone functions, the sensitivity equals the block sensitivity, but for non-monotone functions the inequality may be strict. A function with quadratic gap between sensitivity and block sensitivity is exhibited by Rubinstein [14].

Theorem 6.2 *Let ε and p be any constants so that $\varepsilon \in (0, 1/2)$, $p \in (0, 1/2)$. Let f be any Boolean function with block sensitivity b. If a circuit whose gates fail independently with fixed probability ε computes f with error probability at most p, then the number of gates of the circuit is at least $\Omega(b \log b)$.*

Proof: Let the block sensitivity of f be maximum on input z, and let $S_1, \ldots, S_b$ be disjoint sets so that for all $1 \leq i \leq b$, f is sensitive to S_i on z. We can apply the proof of Theorem 2.4 by defining B_i for $1 \leq i \leq b$ as the set of all wires originating from the inputs with indices from S_i.

Corollary 6.3 *The redundancy of the noisy computation by Boolean circuits of any function of n variables with $O(n)$ noiseless complexity and $\Omega(n)$ block sensitivity is $\Omega(\log n)$.*

7 Discussion and open problems

Note that the $O(L \log L)$ upper bound construction [9], [3], [11] works for monotone circuits as well, since it can be realized using only gates computing the majority function in addition to the gates of the original noiseless circuit. Let $L^m(f)$ be the noiseless complexity of computing the monotone function f by monotone circuits. Theorem 2.4 shows that for some functions f, $\Omega(L^m(f) \log L^m(f))$ noisy gates are necessary for the reliable computation of f by monotone circuits. Is it still true that the redundancy of the noisy computation of almost all monotone functions by monotone circuits with noisy gates is constant? Andreev [1] showed that this is true for a different failure model, where the gates of the circuit do not fail independently, but the number of faulty gates is at most $2^{o(n)}$.

Considering arbitrary circuits, it would be interesting to prove lower bounds stronger than $\Omega(n \log n)$ for the size of reliable circuits with noisy gates computing explicit functions of n variables. This might be a very difficult problem: if such a lower bound holds for the computation of a function f by unrestricted circuits with gates from a finite complete basis, then the noiseless complexity of that function must be superlinear (in n). Thus exhibiting such a function would solve another fundamental open problem.

But this question is open even for restricted models: there are no bounds proving nonconstant redundancy of noisy computation for an explicit function known to have $\Omega(n \log n)$ noiseless complexity of computation by circuits with gates computing functions from some (incomplete) finite set Φ, for example by monotone circuits.

The lower bound result looks strange if we think of our computation as part of some larger computation. More precisely, let us restrict attention to fault-tolerant Boolean circuits in which there is a notion of time: each gate has an integer (its time level) assigned to it and its output goes to a gate on the next time level. For such a fault-tolerant circuit, the lower bound result seems to imply an exponential blowup, if we apply the theorem of the present paper repeatedly to different levels. However, the theorem is generally applicable only to the very first step of such a fault-tolerant computation. Indeed, if the input x under consideration is not the original input but some intermediate result then the earlier parts of the computation could make sure that x is "good" in some sense (with high probability). We can then restrict the function to be computed to the set of good inputs. Now, the partial Boolean function defined on just the good inputs may not have any sensitivity at all. This is indeed the typical case: the good inputs are those that contain the relevant information with redundancy: the function to be computed will not therefore be changed by the change of a single input bit.

If we consider computations in which the input is allowed to be in the form of some (simple) redundant code then it is not known whether the $n \log n$ lower bound still holds. A $\log n$ width-redundancy is certainly not necessary if instead of the repetition code, a more sophisticated algebraic code is used. (See [6] where a code with constant redundancy is used.) The Boolean circuits derivable from these cellular automata constructions have a width that is only constant times larger than the width of the original (not fault-tolerant) circuit to be simulated.

It must be added that the depth of the circuits derived from [6] increases by a logarithmic factor. There is no lower-bound result saying that this latter increase is necessary, or, as it could be conjectured, that the product of the "spatial" and "time" -redundancies of a fault-tolerant computation must sometimes be logaritmic. Even the formulation of such a lower-bound hypothesis causes some difficulties since it probably must include some restriction on the error-correcting code permitted for the input, to make sure the computation is not hidden in the code.

Acknowledgements

The second author would like to thank her advisor, János Simon for his continued help and encouragement during this work. We would also like to thank László Babai and Pál Takácsi-Nagy for suggesting some changes in the earlier version of the proofs of Lemma 4.1 and Lemma 4.2, and other valuable comments.

Appendix

We sketch briefly the problems with the proof in [2].

The events H_ℓ were defined in [2] as in this paper. Instead of $\bigcup_{\ell \in S} H_\ell$ the authors of [2] considered the event that exactly one of the H_ℓ occurs, which they denoted by $\tilde{\bigcup}_{\ell \in S} H_\ell$.

As part of the proof of Lemma 3.3 in [2] the authors claimed to prove the following statement: For all $\gamma \in (0, 1/2)$, the fact that $\Pr[\tilde{\bigcup}_{\ell \in S} H_\ell] \le \gamma$ implies that

$$\Pr[\tilde{\bigcup}_{\ell \in S} H_\ell] \ge (1 - 2\gamma) \sum_{\ell \in S} \Pr[H_\ell] \,. \tag{9}$$

This statement does not hold. Consider for example the case when for all $\ell \in S$, $\Pr[H_\ell] = d$ for some $d \in (0, 1)$. As pointed out in [12] the statement of Lemma 3.3 in [2] does not hold either.

The other questionable part of the proof, as mentioned in [12], is that from

$$\Pr[C(z) \neq f(z) \mid H_\ell] \ge 1 - p \text{ for all } \ell \in S$$

the authors of [2] conclude without suggesting a proof that

$$\Pr[C(z) \neq f(z) \mid \tilde{\bigcup}_{\ell \in S} H_\ell] \ge 1 - p \,.$$

It is shown in [12] that for an arbitrary event E, $\Pr[E \mid H_\ell] \ge 1 - p$ for all $\ell \in S$ does not imply

$$\Pr[E \mid \tilde{\bigcup}_{\ell \in S} H_\ell] \ge 1 - p \,.$$

The relation $\Pr[C(z) \neq f(z) \mid \tilde{\bigcup}_{\ell \in S} H_\ell] \ge 1 - p$ does not seem to hold for the events considered in [2] either. We note that for these particular events it is possible to prove some weaker lower bounds such as:

$$\Pr[C(z) \neq f(z) \mid \tilde{\bigcup}_{\ell \in S} H_\ell] \ge 1 - \frac{p}{1 - p/(1 - \sqrt{p})^2} \,.$$

This lower bound, however, does not eliminate the difficulty of repairing (9).

References

[1] A. E. Andreev, "Circuit synthesis in complete monotone basis," *Mat. Vopr. Kibern.* 1, 1988, pp. 114-139.

[2] R. L. Dobrushin and S. I. Ortyukov, "Lower bound for the redundancy of self-correcting arrangements of unreliable functional elements," *Prob. Inf. Trans.* 13, 1977, pp. 59-65.

[3] R. L. Dobrushin and S. I. Ortyukov, "Upper bound for the redundancy of self-correcting arrangements of unreliable functional elements," *Prob. Inf. Trans.* 13, 1977, pp. 203-218.

[4] U. Feige, D. Peleg, P. Raghavan and E. Upfal, "Computing with unreliable information," In *Proc. of 22th ACM Symposium on the Theory of Computing*, 1990, pp. 128-137.

[5] A. Gál, "Lower Bounds for the Complexity of Reliable Boolean Circuits with Noisy Gates," In *Proc. of 32-nd IEEE Symposium on the Foundations of Computer Science*, 1991, pp. 594-601.

[6] P. Gács, "Self-correcting two-dimensional arrays," In Silvio Micali, editor, *Randomness in Computation*, pp. 223–326, JAI Press, Greenwich, Conn., 1989.

[7] O. B. Lupanov, "On a method of circuit synthesis," *Izv. VUZ Radiofizika* 1, 1958, pp. 120-140.

[8] D. E. Muller, "Complexity in electronic switching circuits," *IRE Trans. Electr. Comput.* 5, 1956, pp. 15-19.

[9] J. von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components," In *Automata Studies*, C. E. Shannon and J. McCarthy Eds., Princeton University Press, Princeton, NJ, 1956, pp. 329-378.

[10] N. Nisan, "CREW PRAMs and decision trees," In *Proc. of 21-st ACM Symposium on the Theory of Computing*, 1989, pp. 327-335.

[11] N. Pippenger, "On networks of noisy gates," In *Proc. of 26-th IEEE Symposium on the Foundations of Computer Science*, 1985, pp. 30-36.

[12] N. Pippenger, G. D. Stamoulis and J. N. Tsitsiklis, "On a lower bound for the redundancy of reliable networks with noisy gates," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, 1991, pp. 639-643.

[13] R. Reischuk, B. Schmeltz, "Reliable Computation with Noisy Circuits and Decision Trees – A General n log n Lower Bound," In *Proc. of 32-nd IEEE Symposium on the Foundations of Computer Science*, 1991, pp. 602-611.

[14] D. Rubinstein, "Sensitivity vs. block sensitivity of Boolean functions," to appear in *Combinatorica.*

[15] C. E. Shannon, "The synthesis of two-terminal switching circuits," *Bell Syst. Techn. J.* 28, 1949, pp. 59-98.

[16] D. Uhlig, "Reliable networks from unreliable gates with almost minimal complexity," In *Proc. of Fundamentals of Computation Theory*, Kazan, 1987, LNCS 278, Springer-Verlag, 1987, pp. 462-469.