ВЕСТНИК ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2023 Управление, вычислительная техника и информатика № 62
Tomsk State University Journal of Control and Computer Science

ДИСКРЕТНЫЕ ФУНКЦИИ И АВТОМАТЫ

DISCRETE FUNCTION AND AUTOMATONS

Научная статья
УДК 519.7
doi: 10.17223/19988605/62/14

Построение аппроксимирующих схем для синхронных автоматов в рамках технологии троирования

Сергей Александрович Останин[1], Анжела Юрьевна Матросова[2], Валентина Валерьевна Андреева[3]

[1, 2, 3] *Томский государственный университет, Томск, Россия*
[1] *sergeiostanin@yandex.ru*
[2] *mau11@yandex.ru*
[3] *avv.21@mail.ru*

Аннотация. Троирование (Triple-Modular Redundancy (TMR) technique) является одним из широко применяемых на практике подходов к обеспечению надежности функционирования логических схем. В рамках этой технологии используется три идентичных схемы, одноименные выходы которых поступают на схему голосования. В такой системе корректное функционирование обеспечивается при неисправности одной из трех схем. Однако появившиеся в последние годы возможности одновременного внесения в каждую копию и соответствующие линии вредоносных подсхем (Trojan Circuits) делают метод троирования уязвимым к таким действиям. Одним из выходов в этой ситуации является использование вместо идентичных трех синхронных последовательностных схем двух аппроксимирующих схем и одной рабочей схемы, выполняющей предписанное разработчиком функционирование синхронного автомата. Предлагаемый подход гарантирует отсутствие незащищенной области, характерной для известных методов применения аппроксимирующих схем в технологии троирования.

Ключевые слова: синхронные последовательностные схемы; безызбыточные системы ДНФ (БСДНФ); аппроксимирующие схемы; троирование; константные неисправности литер БСДНФ.

***Для цитирования*:** Останин С.А., Матросова А.Ю., Андреева В.В. Построение аппроксимирующих схем для синхронных автоматов в рамках технологии троирования // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2023. № 62. С. 124–131. doi: 10.17223/19988605/62/14

Original article
doi: 10.17223/19988605/62/14

Deriving approximate circuits for TMR technique applied to synchronous sequential circuits

Sergey A. Ostanin[1], Angela Yu. Matrosova[2], Valentina V. Andreeva[3]

[1, 2, 3] *Tomsk State University, Tomsk, Russian Federation*
[1] *sergeiostanin@yandex.ru*
[2] *mau11@yandex.ru*
[3] *avv.21@mail.ru*

Abstract. Triple-Modular Redundancy (TMR) technique is one of the conventional approaches to provide reliable functioning of logical circuits. In the frame of this technique three identical circuits are applied, their like outputs are connected with a voting circuit. Correct functioning of such system is guaranteed, if one of three circuits is fault. When using outsourcing it is possible to inject a Trojan Circuit in the same line of each identical circuits of TMR, and TMR technique becomes vulnerable. One way of confronting to vulnerability is connected with applying instead of identical sequential circuits two approximate circuits and one correct circuit that implements the proper functioning. The suggested approach guarantees absence of unprotected area that as a rule appears when using approximate circuits in TMR techniques.

Keywords: synchronous sequential circuits; irredundant system of SoPs; approximate circuits; TMR technique; literal constant faults of Irredundant system of SoPs.

***For citation*:** Ostanin, S.A., Matrosova, A.Yu., Andreeva, V.V. (2023) Deriving approximate circuits for TMR technique applied to synchronous sequential circuits. *Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vychislitelnaja tehnika i informatika – Tomsk State University Journal of Control and Computer Science*. 62. pp. 124–131. doi: 10.17223/19988605/62/14

Введение

Схемы троирования являются одним из широко распространенных подходов к обеспечению надежности функционирования логических схем. Предполагается, что одна из трех схем может быть неисправной. В этом случае в условиях подключения к одноименным выходам трех схем схемы голосования значение выхода определяется значением большинства одноименных выходов. Схемы голосования предполагаются исправными. Однако в современных условиях производство логической схемы может выполняться различными фирмами, в том числе и в разных частях света. В связи с этим появляется возможность включения вредоносной подсхемы в каждую из идентичных схем, например в соответствующую линию каждой из трех схем. Вредоносная подсхема (Trojan Circuit) может изменить в нужный момент значение сигнала на этих линиях на противоположное значение с целью искажения работы схемы или с целью извлечения конфиденциальной информации из устройства, содержащего рассматриваемую схему. Это значит, что технология троирования оказывается уязвимой в условиях возможности включения вредоносных подсхем.

Одним из известных подходов к защите комбинационной схемы в рамках технологии троирования является использование аппроксимирующих схем, которые строятся из рабочей схемы, реализующей нужное разработчику поведение [1, 2]. Аппроксимирующие схемы применяются также при синтезе самопроверяемых логических схем [3]. В статье [3] аппроксимирующие схемы используются с целью сокращения аппаратурных затрат в условиях, когда функционирование самопроверяемой схемы может незначительно отклоняться от функционирования рабочей схемы, что менее важно, чем сокращение аппаратурных затрат. При использовании аппроксимирующих схем в схемах троирования отклонение от корректного функционирования возможно в присутствии неисправности в одной из трех схем в так называемой незащищенной области [1, 2]. При подобном использовании аппроксимирующих схем стремятся сократить незащищенную область. Если комбинационная схема является комбинационной составляющей последовательностной схемы, то ее поведение можно описать системой частичных булевых функций. Эти функции извлекаются либо из таблицы переходов-выходов синхронного автомата, либо из State Transition Graph (STG) описания путем кодирования символов алфавитов синхронного автомата. Использование системы частичных булевых функций открывает возможность для получения различных ее реализаций в качестве задания на синтез аппроксимирующих схем. Такой подход исключает появление незащищенной области в рабочей области функционирования синхронного автомата. Итак, еще на этапе создания рабочей схемы предлагается учесть необходимость ее защиты от внедрения вредоносных подсхем при использовании троирования, причем исключается незащищенная область, характерная при синтезе комбинационных схем, когда задание на синтез представляется системой полностью определенных булевых функций.

В рассматриваемом в данной работе подходе построение аппроксимирующих схем предлагается начать с использования безызбыточной системы ДНФ (БСДНФ), построенной по заданной системе частичных функций. БСДНФ является реализацией этой системы частичных функций. БСДНФ далее используется в качестве задания на синтез рабочей схемы синхронного автомата. Эта же БСДНФ является источником получения БСДНФ для каждой из аппроксимирующих схем, причем получаемые системы являются реализацией заданной системы частичных функций. Такой подход позволяет получать аппроксимирующие схемы, не порождающие незащищенной области. Кроме того, для получения аппроксимирующих схем не требуется введения в рабочую схему дополнительных элементов [1, 2] для обеспечения на выходах этих схем монотонного проявления искажений, вносимых в рабочую схему. Предлагаемый нами подход ориентирован на использование автоматизированного синтеза логических схем, применяемого в современных САПР. В частности, предполагается, что задание на синтез рабочей схемы в рамках САПР представляется БСДНФ. Ее искажения обеспечиваются введением в систему одиночных константных неисправностей литер [4, 5]. Речь идет о неисправностях константа 1, которые сводятся к снижению на единицу ранга конъюнкций отдельных ДНФ из БСДНФ рабочей схемы, то есть к b-неисправностям [4, 5] литер СБДНФ.

Выбор конъюнкций в БСДНФ рабочей схемы для внесения в них неисправностей с целью построения аппроксимирующих систем функций ориентирован на достижение значительного отличия аппроксимирующих систем от БСДНФ рабочей схемы, т.е. на обеспечение возможно больших затруднений при введении вредоносных подсхем в систему троирования. В то же время необходим баланс между вносимыми изменениями и сложностью получаемых аппроксимирующих схем.

1. Построение аппроксимирующих систем булевых функций

Пусть описание поведения рабочей схемы синхронного автомата представлено в виде БСДНФ. БСДНФ состоит из простых импликант системы булевых функций, т.е. ни одна из функций не может быть исключена из характеристик этих импликант. Предполагается, что БСДНФ построена по системе частичных булевых функций, полученной либо из таблицы переходов-выходов синхронного автомата, либо из State transition Graph (STG) описания поведения синхронного автомата. Система частичных функций представляется парами множеств M_{1i}, M_{0i}, задающих единичные и нулевые наборы частичной функции f_i системы. Каждая конъюнкция БСДНФ снабжается характеристикой, в ней перечислены функции системы, для которых эта конъюнкция является допустимой.

Конъюнкция допустима, если пересечение ее интервала с областью нулевых наборов значений переменных частичной функции системы, упомянутой в характеристике конъюнкции, пусто, а с областью единичных наборов значений переменных частичной функции не пусто.

Поскольку конъюнкция БСДНФ является простой импликантой системы булевых функций, то из нее нельзя исключить ни одной (любой) литеры в условиях сохранения характеристики этой конъюнкции.

Кроме того, так как список конъюнкций с соответствующими характеристиками представляет безызбыточную систему ДНФ, то из характеристики конъюнкции этой системы нельзя исключить ни одной функции.

Будем иметь в виду, что исключение переменной x_i из конъюнкции K системы приводит к пересечению с областью нулевых значений не каждой частичной функции из характеристики h этой конъюнкции, а только некоторых из них, причем обязательно хотя бы для одной из функций характеристики h. Функции характеристики h, для которых исключение переменной x_i не приводит к искажению соответствующей частичной функции, будем называть расширяемыми по рассматриваемой переменной для исследуемой конъюнкции.

Таким образом, для каждой переменной x_i конъюнкции K из БСДНФ множество функций ее характеристики h разбивается на два подмножества $h_{\text{р}}$ и $h_{\text{нр}}$, расширяемого по переменной и не расширяемого по переменной x_i.

Исключение переменной из конъюнкции K для функций из множества $h_{\text{р}}$ сохраняет реализацию частичных функций множества $h_{\text{р}}$. Исключение переменной приводит лишь к расширению множества единичных наборов реализации частичных функций из характеристики $h_{\text{р}}$. При исключении переменной x_i получаем конъюнкцию системы $(K/x_i, h_{\text{р}})$. Здесь конъюнкция K/x_i получается из конъюнкции K исключением переменной x_i.

Отметим, что при разбиении характеристики конъюнкции K на два подмножества получаемые из K конъюнкции имеют характеристики меньшей мощности, чем характеристика h, тогда каждая из них может быть расширена до простой импликанты заданной системы частичных функций. Итак, из простой импликанты (K, h) получаем две простые импликанты: K^*, $h_{нр}$; K^*/x_i, $h_р$.

В дальнейшем полученные простые импликанты будем называть продуктами операции расщепления простой импликанты (K, h) из БСДНФ.

Будем иметь в виду, что конъюнкция (K, h) расщепляема по переменной x_i, если переменная x_i порождает для этой конъюнкции непустую характеристику $h_р$.

Договоримся называть операцией расщепления конъюнкции (K, h) по x_i из БСДНФ замену ее конъюнкциями (K^*, $h_{нр}$); (K^*/x_i, $h_р$).

Утверждение 1. Операция расщепления конъюнкции K по переменной x_i приводит к расширению области единичных значений реализации системы частичных функций без искажения системы частичных функций, реализованной БСДНФ.

Действительно, замена простой импликанты (K, h) БСДНФ на допустимую конъюнкцию K^*, $h_{нр}$ сохраняет область единичных значений частичных функций, перечисленных в характеристике $h_{нр}$ при условии, что конъюнкция K^* совпадает с конъюнкцией K либо расширяет область единичных значений этих частичных функций при несовпадении конъюнкций. Замена простой импликанты (K, h) БСДНФ на допустимую конъюнкцию (K^*/x_i, $h_р$) всегда приводит к расширению области единичных значений частичных функций, перечисленных в характеристике $h_р$. Это значит, что расщепление простой импликанты (K, h) по переменной x_i приводит к расширению области единичных значений реализации системы частичных функций без искажения системы частичных функций, представленной СБДНФ.

Пусть $F(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)$ – система из m булевых функций от n переменных. Будем говорить, что система $G(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)$ поглощается системой $F(x_1, \ldots, x_n) = f(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)$, и обозначать это как $G(\alpha_1, \ldots, \alpha_n) < F(\alpha_1, \ldots, \alpha_n)$, если для любого набора $\alpha = \alpha_1, \ldots, \alpha_n$

$$G(\alpha_1, \ldots, \alpha_n) \le F(\alpha_1, \ldots, \alpha_n),$$

то есть для одноименных функций системы выполняется условие

$$g_i(\alpha_1, \ldots, \alpha_n) \le f_i(\alpha_1, \ldots, \alpha_n).$$

Обозначим через $G(x_1, \ldots, x_n)$ систему БСДНФ, реализуемую рабочей схемой, а через $F(x_1, \ldots, x_n)$ – систему, полученную расщеплением некоторых ее простых импликант по тем или иным переменным.

Утверждение 2. Выполнение операций расщепления нескольких конъюнкций по переменной (одна и та же конъюнкция может расщепляться по нескольким переменным) приводит к получению системы $F(x_1, \ldots, x_n)$, поглощающей систему $G(x_1, \ldots, x_n)$: $G(x_1, \ldots, x_n) < F(x_1, \ldots, x_n)$.

Поскольку операция расщепления простой импликанты из $G(x_1, \ldots, x_n)$ приводит к расширению области единичных значений некоторых функций этой системы, то многократное применение расщепления простых импликант системы $G(x_1, \ldots, x_n)$ приводит к тому же результату.

Следствие 1. Поглощающая система $F(x_1, \ldots, x_n)$ является реализацией той же системы частичных функций, что и система $G(x_1, \ldots, x_n)$.

Следствие 2. Различные поглощающие системы $F(x_1, \ldots, x_n)$, полученные расщеплением конъюнкций системы $G(x_1, \ldots, x_n)$ по тем или иным переменным могут использоваться в качестве аппроксимирующих систем для системы $G(x_1, \ldots, x_n)$, обеспечивая отсутствие незащищенной области синхронного автомата (синхронного последовательностного устройства).

Чем сильнее поглощающие системы $F(x_1, \ldots, x_n)$, используемые для представления аппроксимирующих систем, отличаются друг от друга и от системы $G(x_1, \ldots, x_n)$, тем труднее воспользоваться технологией введения вредоносной подсхемы в каждую из трех реализующих эти системы схем с целью обеспечения одинаковых искажений.

Отметим, что операции расщепления конъюнкций БСДНФ приводят к увеличению числа простых импликант, причем возможно одновременное уменьшение суммы рангов продуктов расщепления по сравнению с рангом расщепляемой конъюнкции БСДНФ, а также уменьшение мощности характеристик h в простых импликантах системы, полученных в результате расщепления. Насколько вероятны такие ситуации, трудно сказать, и трудно без экспериментов на моделях реальных схем предсказать, как повлияет расщепление конъюнкций СБДНФ на сложность аппроксимирующей схемы, реализующей полученную безызбыточную систему ДНФ. Скорее всего, схема будет усложняться, что является естественной платой за защиту от внедрения вредоносных подсхем. Необходим компромисс между усложнением аппроксимирующих схем и сложностью введения в них вредоносной подсхемы при использовании технологии троирования.

Заметим, что, чем меньше ранг конъюнкции K простой импликанты (K, h), тем больше искажаются функции, заданные БСДНФ, и в то же время меньше число искажаемых при расщеплении функций. Напротив, чем больше ранг конъюнкции K, тем меньше искажаются функции, заданные БСДНФ, и в то же время больше число искажаемых при расщеплении конъюнкций.

Необходимо построить две аппроксимирующие системы F_1, F_2, поглощающие систему $G(x_1, \ldots, x_n)$, и являющиеся реализацией исходной системы частичных функций.

Предлагается в каждой аппроксимирующей системе использовать результаты расщеплений конъюнкций как меньших, так и больших рангов БСДНФ для обеспечения разнообразия искажений этих систем при одинаковом числе расщеплений, используемых при получении аппроксимирующих систем.

К полученным системам и исходной безызбыточной системе применяем какую-либо из автоматизированных систем синтеза и используем три схемы в системе троирования.

2. Алгоритм получения систем F_1, F_2

Опишем основные шаги алгоритма. Пусть L – допустимое число расщеплений конъюнкций БСДНФ при построении каждой из аппроксимирующих систем. Предварительно упорядочим L простых импликант БСДНФ $G(x_1, \ldots, x_n)$ по неубыванию рангов составляющих их конъюнкций и столько же конъюнкций по невозрастанию рангов. Получаем список простых импликант системы, порождающий обе аппроксимирующие системы. Список разделен на две части, в нем сначала перечисляются импликанты с конъюнкциями меньших рангов, а затем – с конъюнкциями больших рангов.

1. Извлекаем из списка простую импликанту БСДНФ.

2. Расщепляем ее по каждой переменной характеристики. Выбираем пары продуктов расщепления с максимальным значением характеристики $h_р$. Одна и та же простая импликанта БСДНФ в общем случае может порождать несколько пар продуктов расщепления по различным переменным с максимальным значением $h_р$.

3. Заменяем порождающую расщепление простую импликанту БСДНФ парой продуктов расщепления.

4. Выполняем пункты 1–3 для L расщеплений, чередуя выбор из первой и второй половин списка для каждой из аппроксимирующих систем. В результате получаем системы F_1^*, F_2^*.

Для каждой из полученных систем гарантировано, что все ее конъюнкции – простые импликанты, но не гарантирована безызбыточность по характеристикам конъюнкций. Поэтому необходима проверка на безызбыточность по характеристикам. После устранения лишних функций из характеристик получаем безызбыточные аппроксимирующие системы F_1, F_2.

Полученные безызбыточные системы ДНФ для аппроксимирующих и рабочей систем функций поступают в качестве задания на синтез в систему САПР и используются для получения аппроксимирующих и рабочих схем в системе троирования.

Проиллюстрируем получение аппроксимирующей системы на простом примере. С этой целью выполним одно расщепление конъюнкции.

Задана система из двух булевых функций списком простых импликант системы в виде перечисления соответствующих конъюнкциям интервалов системы и характеристик. Интервалы представлены троичными векторами, а характеристики – перечислением функций системы, для которых интервалы допустимы:

x_1	x_2	x_3	x_4	x_5	
1	0	–	–	–	; 1
–	1	1	1	–	; 1, 2
–	0	–	–	1	; 1
–	1	–	1	0	; 1, 2
–	0	–	0	0	; 2

Извлекаем из системы ДНФ для двух функций:

$$f_1 = x_1\bar{x}_2 \vee \underline{x_2x_3x_4} \vee \bar{x}_2x_5 \vee \underline{x_2x_4\bar{x}_5}\,,$$

$$f_2 = \bar{x}_2\bar{x}_4\bar{x}_5 \vee \underline{x_2x_4\bar{x}_5} \vee \underline{x_2x_3x_4}.$$

Эти ДНФ представлены матрицами в коде Грея на рис. 1.

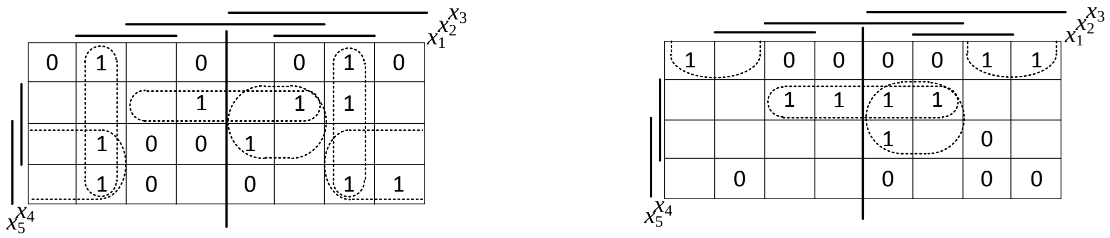

Рис. 1. Матричное представление ДНФ системы
Fig. 1. Matrix presentation of system SoPs

В системе расщепление возможно для двух конъюнкций: $K_1 = x_2x_3x_4$ и $K_2 = x_2x_4\bar{x}_5$, поскольку их характеристики содержат две функции системы. Для расщепления выбираем конъюнкцию системы $K_1 = x_2x_3x_4; 1,\ 2$. Для этой конъюнкции имеем:

$$x_2, h_{\text{р}} = \{f_1\}, h_{\text{нр}} = \{f_2\},$$

$$x_3, h_{\text{р}} = \{f_2\}, h_{\text{нр}} = \{f_1\},$$

$$x_4, h_{\text{р}} = \{\emptyset\}, h_{\text{нр}} = \{f_1, f_2\}.$$

Рассматриваемая конъюнкция может расщепляться как по переменной x_2, так и по переменной x_3. Безразлично, какую переменную выбрать. Выбираем переменную x_2. В этом случае конъюнкция системы $K_1 = x_2x_3x_4; 1,\ 2$ заменяется на конъюнкцию системы $x_3x_4; 1$ которая не может быть расширена и, следовательно, является простой импликантой системы. Вторая конъюнкция системы $x_2x_3x_4; 2$ может быть расширена по переменной x_3. В результате имеем простую импликанту $x_2x_4; 2$. Новая система показана на рис. 2.

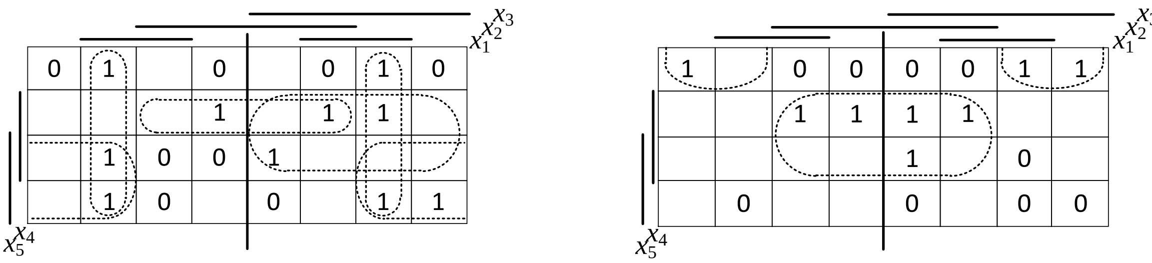

Рис. 2. Матричное представление аппроксимирующей системы
Fig. 2. Matrix presentation of approximate system SoPs

Выполнение операции расщепления требует затем проверки системы на безызбыточность по характеристикам. Так, в полученной системе для конъюнкции $x_2x_4\bar{x}_5; 1,\ 2$ функция f_2 в характеристике является избыточной, и ее следует удалить из характеристики этой конъюнкции. В результате имеем систему

x_1	x_2	x_3	x_4	x_5	
1	0	–	–	–	; 1
–	–	1	1	–	; 1
–	0	–	–	1	; 1
–	1	–	1	0	; 1
–	1	–	1	–	; 2
–	0	–	0	0	; 2

В ней число конъюнкций увеличилось на единицу. Сумма рангов также увеличилась на единицу. В системе отсутствуют общие конъюнкции. Ее можно рассматривать как аппроксимирующую систему. Для нее имеем следующую систему ДНФ:

$$f_1^{\text{апр}} = x_1\bar{x}_2 \lor x_3x_4 \lor \bar{x}_2x_5 \lor x_2x_4\bar{x}_5\,,$$

$$f_2^{\text{апр}} = x_2x_4 \lor \bar{x}_2\bar{x}_4\bar{x}_5,$$

которая представлена матрицами в коде Грея (см. рис. 2).

Заключение

Предложен подход к построению аппроксимирующих схем на основе предварительного получения аппроксимирующих систем булевых функций для синхронного автомата. Аппроксимирующие системы строятся из безызбыточной системы ДНФ (БСДНФ), являющейся реализацией системы частичных функций синхронного автомата. Полученные системы далее используются в качестве задания на синтез соответствующих схем, применяемых в схеме троирования наряду со схемой, построенной по БСДНФ. Аппроксимирующие системы ориентированы на защиту схемы троирования от внедрения вредоносных подсхем (Trojan Circuits). Этот подход позволяет исключить при троировании незащищенную область, которая обязательно присутствует при использовании известных ранее подходов к синтезу аппроксимирующих комбинационных схем.

Список источников

1. Sanchez Clemente A., Entrena L., Garsea-Valderas M., Lopez-Ongil C. Logic masking for SET mitigation using approximate logic circuits // Proc. of 18th IOLTS. 2012. P. 176–181.
2. Sanchez Clemente A.J. Transient error mitigation by means of approximate logic circuits : Thesis Doctoral / Universidad Carlos III de Madrid. Madrid, 2017.
3. Chaudhury M.R., Mohandram K.. Approximate logic circuits for low overhead non-intrusive concurrent error detection // Proceedings of DATE. 2008. P. 902–908.
4. Kohavi I., Kohavi Z. Detection of multiple faults in combinational logic networks // IEEE Transactions on Computers. 1972. V. C-21, № 6. P. 556–558.
5. Матросова А.Ю. Построение полного теста для схем, синтезированных методом факторизации // Автоматика и вычислительная техника. 1978. № 5. С. 42–45.

References

1. Sanchez Clemente, A., Entrena, L., Garsea Valderas, M. & Lopez-Ongil, C. (2012) Logic Masking for SET Mitigation Using Approximate Logic Circuits. *Proc. of 18th IOLTS.* pp. 176–181.
2. Sanchez Clemente, A.J. (2017) *Transient Error Mitigation by Means of Approximate Logic Circuits*. *Doctoral Thesis.* Universidad Carlos III de Madrid.
3. Chaudhury, M.R., Mohandram, K. (2008) Approximate Logic Circuits for Low Overhead Non-Intrusive Concurrent Error Detection. *Proc. of DATE*. pp. 902–908.
4. Kohavi, I. & Kohavi, Z. (1972) Detection of Multiple Faults in Combinational Logic Networks. *IEEE Transactions on Computers.* C-21(6). pp. 556–558.
5. Matrosova, A.Yu. (1978) Construction of a complete test for circuits synthesized by the factorization method. *Avtomatika i vychislitel'naya tekhnika – Automatic Control and Computer Sciences*. 5. pp. 42–45.

***Информация об авторах*:**
Останин Сергей Александрович – доцент, кандидат технических наук, заведующий кафедрой компьютерной безопасности Института прикладной математики и компьютерных наук Национального исследовательского Томского государственного университета (Томск, Россия). E-mail: sergeiostanin@yandex.ru

Матросова Анжела Юрьевна – профессор, доктор технических наук, профессор кафедры компьютерной безопасности Института прикладной математики и компьютерных наук Национального исследовательского Томского государственного университета (Томск, Россия). E-mail: mau11@yandex.ru

Андреева Валентина Валерьевна – доцент, кандидат технических наук, доцент кафедры компьютерной безопасности Института прикладной математики и компьютерных наук Национального исследовательского Томского государственного университета (Томск, Россия). E-mail: avv.21@mail.ru

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Information about the authors:
Ostanin Sergey O. (Candidate of Technical Sciences, Associate Professor, National Research Tomsk State University, Tomsk, Russian Federation). E-mail: sergeiostanin@yandex.ru
Matrosova Angela Yu. (Doctor of Technical Sciences, Professor, National Research Tomsk State University, Tomsk, Russian Federation). E-mail: mau11@yandex.ru
Andreeva Valentina V. (Candidate of Technical Sciences, Associate Professor, National Research Tomsk State University, Tomsk, Russian Federation). E-mail: avv.21@mail.ru

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Received 29.09.2022; accepted for publication 01.03.2023

Поступила в редакцию 29.09.2022; принята к публикации 01.03.2023