# A Path-Precise Analysis for Property Synthesis

*Sean McDirmid and Wilson C. Hsieh*

UUCS-03-027

School of Computing
University of Utah
Salt Lake City, UT 84112 USA

December 1, 2003

## *Abstract*

Recent systems such as SLAM, Metal, and ESP help programmers by automating reasoning about the correctness of temporal program properties. This paper presents a technique called **property synthesis**, which can be viewed as the inverse of property checking. We show that the code for some program properties, such as proper lock acquisition, can be automatically inserted rather than automatically verified. Whereas property checking analyzes a program to verify that property code was inserted correctly, property synthesis analyzes a program to identify where property code should be inserted.

This paper describes a path-sensitive analysis that is precise enough to synthesize property code effectively. Unlike other path-sensitive analyses, our intra-procedural **path-precise analysis** can describe behavior that occurs in loops without approximations. This precision is achieved by computing analysis results as a set of **path machines**. Each path machine describes assignment behavior of a boolean variable along all paths precisely. This paper explains how path machines work, are computed, and are used to synthesize code.