The Reliability of Circuits in the Basis Anticonjunction with Constant Faults of Gates

M. A. Alekhina1,* O. Yu. Barsukova2

Russia, Penza
*Corresponding Author: ama@sura.ru

Abstract We consider the realization of Boolean functions by asymptotically optimal reliable circuits with constant faults at the outputs of the gates in the basis \( \{x|y\} \) (where \( x\land y \rightarrow \neg \land x \land y \rightarrow \neg y \)). It is proved that almost all Boolean functions can be realized by asymptotically optimal reliable circuits that operate with unreliability asymptotically equal to \( 2\varepsilon_0 + \varepsilon_1 \) at \( \varepsilon_0, \varepsilon_1 \to 0 \), where \( \varepsilon_0 \) – probability of faults of type 0 at the output of basic gate, \( \varepsilon_1 \) – probability of faults of type 1 at the output of basic gate.

Keywords Functional Gates Circuit, Unreliability of A Circuit, Faults of the Type 0 and 1 at the Outputs

1 Introduction

J.von Neumann [1] was the first who considered the problem of synthesis of reliable circuits from unreliable gates. He assumed that all gates of the circuit are exposed to inverse faults independently with probability \( c (c < 1/2) \), when functional gate with Boolean function \( e(\bar{x}) \) in the faulty state realizes function \( \bar{e}(\bar{x}) \). Using an iterative method J.von Neumann established, that any Boolean function can be realized by a circuit at \( c < 1/6 \) for which the error’s probability at the output for any input set of variables is not greater than \( e \) (\( e \) is the same constant, \( c \) depends from the basis). With an extension of iteration number the circuit complexity increases exponentially.

The circuit of unreliable gates is characterized by two important parameters: the probability of error at the circuit output (unreliability) and the complexity of the circuit. The optimization of circuit complexity was given the main attention in S.I.Ortyukov’s [2], D.Ulig’s [3] and some other authors’ papers. The problem of constructing circuits that operate with the lowest (or near the lowest) probability of error was solved by M.A. Alekhina [4] on the assumption, that all circuit gates independently pass into faulty states, or only of the type 0 at the outputs (inputs) or only one type of 1 at the outputs (inputs).

In this paper we solve the problem of constructing asymptotically optimal reliable circuits in the basis \( \{x|y\} \) ( \( x|y = \neg x \lor y \)), and in contrast to [4] a circuit gate can be independent of the other circuit gates pass into or faulty state type 0 on the output or faulty state type 1 on the output. Such faults of gates are considered the first, previously it was not studied.

Previously the problem of construction of asymptotically optimal reliable circuits in the basis \( \{x|y\} \) have been solved for various faults of gates (for example, at faults only of the type 0 at the outputs or only type of 1 at the outputs (briefly in [5], detail in [6]), at output inverse faults [7]) by the same method: at first it is constructed reliable circuits, then their reliability is improved by some circuit (that generally depends on the considered basis), and it is proved an upper bound for the unreliability of circuits. Then it is proved the lower bound for the unreliability of circuit realizing functions of a certain class \( K \). If the obtained upper and lower bounds for the unreliability of circuits are asymptotically equal, then the functions of the class \( K \) not just reliable circuits are built, but circuits that are asymptotically optimal reliability.

The same method will be used in this work, however, this time its application is complicated by the presence of both parameters. The problem of constructing asymptotically optimal reliability circuits in which the gates are subjected to two types of faults with different probabilities, is considered the first time.

2 Concepts and Definitions

We consider the realization of Boolean functions by the circuits with unreliable functional gates in the basis \( \{x|y\} \). We assume that the circuit with unreliable functional gates realizes the function \( f(x_1, ..., x_n) \) (\( n \geq 1 \)) if at receipt on the circuit inputs the set \( \bar{a} = (a_1, ..., a_n) \) without faults in the circuit the value \( f(\bar{a}) \) appears on the circuit output. It is assumed that in each tact operation of the circuit at the outputs of all its gates can be independently constant faults or type 0 with probability \( \varepsilon_0 \) or type 1 with probability \( \varepsilon_1 \) (but not simultaneously). It is supposed \( \varepsilon_0 \in (0, 1/2) \) and \( \varepsilon_1 \in (0, 1/2) \).

Faults of type 0 on the outputs of gates are characterized by the fact that in good working order a functional gate realizes Boolean function \( x|y \), and in a
faulty constant it does 0 (zero). Faults of type 1 on the outputs of gates are characterized by the fact that in good working order a functional gate realizes Boolean function \(x_1y\), and in a faulty constant it does 1 (one).

We denote the probabilities of the occurrence 0 and 1 on the output of the gate with \(P_0(E, (x_1, x_2)), P_1(E, (x_1, x_2))\) for the input set \((x_1, x_2)\) of this gate.

We calculate the probability of errors on the output of the basis gate \(E_{x'y}\) (further we will denote it by \(E\), dropping the index) for all input sets of this gate:

\[
P_E, (00) = P_0(E, (01)) = P_0(E, (10)) = \varepsilon_0, P_1(E, (11)) = \varepsilon_1.
\]

Let \(P_{f(g)}(S, \tilde{a})\) be the probability of a appearance \(\tilde{f}(\tilde{a})\) on the output of the circuit \(S\), realizing a Boolean function \(f(\tilde{x})\) when the input set is \(\tilde{a}\). Unreliability \(P(S)\) of the circuit \(S\) is defined as the maximum of the numbers \(P_{f(g)}(S, \tilde{a})\) in all input set \(\tilde{a}\) of the circuit \(S\), i.e.,

\[
P(S) = \max\{P_{f(g)}(S, \tilde{a})\}. \text{Reliability of the circuit } S \text{ is equal to } 1 - P(S).
\]

Obviously the unreliability of the output gate \(E\) is equal to \(P(E) = \max\{\varepsilon_0, \varepsilon_1\}\). Denote \(\varepsilon = \max\{\varepsilon_0, \varepsilon_1\}\), then the reliability of the basis gate \(E\) is equal to \(1 - \varepsilon\).

**Example.** Consider a numerical example of calculating the unreliability of a circuit \(C\) (see picture 1).

![Picture 1](image)

Let value \(a_3\) of the variable \(x_3\) is equal to \(a_3 = 0\). Then the correct value at the output of the circuit \(C\) is equal to 1, and the probability of correct value occurrence is not affected by working the basis gate \(E_1\). Then the probability of error \(P_0(C, \tilde{a})\) is equal to

\[
P_0(C, (a_1, a_2, a_3)) = \varepsilon_0.
\]

Let value \(a_3\) of the variable \(x_3\) is equal to \(a_3 = 1\). Then two cases are possible

a) it is true \(a_1 \& a_2 = 1\) for value \(a_1\) and \(a_2\) of the variable \(x_1, x_2\) then

\[
P_0(C, (a_1, a_2, a_3)) = (1 - \varepsilon_1)\varepsilon_0 + \varepsilon_1(1 - \varepsilon_1) = (1 - \varepsilon_1)(\varepsilon_0 + \varepsilon_1);
\]

b) it is true \(a_1 \& a_2 = 0\) for value \(a_1\) and \(a_2\) of the variable \(x_1, x_2\) then

\[
P_1(C, (a_1, a_2, a_3)) = (1 - \varepsilon_0)\varepsilon_1 + \varepsilon_0(1 - \varepsilon_0) = (1 - \varepsilon_0)(\varepsilon_0 + \varepsilon_1).
\]

Thus the unreliability of the circuit \(C\) is equal to

\[
P(C) = \max\{\varepsilon_0, (1 - \varepsilon_1)(\varepsilon_0 + \varepsilon_1), (1 - \varepsilon_0)(\varepsilon_0 + \varepsilon_1)\}.
\]

Let \(P_{\varepsilon_0, \varepsilon_1} (f) = \inf P(S)\), where infimum is taken over all circuits \(S\) with unreliable gates realizing function \(f\).

The circuit \(A\) with unreliable gates realizing function \(f\) is called asymptotically optimal reliable if \(P(A) \sim P_{\varepsilon_0, \varepsilon_1} (f)\) at \(\varepsilon_0 \rightarrow 0, \varepsilon_1 \rightarrow 0\).

---

**3 Upper bound of the unreliability of circuits**

Let \(f\) be arbitrary Boolean function, \(S\) be a circuit realizing the function \(f\). Take two copies of the circuit \(S\) and connect them outputs to inputs of a basis gate. Constructed circuit is denoted \(\psi(S)\). Obviously the circuit \(\psi(S)\) realizes the function \(\bar{f}\). Take two copies of the circuit \(\psi(S)\) and connect them outputs to inputs of one more basis gate. Obviously the circuit \(\Psi(S)\) realizes the original function \(f\).

**Theorem 1** [4]. Let \(f\) be arbitrary Boolean function, \(S\) be a circuit realizing the function \(f\) with unreliability \(P(S)\). Then the circuit \(\Psi(S)\) realizes the function \(f\) with unreliability \(P(\psi(S)) \leq \max\{2\alpha + \tau + 2(\beta + \delta)P(S) + 2P^2(S), \alpha + (\beta + \delta)(\tau + 2P(S)) + (\tau + 2P(S))^2\}\), where \(\alpha = P_0(E, (00)), \beta = P_2(E, (01)), \delta = P_0(E, (10)), \tau = P_1(E, (11))\).

From the Theorem 1 follows the Theorem 2 if, instead \(\alpha, \beta, \delta, \tau\), we substitute in computed above error probability on the output basis gate.

**Theorem 2** [4]. Let \(f\) be arbitrary Boolean function, \(S\) be a circuit realizing the function \(f\) with unreliability \(P(S)\). Then the circuit \(\psi(S)\) realizes the function \(f\) with unreliability \(P(\psi(S)) \leq \max\{2\varepsilon_0 + \varepsilon_1 + 4\varepsilon_0P(S) + 2P^2(S), \varepsilon_0 + 2\varepsilon_0\varepsilon_1 + \varepsilon_1 + 4(\varepsilon_0 + \varepsilon_1)P(S) + 4P^2(S)\}\).

**Theorem 3** [4]. Any Boolean function \(f\) can be realized by such a circuit \(A\) for that for any \(\mu \in (0.1, 1/160)\) \(\mu\) be any upper bound of the unreliability of circuits realizing the function \(\{x|y\}\) the following inequality holds \(P(A) \leq 4\mu\).

From the Theorem 3 follows the Theorem 4 to prove that should instead \(\mu\) substitute in \(\max\{\varepsilon_0, \varepsilon_1\} = \varepsilon\) (the unreliability of the basis gate).

**Theorem 4**. Any Boolean function \(f\) can be realized by such a circuit \(A\) that for any \(\varepsilon \in (0, 1/160]\) the following inequality holds \(P(A) \leq 4\varepsilon\).

From the Theorems 2 and 4 follows the Theorem 5.

**Theorem 5**. Any Boolean function \(f\) can be realized by such a circuit \(B\) that for any \(\varepsilon \in (0, 1/160]\) the following inequality holds \(P(B) \leq 2\varepsilon_0 + \varepsilon_1 + 48\varepsilon^2\), where \(\varepsilon = \min\{1/160, \varepsilon\}\), where \(z = (\sqrt{2}(\varepsilon_0 + \varepsilon_1 + \varepsilon_1^2 - 2\varepsilon_0\varepsilon_1) - 2\varepsilon_1)/8\).

**Proof.** Let \(f\) be arbitrary Boolean function. By Theorem 4, the function \(f\) can be realized by the circuit \(A\) with the unreliability \(P(A) \leq 4\varepsilon\) at \(\varepsilon \in (0, 1/160]\). By the circuit \(A\) we construct the circuit \(\psi(A)\) and and estimate its unreliability using Theorem 2. Obtain the inequality \(P(\Psi(A)) \leq \max\{2\varepsilon_0 + \varepsilon_1 + 16\varepsilon_0\varepsilon_1 + 32\varepsilon^2, \varepsilon_0 + 2\varepsilon_0\varepsilon_1 + \varepsilon_1^2 + 16(\varepsilon_0 + \varepsilon_1)\varepsilon + 64\varepsilon^2\} = 2\varepsilon_0 + 16\varepsilon_0\varepsilon_1 + 32\varepsilon^2\) at \(\varepsilon \in (0, z]\), where \(z\) be positive root of the equation \(32\varepsilon^2 + 16\varepsilon_1 - \varepsilon_1^2 + 2\varepsilon_0\varepsilon_1 + \varepsilon_1^2 = 0\). Solve this equation and obtain \(z = (\sqrt{2}(\varepsilon_0 + \varepsilon_1 + \varepsilon_1^2 - 2\varepsilon_0\varepsilon_1) - 2\varepsilon_1)/8\). By \(\varepsilon\) denote the value \(\min\{1/160, \varepsilon\}\). Then \(2\varepsilon_0 + \varepsilon_1 + 16\varepsilon_0\varepsilon_1 + 32\varepsilon^2 \leq 2\varepsilon_0 + \varepsilon_1 + 48\varepsilon^2\). Therefore, \(P(\Psi(A)) \leq \max\{2\varepsilon_0 + \varepsilon_1 + 48\varepsilon^2\}, the circuit \(\Psi(A) = B\) is the desired one.

The theorem 5 is proved.
4 Lower bound of the unreliability of circuits

Let \( f \) be arbitrary Boolean non-constant function, and \( S \) be any circuit realizing it. Let a subcircuit \( C \) of the circuit \( S \) contains the output of the circuit \( S \) and realizes boolean function \( f' \) with unreliability \( P(C) \leq 1/2 \). By \( p^i \) denote minimum probability of errors at the output of circuit \( C \) for such input sets \( b \), that \( f'(b) = 0 \). Similarly by \( p^0 \) denote minimum probabilities of errors at the output of circuit \( C \) for such input sets \( b \), that \( f'(b) = 1 \).

**Lemma 1.** [4]. The probabilities of errors at the output of circuit \( S \) satisfy the inequality
\[
P_1(S, \vec{a}) \geq p^1, \text{ if } f(\vec{a}) = 0;
\]
\[
P_0(S, \vec{a}) \geq p^0, \text{ if } f(\vec{a}) = 1.
\]

**Remark 1.** From the Lemma 1 follows that \( P(S) \geq p^i, i = 0; 1 \).

Let the circuit \( S \), realizing the boolean non-constant function \( f \), is such that both of inputs of its output element \( E \) are connected to the output of some subcircuit \( B \). By \( P_1(B, \vec{a}) \) and \( P_0(B, \vec{a}) \) denote the probabilities of errors at the output of circuit \( B \).

**Lemma 2.** The probabilities of errors at the output of circuit \( S \) are equal to
\[
P_1(S, \vec{a}) = \varepsilon_1 + P_0(B, \vec{a})(1 - \varepsilon_0 - \varepsilon_1),
\]
the set \( \vec{a} \) such that \( f(\vec{a}) = 0 \);
\[
P_0(S, \vec{a}) = \varepsilon_0 + P_1(B, \vec{a})(1 - \varepsilon_0 - \varepsilon_1),
\]
the set \( \vec{a} \) such that \( f(\vec{a}) = 1 \).

To prove this it is sufficient to calculate the probabilities of errors.

Let \( h(\vec{x}) \) be arbitrary Boolean function, \( \vec{x} = (x_1, \ldots, x_n) \), and \( K(n) \) be the set of Boolean functions of the type \( f(\vec{x}) = (\vec{x} \lor h(\vec{x}))^{\ast} \), where \( 1 \leq i \leq n, a \in \{0, 1\} \), i.e. if \( a = 0 \) then \( f(\vec{x}) = \vec{x} \lor h(\vec{x}) \), if \( a = 1 \) then \( f(\vec{x}) = \vec{x} \lor h(\vec{x}) \). By \( K \) denote the set \( \bigcup_{n=1}^{\infty} K(n) \), i.e.
\[
K = \bigcup_{n=1}^{\infty} K(n).
\]

**Theorem 6.** Let \( \varepsilon \leq 1/8, f \not\in K \), and \( S \) be any circuit realizing \( f \). Then \( P(S) \geq 2\varepsilon_0 + \varepsilon_1 - 5\varepsilon_0^2 - 5\varepsilon_0\varepsilon_1 - \varepsilon_1^2 - \varepsilon_1^2 - \varepsilon_1^2 \).

**Proof.** Let \( f \) be the function satisfying the conditions of Theorem 6, and \( S \) be any circuit its realizing. We single out in the circuit \( S \) the functional gate \( E_1 \) containing the output \( S \). As the \( f \not\in K(n) \), there are two cases.

1. The outputs of gate \( E_1 \) are connected to the inputs different gates \( E_2 \) and \( E_3 \).

1.1. The output of one gate, for instance \( E_2 \), is connected to the input of gate \( E_3 \). Compute the error probability \( p_1 \) on the output subcircuit consisting of gates \( E_1, E_2 \) and \( E_3 \) to obtain \( p_1 = (1 - \varepsilon_0)^2 \varepsilon_1 + (1 - \varepsilon_0)(2\varepsilon_0 + \varepsilon_1 - \varepsilon_0^2 - \varepsilon_0\varepsilon_1) = \varepsilon_0 \).

2. The outputs of the gate \( E_1 \) is connected to the output of one element \( E_2 \). There are two cases.

2.1. The inputs of gate \( E_2 \) are connected to the outputs different gates \( E_1 \) and \( E_3 \). Then (see paragraph 1 of the proof), the probability \( p_1 \) of error at the output of subcircuit consisting of gates \( E_2, E_3 \) and \( E_4 \) is equal to \( p_1 = (1 - \varepsilon_0)(2\varepsilon_0 + \varepsilon_1 - \varepsilon_0^2 - \varepsilon_0\varepsilon_1) \). It is equal to \( p^1 \). By Lemma 2 the error probability \( p_0 \) at the output of subcircuit consisting of gates \( E_1, E_2, E_3 \) and \( E_4 \) is equal to \( p_0 = \varepsilon_0 + (1 - \varepsilon_0)(2\varepsilon_0 + \varepsilon_1 - \varepsilon_0^2 - \varepsilon_0\varepsilon_1)(1 - \varepsilon_0 - 1) \).

By using Remark 1 taking into account Remark 1 at \( \varepsilon \leq 1/8 \) the following inequality holds \( P(S) \geq 2 \).

2.2. Both inputs of gates \( E_2 \) is connected to the output of one gate \( E_3 \). Then error probabilities \( p_0 \) and \( p_1 \) on the output subcircuit consisting of gates \( E_1, E_2 \) and \( E_3 \) are computed with a two-fold using Lemma 2 and are equal to \( \varepsilon_0 + (1 - \varepsilon_0)(1 - \varepsilon_0 - \varepsilon_1)(1 - \varepsilon_0 - 1) = 2\varepsilon_0 + \varepsilon_1 - (\varepsilon_0 + \varepsilon_1)(2\varepsilon_0 + \varepsilon_1 - \varepsilon_0 - \varepsilon_1) \). Denote \( c = 2\varepsilon_0 + \varepsilon_1 - (\varepsilon_0 + \varepsilon_1)(2\varepsilon_0 + \varepsilon_1 - \varepsilon_0 - \varepsilon_1) \). By Lemma 1 taking into account Remark 1 at \( \varepsilon \leq 1/8 \) the following inequality holds \( P(S) \geq c \).

Thus, in all cases, the following inequality holds
\[
P(S) \geq \min\{a, b, c\} \geq 2\varepsilon_0 + \varepsilon_1 - 5\varepsilon_0^2 - 5\varepsilon_0\varepsilon_1 - \varepsilon_1^2 - \varepsilon_1^2.
\]

The last expression in inequality is obtained by comparing the coefficients of the polynomial, identified \( a, b, c \), in similar terms, and choosing the lesser of the coefficients.

The theorem 6 is proved.

From the Lemma 1 follows that any circuit satisfying the conditions of Theorem 5, and realizing the Boolean function \( f \not\in K \), is asymptotically optimal on reliability and operates with unreliability asymptotically equal to \( 2\varepsilon_0 + \varepsilon_1 \) at \( \varepsilon_0, \varepsilon_1 \rightarrow 0 \).

It is easy to verify that the number of functions in the class \( K(n) \) is not more than \( 2n^{2n-\varepsilon} \), which is small in comparison with the total number of \( 2^n \) Boolean functions of \( n \) variables. Therefore, almost all Boolean functions in this basis can be realized asymptotically optimal reliable circuits that operate with unreliability asymptotically equal to \( 2\varepsilon_0 + \varepsilon_1 \) at \( \varepsilon_0, \varepsilon_1 \rightarrow 0 \).

**Acknowledgements**

The study was financially supported by Russian Foundation for Basic Research (project 11-01-00212).
REFERENCES


