

3. Ткаченко Н. О., Чернов Д. В. Разработка и реализация сервера игры CTF // Прикладная дискретная математика. Приложение. 2010. № 3. С. 62–64.
4. <http://blackbox.sibears.ru/> — Система для проведения соревнований по защите компьютерной информации. 2013.
5. <http://ructf.org/2012> — Всероссийские межвузовские соревнования по защите информации RuCTF 2012. 2012.
6. <http://python.org/> — Python Programming Language — Official Website. 2013.
7. <https://www.djangoproject.com/> — Django. The Web framework for perfectionists with deadlines. 2013.
8. <http://wiki.apparmor.net> — AppArmor security wiki project. 2013.
9. <http://www.linux.com/learn/docs/man/4047-setrlimit2> — Linux Programmer's Manual (2). getrlimit, setrlimit — get/set resource limits. 2008.
10. <http://www.openstack.org/> — OpenStack. Open source cloud computing software. 2013.
11. <https://www.simple-talk.com/sql/database-administration/database-design-a-point-in-time-architecture/> — Database Design: A Point in Time Architecture. 2007.
12. <http://www.celeryproject.org/> — Celery. Distributed Task Queue. 2012.
13. <http://memcached.org/> — Memcached. A distributed memory object caching system. 2012.

УДК 519.718

О БАЗИСАХ С КОЭФФИЦИЕНТОМ НЕНАДЁЖНОСТИ ¹

А. В. Васин

Рассматривается реализация булевых функций схемами из ненадёжных функциональных элементов в произвольном полном базисе B . Предполагается, что все элементы схемы независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$ подвержены инверсным неисправностям на выходах. Найдено множество G функций, таких, что для почти всех функций ненадёжность асимптотически оптимальных по надёжности схем в базисе B , содержащем функции множества G , равна ε (при $\varepsilon \rightarrow 0$).

Ключевые слова: ненадёжные функциональные элементы, асимптотически оптимальные по надёжности схемы, инверсные неисправности на выходах элементов.

Рассматривается реализация булевых функций схемами [1] из ненадёжных функциональных элементов в произвольном полном конечном базисе B . Предполагаем, что все элементы схемы независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$ подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию ψ , а в неисправном — функцию $\bar{\psi}$. Считаем, что схема S из ненадёжных элементов реализует булеву функцию $f(x_1, x_2, \dots, x_n)$, если при поступлении на входы схемы двоичного набора $a = (a_1, a_2, \dots, a_n)$ при отсутствии неисправностей на выходе схемы S появляется значение $f(a)$.

Ненадёжностью $P(S)$ схемы S назовем максимальную вероятность ошибки на выходе схемы S при всевозможных входных наборах схемы. Надёжность схемы S равна $1 - P(S)$. Пусть $P_\varepsilon(f) = \inf P(S)$, где инфимум берется по всем схемам S из ненадёж-

¹Работа выполнена при финансовой поддержке РФФИ, проект № 12-01-31340.

ных элементов, реализующим булеву функцию $f(x_1, x_2, \dots, x_n)$. Схема A из ненадёжных элементов, реализующая функцию f , называется асимптотически оптимальной (асимптотически наилучшей) по надёжности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \rightarrow 0$.

Число k будем называть коэффициентом ненадёжности базиса, если все функции в этом базисе можно реализовать схемами с ненадёжностью, асимптотически не больше $k\varepsilon$ (при $\varepsilon \rightarrow 0$), и найдётся функция f , которую нельзя реализовать схемой с ненадёжностью, асимптотически меньше чем $k\varepsilon$ (при $\varepsilon \rightarrow 0$).

Задача построения асимптотически оптимальных по надёжности схем при инверсных неисправностях на выходах элементов в полных базисах из трёхвходовых элементов решена в [2]. В этой работе найден широкий класс базисов, для которых $k = 1$.

Обозначим через K множество функций, для которых асимптотически оптимальные по надёжности схемы в базисе B функционируют с ненадёжностью, асимптотически равной $k\varepsilon$ (при $\varepsilon \rightarrow 0$), где k — коэффициент ненадёжности базиса B .

Нетрудно проверить, что при инверсных неисправностях на выходах элементов в любом базисе ненадёжность любой схемы, содержащей хотя бы один элемент, не меньше ε . Поэтому коэффициент ненадёжности любого базиса не меньше 1.

Для реализации любой функции, отличной от x_i ($i = 1, 2, \dots, n$), требуется не менее одного функционального элемента. Обозначим через $K(n)$ множество булевых функций $K(n) = P_2 \setminus \{x_i : i = 1, \dots, n\}$. Очевидно, что $\frac{|K(n)|}{2^{2^n}} \rightarrow 1$ при $n \rightarrow \infty$. Тогда в случае $k = 1$ множество K равно $K = \bigcap_{i=1}^{\infty} K(n)$.

Замечание 1. Для любой булевой функции $f \in K$ верно $P_\varepsilon(f) \geq \varepsilon$.

Опишем множество G функций $\varphi(x_1, \dots, x_r)$, обладающих свойством повышения надёжности.

Пусть $e_1, e_2, \dots, e_r \in \{0, 1\}^r$, где e_i — вектор, имеющий ровно одну ненулевую компоненту на i -м месте, $i = 1, 2, \dots, r$. Зададим множество E^k , состоящее из r векторов $\hat{e}_1, \hat{e}_2, \dots, \hat{e}_r \in \{0, 1\}^r$, следующим образом: 1) $\hat{e}_i = e_i$, $i = 1, 2, \dots, k$; 2) $\hat{e}_i = e_i + \sum_{j=1}^{i-1} \lambda_{ij} e_j$, где $\lambda_{ij} \in \{0, 1\}$, $i = k+1, k+2, \dots, r$. Пусть $\varphi(x_1, x_2, \dots, x_r) \in G_0$, если существуют такие двоичные наборы $\tilde{\alpha}, \tilde{\beta}$, что 1) $\varphi(\tilde{\alpha}) = 0$, $\varphi(\tilde{\beta}) = 1$; 2) для любого набора $\tilde{x} = \tilde{\alpha} + \hat{e}_i$ верно $\varphi(\tilde{x}) = 0$; 3) для любого набора $\tilde{x} = \tilde{\beta} + \hat{e}_i$ верно $\varphi(\tilde{x}) = 1$; 4) $A \cap B = \emptyset$, где $A = \{\tilde{\alpha}\} \cup \{\tilde{x} : \tilde{x} = \tilde{\alpha} + \hat{e}_i, i = 1, 2, \dots, r\}$, $B = \{\tilde{\beta}\} \cup \{\tilde{x} : \tilde{x} = \tilde{\beta} + \hat{e}_i, i = 1, 2, \dots, r\}$.

Множество всех функций $\varphi \in G_0$, а также функций, из которых подстановкой переменных можно получить одну из функций φ , обозначим через G .

Теорема 1. Пусть B — базис, содержащий функцию $\varphi(x_1, x_2, \dots, x_r) \in G$. Тогда для любой булевой функции f существует схема S , реализующая f , для которой $P(S) \leq \varepsilon + 1,1(8(3/2)^r + r(r+1))\varepsilon^2$ при $\varepsilon \leq \min(1/960, 1/(8(3/2)^r + r(r+1)))$.

Из теоремы 1 с учётом замечания 1 следует, что при наличии в полном базисе B функций множества G для почти всех булевых функций $f \in K$ асимптотически оптимальные по надёжности схемы S функционируют с ненадёжностью $P(S) \sim \varepsilon$ при $\varepsilon \rightarrow 0$.

ЛИТЕРАТУРА

1. *Лупанов О. П.* Асимптотические оценки сложности управляющих систем. М.: Изд-во Моск. ун-та, 1984.
2. *Васин А. В.* Асимптотически оптимальные по надёжности схемы в полных базисах из трехвходовых элементов: дис. ... канд. физ.-мат. наук. Пенза, 2010. 100 с.