Symbolic execution

```
fn example(s: [string]) {
  if s[0] == "a" {
    if s[99] == "b" {
      assert(s[50] == "c")
    }
  }
}
```

Goal: $s[0] = \text{"a"} \wedge$
$s[99] = \text{"b"} \wedge$
$\neg\, s[50] = \text{"c"}$

```
fn f(x: int):
1:  y = alloc(x, 1)
2:  z = y.0
3:  if z = 0 goto 4 else 5
4:  assert(x = 0)
5:  ...
```

$\Sigma = \{x \mapsto \alpha\}$ $\quad H = \{\}$ $\quad$ path = true

$\Sigma = \{x \mapsto \alpha, y \mapsto \phi\}$ $\quad H = \{\phi \mapsto (\alpha, 1)\}$

$\Sigma = \{\ldots, z \mapsto \alpha\}$

path = "$\alpha = 0$" $\wedge$ true

check $\neg(\alpha = 0)$ in $\alpha = 0$

path = "$\alpha \neq 0$" $\wedge$ true

Instr $I ::= p = rv \mid \text{if } x \text{ goto } i_1 \text{ else } i_2$

Program $P ::= I^*$

Place $p ::= x \mid x.i \mid x[y]$

Rvalue $rv ::= c \mid p \mid x \oplus y \mid \text{alloc}(x^*)$ $\qquad [[s; \infty]]$

SymExpr $s ::= c \mid s_1 \oplus s_2 \mid \alpha \mid (s_1, \ldots s_n) \mid s.i \mid [s] \mid s_1[s_2]$

SymVar α $\qquad \mid \text{store } s_1\ s_2\ s_3$

SymConfig $\mathbb{C} ::= \{\text{prog } P;\ \text{pc } i;\ \text{locals } \Sigma;\ \text{heap } H;\ \text{path } s\}$

Locals $\Sigma \in \text{Var} \rightarrow \text{SymExpr}$

Heap $H \in \mathbb{N} \rightarrow \text{SymExpr}$

$$\boxed{\mathbb{C} \hookrightarrow \mathbb{C}'}$$

$$\frac{\mathbb{C}.\text{prog}[\mathbb{C}.\text{pc}] = \text{"}p = rv\text{"} \quad \mathbb{C} \vdash rv \Downarrow s \quad \mathbb{C} \vdash p = s \Rightarrow \Sigma', H'}{\mathbb{C} \hookrightarrow \{\mathbb{C} \ \underline{\text{with}}\ \text{pc} = \mathbb{C}.\text{pc}+1;\ \Sigma';\ H'\}}$$

$$\boxed{\mathbb{C} \vdash rv \Downarrow s}$$

$rv ::= \ldots \mid \text{alloc}(x^*)$

$\quad\quad \mid p$

$p ::= x \mid x.i \mid x[y]$

$$\frac{}{\mathbb{C} \vdash c \Downarrow c} \qquad \frac{}{\mathbb{C} \vdash x \Downarrow \mathbb{C}.\text{locals}(x)}$$

$$\frac{\mathbb{C} \vdash x_1 \Downarrow s_1 \quad \mathbb{C} \vdash x_2 \Downarrow s_2}{\mathbb{C} \vdash x_1 \oplus x_2 \Downarrow s_1 \oplus s_2}$$

$$\boxed{\mathbb{C} \vdash p = s \Rightarrow \Sigma, H}$$

$$\frac{}{\mathbb{C} \vdash x = s \Rightarrow \Sigma[x \mapsto s], H}$$

$$\frac{\mathbb{C}.\text{prog}[\mathbb{C}.\text{pc}] = \text{"if } x \text{ goto } i_1 \text{ else } i_2\text{"} \quad \mathbb{C} \vdash x \Downarrow s \quad \text{path}' = s \wedge \mathbb{C}.\text{path} \quad \text{path}' \ \text{SAT}}{\mathbb{C} \hookrightarrow \{\mathbb{C} \ \underline{\text{with}}\ \text{pc} = i_1;\ \text{path} = \text{path}'\}}$$

$$\frac{\mathbb{C}.prog[\mathbb{C}.pc] = \text{"if } x \text{ goto } i_1 \text{ else } i_2\text{"} \quad \mathbb{C} \vdash x \Downarrow s \quad path' = \neg s \wedge \mathbb{C}.path \quad path' \text{ SAT}}{\mathbb{C} \hookrightarrow \{\mathbb{C} \text{ with } pc = i_2;\ path = path'\}}$$

$x \mapsto \alpha$ $\quad$ $path = y = 0$
$\wedge \neg(y = 0)$

assert$(x = 0)$

$$\frac{\mathbb{C}.prog[\mathbb{C}.pc] = \text{"\_ = assert}(x)\text{"} \quad \mathbb{C} \vdash x \Downarrow s \quad \neg s \wedge \mathbb{C}.path \text{ SAT}}{\mathbb{C} \hookrightarrow \text{bug found!}}$$

if $x = 0$

then $\swarrow$ $\quad$ $\searrow$ else

$x = 1$ $\quad$ $x = 2$

$\searrow$ $\quad$ $\swarrow$

...

$\mathbb{C} =$

fn $f(x: int)$: $\{x \mapsto \alpha\}$ ...

$y = x + 1$ $\quad$ $\mathbb{C} \vdash x + 1 \Downarrow \alpha + 1$

$\mathbb{C} \vdash y = \alpha + 1$

$\Rightarrow \{x \mapsto \alpha,\ y \mapsto \alpha + 1\},\ \{\}$

if (false) $\quad$ $x = 0$
if$(x = 1)$

$$\frac{\mathbb{C} \vdash x_i \Downarrow s_i \quad n = |\mathbb{C}.heap|}{\mathbb{C} \vdash alloc(x^*) \Downarrow n \Rightarrow H[n \mapsto (s_1, \ldots, s_n)]}$$

$$\frac{\mathbb{C} \vdash x \Downarrow s \quad n \in solutions(s, \mathbb{C}.path)}{\mathbb{C} \vdash x.i \Downarrow \mathbb{C}.heap[n].i \Rightarrow \{path = \mathbb{C}.path \wedge s = n\}}$$

Challenge: $\mathbb{C} \vdash x : i \Downarrow s$

define $\mathbb{C} \vdash alloc(x^*) \Downarrow s$

$\mathbb{C} \vdash x.i = s \Rightarrow \Sigma, H$

Tips ① $\mathbb{C} \vdash rv \Downarrow s \Rightarrow H$

$H = \{ 0 \mapsto (\wedge, *)$
$1 \mapsto (\sigma, \triangle) \}$

② solutions : SymExpr * SymExpr → [Const]

fn f(x : (int, string), y : (int, string)) :

x.0 = 1

$x \mapsto \alpha$

path = $(x = 0 \wedge y = 0) \vee$
$(x = 0 \wedge y = 1) \vee$