

ДИСКРЕТНЫЕ ФУНКЦИИ И АВТОМАТЫ

УДК 519.714

Л.Д. Черемисинова, Д.Я. Новиков

ПРОВЕРКА СХЕМНОЙ РЕАЛИЗАЦИИ ЧАСТИЧНЫХ БУЛЕВЫХ ФУНКЦИЙ

Рассматривается задача верификации логических описаний одного и того же устройства, первое из которых поведенчески не полностью определено и задано в виде системы частично определенных булевых функций, а второе – задано в виде комбинационной схемы (в базисе многовыходовых логических элементов типа И, ИЛИ). Предлагается комбинированный подход к проверке схемной реализации системы частично определенных булевых функций, который основан на моделировании комбинационной схемы на наборах значений входных переменных и сведении к задаче проверки выполнимости конъюнктивной нормальной формы (КНФ).

Ключевые слова: верификация, комбинационная схема, моделирование.

Полупроводниковая промышленность за последнее десятилетие сделала возможным проектирование сверхбольших интегральных схем (СБИС), состоящих из сотен миллионов транзисторов. В то же время все возрастающая важность быстрой поставки продукции на рынок требует производить схемы за короткое время. В таких условиях появление ошибки в функциональности проектируемых устройств обходится очень дорого. По мере усложнения СБИС все более ответственным этапом проектирования становится верификация. Целью верификации является доказательство того, что реализованное и требуемое поведение проектируемого устройства совпадают. В настоящее время верификация используется на всех этапах проектирования: от концептуального проектирования до проектирования комбинационных схем, и занимает до 70% общего времени проектирования.

Задача верификации в традиционной постановке состоит в проверке функциональной эквивалентности пары комбинационных схем, представляющих разные структурные реализации одного и того же устройства. Решению этой задачи посвящены многочисленные научные публикации, ссылки на некоторые из них можно найти в [1 – 5]. При проверке эквивалентности комбинационных схем обе верифицируемые схемы обычно преобразуются в одну схему, называемую схемой сравнения. Схема сравнения – это комбинационная схема с теми же самыми входами, что и исходная схема и одним выходом. Она получается путем объединения пар одноименных входов схем и подачи пар одноименных выходов схем на двухвходовые элементы «исключающее ИЛИ», выходы которых подаются на элемент ИЛИ. Константа 0 на выходе элемента ИЛИ появляется тогда и только тогда, когда исходные схемы эквивалентны, т.е. порождают одинаковые значения на выходах при любых возможных комбинациях сигналов на входах.

В данной статье задача верификации рассматривается для случая, когда заданная функциональность проектируемого устройства не полностью определена. Такая ситуация обычно возникает на начальных этапах проектирования, когда существуют такие комбинации значений входных переменных проектируемого устройства, которые никогда не появятся при нормальном режиме его работы. В процессе проектирования устройства его выходные реакции на такие входные воздействия доопределяются произвольным образом. В этом случае при решении задачи верификации достаточно рассмотреть только возможные сценарии поведения верифицируемого устройства и проверить, имеют ли выходные реакции реализованного устройством поведения специфицированные значения.

В настоящее время наиболее широко используемым в промышленности подходом для проверки функциональности цифровых интегральных схем является логическое моделирование по причине простоты его реализации и предсказуемости времени выполнения. Этот подход основан на тестировании устройства путем подачи на его входы двоичных сигналов, продвижения их по схеме и соответствующей активации выходов, на которых сигналы должны иметь ожидаемые значения. Для рассматриваемого случая верификации можно применить особый тип моделирования, а именно направленное моделирование, когда тестирующие входные воздействия задаются спецификацией на проектирование устройства. Данная идея развивается в настоящей работе для случая, когда исходная спецификация проектируемого устройства задана на наборах значений входных переменных или интервалах (совокупностях наборов) небольшого размера. В том случае, когда исходное задание определено на интервалах большого размера, моделирование практически не применимо, поскольку необходимое расщепление интервалов на отдельные наборы в этом случае приводит к «экспоненциальному взрыву». Для такого случая в настоящей работе предлагается метод, основанный на сведении задачи верификации к задаче проверки выполнимости КНФ.

Таким образом, в данной статье рассматривается задача верификации для случая, когда:

- 1) спецификация на проектирование задана в виде системы частично определенных булевых функций;
- 2) функции системы заданы на интервалах значений входных переменных;
- 3) система реализована комбинационной схемой в базисе многовыходовых логических элементов типа И, ИЛИ, И-НЕ, исключающее ИЛИ и т.д. и инверторов.

Предлагается комбинированный подход к проверке, реализуется ли система частично определенных булевых функций заданной комбинационной схемой. Метод основан на моделировании комбинационной схемы на наборах значений входных переменных части области задания системы функций и сведении проверки реализации остальной части к задаче выполнимости КНФ.

2. Основные определения

2.1. Булевы функции и их представления

Система $F = \{f_1(X), f_2(X), \dots, f_m(X)\}$ (или $f(x)$ в векторной форме, где x и f векторы значений входных и выходных переменных) полностью определенных булевых функций (ПБФ) есть отображение между n -мерным и m -мерным булевыми пространствами $E = \{0, 1\}$: $f(x): E^n \rightarrow E^m$. Частично определенная булева функция (ЧБФ) задается отображением $f(x): E^n \rightarrow \{0, 1, -\}^m$, где символ «-» обозначает неопределенное значение. ЧБФ не полностью определена на всем булевом про-

пространстве E^n . ПБФ $f(x)$ реализует ЧБФ $g(x)$, если $f(x)$ можно получить из $g(x)$ доопределением (до 0 или 1) значений $g(x)$ на тех элементах пространства E^n , на которых ее значения не определены.

Множество равенств типа $x_i = \sigma_i$ (где $\sigma_i \in \{0, 1\}$, $i = \{1, 2, \dots, n\}$) назовем присваиванием значений компонентам вектора $x = (x_1, x_2, \dots, x_n)$. Присваивание a значений компонентам вектора x может быть полным, если задаются все x_i , или частичным в противном случае. Полное присваивание представляет собой элемент (набор), а частичное присваивание – интервал булевого пространства E^n . Интервал ранга k фиксирует значения k переменных и покрывает 2^{n-k} элементов булева пространства. Его можно представить также в виде конъюнкции k литералов (под литералом понимается булева переменная или ее отрицание). В общем случае элементарная конъюнкция k_j и соответствующий ей интервал покрывает (или поглощает) элементарную конъюнкцию k_i (и соответствующий ей интервал), если множество литералов из k_j являются подмножеством литералов из k_i .

ЧБФ $f(x)$ задается множествами U_f^0 , U_f^1 и U_f^{ds} интервалов (или элементов) булева пространства E^n , на которых она принимает соответственно нулевое, единичное и неопределенное значения, при этом $U_f^1 \cup U_f^0 \cup U_f^{ds} = E^n$. Будем задавать систему ЧБФ $f(x)$ множеством многовыходных интервалов. Многовыходной интервал (u, t) представляется парой троичных векторов длины n и m , которые называются соответственно его входной и выходной частями. Входная часть u представляет собой интервал из E^n или конъюнкцию литералов некоторых $x_i \in X$. Выходная часть t является троичным вектором значений функций на интервале u или конъюнкцией литералов некоторых $f_i \in F$. Для каждой функции $f_i \in F$ справедливо: если j -я компонента t^j вектора t есть 1 ($t^j = 1$) или 0 ($t^j = 0$), то все элементы интервала u принадлежат множеству $U_{f_j}^1$ единичных значений функции f_j или соответственно множеству $U_{f_j}^0$ ее нулевых значений; если же значение t^j не определено ($t^j = \langle - \rangle$), то функция f_j либо может принимать разные значения на разных наборах из интервала u , либо ее значение может быть не определено на всем интервале.

Конъюнктивная нормальная форма представляет булеву функцию в виде конъюнкции одного или более дизъюнктов. Каждый дизъюнкт, в свою очередь, является дизъюнкцией одного или более литералов (соответствующих разным переменным).

КНФ задает некоторую полностью определенную булеву функцию $f(x)$, и каждый из ее дизъюнктов соответствует имплиценте этой функции. Задача проверки выполнимости КНФ заключается в нахождении такого присваивания (может быть частичного) значений переменным из X , которое обращает КНФ в 1. Если такое присваивание удастся найти, то говорят, что КНФ выполнима и полученное присваивание называют выполняющим эту КНФ. Иначе КНФ не выполнима, невыполнимая КНФ представляет функцию, тождественно равную 0.

Матричные модели представления булевых функций и КНФ. Матричное представление КНФ, имеющей k дизъюнктов и n переменных, задается троичной матрицей C , строки которой задают дизъюнкты, столбцы соответствуют переменным. Элемент c_{ij} на пересечении i -й строки и j -го столбца матрицы C принимает значение 1, 0 или $\langle - \rangle$, в зависимости от формы (x_j или $\bar{x}_j$) переменной x_j или ее отсутствия в i -ом дизъюнкте КНФ. Аналогичным образом ЧБФ $f(x)$ в матричном виде представляется парой троичных матриц U_f^1 и U_f^0 , в которых каждая строка соответствует некоторому интервалу из U_f^1 и U_f^0 соответственно.

Система ЧБФ $f(x)$, заданная множеством S многовыходных интервалов (u_i, t_i) , может быть представлена парой троичных матриц U и T с одинаковым числом строк (рис. 1). Строки матрицы U задают входные части многовыходных интервалов из S ; аналогично строки матрицы T задают их выходные части.

	x_1	x_2	x_3	x_4	x_5		f_1	f_2	
	—	—	1	1	1		1	—	1
	1	1	—	—	—		1	0	2
$U =$	—	0	0	0	—	$T =$	0	1	3
	0	1	—	1	0		0	0	4
	—	0	1	0	—		—	0	5
	—	0	—	1	0		—	1	6

Рис. 1. Пример матричного задания системы частично определенных булевых функций

Представление функций в форме многовыходных интервалов имеет следующие отличительные особенности. Интервалы $u_i, u_j \in U$ могут пересекаться (в отличие от задания функции на наборах значений аргументов). Неопределенное значение элемента t_i^j матрицы T может трактоваться двояко: или значение функции f_j не определено на всем интервале u_i , или функция f_j принимает разные значения на отдельных наборах этого интервала.

2.2. Комбинационная схема

Рассматриваемая комбинационная схема представляет собой сеть из инверторов и многовыходных логических элементов, которые реализуют простые логические функции типа И, ИЛИ, И-НЕ, ИЛИ-НЕ, исключающее ИЛИ и т.д. На рис. 2 приведен пример комбинационной схемы с пятью входами, двумя выходами и семью логическими элементами. Структура комбинационной схемы может быть представлена направленным ациклическим графом, в котором вершины соответствуют логическим элементам, внешним входам и выходам схемы, а ребра — соединениям элементов и внешних полюсов.

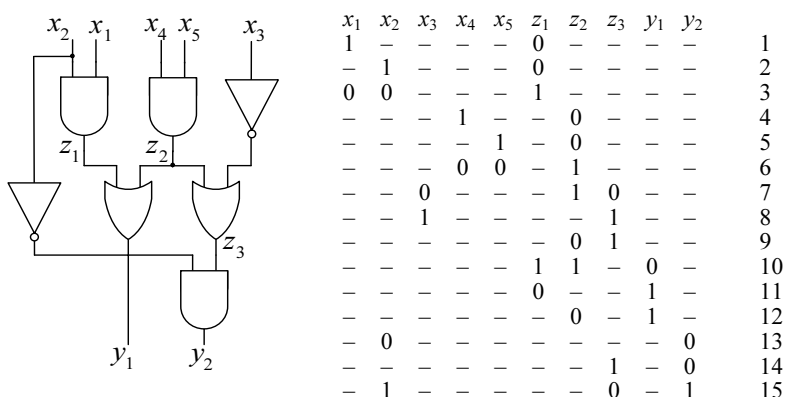


Рис. 2. Комбинационная схема и ее КНФ разрешения

Будем обозначать выходные полюсы элементов и сами элементы одним и тем же именем. Локальная функция элемента (полюса схемы) определяет зависимость сигнала на выходе элемента от сигналов на его входах (т. е. задается в терминах локальных входных переменных). Глобальная функция элемента (полюса) определяет зависимость сигнала на выходе элемента от сигналов на входах схемы (т. е. задается в терминах входных переменных схемы).

3. Верификация, основанная на моделировании комбинационной схемы

При проверке реализуемости системы частично определенных булевых функций поведение комбинационной схемы моделируется на области задания этой системы. Система F булевых функций, заданная множеством S многовыходных интервалов, реализуется схемой, если для каждого набора b_k значений переменных, покрываемого входной частью $u_i \in U$ каждого из многовыходных интервалов $(u_i, t_i) \in S$, выполняется условие поглощаемости булева вектора $y(b_k)$ значений функций, реализуемых на выходах схемы, троичным вектором $t_i \in T$.

Будем использовать идею параллельного моделирования [6, 7], проводя моделирование многовыходной логической схемы сразу на всех двоичных наборах, покрываемых входными частями $u_i \in U$ многовыходных интервалов $(u_i, t_i) \in S$. При переходе к представлению системы F на наборах многовыходной интервал $(u_i, t_i) \in S$ порождает 2^{n-k} многовыходных наборов (b_{ji}, t_i) , где k – ранг интервала u_i , b_{ji} – набор значений переменных, покрываемый интервалом u_i . После «раскрытия» многовыходных интервалов и группирования полученных многовыходных наборов, имеющих равные входные части, каждое из множеств многовыходных наборов (b, t_i) (с одной и той же входной частью b) заменяется одним многовыходным набором (b, t) , где t поглощается каждой из выходных частей t_i этих наборов.

Таким образом, троичная матрица U преобразуется в булеву матрицу B , задающую наборы значений входных переменных системы F , а матрица T преобразуется в матрицу T' , задающую значения частично определенных булевых функций на этих наборах.

При параллельном моделировании схемы на l наборах состояние каждого полюса (включая входные и выходные) схемы представляется булевым вектором размерности l . Таким образом, каждый вектор представляет состояния одного полюса для всех l состояний на входе схемы, а совокупность одноименных компонент всех векторов соответствует состоянию всех полюсов схемы для одного и того же входного набора.

В начале моделирования имеется упорядоченное множество n булевых векторов размерности l , представляющих состояния n входных полюсов для всех l наборов. Затем последовательно просматриваются элементы (в порядке возрастания их номеров) предварительно ранжированной схемы, и для каждого i -го элемента вычисляется локальная функция $\varphi_i(z_{1i}, z_{2i}, \dots, z_{ki})$ путем выполнения операции φ_i над переменными $z_{1i}, z_{2i}, \dots, z_{ki}$, приписанными входам элемента. Так как каждому из аргументов z_{ji} рассматриваемой функции соответствует булев вектор z_{ji} , то операция φ_i выполняется покомпонентно над булевыми векторами $z_{1i}, z_{2i}, \dots, z_{ki}$. Результатом операции является новый вектор z_i той же размерности l .

После просмотра последнего элемента схемы будут найдены ее реакции на все наборы значений входных переменных, покрываемые входными частями $u_i \in U$

многовыходных интервалов $(u_i, t_i) \in S$. При этом каждая выходная функция y_j схемы имеет определенное значение (0 или 1) на всех наборах значений входных переменных, в частности и на тех, на которых определенное значение имеет и соответствующая функция $f_j \in F$. Остается только сравнить векторы y_j и f_j на ортогональность, это сводится к проверке, не ортогональны ли следующие пары векторов: троичный вектор t_j , соответствующий j -му столбцу матрицы T' , и булев вектор z_p , соответствующий j -му выходному полюсу схемы. Реализуемость системы комбинационной схемой имеет место, если пары векторов для всех j не ортогональны. В случае ортогональности некоторой пары можно путем обратного прослеживания логической схемы найти элемент, ответственный за нарушение условия реализации.

Проверку схемной реализации системы функций путем моделирования целесообразно использовать в том случае, когда невелико число многовыходных интервалов (u_i, t_i) множества S , входные части которых (т.е. векторы u_i) имеют малые ранги, т.е. много неопределенных компонентов. В этом случае можно надеяться, что число строк матрицы U , задающей систему ЧБФ, не возрастет резко при расщеплении интервалов на наборы. Если же входные части многовыходных интервалов, задающих систему ЧБФ, представляют собой интервалы малого ранга, то при переходе к заданию функций на наборах значений переменных число строк матрицы U может возрасти в такой степени, что задача верификации может стать практически не решаемой. В этом случае для проверки реализации системы ЧБФ комбинационной схемой целесообразно использовать метод, основанный на сведении к задаче проверки выполнимости КНФ.

4. Верификация, основанная на сведении к задаче проверки выполнимости КНФ

Традиционно задача верификации состоит в проверке функциональной эквивалентности пары комбинационных схем, представляющих разные структурные реализации одного и того же устройства. Проверка функциональной эквивалентности производится с помощью SAT-решателей и обычно сводится к проверке выполнимости КНФ. Соответственно для того, чтобы воспользоваться SAT-решателем необходимо привести задание сравниваемых комбинационных схем к виду КНФ [1, 5].

4.1. Построение КНФ разрешения комбинационной схемы

Во многих SAT-приложениях строится так называемая КНФ разрешения схемы [5, 8], которая задает все возможные допустимые комбинации сигналов на всех ее $n + l$ полюсах, где n – число входных полюсов схемы, l – число элементов.

При применении данного преобразования для каждого логического элемента комбинационной схемы вводятся внутренние булевы переменная, приписываемая его выходному полюсу. Далее рассматриваются локальные функции логических элементов. Построение функции разрешения элемента, реализующего локальную функцию $y = f(z_1, z_2, \dots, z_k)$, основано на построении таблицы истинности для функции $g(y, f(z))$, которая определяет допустимые комбинации на его выходном полюсе y и k входных полюсах, то есть комбинации, для которых $f(z) = y$. КНФ такой функции $g(z, f(x))$ традиционно называется КНФ разрешения соответст-

вующего элемента. КНФ разрешения всех элементов схемы объединяются операцией конъюнкции в одну КНФ – КНФ разрешения схемы. Размер КНФ разрешения схемы и сложность данного преобразования линейно зависят от числа логических элементов комбинационной схемы.

КНФ разрешения для логических элементов НЕ, k -входовых элементов И и ИЛИ, из которых построена комбинационная схема, приведенная на рис. 2, имеют следующий вид:

$$\begin{aligned} & (z \vee y)(\bar{z} \vee \bar{y}); \\ & (z_1 \vee \bar{y})(z_2 \vee \bar{y}) \dots (z_k \vee \bar{y})(\bar{z}_1 \vee \bar{z}_2 \vee \dots \vee \bar{z}_k \vee y); \\ & (\bar{z}_1 \vee y)(\bar{z}_2 \vee y) \dots (\bar{z}_k \vee y)(z_1 \vee z_2 \vee \dots \vee z_k \vee \bar{y}). \end{aligned}$$

КНФ разрешения инвертора (и соответствующую переменную y , приписанную его выходному полюсу) можно не включать в КНФ разрешения схемы, заменив все переменные y отрицанием входной переменной z инвертора.

На рис. 2 изображена комбинационная схема и ее КНФ разрешения.

4.2. Анализ КНФ разрешения

Если некоторая задача сформулирована в терминах проверки выполнимости КНФ, для ее решения можно привлечь SAT-решатель. Напомним, что КНФ выполнима тогда и только тогда, когда существует такое присваивание значений ее переменным, которое удовлетворяет каждый дизъюнкт данной КНФ. Это присваивание называется выполняющим присваиванием. Если к КНФ разрешения схемы добавить некоторый однолитеральный дизъюнкт, например y_i , то в любом наборе значений переменных, выполняющем полученную КНФ, переменная y_i будет иметь значение 1. Таким образом, значение 1 функции y_i , реализуемой схемой, доставляют наборы, выполняющие полученную КНФ, и только они.

В общем случае, пусть y_i^σ (где $\sigma \in \{0, 1\}$) – литерал переменной y_i , а точнее, $y_i^1 = y_i$ и $y_i^0 = \bar{y}_i$. Тогда однолитеральный дизъюнкт y_i^σ задает присваивание $y_i = \sigma$. Для того чтобы проверить, реализуется ли на выходе y_i комбинационной схемы константа σ , воспользуемся доказательством от противного: докажем, что на выходе y_i реализуется константа $\bar{\sigma}$. На первом шаге добавим к КНФ разрешения схемы однолитеральный дизъюнкт $y_i^{\bar{\sigma}}$, затем с помощью SAT-решателя будем искать выполняющее полученную КНФ присваивание a , в котором $y_i = \bar{\sigma}$. Такое присваивание является контрпримером. Если контрпримера не существует, то на выходе y_i схемы реализуется константа σ .

4.3. Проверка реализуемости схемой многовыходных интервалов

Пусть имеется КНФ разрешения C , описывающая некоторую комбинационную схему, и система ЧБФ $f(x)$, аргументы и функции которой соответствуют входам и выходам схемы. Для демонстрации предлагаемого ниже метода будем использовать систему $f(x)$ и комбинационную схему, изображенные на рис. 1 и 2.

Задача заключается в том, чтобы проверить, реализует ли заданная схема системе ЧБФ $f(x)$. Глобальная ПБФ $y_i(x)$ ($i = 1, 2, \dots, m$), реализуемая на i -м выходе схемы, реализует функцию $f_i(x) \in f(x)$ тогда и только тогда, когда

$$U_{f_i}^1 \subseteq U_{y_i}^1 \text{ и } U_{f_i}^0 \subseteq U_{y_i}^0. \quad (1)$$

которые необходимо добавить в КНФ. Для расширенной таким образом КНФ не существует выполняющего ее присваивания, что доказывает равенство значений глобальных функций $y_1(u_2)$ и $y_2(u_2)$ схемы соответственно функциям $f_1(u_2)$ и $f_2(u_2)$ для всех входных наборов из интервала u_2 : $f_1(u_2) = y_1(u_2), f_2(u_2) = y_2(u_2)$.

5. Комбинированный подход к проверке реализуемости системы частично определенных функций

Описанное выше параллельное двоичное моделирование комбинационной схемы на области задания системы частично определенных булевых функций применимо к заданию системы на наборах значений аргументов и наиболее эффективно для этого случая. В случае интервального задания системы функций целесообразен комбинированный метод проверки реализуемости системы частично определенных функций, который предполагает разбиение множества многовыходных интервалов области задания системы на два подмножества, проверяемые по отдельности. В первое подмножество включаются многовыходные наборы и многовыходные интервалы, входная часть которых представлена интервалом большого ранга (интервалом, покрывающим малое число наборов $l \ll n$). Остальные многовыходные интервалы (интервалы малого ранга) составляют второе подмножество.

Реализуемость первой части области задания системы частично определенных булевых функций (подмножества многовыходных наборов) предлагается производить путем параллельного двоичного моделирования. Реализуемость второй части области задания системы частично определенных булевых функций (подмножества многовыходных интервалов) предлагается проверять сведением к задаче проверки выполнимости КНФ. В этом случае сначала строится КНФ разрешения комбинационной схемы. Затем каждый многовыходной интервал второго подмножества проверяется вышеописанным методом сведения к задаче проверки выполнимости КНФ. Чем больше многовыходных интервалов в задании исходной системы частично определенных булевых функций, тем сложнее становится такой подход. Поэтому данный метод целесообразно использовать для проверки реализуемости только тех многовыходных интервалов, у которых входная часть содержит относительно большое число неопределенных компонент.

Заключение

В работе предлагаются алгоритмические средства верификации, ориентированные на случай частично определенных систем функций и в комплексе позволяющие решить задачу проверки их реализуемости для разных способов задания и разной степени определенности булевых функций.

ЛИТЕРАТУРА

1. Drechsler R. (Ed.). Advanced Formal Verification. Kluwer Academic Publishers, 2004.
2. Mishchenko A., Chatterjee S., Brayton R., Een N. Improvements to Combinational Equivalence Checking // Proc. ICCAD'06, Nov. 5 – 9, 2006. San Jose, CA, 2006.
3. Ganai M.K., Zhang L., Ashar P., Gupta A., Malik S. Combining strengths of circuit-based and CNF-based algorithms for a high-performance SAT solver // Proc. ACM/IEEE Design Automation Conference, 2002. P. 747 – 750.
4. Goldberg E., Novikov Y. BerkMin: A fast and robust SAT-Solver // Proc. European Design and Test Conference, 2002. P. 142 – 149.

5. *Kuehlmann A., Cornelis A.J. van Eijk.* Combinational and Sequential Equivalence Checking // *Logic synthesis and Verification* / Eds. S. Hassoun, T. Sasao, R.K. Brayton). Kluwer Academic Publishers, 2002. P. 343 – 372.
6. *Закревский А.Д., Поттосин Ю.В., Черемисинова Л.Д.* Основы логического проектирования. Кн. 3. Проектирование устройств логического управления. Минск: ОИПИ НАН Беларуси, 2006.
7. *Cheremisinova L.* Simulation-based approach to verification of logical descriptions with functional indeterminacy / L. Cheremisinova, D. Novikov // *Information Theories & Applications* (IJ ITA). 2008. V. 15. No. 3. P. 218 – 224.
8. *Tseitin G.C.* On the Complexity of Derivation in Propositional Calculus // *Studies in Constructive Mathematics and Mathematical Logic*. 1968. Part 2. P. 115 – 125. Reprinted in J. Siekmann and G. Wrightson, eds., *Automation of Reasoning*, Springer-Verlag, 1983. V. 2. P. 466 – 483.

Статья представлена кафедрой программирования факультета прикладной математики и кибернетики Томского государственного университета и оргкомитетом 7-й Российской конференции с международным участием «Новые информационные технологии в исследовании сложных структур», поступила в научную редакцию 3 октября 2008 г.