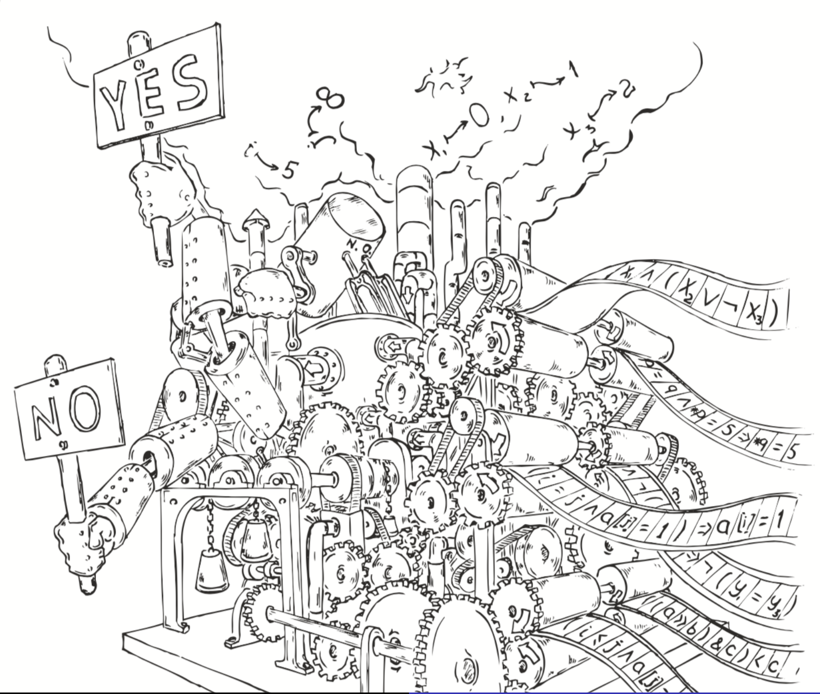

YES
NO

Задачи разрешимости логических формул и приложения
Лекция 7. Логика массивов

Роман Холин

Московский государственный университет

Москва, 2022

Пример

```
a: array 0..99 of integer;
i: integer;

for i:=0 to 99 do
        assert(∀x ∈ ℕ₀. x < i ⟹ a[x] = 0);
        a[i]:=0;
        assert(∀x ∈ ℕ₀. x ≤ i ⟹ a[x] = 0);
done;
assert(∀x ∈ ℕ₀. x ≤ 99 ⟹ a[x] = 0);
```

Пример

```
a: array 0..99 of integer;
i: integer;

for i:=0 to 99 do
        assert(∀x ∈ ℕ₀. x < i ⟹ a[x] = 0);
        a[i]:=0;
        assert(∀x ∈ ℕ₀. x ≤ i ⟹ a[x] = 0);
done;
assert(∀x ∈ ℕ₀. x ≤ 99 ⟹ a[x] = 0);
```

$$\begin{aligned} & (\forall x \in \mathbb{N}_0.\ x < i \implies \mathsf{a}[x] = 0) \\ \wedge\ & \mathsf{a}' = \mathsf{a}\{i \leftarrow 0\} \\ \implies & (\forall x \in \mathbb{N}_0.\ x \leq i \implies \mathsf{a}'[x] = 0) \end{aligned}$$

$a\{i \leftarrow x\}$

$a\{i \leftarrow x\}$ - присвоить x элементу массива с индексом i

$a\{i \leftarrow x\}$

$a\{i \leftarrow x\}$ - присвоить x элементу массива с индексом i

$(\forall x \in \mathbb{N}_0 . x < i \implies a[x] = 0) \wedge a' = a\{i \leftarrow 0\} \implies$
$(\forall x \in \mathbb{N}_0 . x \leq i \implies a'[x] = 0)$

Синтаксис

T_I - тип индекса
T_E - тип элемента
T_A - тип массива, сокращение от $T_I \rightarrow T_E$ - т.е. множество функций из индексы в элементы

Синтаксис

T_I - тип индекса
T_E - тип элемента
T_A - тип массива, сокращение от $T_I \to T_E$ - т.е. множество функций из индексы в элементы
Теория массивов параметризирована теориями индексов и элементов.

Синтаксис

term A : array-identifier $|$ $\text{term}_A\{\text{term}_I \leftarrow \text{term}_E\}$
term E : $\text{term}_A[\text{term}_I]$ $|$ $\ldots$
formula : $\text{term}_A = \text{term}_A$ $|$ $\ldots$

Семантика

Аксиома чтения:
$\forall a_1 \in T_A . \forall a_2 \in T_A . \forall i \in T_I . \forall j \in T_I . (a_1 = a_2 \land i = j) \implies a_1[i] = a_2[j]$

Аксиома записи:
$\forall a \in T_A . \forall e \in T_E . \forall i \in T_I . \forall j \in T_I . a\{i \leftarrow e\}[j] = (i = j)?e : a[j]$

Экстенсиональное аксиома :
$\forall a_1 \in T_A . \forall a_2 \in T_A . (\forall i \in T_I . a_1[i] = a_2[i]) \implies a_1 = a_2$

Пример элиминация термов

$$(i = j \wedge a[j] =' z') \implies a[i] =' z'$$

Пример элиминация термов

$$(i = j \wedge a[j] =' z') \implies a[i] =' z'$$
$$(i = j \wedge F_a(i) =' z') \implies F_a(i) =' z'$$

Правило записи

Перепишем формулу:
для $a\{i \leftarrow e\}$ добавим a', т.ч. $a'[i] = e$ и $\forall j \neq i . a'[j] = a[j]$

Правило записи

Перепишем формулу:

для $a\{i \leftarrow e\}$ добавим a', т.ч. $a'[i] = e$ и $\forall j \neq i. a'[j] = a[j]$

$a[0] = 10 \implies a\{1 \leftarrow 20\}[0] = 10$

Правило записи

Перепишем формулу:

для $a\{i \leftarrow e\}$ добавим a', т.ч. $a'[i] = e$ и $\forall j \neq i . a'[j] = a[j]$

$a[0] = 10 \implies a\{1 \leftarrow 20\}[0] = 10$

$(a[0] = 10 \wedge a'[1] = 20 \wedge (\forall j \neq 1 . a'[j] = a[j])) \implies a_0[0] = 10$

$(F_a(0) = 10 \wedge F_{a'}(1) = 20 \wedge (\forall j \neq 1 . F_{a'}(j) = F_a(j))) \implies F_{a'}(0) = 10$

Правило записи

Перепишем формулу:

для $a\{i \leftarrow e\}$ добавим a', т.ч. $a'[i] = e$ и $\forall j \neq i . a'[j] = a[j]$

$a[0] = 10 \implies a\{1 \leftarrow 20\}[0] = 10$

$(a[0] = 10 \wedge a'[1] = 20 \wedge (\forall j \neq 1 . a'[j] = a[j])) \implies a_0[0] = 10$

Свойство массива

$$\forall i_1 \ldots \forall i_k \in T_I . \phi_I(i_1, \ldots, i_k) \implies \phi_V(i_1, \ldots, i_k)$$

Свойство массива

$\forall i_1 \dots \forall i_k \in T_I . \phi_I(i_1, \dots, i_k) \implies \phi_V(i_1, \dots, i_k)$

1) Грамматика для ϕ_I:

iguard : iguard $\wedge$ iguard | iguard $\vee$ iguard | iterm $\leq$ iterm | iterm $=$ iterm

iterm : i_1 | $\dots$ | i_k | term

term : integer-constant | integer-constant $\times$ index-identifier | term $+$ term

index-identifier и term не могут быть $i_1, \dots, i_k$

2) $i_1, \dots, i_k$ могут быть только частью выражения чтения вида $a[i_j]$

Пример

$$a' = a\{i \leftarrow 0\}$$

Пример

$a' = a\{i \leftarrow 0\}$
$\forall j \neq i . a'[j] = a[j]$

Пример

$$a' = a\{i \leftarrow 0\}$$
$$\forall j \neq i . a'[j] = a[j]$$
$$\forall j . (j \leq i - 1 \wedge i + 1 \leq j) \implies a'[j] = a[j]$$

$\iota(\phi)$

$\iota(\phi)$ - множество элементов, которые могут быть равны какому-нибудь индексу, т.е.:
1) Все выражения, которые используются как индекс массива и которые не связаны квантором
2) Все выражения, которые используются внутри ограничений на индексы и которые не связаны квантором
3) Если ϕ ничего такого не содержит, то $\iota(\phi) = \{0\}$, чтобы оно не было пусто

Редукция массивов

Input: An array property formula ϕ_A in NNF
Output: A formula ϕ_{UF} in the index and element theories with uninterpreted functions

1. Apply the write rule to remove all array updates from ϕ_A.
2. Replace all existential quantifications of the form $\exists i \in T_I.\ P(i)$ by $P(j)$, where j is a fresh variable.
3. Replace all universal quantifications of the form $\forall i \in T_I.\ P(i)$ by
$$\bigwedge_{i \in \mathcal{I}(\phi)} P(i)\,.$$
4. Replace the array read operators by uninterpreted functions and obtain ϕ_{UF};
5. **return** ϕ_{UF};

Пример

$$(\forall x \in \mathbb{N}_0 . x < i \implies a[x] = 0) \wedge a' = a\{i \leftarrow 0\} \implies$$
$$(\forall x \in \mathbb{N}_0 . x \leq i \implies a'[x] = 0)$$

Пример

$$(\forall x \in \mathbb{N}_0 . x < i \implies a[x] = 0) \land a' = a\{i \leftarrow 0\} \implies$$
$$(\exists x \in \mathbb{N}_0 . x \leq i \land a'[x] \neq 0)$$

Пример

$$(\forall x \in \mathbb{N}_0 . x < i \implies a[x] = 0) \wedge a'[i] = 0 \wedge \forall j \neq i . a'[j] = a[j] \implies (\exists x \in \mathbb{N}_0 . x \leq i \wedge a'[x] \neq 0)$$

Пример

$$(\forall x \in \mathbb{N}_0 . x < i \implies a[x] = 0) \land a'[i] = 0 \land \forall j \neq i . a'[j] = a[j] \implies (z \leq i \land a'[z] \neq 0)$$

Пример

$$\iota(\phi) = \{i, z\}$$

Пример

$$\iota(\phi) = \{i, z\}$$
$$(i < i \implies a[i] = 0) \land (z < i \implies a[z] = 0) \land$$
$$a'[i] = 0 \land \forall j \neq i . a'[j] = a[j] \implies$$
$$(z \leq i \land a'[z] \neq 0)$$

Пример

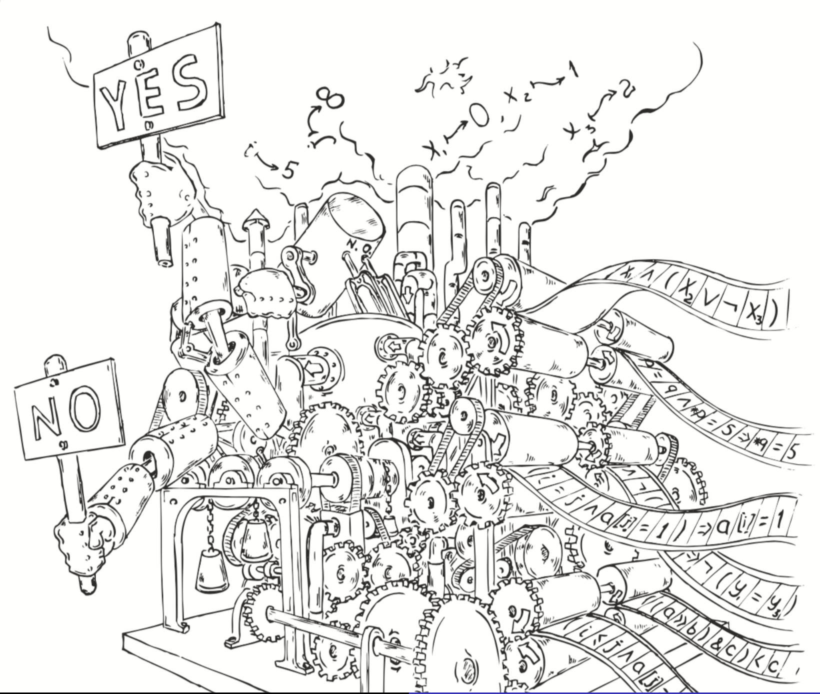
$$\iota(\phi) = \{i, z\}$$
$$(i < i \implies a[i] = 0) \wedge (z < i \implies a[z] = 0) \wedge$$
$$a'[i] = 0 \wedge (i \neq i \implies a'[i] = a[i]) \wedge (z \neq i \implies a'[z] = a[z]) \implies$$
$$(z \leq i \wedge a'[z] \neq 0)$$

Пример

$$(z < i \implies a[z] = 0) \wedge$$
$$a'[i] = 0 \wedge (z \neq i \implies a'[z] = a[z]) \implies$$
$$(z \leq i \wedge a'[z] \neq 0)$$

Пример

$$(z < i \implies F_a(z) = 0) \wedge$$
$$F_{a'}(i) = 0 \wedge (z \neq i \implies F_{a'}(z) = F_a(z)) \implies$$
$$(z \leq i \wedge F_{a'}(z) \neq 0)$$


YES
NO
N.O.
i → 5
x1 → 0
x2 → 1
x3 → 2