**Чеботарьов Анатолій Миколайович. Доказове проектування алгоритмів функціонування реактивних систем : Дис... д-ра наук: 05.13.13 – 2002**

|  |  |
| --- | --- |
| |  | | --- | | Чеботарьов А.М. Доказове проектування алгоритмів функціонування реактивних систем. – Рукопис.  Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.13 – обчислювальні машини, системи та мережі, Інститут кібернетики ім. В.М.Глушкова НАН України, Київ, 2002.  Розроблено загальну теорію та методологію доказового проектування реактивних алгоритмів на початкових етапах їхньої розробки. Запропонований підхід до доказового проектування базується на методах синтезу відкритих систем і гарантує точну відповідність одержаного алгоритму його специфікації в логічній мові першого порядку. | |
| |  | | --- | | Результатом дисертаційної роботи є *розв’язання важливої прикладної проблеми забезпечення безпомилковості процесу проектування реактивних алгоритмів промислового рівня складності на етапі побудови процедурного представлення алгоритму*. Для цього було побудовано теорію доказового проектування алгоритмів і на її основі розроблено методологію проектування, яка гарантує одержання процедурного представлення алгоритму, що задовольняє вимоги до його функціонування, сформульовані у початковій специфікації.  Головною перешкодою на шляху побудови теорії і методології автоматизованого проектування алгоритмів функціонування реактивних систем є надто велика обчислювальна складність розв’язання багатьох задач проектування. Ці задачі, зазвичай, належать до класів NP- і PSPACE-повних проблем, тому не можна розраховувати на одержання ефективних алгоритмів (що дозволяють розв’язувати практичні задачі на сучасних обчислювальних засобах) для розв’язання будь-яких задач проектування. Запропонований підхід до побудови теорії та засобів автоматизованого проектування реактивних систем полягає в розумному обмеженні класу задач, що розв’язуються, такими задачами, для яких можна отримати рішення з припустимими обчислювальними витратами. “Розумність” обмеження полягає в тому, щоб цей клас містив у собі практично важливі задачі, тобто задачі такого рівня складності, який відповідає складності сучасних реактивних систем. Природним способом обмеження класу задач є обмеження виражальних можливостей мови, на якій формулюється задача, у даному випадку – мови специфікації реактивних алгоритмів. Виражальні можливості мови, у свою чергу, визначаються її синтаксисом та семантикою.  Отже, основна ідея запропонованого підходу полягає в тому, щоб визначити такі обмеження на синтаксис та семантику мови специфікації, які б дозволили побудувати теоретично обгрунтовані формальні методи проектування реактивних алгоритмів промислового рівня складності.  В процесі вирішення зазначеної вище проблеми одержано такі основні теоретичні та практичні результати.  1. Запропоновано та теоретично обгрунтовано дворівневу організацію системи мов опису, основаних на логіці першого порядку з одномісними предикатами. Виражальні засоби мови нижнього рівня максимально обмежені так, щоб одержати ефективні методи розв'язку задач проектування для специфікацій у цій мові й водночас мати прості алгоритми трансляції в неї із значно виразнішої мови верхнього рівня. Використання для інтерпретації мов множини цілих чисел замість натуральних дозволило спростити побудову специфікації алгоритму, зробити її більш природною (формули описують вимоги до поведінки системи, виходячи з історії її функціонування) і, головне, суттєво поліпшити ефективність відповідних логічних методів розв'язку задач проектування.  2. Сформульовано й доведено теорему про специфікацію, яка визначає зв'язок між структурою певного представлення формули мови специфікації і процедурним (у термінах станів і функцій переходів і виходів) представленням автомата, який специфікується цією формулою. На основі цієї теореми запропоновано підхід до вибору мови верхнього рівня, який дозволяє використовувати теорему про специфікацію для побудови алгоритмів синтезу, суттєво простіших за алгоритми синтезу, які базуються на методі табло для мов темпоральних логік.  3. Розроблено та теоретично обгрунтовано методи перевірки несуперечності специфікацій на основі резолюційної процедури пошуку логічного виведення. Використання специфіки запропонованого методу інтерпретації мов і побудови їхньої семантики дозволило суттєво поліпшити ефективність методу резолюцій порівняно з традиційними його варіантами. Методи перевірки несуперечності специфікацій реалізовано у вигляді процедур *R*- і *S*-поповнення, які використовуються не тільки як засоби перевірки несуперечності, але й як складові багатьох процедур проектування.  4. Для сформульованої у дисертації проблеми детермінізації логічних специфікацій одержано математично обгрунтоване її рішення. Побудовано реалізацію одержаного методу детермінізації, яка дозволяє задавати різні способи детермінізації, що в загальному випадку приводять до різних реалізацій алгоритму, що проектується.  5. Для сформульованої у новій постановці проблеми забезпечення коректності взаємодії між системою, що проектується, і зовнішнім середовищем одержано ефективне рішення на основі теоретико-автоматних і логічних методів. Ефективність її рішення особливо важлива в методології доказового проектування, де ця проблема виникає при перевірці коректності перетворень, що виконуються неформально.  6. На основі теореми про специфікацію одержано ряд нових методів розв’язання задачі синтезу автомата за його логічною специфікацією. Уперше в рішенні практичної задачі синтезу використовувалися топологічні властивості мови специфікації, що дозволило сформулювати обмеження на виражальні можливості мови, які призвели до значного підвищення ефективності методів синтезу.  7. В області верифікації алгоритмів запропоновано метод синтезу автомата-розпізнавача за формулою лінійної темпоральної логіки, що відрізняється від відомих методів модифікованою моделлю автомата-розпізнавача та способом визначення поняття стану автомата, що синтезується. Це дозволило одержати значно кращі результати щодо кількості станів та переходів у автоматах, що синтезуються, порівняно з останніми із відомих методів. Запропоновано також метод редукції моделі системи, що верифікується, який дозволяє в багатьох випадках значно зменшити кількість станів. На відміну від евристичних методів, які звичайно використовуються і потребують побудови редукції методом послідовних проб, або методів редукції на основі гомоморфізму, які не завжди можна застосувати, запропонований метод може виконуватися цілком автоматично і завжди дає результат, еквівалентний початковій моделі відносно властивостей, що перевіряються.  *Усі запропоновані в дисертації методи розв’язання задач проектування базуються на строго доведених теоретичних результатах, багато з яких сформульовано у вигляді теорем, що мають самостійне значення.* | |