Can Large Fanin Circuits Perform Reliable Computations in the Presence of Faults?*

Rüdiger Reischuk

Med. Universität zu Lübeck
Institut für Theoretische Informatik
Wallstraße 40, 23560 Lübeck, Germany
`reischuk@informatik.mu-luebeck.de`

August 1998

Abstract

For ordinary circuits with a fixed upper bound on the fanin of its gates it has been shown that logarithmic redundancy is necessary and sufficient to overcome random hardware faults (noise). Here, we consider the same question for unbounded fanin circuits which in the fault-free case can compute Boolean functions in sublogarithmic depth. Now the details of the fault model become more important. One may assume that only gates, resp. only wires may deliver wrong values, or that both gates and wires may behave faulty.

The fault tolerance depends on the types of gates that are used, and whether the error probabilities are known exactly or only an upper bound for them. Concerning the first distinction the two most important models are circuits consisting of *and*- and *or*-gates with arbitrarily many inputs, and circuits built from the more general type of threshold gates.

We will show that in case of faulty `and/or`–circuits as well as threshold circuits an increase of fanin and size cannot be traded for a depth reduction if the error probabilities are unknown. Gates with large fanin are of no use if errors may occur. Circuits of arbitrary size, but fixed depth can compute only a tiny subset of all Boolean functions reliably.

Only in case of threshold circuits and exactly known error probabilities redundancy is able to compensate faults. We describe a transformation from fault-free to fault-tolerant circuits that is optimal with respect to depth keeping the circuit size polynomial.

1 Introduction

John v. Neumann [N56] was one of the first to consider reliability questions in large systems like circuits and neural nets. Results of Dobrushin/Ortyukov [DO77a] and Pippenger [P85] have shown that logarithmic redundancy is sufficient to achieve optimal fault tolerance in the standard circuit model with a fixed finite set of basic gates. It is assumed that every element of the circuit works incorrectly with some

*a preliminary version has been presented at COCOON'97 (3. Ann. Int. Computing and Combinatorics Conference, August 1997, Shanghai), the preparation of this paper was supported by the Japanese Society for the Promotion of Science (JSPS) while visiting Kyushu University, Fukuoka

probability independently of the others and that there is an upper bound on these error probabilities. *Redundancy* here means the factor by which the circuit size has to be increased to make a circuit designed for a fault-free situation fault-tolerant, or more formally, the circuit size ratio between a fault-tolerant circuit and an optimal circuit in case of no faults.

That this amount of redundancy is also necessary in general has later been proved rigorously in a sequence of papers, which follow a previous attempt made by Dobrushin/Ortyukov [DO77b]. This was done by Pippenger/Stamoulis/Tsitsiklis [PST91], Gál/Gács [G91,GG94] and Reischuk/Schmeltz [RS91]. These results are essentially independent of the specific basis (for a detailed discussion see [P89]) and whether errors are assumed to occur in the gates or in the wires. To prove the lower bound on the redundancy it suffices to consider the restricted fault model in which all gates err with exactly the same probability $\epsilon > 0$. We call this **weak fault tolerance**. The upper bound construction of [DO77a] and [P85], however, works in the **stronger fault model** where the actual error probabilities of gates and wires are unknown. These probabilities may even be chosen by an adversary.

In [RS89] we have described other constructions to make circuits reliable. These methods guarantee only a small increase in the layout area of the circuits – in many cases only a constant factor.

Thus, for Boolean circuits with bounded fanin fault tolerance is quite well understood. Considering the human brain and neural networks the fault tolerance of circuits with gates of large fanin is an important question. Hajnal, Maass, Pudlák, Szegedy and Turán seem to be the only ones so far that have considered this problem [HMP93]. In their error model faults only happen at the gates of a circuit. For `and/or`–circuits they prove an upper bound $\exp O(d \log d)$ on the number of subcubes a function may depend on if it can be computed reliably in depth d.

In this paper we investigate fault-tolerant circuits of sublogarithmic depth in more detail. We will consider different bases of gates with arbitrarily large fanin and different fault models. For `and/or`–circuits and faults at the wires a lower bound will be obtained for the number of input variables a function may depend on if it can be computed reliably in bounded depth. This shows that only a small number of nondegenerated Boolean functions have fault-tolerant circuits of bounded depth. Even allowing depth $o(\log n / \log\log n)$ most Boolean functions of n variables cannot be computed by a fault-tolerant circuit based on unbounded fanin `and`- and `or`-gates. Our analysis also gives an upper bound on the deterministic, resp. probabilistic complexity of functions that can be computed in the presence of faults in bounded depth.

For threshold circuits and the weak fault model [HMP93] provides a construction to achieve fault tolerance in weighted threshold circuits. Their method uses redundancy that grows exponentially with respect to the circuit depth. Given a circuit of size g and depth d its fault-tolerant equivalent requires size $g^{O(d^2)}$. We will describe a different approach for standard threshold circuits that keeps this blowup much smaller, in particular, independent of d.

Both constructions do not work for the stronger fault model. Our second lower bound shows that fault tolerance cannot be achieved for bounded depth threshold circuits if the error probabilities are not known precisely. In this case one faces similar restrictions as for unbounded fanin `and/or`–circuits. Only a vanishing proportion of all Boolean functions can be computed reliably.

This paper is organized as follows. In the next section we define the fault models for unbounded fanin circuits. Section 3 contains the lower bound for `and/or`–circuits. Then we will present the impossibility result for strongly reliable threshold circuits. Finally, it will be shown how threshold circuits can be made weakly reliable with only a polynomial increase in size.

2 The Model

For the basic circuit terminology see, for example, Wegener's monograph [W87]. For an unbounded fanin circuit $C = (V, E)$ consisting of gates $v \in V$ and wires $e \in E$ by $size(C)$ we mean the number of wires $|E|$. We will consider unbounded fanin circuits constructed from gates of the following type (the *basis*).

Definition 1

- `and/or`–**circuits:** The basis contains `and`- and `or`-gates of arbitrary fanin; inputs of a gate may be negated.
- **threshold circuits:** For each $k, l \in \mathbb{N}$ the basis contains the following (positive) monotone threshold gate and its negation:

$$T_l^k(x_1, \ldots, x_l) \;:=\; \begin{cases} 1, & \text{if } \sum_{j=1}^{l} x_j \geq k, \\ 0, & \text{else.} \end{cases}$$ □

To provide such a circuit with the values of the input variables, special input gates are given. We will consider only circuits with a single output. Note that an `and/or`–circuit is a restricted form of a threshold circuit. Since it can be helpful to weight signals differently, several wires may run in parallel connecting the same pair of gates. Alternatively, one could assign weights to the wires. The fault tolerance of this weighted threshold circuit model will be discussed at the end.

We formalize faults/noise in a circuit C as follows.

Definition 2 Let $C_v(x)$ and $C_e(x)$ be random variables that describe the Boolean value of the gates v (resp. wires e) for input vector x. $C(x)$ is a random variable specifying the output bit computed by C on x. If the input vector x is fixed we simply write C_v instead of $C_v(x)$, and similarly C_e.

Let v be a gate realizing the function φ_v, and let $e_1, \ldots, e_l$ be its input wires originating at gates $v_1, \ldots, v_l$. Then,

$$X_v \;:=\; \varphi_v(C_{e_1}, \ldots, C_{e_l})$$

defines the Boolean value computed by v. If all its input wires operate correctly then $C_{e_i} = C_{v_i}$, thus $X_v = \varphi_v(C_{v_1}, \ldots, C_{v_l})$. Faults may change the value of a wire or a gate with a certain probability ϵ. For each gate v and each wire e there is a binary random variable B_v (resp. B_e) with $\Pr[B_v = 1] = \epsilon_v$ and $\Pr[B_e = 1] = \epsilon_e$. All random variables B_v and B_e are assumed to be stochastically independent. Then,

$$C_v \;:=\; X_v \oplus B_v \;, \quad \text{and for each wire } e \text{ originating at } v \quad C_e \;:=\; C_v \oplus B_e \;.$$

Thus the distortion of C is described by a vector of individual error probabilities $(\epsilon_u)_{u \in C}$. For an internal gate v we get

$$\begin{aligned} X_v &= \varphi_v(C_{e_1}, \ldots, C_{e_l}) \;=\; \varphi_v(C_{v_1} \oplus B_{e_1}, \ldots, C_{v_l} \oplus B_{e_l}) \\ &= \varphi_v(X_{v_1} \oplus B_{v_1} \oplus B_{e_1}, \ldots, X_{v_l} \oplus B_{v_l} \oplus B_{e_l}) \;. \end{aligned}$$

For the lower bounds to be shown below it suffices to consider restrictions of this general fault model. In the **gate fault model** only gates are assumed to be faulty, that means $B_e \equiv 0$ for all wires e. Alternatively, only wires make errors ($B_v \equiv 0$) in the **wire fault model**. □

Input gates are assumed to be fault-free, otherwise there is no chance to compute a Boolean function correctly. Thus, for an input gate v representing the input variable x_i it holds $B_v \equiv 0$ and $C_v \equiv x_i$.

One may pose the question which of these restricted models is more appropriate. For the case of bounded fanin circuits, the logarithmic lower bound on the redundancy already holds for the wire fault model, and Dobrushin/Ortyukov have described a transformation technique from the gate fault model to the general model. Their idea was to distribute portions of the error of a gate to its incoming wires. On the other hand, the upper bound constructions achieve the same redundancy bound (up to constant factors) and work for the general fault model. This shows that the wire and the gate fault model already require maximal complexity. There is neither a qualitative, nor a quantitative difference.

This property is not obvious for unbounded fanin circuits. In particular, the technique of Dobrushin/Ortyukov does not work for gates with unbounded fanin. Assuming only faults at gates with a fixed upper bound on their probability independent of the size of the gate may be too unrealistic. The more complex a gate is, i.e., the larger its fanin, the more likely one would expect faults to occur. In this respect the wire fault model is more perceptive.

Definition 3 C is said to compute a function f **weakly** $(\boldsymbol{\epsilon}, \boldsymbol{\delta})$**–reliably** if assuming that every faulty circuit element has error probability exactly ϵ, for every input vector x it holds that

$$\Pr\{C(x) = f(x)\} \;\geq\; 1 - \delta \; .$$

If C yields the value $f(x)$ with probability at least $1-\delta$ for any vector of error probabilities with entries from the real interval $[0, \epsilon]$ then it is **strongly** $(\boldsymbol{\epsilon}, \boldsymbol{\delta})$**–reliable**. □

For the lower bounds we consider any pair of error/reliability probabilities $\epsilon, \delta \in (0, 1/2)$. Unless one restricts to wire faults only the positive results require $\delta > \epsilon$ since with probability ϵ the final output gate can be faulty and then change the result of the whole circuit. In general, these probabilities will be treated as given constants. In some cases, to simplify the statements of the results we hide their influence on the complexity bounds in the O-notation, in particular the dependence on the reliability parameter δ will be neglected.

Definition 4 A class of Boolean functions is said to be **computable strongly (resp. weakly) reliably** if for every small error probability $\epsilon > 0$ there exists a reliability value $\delta < 1/2$ such that for each element f in this class one can find a circuit C that computes f strongly (resp. weakly) (ϵ, δ)–reliably. In addition, it is required that when ϵ converges to 0 the sequence of δ's should also converge to 0.

One could also consider an *intermediate model* between strong and weak reliability where there is some uncertainty α about the error probabilities, i.e., every probability lies in the interval $[\epsilon - \alpha, \epsilon]$. The lower bound for the strong model shown below can be extended to this case. Now instead of the maximal error probability ϵ the uncertainty α matters. This generalization is quite straightforward and we will not further elaborate on it.

The main reason for distinguishing between weak and strong fault tolerance is the following property:

Lemma 1 *Let C be an arbitrary circuit that computes a function f (ϵ, δ)–reliably in the strong sense for some arbitrary ϵ and some $\delta < 1$. Then in the fault-free case C is a deterministic circuit for f.*

Proof: Consider the case where all individual error probabilities are set to 0. Then the output of C is a constant, and $\Pr\{C(x) = f(x)\} \;\geq\; 1 - \delta > 0$ implies $C(x) \equiv f(x)$. ∎

This property does not necessarily hold for weak fault tolerance since the random noise may be "misused" to generate some kind of random bits (see [P85]). In this case, any Boolean function can be "computed" with error probability close to $1/2$ in a trivial way by just tossing coins ($1/2$ may not be achievable exactly if ϵ is not a multiple of a negative power of 2). Thus, for weak reliability one should restrict δ to values smaller than $1/2$.

3 The Lower Bound for `and/or`–Circuits

Our first result will show that unbounded fanin `and/or`–gates are extremely sensitive to random faults. Bounded depth circuits built from such gates can compute only very simple functions. Technically speaking, large fanin gates of such type are of very little use in case of faults.

Proposition 1 *Let f be a Boolean function that in the wire fault model can be computed by a weakly (ϵ, δ) –reliable* `and/or`*–circuit C of depth d . Then, for every $\delta' > \delta$, there exists a weakly (ϵ, δ') –reliable* `and/or`*–circuit C' for f with the same depth, but fanin bounded by $O(\epsilon^{-1}\,(d\,\log d\;-\;\log(\delta'-\delta)))$.*

Proof: Let λ be the smallest natural number larger than 1 satisfying

$$(\lambda-1)^{d-1}(1-\epsilon)^{\lambda}\;\leq\;\delta'-\delta\;.$$

A simple calculation shows that λ is bounded by

$$\lambda\;\leq\;O\left(\frac{d\,\log d+\log(\delta'-\delta)^{-1}}{\log(1-\epsilon)^{-1}}\right)\;\leq\;O\left(\frac{d\,\log d\;-\;\log(\delta'-\delta)}{\epsilon}\right)\;.$$

We replace each gate with fanin at least λ by a constant gate with value 1 in case of an `or`–gate and value 0 in case of an `and`–gate to get a new circuit C' .[1] For any input x it holds

$$|\Pr\{C(x)=f(x)\}-\Pr\{C'(x)=f(x)\}|\;\leq\;\delta'-\delta\;.$$

To see this inequality, let v' be a constant value gate in C' replacing gate v of fanin $l \geq \lambda$ in C . If v is an `and`–gate then

$$\Pr\{C_v=1\}\;\leq\;(1-\epsilon)^{l}\;\leq\;(1-\epsilon)^{\lambda}\;.$$

This holds because $\epsilon < 1/2$ and in order to produce a 1 at v , all incoming wires have to supply the value 1. Each such event occurs with probability at most $1-\epsilon$. For the corresponding gate v' in C' , this probability is 0.

Similarly, in case of an `or`–gate

$$\Pr\{C_v=0\}\;\leq\;(1-\epsilon)^{\lambda}\;,$$

while $\Pr\{C'_{v'}=0\}\;=\;0$. Let us say that v' *deviates* from v if $C_v \neq C'_{v'}$. Hence, the probability for such an event is at most $(1-\epsilon)^{\lambda}$.

If gate v at depth h has fanin less than λ its corresponding gate v' in C' is the same. v' has at most $(\lambda-1)^{h-1}$ predecessor gates that have been set to a constant value. In order for v' to compute a value different from v at least one of these constant value gates must deviate from its original. This happens with probability at most

$$(\lambda-1)^{h-1}(1-\epsilon)^{\lambda}\;.$$

Thus, the output gate of C' deviates from that of C with probability at most

$$\begin{aligned}
\Pr\{C(x)\neq C'(x)\}\;&\leq\;(\lambda-1)^{d-1}(1-\epsilon)^{\lambda}\;\leq\;\delta'-\delta\;,\qquad\text{and}\\
\Pr\{C'(x)\neq f(x)\}\;&\leq\;\Pr\{[C'(x)\neq C(x)]\;\vee\;[C(x)\neq f(x)]\}\\
&\leq\;\Pr\{C'(x)\neq C(x)\}\;+\;\Pr\{C(x)\neq f(x)\}\;\;\leq\;\delta'\;.\qquad\blacksquare
\end{aligned}$$

Treating the reliability parameters as constants, the depth and fanin bounds imply that the size of C' is at most

$$n[\epsilon,d|\;:=\;O\left(\frac{d}{\epsilon}\,\log d\right)^{d}\;\leq\;\left(\frac{d}{\epsilon}\right)^{O(d)}\;,$$

in particular there are at most that many input gates that have a connection to the output gate. It is not clear whether this size bound and the bound $O(d\log d)$ for the fanin are best possible. We believe that the fanin bound can be improved to $O(d)$.

[1] C' can be further simplified since in an `and/or`–circuit constant gates can be removed: either they have no influence on a successor or they set a successor to a constant value, too.

If δ is suitably larger than ϵ then the error probability of C' can be reduced from δ' to δ by standard majority voting techniques. This gives a bounded fanin circuit that achieves the same reliability δ as C and for which the depth (resp. size) is larger only by a small additive constant (resp. a small constant factor).

As discussed above, this result on weak reliabilty is only interesting for values $\delta < 1/2$. Thus, let us fix such a δ. For the output gate of such a circuit and its direct predecessors one gets an even better fanin bound. For example, the fanin l of the final output gate has to fulfill $(1-\epsilon)^l \geq 1-\delta > 1/2$, otherwise a single fault on one of its input wires would already impose an incorrect result of the whole circuit. This implies $l < (\log(1-\epsilon)^{-1})^{-1} \approx \epsilon^{-1}$.

If a circuit has to achieve reliability less than $1/2$ for a given function f any input that can influence the value of f has to be connected to the output gate. Otherwise, changing this input bit in a critical input vector[2] does not change the probability distribution of the result. Hence, on this input vector or its companion the circuit computes a wrong result with probability at least $1-\delta > 1/2 > \delta$. Hence, Proposition 1 implies

Theorem 1 *If a Boolean function f can be computed by a weakly (ϵ, δ)–reliable* `and`/`or`*–circuit of depth d in the wire fault model with $\delta < 1/2$ then it can also be computed by a fault-tolerant circuit of depth d, size $n[\epsilon, d|$, and fanin $O(\epsilon^{-1} d \, \log d)$. In particular, f depends on at most $n[\epsilon, d|$ many arguments.*

The construction in the proof of Proposition 1 also works for the strong reliability model. Construct C' from a given circuit C as above replacing gates of large fanin by constants. Given an arbitrary vector of error probabilities for C' we have to show that the correct result will be obtained with probability at least $1-\delta'$. Consider that fault vector for C extended from the one for C' where wires running into a gate of large fanin – those are missing in C' – have maximal error probability ϵ. By assumption, since C' is strongly (ϵ, δ)–reliable it will compute the correct result with probability at least $1-\delta$. Since the deviation between C and C' is at most $\delta' - \delta$, C' achieves the required reliability. Thus we have shown

Proposition 2 *Let f be a Boolean function that in the wire fault model can be computed by a strongly (ϵ, δ)–reliable* `and`/`or`*–circuit C of depth d. Then, for every $\delta' > \delta$, there exists a strongly (ϵ, δ')–reliable* `and`/`or`*–circuit C' for f with the same depth, but fanin bounded by $O(\epsilon^{-1} d \, \log d)$.*

In the fault-free case, if a function f is computable by a circuit of depth d it can also be computed by a formula, i.e. a circuit with fanout 1, of the same depth. The proof technique duplicating gates does not simply work for faulty circuits because of dependencies/independencies. Proposition 2 together with Lemma 1 yields

Theorem 2 *A necessary condition for a Boolean function to be computable strongly reliably with respect to wire faults by an unbounded fanin* `and`/`or`*–circuit in depth d is that it depends on at most $\exp O(d \log d)$ arguments and has a fault-free circuit of depth d, fanin bounded by $O(d \log d)$, and size $\exp O(d \log d)$. This fault-free circuit can even be chosen as a formula with the same complexity bounds.*

In the case of weak fault tolerance we can show a corresponding result for probabilistic circuits.

Theorem 3 *Let f be a Boolean function computable in case of wire faults by a weakly (ϵ, δ)–reliable* `and`/`or`*–circuit C of depth d and let $\delta' > \delta$. Then without any noise there exists a probabilistic circuit C' of depth at most $3d$, fanin $O(d \log d)$ and size $\exp O(d \log d)$ with error probability bounded by δ'.*

[2] vector $x = x_1 \ldots x_i \ldots x_n$ is critical for f and input bit i if $f(x) \neq f(x_1 \ldots \bar{x_i} \ldots x_n)$, where $\bar{x_i}$ denotes the complement of x_i.

Proof: The idea is to simulate the weakly fault-tolerant circuit C by constructing random bits that take the value 1 with probability $\epsilon' \approx \epsilon$. We start with the construction above to get an (ϵ, δ'')–reliable circuit C'' with $\delta'' = \frac{\delta+\delta'}{2}$ and fanin at most $l \leq O(d \log d)$. C'' has at most $O(l^d)$ wires. Each wire e of C'', which flips the value X_v from its origin v with probability exactly ϵ, is replaced by two wires with a gate v_e in the middle that computes the function $X_v \oplus z$ where z is a random bit with $\Pr\{z = 1\} = \epsilon'$. In order to turn this into an `and`/`or`–circuit we then may replace each v_e by an equivalent depth 2 circuit based on $\vee, \wedge$. This defines a probabilistic circuit C' which deviates from C'' with probability at most $O(l^d \cdot |\epsilon - \epsilon'|)$. In order to achieve error probability δ' for C' it suffices to bound this quantity by $\frac{\delta'-\delta}{2}$, that means

$$|\epsilon - \epsilon'| \ \leq \ \pi \ := \ (\delta' - \delta) \cdot \exp -O(d \log d) \ .$$

ϵ can be approximated within this precision by tossing $\log 1/\pi \ = \ O(d \log d)$ random coins. The result of this experiment can then be computed in depth 2 using `and`- and `or`-gates with fanin bounded by $O(d \log d)$. ∎

Unbounded fanin circuits have been introduced in order to compute Boolean functions in very small depth. For the fault-free case it is well known that depth 2 is already sufficient. Our results imply that circuits with faults cannot achieve such a speedup. The depth has to grow almost logarithmically with respect to the number of arguments the function depends on. Since among all Boolean functions of n arguments at most a fraction $2^{-2^{n-1}+\log n}$ does not depend on all its arguments we get as a

Corollary 1 `and`/`or`*–circuits with gates of unbounded fanin require depth at least* $\Omega(\log n \ / \ \mathrm{loglog} n)$ *for almost all* n*-ary Boolean functions for a weak (or strong) reliable computation in case of wire faults.*

Since almost all n-ary Boolean functions require formula size $\Omega(2^n \ / \ \log n)$ [We87], Theorem 2 implies further

Corollary 2 *Strongly reliable* `and`/`or`*–circuits require depth at least* $\Omega(n \ / \ \log n)$ *for almost all* n*-ary Boolean functions even if we restrict to wire faults and put no bound on the maximal fanin.*

Similar results can be obtained for the gate fault model. In this case the gates in depth 1, the first layer, make an essential difference: each such gate has distortion ϵ independent of its fanin. Note that a gate in depth 1 computes a monomial or clause of the input variables. All claims above hold if we replace the bounds on the number of arguments by a bound on the number of such monomials and clauses, and if in the size bound we do not count wires from input gates (see [HMP93]). Equivalently, the size now refers to the number of internal gates.

Again, a simple counting argument shows that only a tiny fraction of all n argument Boolean functions can be computed by such circuits of depth $o(\log n \ / \ \mathrm{loglog} n)$.

In the gate fault model, a strongly reliable circuit of depth d can be replaced by a deterministic formula of depth d, where the first layer has fanin up to n and the remaining ones at most $O(d \log d)$. Counting the number of such formulas shows that almost all n-ary Boolean functions require size $\Omega(2^n/n)$. Thus, we get

Corollary 3 *Strongly reliable* `and`/`or`*–circuits require depth at least* $\Omega(n \ / \ \log n)$ *for almost all* n*-ary Boolean functions even if we restrict to gate faults and put no bound on the maximal fanin.*

4 Strongly Reliable Threshold Circuits

A gate v of a circuit is considered to depend on an input variable x_i if there is a path from the corresponding input gate to v. For certain input vectors changing the value of x_i may then lead to a change of the value at v. A threshold gate with a large fanin may still have this property if one of its input wires connects to that input gate. But it is very likely that a single change of x_i will hardly be noticed because of those many potential faults that may occur on the other wires running into v. This means the probability distribution of the two random variables $X_v(x)$ and $X_v(x')$, where x' is obtained from x by changing the i-th coordinate, are almost identical.

We try to capture this property be defining the notion of *strong dependence,* which means that an input x_i is able to influence a gate substantially even when faults are present. It will be shown that a gate cannot strongly depend on too many variables. Hence, a reliable threshold circuit can essentially be built only from gates of moderately large fanin.

Definition 5 For the notion of strong dependence two parameters

$$\boldsymbol{L} := c_1 \log(1/\epsilon) \cdot d/\epsilon \qquad \text{and} \qquad \boldsymbol{\zeta} := \epsilon/16$$

will be used, where the constant $c_1 > 0$ will be chosen later. An input gate **strongly depends** only on the variable it represents. For an internal gate v of indegree l let $\boldsymbol{\Gamma_i}$ be the number of direct predecessors that strongly depend on x_i. Then v **strongly depends** on x_i iff $\Gamma_i > 0$, and in addition $l \leq L$ or $\Gamma_i \geq \zeta\, l$. □

The intuition behind this definition says that if these properties are not fulfilled then there are many wires running into v and almost all do not depend strongly on x_i. Then, faults occurring on such wires are very likely to outbalance the total number Γ_i of wires coming from gates that strongly depend on x_i.

Lemma 2 *A gate at depth h strongly depends on at most*

$$\max\{\zeta^{-1}, L\}^h \;\leq\; \exp O(h \cdot \log(d/\epsilon))$$

many input gates (input variables).

Proof: This bound can easily be shown by induction on h. Let v be a gate in depth h with fanin l. If every predecessor strongly depend on at most $m = \max\{\zeta^{-1}, L\}^{h-1}$ many input gates and $l \leq L$ then v strongly depends on at most $L \cdot m$ many inputs. Otherwise, there are at most $l \cdot m$ pairs of a predecessor u and an input x_i such that u depends strongly on x_i. In order for v to depend strongly on x_i the number of such u's has to be at least $\zeta\, l$. Hence, there can be at most $\zeta^{-1} \cdot m$ many different such x_i. ∎

Define

$$n[\epsilon, d| \;:=\; \max\{\zeta^{-1}, L\}^d \;\leq\; \left(\frac{d}{\epsilon}\right)^{O(d)} .$$

Theorem 4 *Strongly (ϵ, δ)–reliable threshold circuits of depth d can compute only functions that depend on at most $n[\epsilon, d|$ many variables. This property already holds for the restricted wire fault model.*[3]

[3] This impossibility result contrasts to Th. 5.8 in [HMP93], where a fault-tolerant transformation for the strong gate fault model is indicated. However, this only works under the (unrealistic) assumption that the error probability decreases with the fanin (as $1/\lambda$).

Proof: Assume that f depends on more than $n[\epsilon, d|$ inputs and let C be a strongly reliable circuit for f. According to Lemma 2, there is an input variable x_i on which the output of the circuit does not depend strongly. Let x and x' be two input vectors which differ only at position i such that $f(x) \neq f(x')$.

Proposition 3 *If a gate v at depth h does not depend strongly on x_i then for any pair of inputs $x^{(0)}$ and $x^{(1)}$ that differ only in the i-th coordinate there exist error probabilities ϵ_j for the wires running into v and a Boolean value y_v such that for both $x^{(\alpha)}$ and $X_v^\alpha := X_v(x^{(\alpha)})$ holds*

$$\Pr\{X_v^\alpha \neq y_v\} \;\leq\; \boldsymbol{p_h} := (\epsilon/8)^{d-h+1} .$$

This Proposition implies Theorem 4. For the output gate v of the circuit at depth d it means

$$\Pr\{X_v \neq y_v\} \;\leq\; p_d \;=\; \frac{\epsilon}{8}$$

for both input vectors x and x'. But for one of them the value y_v is wrong. Thus, for this input the circuit gives the correct result with probability at most $\epsilon/8 < \frac{1}{2} < 1 - \delta$. ∎

Proof of Proposition 3: By induction on the depth h exploiting only wire faults.
Define $\boldsymbol{\Gamma} := \Gamma_i$, and call a gate **strong** if it strongly depends on x_i, otherwise **weak**. Let us denote by $\boldsymbol{G^+}$ and $\boldsymbol{G^-}$ the set of strong (resp. weak) gates.

For weak input gates choose y_v equal to the value of this input bit, which is different from x_i and thus equal for both x^α. Then the probability $\Pr\{X_v^\alpha \neq y_v\}$ is actually 0.

Now, let v be a weak gate in depth $h > 0$ with threshold k and incoming wires $e_1, \ldots, e_l$ from predecessors $v_1, \ldots, v_l$ (with $B_{v_j} \equiv 0$). To simplify the notation we will write X_j^α instead of $X_{v_j}^\alpha$, y_j instead of y_{v_j}, C_j instead of C_{e_j} and B_j for the random fault on wire e_j. Assume that every weak predecessor v_j satisfies

$$\Pr\{X_j^\alpha \neq y_j\} \;\leq\; p_{h-1} .$$

The output value of v is determined by the sign of

$$Y^\alpha \;:=\; \sum_{j=1}^{l} X_j^\alpha \oplus B_j \;-\; k \;=\; \sum_{v_j \in G^+} X_j^\alpha \oplus B_j \;+\; \sum_{v_j \in G^-} (X_j^\alpha \oplus y_j) \oplus (y_j \oplus B_j) \;-\; k .$$

From the definition of strong dependence it follows

$$0 \;\leq\; S_0 \;:=\; \sum_{v_j \in G^+} (X_j^\alpha \oplus B_j) \;\leq\; \sum_{v_j \in G^+} 1 \;=\; \Gamma \;\leq\; \zeta\, l .$$

For $0/1$-values the identity $x \oplus b \;=\; x + (-1)^x\, b$ holds, or generalizing to larger sums

$$(x \oplus y) \oplus (y \oplus b) \;=\; y + (-1)^y\, b + (-1)^{y \oplus b}(x \oplus y) .$$

Then, the sum over G^- in the expression for Y^α can be split into 3 sums $S_1 + S_2 + S_3$ as

$$\sum_{v_j \in G^-} y_j - k \;+\; \sum_{v_j \in G^-} (-1)^{y_j} B_j \;+\; \sum_{v_j \in G^-} (-1)^{y_j \oplus B_j} (X_j^\alpha \oplus y_j) .$$

The first term $S_1 = \sum y_j - k$ has a fixed value independent of the input and the error probabilities.

The third sum S_3 can be bounded in absolute value by $\sum X_j^\alpha \oplus y_j$. By induction hypothesis, with probability at most p_{h-1} the values X_j^α and y_j are different, thus the expectation of this sum is bounded by $|G^-| \cdot p_{h-1}$. For $s \geq 1$ let F_s denote the event that the absolute value of S_3 is bounded by

$$\Big|S_3\Big| \;=\; \Big|\sum_{v_j \in G^-} (-1)^{y_j \oplus B_j} (X_j^\alpha \oplus y_j)\Big| \;\leq\; s \cdot |G^-| \cdot p_{h-1} \;.$$

By Markov's inequality,

$$\Pr\{\neg F_s\} \;\leq\; 1/s \;.$$

It remains to estimate the second sum $S_2 \;=\; \sum (-1)^{y_j} B_j$. It will be shown that it dominates the rest. By choosing the error probabilities ϵ_j for the B_j appropriately we will achieve that the whole expression for Y^α can be bounded away from 0 independent of α . For $\beta \in \{0,1\}$ let $G_\beta^- \subseteq G^-$ be the subset of v_j with $y_j = \beta$, and J be the larger of these sets. Thus $|J| \;\geq\; |G^-|/2$. We set $\epsilon_j = 0$ for $v_j \in G^- \setminus J$.

Scenario 1: For $v_j \in J$ the error probabilities ϵ_j are chosen as 0, too. Then $S_2 = 0$ with probability 1.

Scenario 2: Alternatively, if we choose $\epsilon_j \;=\; \epsilon$ maximal for all $v_j \;\in\; J$ then the expectation of the absolute value of S_2 is at least

$$\sum_{v_j \in J} \epsilon_j \;=\; \epsilon\, |J| \;\geq\; \epsilon\, |G^-| \;/\; 2 \;.$$

Let F denote the event that the absolute value of S_2 is bounded as follows:

$$|S_2| \;=\; |\sum_{v_j \in G^-} (-1)^{y_j} B_j| \;\;\geq\;\; \frac{7}{8}\epsilon \frac{|G^-|}{2} \;.$$

Using the Chernoff Bound one can deduce for a suitable constant $c > 0$

$$\begin{aligned} \Pr\{\neg F\} \;&\leq\; \exp(-c\,\epsilon \cdot |G^-|) \;\leq\; \exp(-c\,\epsilon \cdot (1-\zeta)\; l) \;\leq\; \exp\left(-c\,\frac{15}{16}\,\epsilon\, L\right) \\ &\leq\; \exp\left(-c\,\frac{15}{16}\,c_1 \log(8/\epsilon)\cdot d\right) \;\leq\; \frac{1}{5}\left(\frac{\epsilon}{8}\right)^d \end{aligned}$$

if c_1 , introduced in the definition of strong dependence, is chosen sufficiently large. If we set $s := 5\,\epsilon \;/\; 32\, p_{h-1}$ then

$$\Pr\{\neg F_s \;\vee\; \neg F\} \;\leq\; \frac{32}{5}\frac{p_{h-1}}{\epsilon} \;+\; \frac{1}{5}\left(\frac{\epsilon}{8}\right)^d \;\leq\; \frac{8}{\epsilon}\left(\frac{\epsilon}{8}\right)^{d-h+2} \;=\; p_h \;.$$

Thus, if $F_s \wedge F$ holds then we can bound the sum $S_0 + S_1 + S_3$ by

$$S_1 - s \cdot |G^-| \cdot p_{h-1} \;\leq\; S_0 + S_1 + S_3 \;\leq\; \zeta\, l + S_1 + s \cdot |G^-| \cdot p_{h-1} \;.$$

In other words, the range of this sum is bounded by

$$\zeta\, l + 2\, s \cdot |G^-| \cdot p_{h-1} \;\leq\; \frac{\epsilon}{16}\, l + \frac{5}{16}\, \frac{\epsilon}{p_{h-1}} \cdot l \cdot p_{h-1} \;=\; \frac{3}{8}\,\epsilon\, l \;.$$

On the other hand, S_2 satisfies the lower bound

$$\frac{7}{8}\,\epsilon\, \frac{|G^-|}{2} \;\geq\; \frac{7}{16}\,\epsilon\, \frac{15}{16}\, l \;>\; \frac{3}{8}\,\epsilon\, l \;.$$

If the critical value 0 is not in the range of $S_0 + S_1 + S_3$ then we use scenario 1. Thus, independent of α with probability at least $1 - p_h$ the value Y^α lies in an interval that does not contain 0 . As the value y_v for gate v we choose the result computed by v in these cases.

If the range of $S_0 + S_1 + S_3$ contains 0 then we apply scenario 2. It shifts the range of Y^α away from 0 . Choose y_v correspondingly. This proves Prop. 3. ∎

Corollary 4 *Almost all n -ary Boolean functions require strongly fault-tolerant threshold circuits of depth at least $\Omega(\log n \;/\; \mathrm{loglog} n)$.*

5 Weakly Reliable Threshold Circuits

The case of weakly reliable threshold circuits differs from all previously studied situations. In this model, arbitrary circuits *can* be made reliable with a moderate amount of additional hardware. Let us first restrict to the wire fault model.

Theorem 5 *Let f be a function that is computable in the fault-free case by a threshold circuit of at most g gates, e wires and fanin λ. Then for the wire fault model with any $\epsilon < 1/4$ and arbitrary $\delta > 0$ there exists a weakly (ϵ, δ)–reliable threshold circuit for f of the same depth and number of gates. The number of wires and the fanin increase by a factor $O(\lambda \log g)$.*

Proof: The idea is to duplicate each wire r times for a suitable redundancy factor $r \leq O(\lambda \log g)$. Let v be a gate with fanin l and threshold k and $y_1, \ldots, y_l$ be the outputs of its direct predecessor gates $v_1, \ldots, v_l$. The fanin increases by the factor r when feeding the r copies of each wire from v_i to v. This way we get the new fault-tolerant gate v'. The summation of the input signals at v' gives

$$S(v') \;=\; \sum_{i=1}^{l} \sum_{j=1}^{r} \; y_i \oplus B_{i,j} \;,$$

where $B_{i,j} = 1$ iff a fault occurs in the j-th wire from v_i to v'. For a given input x let m denote the number of predecessors with $y_i = 1$. Then the expectation of $S(v')$ can be estimated by

$$E[S(v')] \;=\; r \cdot (m(1-\epsilon) + (l-m)\epsilon) \;=\; r \cdot (m + (l-2m)\epsilon) \;.$$

In the critical region around the threshold k this expression evaluates for $m = k-1$ to

$$E_{k-1} \;=\; r \cdot (k - 1 + (l - 2k + 2)\epsilon) \;,$$

resp. to

$$E_k \;=\; r \cdot (k + (l-2k)\epsilon)$$

for $m = k$. Thus, the difference is

$$E_k - E_{k-1} \;=\; \Delta \;:=\; r(1-2\epsilon) \;.$$

To define the threshold k' for v' we select the middle between the two expectations, that is

$$E_{k-1} + \Delta/2 \;=\; E_k - \Delta/2 \;=\; r \cdot \left(k + (l-2k)\epsilon - (\frac{1}{2} - \epsilon) \right) \;,$$

and set $k' := \lceil E_{k-1} + \Delta/2 \rceil$. Now in order to guarantee error probability at most δ/g at gate v' it suffices to achieve

$$\Pr\left\{ |S - E[S]| \geq \frac{\Delta}{2} \right\} \;\leq\; \frac{\delta}{g} \;.$$

For $\alpha \in \{0,1\}$ define

$$S_\alpha \;:=\; \sum_{i:\; y_i = \alpha} \; \sum_{j=1}^{r} y_i \oplus B_{i,j} \;.$$

S_0 as the sum of $r(l-m)$ independent and identically distributed binary variables, which take the value 1 with probability ϵ, is binomially distributed with expectation $E[S_0] = r(l-m)\epsilon$. Similarly, $r \cdot m - S_1$ consists of rm terms and has expectation $r\, m\, \epsilon$.
We will guarantee

$$\Pr\left\{ |S_0 - E[S_0]| \geq \frac{\Delta}{4} \right\} \;\leq\; \frac{\delta}{2g} \qquad \text{and} \qquad \Pr\left\{ |S_1 - E[S_1]| \geq \frac{\Delta}{4} \right\} \;\leq\; \frac{\delta}{2g} \;.$$

By Chernoff's bound, choosing $r = c\, l \log(g/\delta)$ for a suitable constant $c \geq 1$ makes this probability that small since

$$\Pr\left\{|S_0 - E[S_0]| \geq \frac{\Delta}{4}\right\} \;\leq\; 2\exp\left(-\frac{\Delta^2}{48E[S_0]}\right) \;=\; 2\exp-\left(\frac{r}{l-m}\;\frac{(1-2\epsilon)^2}{\epsilon}\right)\;.$$

Thus,

$$\Pr\{C_{v'}(x) \neq C_v(x)\} \;\leq\; \delta/g\;.$$

Summing up over all gates of C gives $\Pr\{C(x) \neq f(x)\} \;\leq\; \delta$. ∎

This result implies in particular that functions like `MAJORITY` can be computed reliably in constant depth and polynomial size. It has been shown for the fault-free case that `and/or`–circuits require exponential size to perform this task in constant depth (see, for example, Corollary 3.12 in [BS90]) . Theorem 2 implies that in case of faults `and/or`–circuits cannot solve this task at all, they require depth $\Omega(\log n \;/\; \mathrm{loglog}n)$.

Corollary 5 *In the weakly fault-tolerant constant depth circuit model* `and/or`*–circuits cannot simulate threshold circuits.*

Extending this construction gives an upper bound for the general fault model. Again redundancy $r = O(\lambda \log g)$ will be used, now for fanin and gates.

Theorem 6 *Let f be a function that is computable in the fault-free case by a threshold circuit of at most g gates, e wires and fanin λ . In the general fault model, for any $\epsilon < 1/8$ and arbitrary $\delta > 0$ there exists a weakly $(\epsilon, \epsilon + \delta)$ –reliable threshold circuit for f of the same depth with $O(\lambda g \log g)$ gates and fanin $O(\lambda^2 \log g)$.*

Proof: If also gates may become faulty the events that different wires originating from the same gate supply wrong values are quite dependent. Thus, instead of simply duplicating wires we make r copies of each gate. If in the original circuit u is connected to v in the fault-tolerant design there is a wire from every copy of u to every copy of v . Again, the fanin of gates increases by the factor r . Now consider the values $y_{i,j}$ computed by the copies $v_{i,j}$ of a direct predecessor gate v_i of v . Then a copy v_a of v will receive the value

$$y_{i,j} \oplus B_{i,j} \oplus B_{i,j,a}$$

from $v_{i,j}$, where $B_{i,j}$ models the fault at $v_{i,j}$ and $B_{i,j,a}$ the fault on the connecting wire. Let us say that gate v_i is okay if all the r values $y_{i,j}$ equal C_{v_i} and at most a fraction 2ϵ of the $v_{i,j}$ gates are faulty, that is $B_{i,j} = 1$. Assume that all predecessors v_i of v are okay. Then similar to above choosing r slightly larger one can guarantee that v is not okay with probability less than δ/g , that is a copy of v will receive too many wrong values from its input wires with probability less than δ/gr . Thus, all gates will be okay simultaneously with probability at least $1-\delta$. To estimate the fault tolerance of this circuit one has to add the error probability ϵ of the final output gate, which proves the claim. ∎

Note that this construction increases the number of wires by a factor of r^2 . For the gate fault model [HMP93] give a different analysis how to achieve weak reliability. The redundancy there grows exponentially with the depth.

6 Conclusion And Open Problems

Making circuits with large fanin gates fault-tolerant has turned out to be more complicated than in the case of small fanin. In most variations of the model reliable constant depth circuits can compute only very simple functions. For `and/or`–circuits of depth d there is a limit $O(\epsilon^{-1} d \log d)$ on the fanin that can effectively be used in case of faults. We conjecture that this bound can be lowered further. So far, we have not found an example where fanin larger than $O(\epsilon^{-1})$ helps significantly.

For strongly reliable threshold circuits we have got the bound $\exp O(d \log d)$ on the number of input variables on which the circuit may depend on even if only wires may be faulty. We believe that a similar bound holds for the restricted gate fault model.

One may also consider a model in which wires, in addition, carry weights (weighted threshold circuits). For polynomially bounded weights the analysis above can be extended to yield the same lower bound (up to constant factors). In the case of arbitrary weights the analysis seems to be significantly more complicated. Hofmeister has recently described a simple construction that replaces exponentially bounded weighted threshold circuits by polynomially bounded at the expense of increasing the depth by 1 [H96], which simplifies previous work [GHR92,GK93]. However, this construction does not seem to translate directly into fault-tolerant circuit designs.

Finally, in the weak model threshold circuits can be made arbitrarily fault-tolerant by moderate redundancy. This indicates a fundamental difference between both fault models, which has not been observed for bounded fanin circuits.

Extending these results to other kind of gates, one first notices that all we have exploited to make threshold gates weakly reliable is the following. They are symmetric and counting the number of 1-inputs they have a range of certain size where on the one half the output is 0 and on the other half it is 1. The other extreme of symmetric gates are `mod` m gates for some constant m, where the output value alternates in a continuous fashion. We conjecture that they are also useless for reliable computation within small depth. In particular, parity gates just by themselves or in combination with `and-/or-`-gates seem to be of little value. Even in combination with threshold gates it is not clear whether a large fanin `mod` m gate can be exploited in case of faults.

From a practical and biological point of view this may indicate that `mod` m-, `and-`-, and `or-`-gates of large fanin are not advantageous computing devices because of the incapability to handle statistically distributed noise. Threshold gates, however - even with some imprecision at the threshold - can be used to compensate such faults.

7 References

[BS90] R. Boppana, M. Sipser, *The Complexity of Finite Functions,* in J. v. Leeuwen (ed.), Handbook of Theoretical Computer Science, Vol. A, Algorithms and Complexity, Elsevier, 1990, 759-804.

[DO77a] R. Dobrushin, S. Ortyukov, *Lower Bound for the Redundancy of Self-Correcting Arrangements of Unreliable Functional Elements,* Prob. Inf. Trans. 13, 1977, 59 – 65.

[DO77b] R. Dobrushin, S. Ortyukov, *Upper Bound for the Redundancy of Self-Correcting Arrangements of Unreliable Functional Elements,* Prob. Inf. Trans. 13, 1977, 203 – 218.

[G91] A. Gál, *Lower Bounds for the Complexity of Reliable Boolean Circuits with Noisy Gates,* Proc. 32. IEEE Symp. on Foundations of Computer Science, FOCS'91, 1991, 602 – 611.

[GG94] A. Gál, P. Gács, *Lower Bounds for the Complexity of Reliable Boolean Circuits with Noisy Gates,* IEEE Tr. Inf. Theory 40, 1994, 579-583.

[GHR92] M. Goldmann, J. Håstad, A. Razborov, *Majority Gates vs. General Weighted Threshold Gates,* Proc. 7. Structure in Complexity Theory, STRUCTURES'92, 1992, 2 – 13.

[GK93] M. Goldmann, M. Karpinski, *Simulating Threshold Circuits by Majority Circuits,* Proc. 25. ACM Symp. on the Theory of Computing, STOC'93, 1993, 551 – 560.

[H96] T. Hofmeister, *A Note on the Simulation of Exponential Threshold Weights,* Proc. 2. Int. Conf. Computing and Combinatorics, COCOON'96, Springer LNCS 1090, 1996, 136 – 141.

[HMP93] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, G. Turán, *Threshold Circuits of Bounded Depth,* J. CSS 46, 1993, 129 – 154.

[N56] J. von Neumann, *Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components,* in C. Shannon, J. McCarthy (Ed.), Automata Studies, Princeton University Press, 1956, 43 – 98.

[P85] N. Pippenger, *On Networks of Noisy Gates,* Proc. 26. IEEE Symp. on Foundations of Computer Science, FOCS'85, 1985, 30 – 38.

[P89] N. Pippenger, *Invariance of Complexity Measures for Networks with Unreliable Gates,* J. ACM 36, 1989, 531 – 539.

[PST91] N. Pippenger, G. Stamoulis, J. Tsitsiklis, *On a Lower Bound for the Redundancy of Reliable Networks with Noisy Gates,* IEEE Tr. Inf. Theory 37, 1991, 639-643.

[RS89] R. Reischuk, B. Schmeltz, *Area Efficient Methods to Increase the Reliability of Boolean Circuits,* Proc. 6. GI-AFCET Symp. on Theoretical Aspects of Computer Science, STACS'89, Springer LNCS 349, 1989, 314 – 326.

[RS91] R. Reischuk, B. Schmeltz, *Reliable Computation with Noisy Circuits, a General $n \log n$ Lower Bound,* Proc. 32. IEEE Symp. on Foundations of Computer Science, FOCS'91, 1991, 594 – 601.

[W87] I. Wegener, *The Complexity of Boolean Functions,* Teubner, 1987.