Tamarin: Concolic Program Disequivalence for MIPS

Abel Nieto

University of Waterloo
anietoro@uwaterloo.ca

Abstract. TODO

1 Introduction

2 Tamarin

Overview.

2.1 Trace Collection

CPU instrumentation, PC concretization, error boxing, and fuel.

2.2 Transformations

Desugaring, simplification, trimming, and conversion to SSA.

2.3 Query Representation

Memory, jumps, arithmetic operators.

2.4 Concolic Execution

3 Evaluation

4 Related Work

5 Conclusions