Грузинский университет им. Св. Андрея Первозванного при Патриархии Грузии
Школа (факультет) физико-математическая и компьютерных наук
Направление компьютерных технологий и математического моделирования

На правах рукописи

Нана Бенидзе

Установление критериев верификации(корректности) алгоритмов и программ методами теории автоматов.

Компьютерные науки 04.01.04

Автореферат
научной работы, представленной на соискание академической степени доктора информатики

Тбилиси
2012

Диссертационная работа выполнена в Грузинском Университете им. Св. Андрея Первозванного при Патриархии Грузии, в школе (на факультете) физико-математической и компьютерных наук, по направлению компьютерные технологии и математическое моделирование

Научный руководитель: Церцвадзе Гурам, доктор физико-математических наук, профессор

Официальные рецензенты: 1. **Намичеишвили Олег,** доктор технических наук, профессор.
2. **Пховелишвили Мераб,** кандидат физико-математических наук.
3. **Церетели Паата,** кандидат физико-математических наук.

Защита диссертации состоится 8 октября 2012 г. в 16^{00} часов на заседании диссертационной комисии школы (факультета) физико-математической и компьютерных наук Грузинского Университета им. Св. Андрея Первозванного при Патриархии Грузии.
Адрес: 0162, г. Тбилиси, пр. Ильи Чавчавадзе д. 53^{a}, в зале заседаний.

С диссертацией можно ознакомиться в научной библиотеке Грузинского Университете им. Св. Андрея Первозванного при Патриархии Грузии.

Автореферат разослан 16 июля 2012 г.

Учёный секретарь диссертационного совета **Манана Качахидзе**
Доктор физико-математических наук, профессор

Общая характеристика работы

Актуальность темы исследования. В условиях быстрого и интенсивного роста информационных технологий особо актуальной стала разработка надежного программного обеспечения. Ясно, что чем меньше число случаев допущения ошибок при разработке программ, тем надежнее работа компьютерной техники с таким программным обеспечением. Практика создания программного обеспечения систем информаценной технологии показала, что 2/3 времени, потраченной на создание системы, приходится на ее наладку, т. е. на проверку того, насколько корректна соответствующая программа. К сегодняшнему дню наиболее простым способом проверки корректности(правильности) алгоритмов и соответствующих программ является тестирование. Вместе с тем альтернативой тестированию программ служит возможность их математической верификации(корректности).

Возможность математической верификации программы существенным образом опирается на ее математическую спецификации. Так как программа, реализованная на достаточноточно точно определенном языке программирования, имеет однозначное математическое толкование, поэтому требования к программе могут быть выражены на языке математики и логики как точная спецификация. Однако возможна ситуация, когда спецификация не соответствует в точности тем требованиям , которые предъявляются к программе. В действительности, зачастую оказывается особенно трудно сформулировать математически корректную версию неформальных требований, предъявляемых к программе. Вместе с тем существенно, что такая формализация открывает вожможность строгого доказательства соответствия программы и спецификации.

Описанную выше ситуацию отнасительно общей схемы верификации программ можно представить диаграммой на рисунке 1.

Ввиду того, что постановка и решение задачи верификации существенным образом зависит от неформальных требований, предъявляемых к программе, то поэтому большое значение приобретает в первую очередь постановка математически корректной задачи

исследовании ведущее место занимает вопрос о синтаксической правильности этих программ. Особое значение придается тому, что задача распознавания(т.е. вопрос о том, принадлежит ли заданное слово языку) для языков программирования тесно связана с задачей грамматического разбора. В связи с этим в диссертации подробно рассматривается конечно-автоматное решение этой задачи для случая контекстно – свободных грамматик.

Научная новизна и основные результаты. В диссертационной работе рассмотрена задача верификации(корректности) программ, написанных на контекстно – свободных алгоритмических языках. Для решения поставленной задачи верификации в диссертации развивается новый подход , который основывается на классической теории конечных автоматов и порожденных ими автоматных языков. Изучены математические и синтаксические аспекты задачи верификации программ, написанных на алгоритмических языках. Пользуясь тем, что конечные автоматы являются удобным формализмом, который конечным образом задает обычные формальные языки – бесконечные множества цепочек конечной длины, в диссертации установлены критерии синтаксической правильности программ для определенного класса задач.

Теоретические и методические основы исследования. Теоретические и методические основы исследования составляют идеи, методы и результаты теории автоматов, формальных языков и грамматик, которые яиляются основополагающими для теоретической информатики. Важность этих теориий для информатики обусловлена тем, что наиболее простой и удобной моделью данных, используемых в компьютерных программах, является конечная последовательность, каждый элемент которой взят из некоторого заранее зафиксированного конечного множества.

Практическое значение работы. Формальные методы разработки и анализа корректности(правильности) программ, составляющие содержание диссертации, имеют не только теоретическое, но и практическое значение, так как на их основе может быть создана программная система, предназначенная для задачи синтаксического разбора контекстно – свободных алгоритмических языков. Практическое использование этой программной системы было осуществлено в одной криптологической задаче блочного шифрования. В приложении

приведены программные коды, соответствующие алгоритму этой криптологической задачи

Апробация работы. Основные результаты диссертационной работы докладывались и обсуждались на следующих научных семинарах и конференциях:

1. Международная научная конференция " Информафионные и компьютерные технологии, моделирование и управление". Грузинский технический университет, Тбилиси, 2010.
2. Международная научная конференция "Информафионные и вычислительные технологии".
   Институт вычислительной математики им. Н. Мусхелишвили и Грузинский университет им. Св. Андрея Первозванного при Патриархии Грузии, Тбилиси, 2010.
3. Научный семинар института вычислительной математики им. Н. Мусхелишвили, Тбилиси, 2009.
4. Научно - методический семинар Грузинского университета им. Св. Андрея Первозванного при Патриархии Грузии, Тбилиси, 2012.
5. Шестая и седьмая международная конференция "Интернет - Образование - Наука". Украина, Виница, 2008, 2010 .

Структура и объем работы. Диссертация состоит из введения, трех глав основного текста, заключения, списка цитированной литературы и приложения. Всего диссертация содержит 120 страниц.

Краткое содержание работы

Введение. Во введении обосновывается выбор направления исследования и сформулированы основные задачи, решаемые в диссертации, приводится обзор научной литературы, связанной с темой работы и краткое содержание диссертации.

I глава диссертации – "Обзор методов верификации" – является вводной. Она содержит обзор известных методов верификации программ написанных на алгоритмических языках. Глава содержит три параграфа.

В параграфе 1 рассматривается известный метод Хоара аксиоматической семантики как нерекурсивных, так и рекурсивных программ. Подробно обсуждается принцип декомпозиции и приводятся правила верификации Хоара.

Параграф 2 полностью посвящен рассмотрению метода индуктивных допущении Флоида и анализируются понятия полной и частичной корректности программ.

В параграфе 3 приводится общая схема верификации и рассматривается метод Model Cheking как один из подходов к формальной верификации. Здесь же описывается известная структура Крипке и рассматривается схема работы пакета верификации Spin.

II глава диссертации – "Определение языков программирования с помощью конечных автоматов"

состоит из шести параграфов. В ней рассматривается наиболее расспространенные способы конечного задания формального языка: грамматики и автоматы, соответствующие в иерархии Хомского праволинейным и контекстно – свободным грамматикам. Здесь же рассматривается наболее удобный и компактный способ конечного описания формального языка – регулярные выражения, который находит практическое применение во многих компьютерных приложениях, таких как текстовые редакторы, интерпретаторы командной строки и т.д.

Параграф 1 содержит основные определения и сведения о формальных языках и грамматиках. Приводится их классификация по Хомскому.

В параграфе 2 определяются понятия конечного автомата и распознаваемого конечным автоматом языка.

В параграфе 3 рассматривается связь между автоматами, формальными языками и грамматиками и определяется понятие синтаксического разбора и связанные с ним определения. В этом же параграфе доказана следующая

Теорема. Любому алгоритму синтаксического анализа конкретной $G = (N, \Sigma, P, S)$ грамматики, соответствует конечный автомат $A = (Q, \Sigma', \delta, q_0, F)$.

Параграф 4 посвящен рассмотрению задачи синтаксического разбора, соответствующая контекстно – свободной грамматике. В связи с этой задачей в параграфе доказана следующая

Теорема. Алгоритмам синтаксического разбора контекстно – свободных грамматик соответствует система конечных автоматов.

В параграфе 5 рассматривается алгоритм синтаксического разбора арифметического выражения и решается задача синтеза конечного автомата , соответствующего этому алгоритму.

В параграфе 6 устанавливается критерий правильности алгоритмов синтаксического разбора контекстно – свободных языков. Критерий правильности состоит в следующем:

Ag **алгоритм синтаксического анализа грамматики** G **является корректным, тогда и только тогда, когда можно построит конечный автомат, соответствующий этому алгоритму, т. е.** ***Ag*** **алгоритм синтаксического анализа грамматики** G **является правильным, если он написан на языке регулярных выражении.**

III глава диссертации – "Задача верификации программного обеспечения для криптологических систем" состоит из трех параграфов. В ней рассматривается криптологическая задача блочного шифрования, для которой устанавливается критерий правильности программной системы:

Если D - программа блочного шифрования, а A набор начальных данных, тогда программа D правильна(корректна) тогда и только тогда, когда существует программа дешифровки G такая, что

$$G(B)=A,$$

где $B=D(A)$. Справедливо и обратное утверждение.

В приложении представлены програмные коды, соответствующие алгоритму криптологической задачи, рассматренной в III главе диссертации, а также общий синтаксис алгоритмических языков(C, C++ и java), в рамках формализма Бекуса-Наура.

Заключение В работе достигнуты цели, определенные темой диссертации, т. е. поставлена и решена задача установления критериев верификации(корректности) алгоритмов и программ методами теории автоматов. Вожможность верификации программ существенным образом опирается на ее спецификацию. Однако язык спецификации своиств программной системы может быть неполным, для формулировки всех желаемых требований поведениия системы. Вместе с тем, формулировка неформальных требований на языке спецификациии требует знаний логики своиств программных систем и способов выражения этих своиств на языке логики.

С целью решения поставленной задачи верификации, в диссертации развит новый подход, основанный на теории конечных автоматов и порожденных ими формальных языков. Формальные методы анализа корректности(правильности) программ, разработанный в диссертации, позволили решить задачу установления критериев правильности алгоритмов синтаксического разбора контекстно-свободных языков.

Решена также задача синтеза конечного автомата, соответствующего алгоритму синтаксического разбора.

Практическое использование программной системы синтаксического разбора контекстно-свободных языков было осуществлено в криптологической задаче блочного шифрования, для которой установливаются критерии правильности.

Список опубликованных работ на тему диссертации

1. Бенидзе Н. Задача оценки верификации (корректности) алгоритмов и компьютерных программ. //Международний научно-технический журнал «OPTOELECTRONIC INFORMATION-POWER TECHNOLOGIES». Винница, 2010, №2(20), ст. 80-84.
2. Бенидзе Н. Об устанавлении правильности компьютерных программ. // "Internet Education Science" IES-2010. New Informational and Computer Technologies in Education and Science. Vinnytsia VNTU. septembre 28 - octomber 3, 2010 ,vol. 1, сесю E, page 221-224.
3. Бенидзе Н. К вопросу о корректности программ. "Internet Education Science" IES-2008. New Informational and Computer Technologies in Education and Science. Vinnytsia VNTU. Octomber 7-11, 2008, vol. 2, sec. H, page 545-550.
4. Бенидзе Н. О верификации компьютерных программ. //Тезисы докладов. Международная научная конференция "Информафионные и вычислительные технологии". Институт вычислительной матема-тики им. Н. Мусхелишвили и Грузинский университет им. Святого Андрея Первозванного при Патриархии. Тбилиси, 2-6 мая, 2010, ст. 24 (на Грузинском языке).
5. Бенидзе Н. О корректности компьютерных программ. //Тезисы докладов. Международная научная конференция " Информафионные и компьютерные технологии, моделирование и управление". Грузинский технический университет, Тбилиси, 1-4 ноября, 2010, ст. 123 (на Грузинском языке).
6. Кипшидзе З., Бенидзе Н. Симметричная криптологическая система блочного шифравания. //Тезиси докладов. Международная научная конференция " Информафионные и компьютерные технологии, моделирование и управление". Грузинский технический университет, Тбилиси, 1-4 ноября, 2010, ст. 140 (на Грузинском языке).