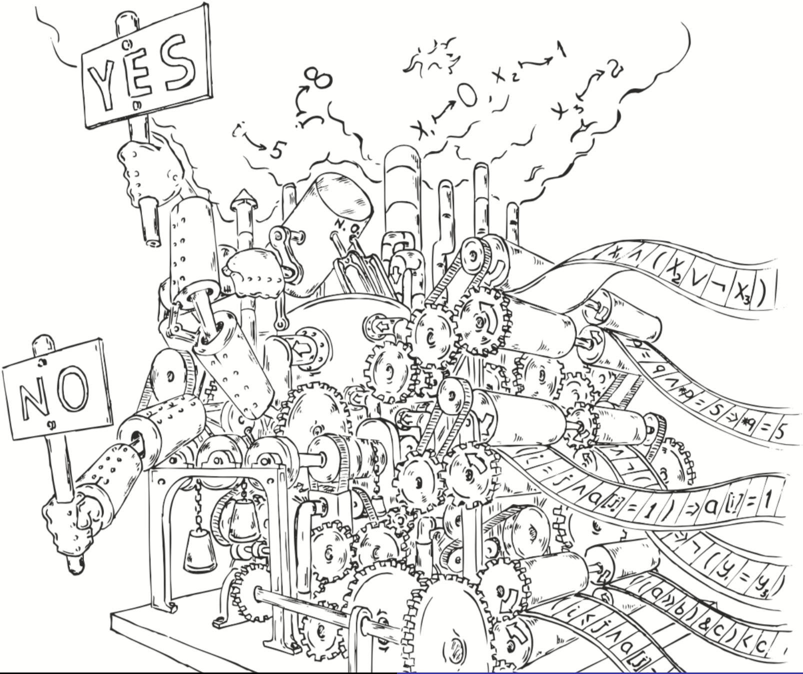

YES
NO
N.O.

Задачи разрешимости логических формул и приложения
Лекция 8. Логика указателей

Роман Холин

Московский государственный университет

Москва, 2022

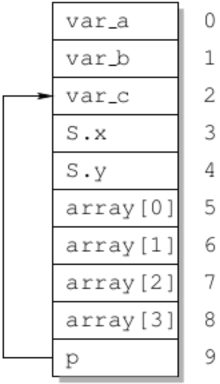
Модель памяти

- V - множество переменных
- A - множество адресов ($\{0, \dots, n-1\}$)
- D - множество слов
- Оценка памяти M - отображение из A в D
- $\sigma(v)$ - размер переменной (в словах)
- L - отображение из V в A - расположение памяти

Пример

```
int var_a, var_b, var_c;
struct { int x; int y; } S;
int array[4];
int *p = &var_c;

int main() {
  *p=100;
}
```



Пример

```
void f(int *sum) {
  *sum = 0;

  for(i=0; i<10; i++)
    *sum = *sum + array[i];
}
```

```
int *p, *q;

p = new int[10];
q = &p[3];
delete p;
*q = 2;
```

Синтаксис

$$
\begin{aligned}
formula &: formula \wedge formula \mid \neg formula \mid (formula) \mid ator \\
atom &: pointer \ = \ pointer \mid term \ = \ term \mid \\
&\quad pointer \ < \ pointer \mid term \ < \ term \\
pointer &: pointer\text{-}identifier \mid pointer + term \mid (pointer) \mid \\
&\quad \&identifier \mid \& * pointer \mid * pointer \mid \mathrm{NULL} \\
term &: identifier \mid * pointer \mid term \ op \ term \mid (term) \mid \\
&\quad integer\text{-}constant \mid identifier \ [\ term\ ] \\
op &: + \mid -
\end{aligned}
$$

Пример

$$
\begin{aligned}
&*(p+i) = 1,\\
&*(p+*p) = 0,\\
&p = q \wedge *p = 5,\\
&*****p = 1,\\
&p < q.
\end{aligned}
$$

Пример

$$
\begin{array}{ll}
*(p+i)=1, & p+i, \\
*(p+*p)=0, & p=i, \\
p=q \wedge *p=5, & *(p+q), \\
*****p=1, & *1=1, \\
p<q. & p<i.
\end{array}
$$

$$
\begin{array}{rcll}
[\![f_1 \wedge f_2]\!] & \doteq & [\![f_1]\!] \wedge [\![f_2]\!] & \\
[\![\neg f]\!] & \doteq & \neg [\![f]\!] & \\
[\![p_1 = p_2]\!] & \doteq & [\![p_1]\!] = [\![p_2]\!] & \text{where } p_1,\ p_2 \text{ are pointer expressions} \\
[\![p_1 < p_2]\!] & \doteq & [\![p_1]\!] < [\![p_2]\!] & \text{where } p_1,\ p_2 \text{ are pointer expressions} \\
[\![t_1 = t_2]\!] & \doteq & [\![t_1]\!] = [\![t_2]\!] & \text{where } t_1,\ t_2 \text{ are terms} \\
[\![t_1 < t_2]\!] & \doteq & [\![t_1]\!] < [\![t_2]\!] & \text{where } t_1,\ t_2 \text{ are terms} \\
[\![p]\!] & \doteq & M[L[p]] & \text{where } p \text{ is a pointer identifier} \\
[\![p + t]\!] & \doteq & [\![p]\!] + [\![t]\!] & \text{where } p \text{ is a pointer expression, and } t \text{ is a term} \\
[\![\&v]\!] & \doteq & L[v] & \text{where } v \in V \text{ is a variable} \\
[\![\& * p]\!] & \doteq & [\![p]\!] & \text{where } p \text{ is a pointer expression} \\
[\![\mathrm{NULL}]\!] & \doteq & 0 & \\
[\![v]\!] & \doteq & M[L[v]] & \text{where } v \in V \text{ is a variable} \\
[\![*p]\!] & \doteq & M[[\![p]\!]] & \text{where } p \text{ is a pointer expression} \\
[\![t_1\ op\ t_2]\!] & \doteq & [\![t_1]\!]\ op\ [\![t_2]\!] & \text{where } t_1,\ t_2 \text{ are terms} \\
[\![c]\!] & \doteq & c & \text{where } c \text{ is an integer constant} \\
[\![v[t]]\!] & \doteq & M[L[v] + [\![t]\!]] & \text{where } v \text{ is an array identifier, and } t \text{ is a term}
\end{array}
$$

Пример

$$
\begin{aligned}
[\![*((\&a)+1) \;=\; a[1]]\!] \iff & [\![*((\&a)+1)]\!] \;=\; [\![a[1]]\!] \\
\iff & M[[\![(\&a)+1]\!]] \;=\; M[L[a]+[\![1]\!]] \\
\iff & M[[\![\&a]\!]+[\![1]\!]] \;=\; M[L[a]+1] \\
\iff & M[L[a]+1] \;=\; M[L[a]+1]
\end{aligned}
$$

Аксиомы

$$\forall v \in V.\ L[v] \neq 0$$

Аксиомы

$$\forall v \in V.\ L[v] \neq 0$$
$$\forall v \in V.\ \sigma(v) \geq 1$$

Аксиомы

$$\forall v \in V.\ L[v] \neq 0$$

$$\forall v \in V.\ \sigma(v) \geq 1$$

$$\forall v_1, v_2 \in V.\ v_1 \neq v_2 \implies \{L[v_1], \ldots, L[v_1] + \sigma(v_1) - 1\} \cap \{L[v_2], \ldots, L[v_2] + \sigma(v_2) - 1\} = \emptyset$$

Структуры

$$s.f \quad \doteq \quad *((\&s) + o(f))$$

Структуры

$$s.f \quad \doteq \quad *((\&s) + o(f))$$

$$*(p+0) = a \ \wedge$$
$$*(p+1) = b \ \wedge$$
$$*(p+2) = c \ \ldots$$

Разрешающая процедура

- Логика указателей сводится к догике массивов
- Благодаря семантической трансляции формула из логики указателей транслируется в формулу из логики массивов с операцией чтения; логика индексов - линейная арифметика либо битовые вектора
- Единственная проблема - кванторы

Пример

$$
\begin{aligned}
&[\![p = \&x \wedge x = 1 \implies *p = 1]\!] \\
&\quad\iff [\![p = \&x]\!] \wedge [\![x = 1]\!] \implies [\![*p = 1]\!] \\
&\quad\iff [\![p]\!] = [\![\&x]\!] \wedge [\![x]\!] = 1 \implies [\![*p]\!] = 1 \\
&\quad\iff M[L[p]] = L[x] \wedge M[L[x]] = 1 \implies M[M[L[p]]] = 1
\end{aligned}
$$

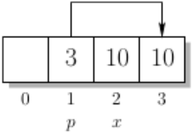
Пример

$$
\begin{aligned}
&[\![p \hookrightarrow x \implies p = \&x]\!] \\
&\quad\iff [\![p \hookrightarrow x]\!] \implies [\![p = \&x]\!] \\
&\quad\iff [\![*p = x]\!] \implies [\![p]\!] = [\![\&x]\!] \\
&\quad\iff [\![*p]\!] = [\![x]\!] \implies M[L[p]] = L[x] \\
&\quad\iff M[M[L[p]]] = M[L[x]] \implies M[L[p]] = L[x]
\end{aligned}
$$

Пример

$$
\begin{aligned}
&\llbracket p \hookrightarrow x \implies p = \&x \rrbracket \\
&\quad \iff \llbracket p \hookrightarrow x \rrbracket \implies \llbracket p = \&x \rrbracket \\
&\quad \iff \llbracket *p = x \rrbracket \implies \llbracket p \rrbracket = \llbracket \&x \rrbracket \\
&\quad \iff \llbracket *p \rrbracket = \llbracket x \rrbracket \implies M[L[p]] = L[x] \\
&\quad \iff M[M[L[p]]] = M[L[x]] \implies M[L[p]] = L[x]
\end{aligned}
$$

$$L[p] = 1,\ L[x] = 2,\ M[1] = 3,\ M[2] = 10,\ M[3] = 10$$



Оптимизация: применение аксиомы модели памяти

$$\sigma(x) = 2 \implies \&y \neq \&x + 1$$

Оптимизация: применение аксиомы модели памяти

$$\sigma(x) = 2 \implies \&y \neq \&x + 1$$

$$\sigma(x) = 2 \implies L[y] \neq L[x] + 1$$

Оптимизация: применение аксиомы модели памяти

$$\sigma(x) = 2 \implies \&y \neq \&x + 1$$

$$\sigma(x) = 2 \implies L[y] \neq L[x] + 1$$

$$\{L[x], \ldots, L[x] + \sigma(x) - 1\} \cap \{L[y], \ldots, L[y] + \sigma(y) - 1\} = \emptyset$$

Оптимизация: применение аксиомы модели памяти

$$\sigma(x) = 2 \implies \&y \neq \&x + 1$$

$$\sigma(x) = 2 \implies L[y] \neq L[x] + 1$$

$$\{L[x], \ldots, L[x] + \sigma(x) - 1\} \cap \{L[y], \ldots, L[y] + \sigma(y) - 1\} = \emptyset$$

$$(L[x] + \sigma(x) - 1 < L[y]) \vee (L[x] > L[y] + \sigma(y) - 1)$$

Оптимизация: применение аксиомы модели памяти

$$\sigma(x) = 2 \implies \&y \neq \&x + 1$$

$$\sigma(x) = 2 \implies L[y] \neq L[x] + 1$$

$$\{L[x], \ldots, L[x] + \sigma(x) - 1\} \cap \{L[y], \ldots, L[y] + \sigma(y) - 1\} = \emptyset$$

$$(L[x] + \sigma(x) - 1 < L[y]) \vee (L[x] > L[y] + \sigma(y) - 1)$$

$$(L[x] + 1 < L[y]) \vee (L[x] > L[y])$$

Оптимизация: чистые переменные

$$
\begin{aligned}
&[\![x = y \implies y = x]\!] \\
&\quad \iff [\![x = y]\!] \implies [\![y = x]\!] \\
&\quad \iff M[L[x]] = M[L[y]] \implies M[L[y]] = M[L[x]]
\end{aligned}
$$

Оптимизация: чистые переменные

$$
\begin{aligned}
&[\![x = y \implies y = x]\!] \\
&\quad \iff [\![x = y]\!] \implies [\![y = x]\!] \\
&\quad \iff M[L[x]] = M[L[y]] \implies M[L[y]] = M[L[x]]
\end{aligned}
$$

$$x = y \implies y = x$$

Оптимизация: чистые переменные

$$\mathcal{P}(\&x = y)$$

$$\begin{array}{rcll} [\![v]\!]^{\mathcal{P}} & \doteq & \Upsilon_v & \text{for } v \in \mathcal{P}(\varphi) \\ [\![v]\!]^{\mathcal{P}} & \doteq & M[L[v]] & \text{for } v \in V \setminus \mathcal{P}(\varphi) \end{array}$$

Оптимизация: чистые переменные

$$\mathcal{P}(\&x = y)$$

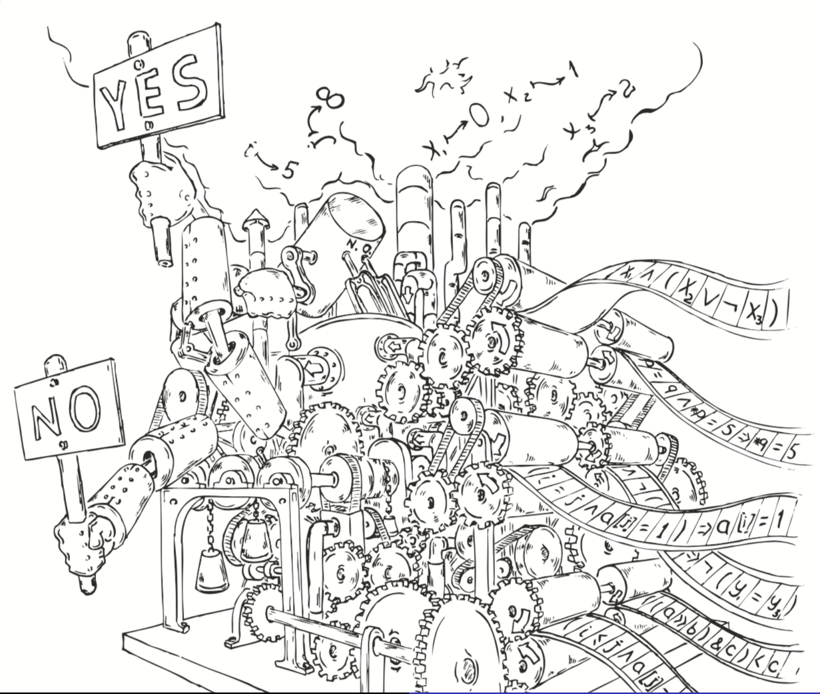
$$\begin{aligned} [\![v]\!]^{\mathcal{P}} &\doteq \Upsilon_v && \text{for } v \in \mathcal{P}(\varphi) \\ [\![v]\!]^{\mathcal{P}} &\doteq M[L[v]] && \text{for } v \in V \setminus \mathcal{P}(\varphi) \end{aligned}$$

Теорема:

$$[\![\varphi]\!]^{\mathcal{P}} \iff [\![\varphi]\!]$$

Оптимизация: чистые переменные

$$
\begin{aligned}
&[\![x = y \implies y = x]\!]^{\mathcal{P}} \\
&\quad \iff [\![x = y \implies y = x]\!]^{\mathcal{P}} \\
&\quad \iff [\![x = y]\!]^{\mathcal{P}} \implies [\![y = x]\!]^{\mathcal{P}} \\
&\quad \iff \Upsilon_x = \Upsilon_y \implies \Upsilon_y = \Upsilon_x \; .
\end{aligned}
$$


YES
NO