První kroky s Frama-C

Jan Tušil

16. 3. 2015

Table of Contents

Materiály k prezentaci

https://github.com/h0nzZik/Frama-C_Examples

Představení

Statická analýza C kódu

Založeno na pluginech

Ověřování proti specifikaci (jazyk ACSL)

Možná specifikace: absence běhových chyb

Jak získat?

ACSL - Co je to za jazyk?

ANSI / ISO C Specification language

V komentářích C kódu.

Asserty

Invarianty

Funkční kontrakty (DbC)

http://frama-c.com/acsl.html

ACSL - vyjadřovací schopnosti

C operátory a datové typy

Matematické datové typy

Prvořádová logika (s rozšířeními)

Asserty

```
int x = 17;
/*@ assert x > 5 */
```

Základní specifikační jednotka

Tvrzení o stavu programu v daném bodě.

(ACSL specifikace zabudována v komentáři)

Kvantifikátory

```
int array[4] = {-15, 3, 17, 104};
/*@
assert \forall integer i, j;
0 <= i <= j < 4 ==> array[i] <= array[j];
*/
```

Vázaná proměnná má daný typ

Typ může být uživatelem definovaný

`integer` označuje (matematické) celé číslo

Pointery

```
int array[4] = {-15, 3, 17, 104};
/*@ assert \valid(array + (0..3)); */
```

Predikát \valid bere množinu termů

0..3 označuje množinu $\{0, 1, 2, 3\}$

Význam: výrazy $\{array + 0, \ldots, array + 3\}$ jsou platné ukazatele

Obvyklá pointer aritmetika

Uživatelské predikáty

```
/*@
predicate is_sorted ( int *array, integer len ) =
\forall integer i, j; 0 <= i <= j < len
==> array[i] <= array[j];
*/
```

Predikát lze využít později

```
/*@ assert is_sorted ( array, 4 ); */
```

Invarianty smyček

```
int arr[7];
[ ... ]
/*@ loop invariant is_sorted(arr, i) */
for ( int i = 0; i < 7; i++ ) {
        [ ... ]
}
```

Funkční kontrakty

```
/*@
requires \valid ( array + (0 .. ( len-1 ) ) );
ensures is_sorted ( array, len );
 */
void sort ( int *array, size_t len);
```

Paradigma "Design by Contract"

Jednoduché použití

Soubor hello.c je v adresáři 01_hello

```
$ frama-c hello.c -val
```

Jak ověřit větší projekt z více souborů?

Na co je preprocesor v C?

Na co je preprocesor v C?

Makra a náhrady textu

Na co je preprocesor v C?

Makra a náhrady textu

Vkládání (hlavičkových) souborů

Preprocessing ve Frama-C

Výchozí: `gcc -C -E -I`

Možno předefinovat přepínačem `-cpp-command`

Frama-C umí předzpracovat i anotace (s GCC)

Viz soubor build.mk

Pouze pro C

Nikoliv C++