# CompCert with integer-pointer casting

yonghyun Kim
Seoul National University
yonghyun.kim@sf.snu.ac.kr

## Abstract

The certified C compiler CompCert uses an abstract memory model which allows for many optimizations, but in which the behavior of integer-pointer casts is undefined. In [1], Kang et al. present a new formal memory model named "Quasi-concrete model" that supports integer-pointer casts semantics, while still allowing common optimizations. In this talk, I am going to introduce CompCert with Quasi-concrete model so-called "CompCert-Intptr". I will present several concepts: (1) Quasi-Concrete model (2) Mixed Simulation.

## 1. Quasi-concrete model

At first, I will remind you about "Quasi-Concrete model" that introduced in [1]. It is a hybrid of Logical and Concrete Memory model. In this model, memory blocks can be either concrete like flat memroy model or logical. Logical block allows more optimizations. Concrete memory blocks support integer-pointer casts. To allow for as much optimizations as possible, memory blocks should be logical when allocated, and only be made concrete before an integer-pointer cast. This transformation is done with a new external function, the "capture" of a memory block.

## 2. Mixed Simulation

CompCert's correctness proof proves that the behavior of the target program is one of the behaviors of the source program. To do so, CompCert proves the backward simulation between the source program and the target program. To construct this simulation, CompCert used to prove forward simulation for each pass. This kinds of proof technique exploit determinism of target program to build backward simulation. However, CompCert using the quasi-concrete model is no longer deterministic, because the capture function is non-deterministic. We can solve this problem by replacing forward simulation with mixed simulation. We present the definition of mixed simulations, show that we can prove mixed simulations for every CompCert pass.

[1] Jeehoon Kang, Chung-Kil Hur, William Mansky, Dmitri Garbuzov, Steve Zdancewic, and Viktor Vafeiadis. A formal C memory model supporting integer-pointer casts. In Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation, Portland, OR, USA, June 15-17, 2015, pages 326335, 2015.