A Bounded Verification Tool for Java

Stefan Koppier

January 8, 2019

Introduction

Contents

Chapter 1

CProver

1.1 Properties

array bounds	test
pointer	test
division by zero	test
arithmetic over- and underflow	test
shift greater than bit-width	test
floating-point for +/-Inf	test
floating-point for NaN	test
user assertions	test

Chapter 2

Translation of Java to C

2.1 Primitive data types

Table 2.1: Equivalence of primitive Java data types.

Type	Description	C equivalent
boolean	true or false	_Bool
char	16-bit Unicode value	
byte	8-bit signed integral value	_int8
short	16-bit signed integral value	_int16
int	32-bit signed integral value	_int32
long	64-bit integral value	_int64
float	IEEE 754 64-bit floating point value	float
double	IEEE 754 32-bit floating point value	double

Bibliography