New York University
Analysis of Computer Systems (ACSys) Group

Clark Barrett

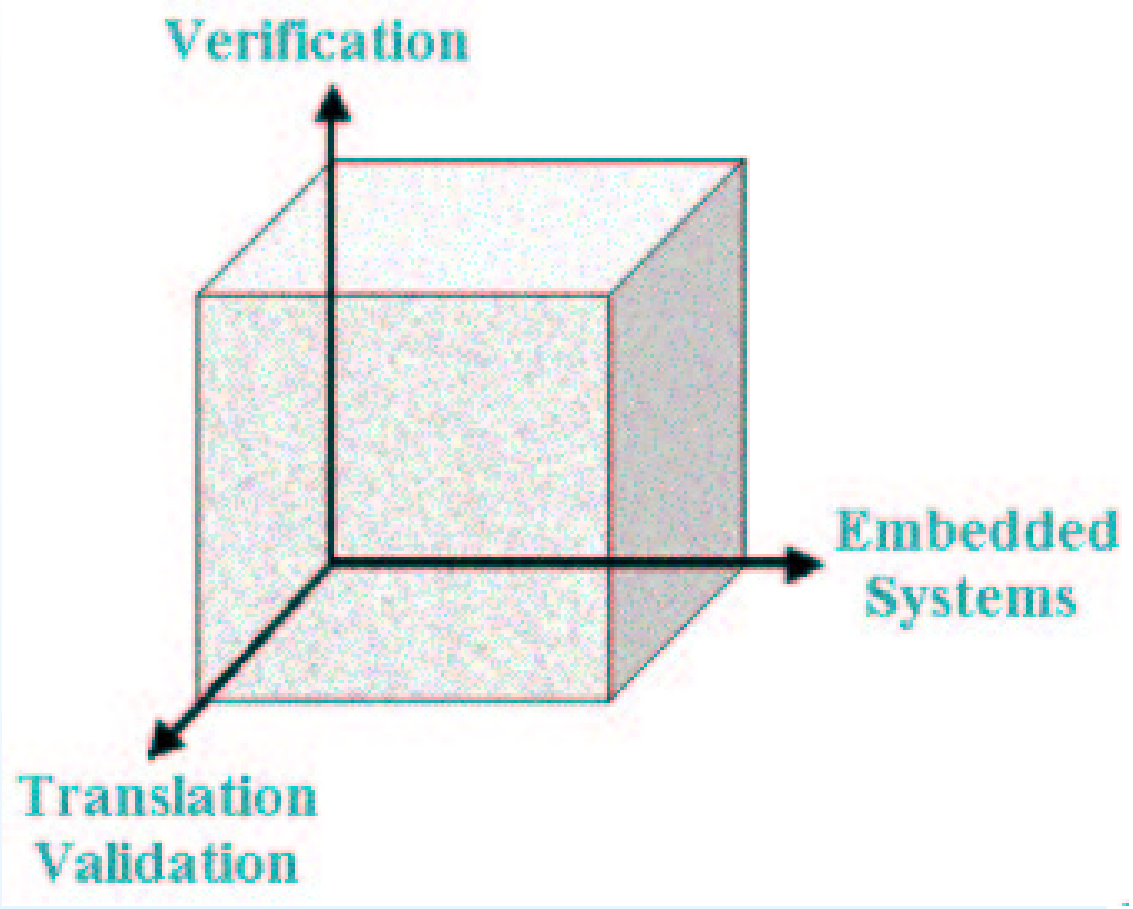
North-East Verification Seminar

Bell Labs, Lucent Technologies

March 10, 2006

ACSys Group

Ensuring provably correct,
reliable, and trustworthy
software and hardware designs.



People

Faculty:

- Clark Barrett
- Ben Goldberg
- Amir Pnueli

Affiliated Faculty:

- Lenore Zuck (U. Illinois at Chicago)

Postdoctoral Researchers:

- Hillel Kugler

PhD Students:

- Ittai Balaban, Ariel Cohen, Yeting Ge, Cory Plock, Nikhil Sethi, Igor Shikanian, Aleksandr Zaks, Anna Zaks.

Satisfiability Modulo Theories

Given a first order theory T and a formula φ, the *Satisfiability Modulo Theories* (SMT) problem consists of deciding whether there exists a model $\mathcal{A}$ of T and variable assignment α such that $(\mathcal{A}, \alpha) \models \varphi$.

Satisfiability Modulo Theories

Given a first order theory T and a formula φ, the *Satisfiability Modulo Theories* (SMT) problem consists of deciding whether there exists a model $\mathcal{A}$ of T and variable assignment α such that $(\mathcal{A}, \alpha) \models \varphi$.

SMT solvers are used in a wide variety of applications both in academia and industry.

- Hardware Verification
- Predicate Abstraction
- Translation Validation
- Assertion Checking
- ...and many more

Satisfiability Modulo Theories

Given a first order theory T and a formula φ, the *Satisfiability Modulo Theories* (SMT) problem consists of deciding whether there exists a model $\mathcal{A}$ of T and variable assignment α such that $(\mathcal{A}, \alpha) \models \varphi$.

Some theories of interest

- Equality with “Uninterpreted Functions”
- Arithmetic (Real and Integer)
- Arrays
- Bit-vectors
- Sets
- Recursive Datatypes
- *Combinations of Theories*

Satisfiability Modulo Theories

Most of my current efforts are SMT-related and can be placed in one of the following categories:

- Theory
- Implementation
- Applications

Theory

Past work

- Relationship of Nelson-Oppen and Shostak
- Efficient refinements of Nelson-Oppen
- Theory decision procedures (bit-vectors, arrays)

Recent work

- Reasoning about partial functions in SMT
- A decision procedure for recursive data types
- Extending the Abstract DPLL Modulo Theories framework

Implementation

Past work

- Previous systems: SVC, CVC
- Combining SAT with SMT

Recent work

- CVC Lite
- Decision Heuristics for SMT systems
- Adding proof production to SMT systems
- Heuristics for quantifier instantiation
- SMT-LIB and SMT-COMP initiatives

Applications

Past work

- Processor verification

Recent work

- Translation Validation
- CAsCaDE
- Your application here?