საქართველოს საპატრიარქოს წმ. ანდრია პირველწოდებულის სახელობის
ქართული უნივერსიტეტი

ფიზიკა-მათემატიკის და კომპიუტერულ მეცნიერებათა სკოლის
(ფაკულტეტი) კომპიუტერული ტექნოლოგიებისა და მათემატიკური
მოდელირების მიმართულება

ხელნაწერის უფლებით

ნანა ბენიძე

ალგორითმებისა და პროგრამების ვერიფიკაციის (კორექტულობის) კრიტერიუმების დადგენა ავტომატების თეორიის მეთოდებით

კომპიუტერული მეცნიერებები - 04.01.04
ინფორმატიკის დოქტორის აკადემიური ხარისხის მოსაპოვებლად
წარმოდგენილი ნაშრომის
ავტორეფერატი

თბილისი
2012

სადისერტაციო ნაშრომი შესრულებულია წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტის ფიზიკა-მათემატიკისა და კომპიუტერულ მეცნიერებათა სკოლის(ფაკულტეტის) კომპიუტერული ტექნოლოგიებისა და მათემატიკური მოდელირების მიმართულებაზე

სამეცნიერო ხელმძღვანელი: **ცერცვაძე გურამი**, ფიზიკა-მათემატიკის მეცნიერებათა დოქტორი, პროფესორი

ოფიციალური რეცენზენტები: ……
……
……
……
……
……

დისერტაციის დაცვა შედგება 2012 წლის „_____“ _____ _____ საათზე, საქართველოს საპარტიარქოს წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტის ფიზიკა-მათემატიკისა და კომპიუტერულ მეცნიერებათა სკოლის(ფაკულტეტის) სადისერტაციო კომისიის სხდომაზე.
მისამართი: 0162, თბილისი, ილია ჭავჭავაძის №53ა. აუდიტორია № .
დისერტაციის გაცნობა შეიძლება საქართველოს საპატრიარქოს წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტის სამეცნიერო ბიბლიოთეკაში

ავტორეფერატი დაიგზავნა 2012 წლის „__“ _____

სადისერტაციო საბჭოს სწავლული მდივანი მანანა კაჭახიძე
ფიზ.-მათ. მეცნიერებათა დოქტორი, პროფესორი

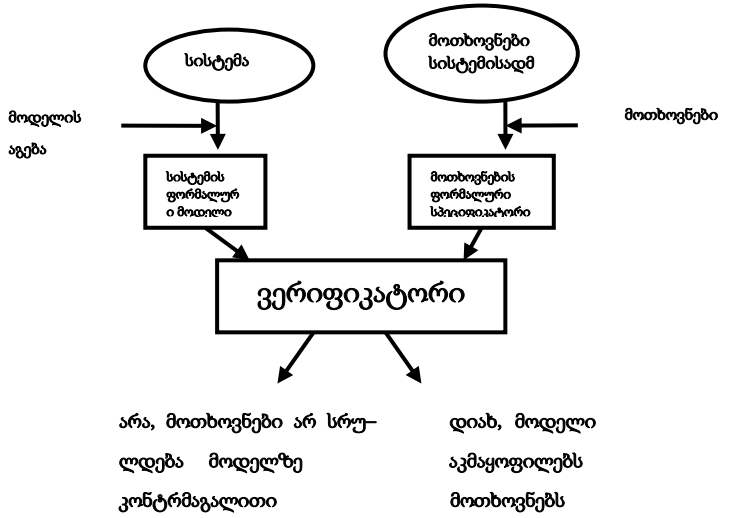
ნაშრომის ზოგადი დახასიათება

კვლევითი თემის აქტუალობა. საინფორმაციო ტექნოლოგიების სწრაფი და ინტენსიური ზრდის პირობებში განსაკუთრებით აქტუალური გახდა საიმედოდ გამართული პროგრამული უზრუნველყოფის შემუშავება. ცხადია, რაც უფრო ნაკლებია შეცდომების დაშვების შემთხვევები შესაბამის პროგრამულ უზრუნველყოფაში, მით უფრო საიმედოა ასეთი პროგრამული უზრუნველყოფის პირობებში მომუშავე კომპიუტერული ტექნიკა. საინფორმაციო ტექნოლოგიების პროგრამული უზრუნველყოფის შექმნის პრაქტიკამ აჩვენა, რომ სისტემის შექმნაზე დახარჯული დროის 2/3 მოდის მის გამართვაზე, ანუ იმის შემოწმებაზე, თუ რამდენად კორექტულია შესაბამისი პროგრამა. დღეისათვის ალგორითმებისა და შესაბამისი პროგრამების კორექტულობის(სისწორის) შემოწმების ყველაზე მარტივ საშუალებას წარმოადგენს ტესტირება. თუმცა პროგრამული ტექნოლოგიების განვითარების კვალდაკვალ ტესტირების ალტერნატივად მოიაზრება პროგრამების მათემატიკური ვერიფიციკაცია(კორექტულობა).

პროგრამის მათემატიკური ვერიფიკაციის შესაძლებლობა არსებითად ეფუძნება მის მათემატიკურ სპეციფიკაციას. მაგრამ ხშირია შემთხვევები და სიტუაციები, როდესაც პროგრამის მათემატიკური სპეციფიკაცია ზუსტად არ შეესაბამება პროგრამის მიმართ რეალურად წაყენებულ მოთხოვნებს. აქ განსაკუთრებული სირთულეების დაძლევასთან არის დაკავშირებული პროგრამის მიმართ არაფორმალური მოთხოვნების მათემატიკურად კორექტული ვერსიის ფორმულირება. არსებითია ის, რომ ასეთი ფორმალიზაცია იძლევა პროგრამისა და სპეციფიკაციის შესაბამისობის მკაცრად დამტკიცების შესაძლებლობას.

საკითხები, რომლებიც წარმოდგენილ სადისერტაციო ნაშრომშია განხილული, ეხება ალგორითმულ ენებზე დაწერილი პროგრამების ვერიფიკაციის ამოცანას ამ პროგრამების მიმართ წაყენებული არაფორმალურ მოთხოვნათა გათვალისწინებით.

ზემოთ აღნიშნულის გათვალისწინებით ალგორითმულ ენებზე დაწერილი პროგრამების ვერიფიკაციის საერთო სქემა შემდეგნაირია



ნახ 1. ვერიფიკაციის საერთო სქემა

ვინაიდან პროგრამების ვერიფიკაციის ამოცანის დასმა და გადაწყვეტა არსებითად დაკავშირებულია პროგრამების მიმართ წაყენებულ არაფორმალურ მოთხოვნებთან, ამიტომ განსაკუთრებულ მნიშვნელობას იძენს ვერიფიკაციის მათემატიკურად კორექტული ამოცანის დასმა ზემოთ აღნიშნული არაფორმალური მოთხოვნების პირობებში.

ამ ამოცანის გადაწყვეტის მიზნით დისერტაციაში განვითარებულია ახალი მიდგომა, რომელიც ეფუძნება სასრული ავტომატის ფორმალურ მოდელს, რომლის ფარგლებში მოხერხებული აღმოჩნდა არა მარტო სასრულ-ავტომატური ალგორითმული ენების აღწერა და ანალიზი, არამედ ამ ენებზე დაწერილი პროგრამების ვერიფიკაციის მათემატიკურად კორექტული ამოცანის დასმა და გადაწყვეტა.

ამრიგად, წარმოადგენს რა ალგორითმებისა და მათი შესაბამისი პროგრამების ტესტირების ალტერნატივას, პროგრამების ვერიფიკაციის სასრულ–ავტომატური მეთოდი არსებითად ემყარება ზუსტ სპეციფიკაციას, როგორც პროგრამის მიმართ არაფორმალური მოთხოვნების მათემატიკურად კორექტული ვერსიის გამოხატვის შესაძლებლობას ავტომატების თეორიის ენაზე.

კვლევის მიზანი. სადისერტაციო ნაშრომის კვლევის მიზანს წარმოადგენს ალგორითმულ ენებზე დაწერილი პროგრამების ვერფიკაციის(კორექტულობის) ამოცანასთან დაკავშირებული საკითხების შესწავლა და მისი გადაწყვეტის სასრულ–ავტომატური მეთოდების დამუშავება. კვლევაში წამყვანი ადგილი უჭირავს პროგრამების სისწორის საკითხს. განსაკუთრებული მნიშვნელობა ენიჭება იმას, რომ ამოცნობის ამოცანა(ე.ი. საკითხი იმის შესახებ, რომ მოცემული სიტყვა ეკუთვნის თუ არა ენას) დაპროგრამების ენებისათვის პირდაპირ დაკავშირებულია გრამატიკული გარჩევის ამოცანასთან. ამასთან დაკავშირებით დისერტაციაში დეტალურად არის განხილული მისი სასრულ–ავტომატური გადაწყვეტა კონტექსტურად–თავისუფალი გრამატიკების შემთხვევისათვის.

მეცნიერული სიახლე და ძირითადი შედეგები. დისერტაციაში განხილულია ალგორითმული ენებისა და მათზე დაწერილი პროგრამების ვერიფიკაციის(კორექტულობის) ამოცანასთან დაკავშირებული საკითხები. აღნიშნული ამოცანის გადაწყვეტის მიზნით დისერტაციაში განვითარებულია ახალი მიდგომა, რომელიც დაფუძნებულია სასრული ავტომატების კლასიკურ თეორიაზე.

შესწავლილია ალგორითმული ენებისა და პროგრამების ვერიფიკაციის მათემატიკური და სინტაქსური ასპექტები. დადგენილია პროგრამების კორექტულობის კრიტერიუმები გარკვეული კლასის ამოცანებისათვის.

კვლევის თეორიული და მეთოდოლოგიური საფუძვლები. სადისერტაციო თემის შესრულების მიზნით ჩატარებული კვლევის თეორიულ და მეთოდოლოგიურ საფუძველს შეადგენს ავტომატების თეორიისა და ფორმალური ენების მათემატიკური თეორიის ძირითადი ცნებები და მეთოდები.

ნაშრომის პრაქტიკული მნიშვნელობა. პროგრამების დამუშავებისა და კორექტულობის(სისწორის) ანალიზის ფორმალურ მეთოდებს, რომლებიც დისერტაციაშია დამუშავებული და წარმოდგენილი, თეორიულ მნიშვნელობასთან ერთად გააჩნიათ პრაქტიკული მნიშვნელობაც, ვინაიდან მათი საშუალებით შეიძლება აიგოს პროგრამული სისტემა, რომელიც განკუთვნილია კონტექსტურად-თავისუფალი ალგორითმული ენების სინტაქსური გარჩევის ამოცანისათვის. ამ სისტემის პრაქტიკაში გამოყენება მოხდა ბლოკური

დაშიფვრის სიმეტრიული კრიპტოლოგიური სისტემის შესაბამისი ალგორითმისთვის. დანართში მოყვანილია ამ ალგორითმის შესაბამისი პროგრამის პროგრამული კოდები.

ნაშრომის აპრობაცია. დისერტაციაში მიღებული ძირითადი შედეგები წარდგენილი იყო საქართველოს ტექნიკური უნივერსიტეტის საერთაშორისო სამეცნიერო კონფერენციაზე „საინფორმაციო და კომპიუტერული ტექნოლოგიები, მოდელირება, მართვა“ (2010წ.), ნიკო მუსხელიშვილის გამოთვლითი მათემატიკის ინსტიტუტისა და საქართველოს საპატრიარქოს წმიდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტის ერთობლივ საერთაშორისო კონფერენციაზე „ინფორმაციული და გამოთვლითი ტექნოლოგიები“ (2010წ.), ნიკო მუსხელიშვილის გამოთვლითი მათემატიკის ინსტიტუტის სემინარზე (2009წ.), დისერტაციის შედეგები გამოქვეყნებულია “Internet Education Science” IES-2008 New Informational and Computer Technologies in Education and Science. Ukraine, Vinnytsia VNTU საერთაშორისო კონფერენციის მასალებში (2008, 2010), საერთაშორისო მეცნიერულ–ტექნიკურ ჟურნალში «OPTOELECTRONIC INFORMATION-POWER TECHNOLOGIES» №2(20) (2010), ქართული უნივერსიტეტის სამეცნიერო-მეთოდურ სემინარებზე(2012).

დისერტაციის მოცულობა და სტრუქტურა. სადისერტაციო ნაშრომი შედგება შესავალის, სამი თავის, დასკვნის, გამოყენებული ლიტერატურის სიისა და დანართისაგან. დისერტაცია შედგება 120 გვერდისაგან.

დისერტაციის მოკლე შინაარსი თავების მიხედვით.

შესავალი ჩამოყალიბებულია ამოცანის დასმა, მიმოხილულია სადისერტაციო თემასთან დაკავშირებული პრობლემატიკა და ლიტერატურა. ასევე შესავალში მოცემულია დისერტაციის ზოგადი სტრუქტურა.

დისერტაციის პირველ თავში – „ვერიფიკაციის მეთოდების მიმოხილვა“ – განხილულია ვერფიკაციის ყველაზე ცნობილი, კლასიკური მეთოდები. თავი შედგება სამი ქვეთავისაგან.

პირველ ქვეთავში განხილულია ხოარის აქსიომატური სემანტიკის მეთოდი, როგორც არარეკურსიული, ასევე რეკურსიული

პროგრამებისათვის. გადმოცემულია დეკომპოზიციის პრინციპის არსი, მოყვანილია ე.წ. ხოარის ვერიფიკაციის წესები.

მეორე ქვეთავში შეეხება ფლოიდის ინდუქციურ დაშვებათა მეთოდს. ამ თავში მოყვანილია პროგრამის სრული და ნაწილობრივი ჭეშმარიტების(სამართლიანობის) განმარტება და შესაბამისი თეორემები.

მესამე ქვეთავში განხილულია მეთოდი – მოდელებზე შემოწმება (Model cheking). ამავე ქვეთავში მოყვანილია ტემპორალური(დროითი) ლოგიკის განმარტება და ამ ლოგიკისათვის დამახასიათებელი ლოგიკური ოპერაციები, გარჩეულია კრიპკეს სტრუქტურა და ვერიფიკაციის პაკეტის SPIN მუშაობის სქემა.

დისერტაციის მეორე თავი – „დაპროგრამების ენების განსაზღვრა სასრული ავტომატების საშუალებით“

შედგება ექვსი ქვეთავისაგან.

პირველ ქვეთავი შეეხება გრამატიკებსა და ფორმალური ენებს, მოყვანილია გრამატიკებისა და ფორმალური ენების ხომსკის კლასიფიკაცია.

მეორე ქვეთავი მოიცავს ავტომატების თეორიის ზოგიერთი ცნებებს, როგორი სახის ავტომატები არსებობს,როგორ ხდება ენების წარმოდგენა სასრული ავტომატის საშუალებით.

მესამე ქვეთავში – „კავშირი სასრულ ავტომატებსა, ფორმალურ გრამატიკებსა და ენებს შორის“ განხილულია რამდენიმე მნიშვნელოვანი თეორემები, რომელიც ამ კავშირს შეეხება. ამავე თავში დამტკიცებულია ახალი

თეორემა. ნებისმიერი სინტაქსური გარჩევის ალგორითმს (რომელიმე კონკრეტული G გრამატიკის ფარგლებში) შეესაბამება სასრული ავტომატი.

მეოთხე ქვეთავში ჩამოყალიბებულია შემდეგი

თეორემა. კონტექსტურად–თავისუფალი G გრამატიკის შესაბამისი სინტაქსური გარჩევის ალგორითმებს შეესაბამება სასრულ ავტომატთა სისტემა.

მეხუთე ქვეთავში განხილულია არითმეტიკული გამოსახულების სინტაქსური გარჩევის ალგორითმი და აგებულია შესაბამისი სასრული ავტომატი, რომელიც ბუნებრივია ასრულებს თავის მუშაობას, თუ ალგორითმის შესაბამისი პროგრამა კორექტულია.

მეექვსე ქვეთავში ჩამოყალიბებულია სინტაქსური გარჩევის ალგორითმების კორექტულობის პრინციპი:

G გრამატიკის შესაბამისი სინტაქსური ანალიზის Ag ალგორითმი კორექტულია მაშინ და მხოლოდ მაშინ, თუ შესაძლებელია აიგოს ისეთი სასრული ავტომატი, რომელიც შეესაბამება Ag ალგორითმის შესაბამისს პროგრამას. სხვა სიტყვებით ნიშნავს, რომ

G გრამატიკის შესაბამისი სინტაქსური ანალიზის Ag ალგორითმი კორექტულია მაშინ და მხოლოდ მაშინ, თუ ის ჩაწერილია რეგულარულ ხდომილებათა ენაზე.

დისერტაციის მესამე თავში – „პროგრამული უზრუნველყოფის ვერიფიკაციის ამოცანა კრიპტოლოგიური სისტემებისათვის“ – განხილულია ბლოკური დაშიფვრის სიმეტრიული კრიპტოლოგიური სისტემა. თავი შედგება სამი ქვეთავისაგან.

პირველ ქვეთავში აღწერილია ბლოკური დაშიფვრის სიმეტრიული კრიპტოლოგიური სისტემის არსი. განხილულია სისტემის საკვანძო მომენტები – გასაღების ფორმირებისა და სისტემის საერთო სქემის აღწერა.

მეორე ქვეთავში მოყვანილია ამოცანის შესაბამისი ალგორითმები, ხოლო ამ ალგორითმების შესაბამისი პროგრამული კოდები კი დანართი №2-ში.

მესამე ქვეთავში ჩამოყალიბებულია კრიპტოლოგიური ამოცანის შესაბამისი პროგრამების ჭეშმარიტების კრიტერიუმი.

საკუთრივ დაშიფვრის ალგორითმისა და შესაბამისი დეშიფრაციის პროგრამების სამართლიანობის დამტკიცება თავისთავად არ იძლევა იმის გარანტიას, რომ მთლიანად სისტემის შესაბამისი პროგრამული უზრუნველყოფა სწორად მუშაობს. ამიტომაც სავსებით ლოგიკური და გამართლებულია შემდეგი კრიტერიუმი:

თუ D არის დაშიფრაციის პროგრამა და A არის ამ პროგრამის საწყის მონაცემები, მაშინ D პროგრამა ჭეშმარიტია მაშინ და მხოლოდ მაშინ, თუ არსებობს დეშიფრაციის ისეთი G პროგრამა, რომ

$$G(B) = A,$$

სადაც $B = D(A)$ და პირიქით.

დანართში წარმოდგენილია დისერტაციის მესამე თავში განხილული კრიპტოლოგიური ამოცანის ალგორითმების შესაბამისი პროგრამების პროგრამული კოდები და ალგორითმული ენების ზოგადი სინტაქსი ბეკუს–ნაურის ფორმალიზმის ფარგლებში.

დასკვნა სადისერტაციო ნაშრომში მიღწეულია თემით განსაზღვრული მიზნები - დასმულია და გადაწყვეტილია სპეციალური კლასის ალგორითმულ ენებზე დაწერილი კომპიუტერული პროგრამების ვერიფიკაციის(კორექტულობის) ამოცანა.

ალგორითმული ენებისა და პროგრამების ვერიფიკაციის ზემოთ აღნიშნულ ამოცანასთან დაკავშირებით დისერტაციაში განვითარებულია ახალი მიდგომა, რომელიც არსებითად ეფუძნება სასრული ავტომატების კლასიკურ თეორიას. ამ მიდგომის საფუძველს წარმოადგენს ფორმალური მოდელი - სასრული ავტომატი, რომლის ფარგლებში მოხერხებული აღმოჩნდა არა მარტო ალგორითმული ენების(სინტაქსი და სემანტიკა) აღწერა და ანალიზი, არამედ ამ ენებზე დაწერილი პროგრამების ვერიფიკაციის მათემატიკურად კორექტული ამოცანის როგორც დასმა, ისე გადაწყვეტა. განსაკუთრებული მნიშვნელობა ენიჭება პროგრამების მიმართ წაყენებულ არაფორმალურ მოთხოვნების მათემატიკურად კორექტული ვერსიის ფორმულირებას. ასეთი თეორიულ-ავტომატური ფორმალიზაცია საშუალებას იძლევა მკაცრად დამტკიცდეს კონკრეტული პროგრამისა და სპეციფიკაციის შესაბამისობა.

დისერტაციაში მიღებული შედეგები გამოქვეყნებულია შემდეგ შრომებში:

1. ბენიძე ნ. კომპიუტერული პროგრამების კორექტულობის შესახებ //მოხსენებათა თეზისები. საქართველოს ტექნიკური უნივერსიტეტის საერთაშორისო სამეცნიერო კონფერენციის „საინფორმაციო და კომპიუტერული ტექნოლოგიები, მოდელირება, მართვა“. თბილისი, 1–4 ნოემბერი, 2010, გვ. 140.
2. ყიფშიძე ზურაბი, ბენიძე ნანა. ბლოკური დაშიფვრის სიმეტრიული კრიპტოგრაფიული სისტემა. //მოხსენებათა თეზისები. საქართველოს ტექნიკური უნივერსიტეტის საერთაშორისო სამეცნიერო კონფერენციის „საინფორმაციო და კომპიუტერული ტექნოლოგიები, მოდელირება, მართვა“. თბილისი, 1–4 ნოემბერი, 2010, გვ. 123.
3. ბენიძე ნ. კომპიუტერული პროგრამების ვერიფიკაციის შესახებ. // მოხსენებათა თეზისები. ნიკო მუსხელიშვილის გამოთვლითი მათემატიკის ინსტიტუტისა და საქართველოს საპატრიარქოს წმიდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტის ერთობლივ საერთაშორისო კონფერენციის „ინფორმაციული და გამოთვლითი ტექნოლოგიები“. თბილისი, 2–6 მაისი, 2010, გვ. 23 .
4. 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.
5. Бенидзе Н. Об устанавлении правильности компьютерных //программ. “Internet Education Science” IES-2010. New Informational and Computer Technologies in Education and Science. Vinnytsia VNTU. september 28 - octomber 3, 2010 ,volume 1, section E, page 221-224.
6. 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 Volume 2, Section H, page 545-550 .