Верификация асимптотической оценки временной сложности в задачах динамического программирования

Григорянц Сергей Арменович

Московский физико-технический институт
Физтех-школа Прикладной Математики и Информатики
Кафедра дискретной математики

Научный руководитель: Дашков Евгений Владимирович

27 июня 2021 г.

Постановка задачи

Цель работы

Постановка задачи

Цель работы

- Исследование методов формальной верификации корректности и асимптотики алгоритмов.

Постановка задачи

Цель работы

- Исследование методов формальной верификации корректности и асимптотики алгоритмов.
- Применение исследованных методов на примере верификации алгоритма динамического программирования LCS.

Зачем нужна формальная верификация?

Сферы применения

Зачем нужна формальная верификация?

Сферы применения

- Аппаратное обеспечение – Intel [2].

Зачем нужна формальная верификация?

Сферы применения

- Аппаратное обеспечение – Intel [2].
- Криптография – Scilla [5], CertiK [6].

Зачем нужна формальная верификация?

Сферы применения

- Аппаратное обеспечение – Intel [2].
- Криптография – Scilla [5], CertiK [6].
- Критическое ПО – CompCert [4], seL4 [3].

Зачем нужна формальная верификация?

Сферы применения

- Аппаратное обеспечение – Intel [2].
- Криптография – Scilla [5], CertiK [6].
- Критическое ПО – CompCert [4], seL4 [3].
- Медицина, банковское дело, транспортные технологии, и т.д.

Что бывает, если не верифицировать ПО

Истории неудач

Что бывает, если не верифицировать ПО

Истории неудач

- Сорвалась миссия НАСА Mars Climate Orbiter.

Что бывает, если не верифицировать ПО

Истории неудач

- Сорвалась миссия НАСА Mars Climate Orbiter.
- Ненадлежащее тестирование Лондонской службы скорой помощи привело к гибели людей.

Что бывает, если не верифицировать ПО

Истории неудач

- Сорвалась миссия НАСА Mars Climate Orbiter.
- Ненадлежащее тестирование Лондонской службы скорой помощи привело к гибели людей.
- Самолет Airbus A320 разбился на демонстрационном полете из-за ошибке в софте.

Что бывает, если не верифицировать ПО

Истории неудач

- Сорвалась миссия НАСА Mars Climate Orbiter.
- Ненадлежащее тестирование Лондонской службы скорой помощи привело к гибели людей.
- Самолет Airbus A320 разбился на демонстрационном полете из-за ошибке в софте.
- Много страшных историй: [1]

Coq

Coq

- Coq – программное средство доказательства теорем.

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)
- CIC способна представлять:

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)
- CIC способна представлять:
  - Функциональные программы в стиле ML.

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)
- CIC способна представлять:
  - Функциональные программы в стиле ML.
  - Доказательства в логике высшего порядка.

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)
- CIC способна представлять:
  - Функциональные программы в стиле ML.
  - Доказательства в логике высшего порядка.
- Утверждения и доказательства представляются с помощью Соответствия Карри — Ховарда:

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)
- CIC способна представлять:
  - Функциональные программы в стиле ML.
  - Доказательства в логике высшего порядка.
- Утверждения и доказательства представляются с помощью Соответствия Карри — Ховарда:
  - Пропозициональное утверждение $\iff$ Тип

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)
- CIC способна представлять:
  - Функциональные программы в стиле ML.
  - Доказательства в логике высшего порядка.
- Утверждения и доказательства представляются с помощью Соответствия Карри — Ховарда:
  - Пропозициональное утверждение $\iff$ Тип
  - Доказательство утверждения $\iff$ Элемент данного типа

Coq

- Coq – программное средство доказательства теорем.
- Coq основан на теории типов (Исчисление Индуктивных Конструкций, Calculus of Inductive Constructions, CIC)
- CIC способна представлять:
  - Функциональные программы в стиле ML.
  - Доказательства в логике высшего порядка.
- Утверждения и доказательства представляются с помощью Соответствия Карри — Ховарда:
  - Пропозициональное утверждение $\iff$ Тип
  - Доказательство утверждения $\iff$ Элемент данного типа
- Vernacular – язык команд Coq.

Логика Хоара

Здесь могла быть логика Хоара.

Список литературы I


N. Dershowitz. *SOFTWARE HORROR STORIES*. URL: https://www.cs.tau.ac.il/~nachumd/verify/horror.html.


J. Harrison. "Formal verification at Intel". в: *18th Annual IEEE Symposium of Logic in Computer Science, 2003. Proceedings.* 2003, с. 45—54. DOI: 10.1109/LICS.2003.1210044.


Gerwin Klein и др. "SeL4: Formal Verification of an OS Kernel". в: *Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles*. SOSP '09. Big Sky, Montana, USA: Association for Computing Machinery, 2009, с. 207—220. ISBN: 9781605587523. DOI: 10.1145/1629575.1629596. URL: https://doi.org/10.1145/1629575.1629596.


Xavier Leroy. "Formal Verification of a Realistic Compiler". в: *Commun. ACM* 52.7 (июль 2009), с. 107—115. ISSN: 0001-0782. DOI: 10.1145/1538788.1538814. URL: https://doi.org/10.1145/1538788.1538814.

Список литературы II

Ilya Sergey и др. “Safer Smart Contract Programming with Scilla”. в: *Proc. ACM Program. Lang.* 3.OOPSLA (окт. 2019). DOI: 10.1145/3360611. URL: https://doi.org/10.1145/3360611.

CertiK team. *CertiK framework*. URL: https://www.certik.io/.