

## Opis problema

U okvir LLVM infrastrukture ulazi kompilator Clang. Clang sadrži analizator (alat) namenjen statičkoj analizi programskog koda. Zadatak je napraviti novu proveru u okviru ovog alata.

## Opis arhitekture sistema (opis osnovnih modula implementacije)

Jezgro analizatora vrši simboličko izvršavanje datog programa. Sve ulazne vrednosti su predstavljene simboličkim vrednostima, dalje endzin zaključuje vrednosti svih izraza u programu na osnovu ulaznih simbola i putanje. Izvođenje je osetljivo na putanju i istražuje se svaki mogući put kroz program. Istraženi tragovi izvođenja predstavljeni su objektom **EkplodedGraph**. Svaki čvor grafikona je **EkplodedNode**, koji se sastoji od **ProgramPoint** i **ProgramState** delova.

**ProgramPoint** predstavlja odgovarajuću lokaciju u programu (ili CFG). ProgramPoint se takođe koristi za snimanje dodatnih informacija o tome kada/kako je stanje dodato. Na primer, `PostPurgeDeadSymbolsKind` znači da je stanje rezultat brisanja mrtvih simbola - ekvivalent analizatora za sakupljanje smeća (garbage collection).

**ProgramState** predstavlja apstraktno stanje programa. Sastoji se od:

Environment - preslikavanje izraza izvornog koda u simbolične vrednosti

Store - mapiranje sa memorijskih lokacija na simbolične vrednosti

GenericDataMap - ograničenja simboličkih vrednosti

## Undefined Value Checker

Predstavlja čeker koji prepoznaje nedefinisane vrednosti operanada binarnih operatora i prijavljuje upozorenje sa porukom da li nedefinisana vrednost operatora levi ili desni operand. Dodatno proverava i da li je neki od operanada nedefinisana vrednost koja je uzrokovana pristupu niza van granica.

## Opis rešenja problema

Ukratko nasleđena je klasa Checker i implementirana funkcija koja proverava binarne operacije (nakon izvršavanja) kao i funkcija koja prijavljuje upozorenje korisniku. Proverava se da li postoji nedefinisan vrednost među operandima, ako postoji dalje se proverava koji operand je nedefinisan i da li je takva nedefinisana vrednost specifično pristup nizu van njegovih granica. Puni se bafer koji sadrži tekst upozorenja i prijavljuje se korisniku. Čeker se obavezno mora registrovati, dodatno je implementirana i funkcija koja proverava da li je operand naredba koja predstavlja pristup niza (array subscript) i ako jeste da li je takav pristup van njegovih granica.