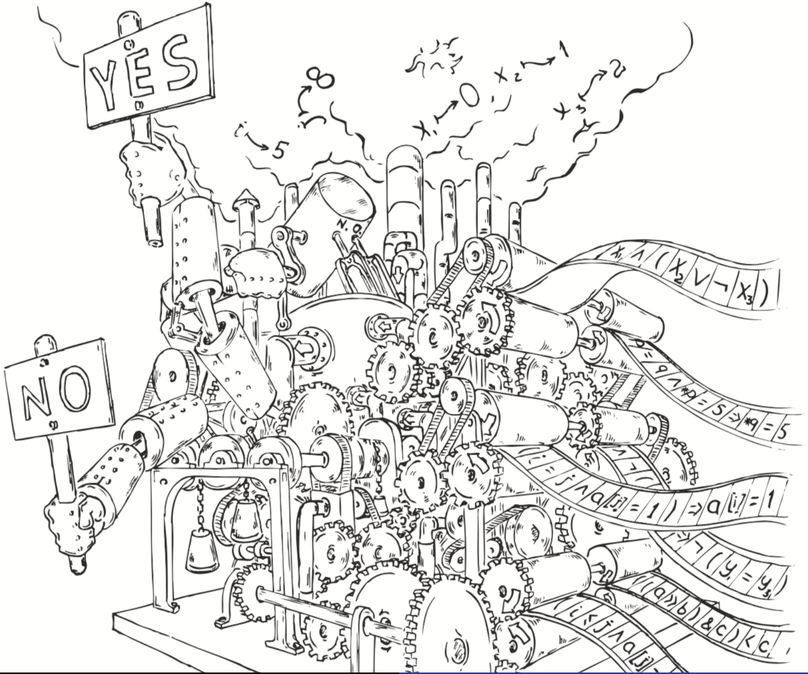

YES
NO
N.O.

Задачи разрешимости логических формул и приложения
Лекция 6. Линейная логика. Логика битовых векторов

Роман Холин

Московский государственный университет

Москва, 2022

Логика линейной арифметики

$$\begin{aligned}
formula &: formula \land formula \mid (formula) \mid atom \\
atom &: sum \ op \ sum \\
op &: = \mid \leq \mid < \\
sum &: term \mid sum + term \\
term &: identifier \mid constant \mid constant \ identifier
\end{aligned}$$

Логика линейной арифметики

$$
\begin{aligned}
formula &: formula \wedge formula \mid (formula) \mid atom \\
atom &: sum\ \ op\ \ sum \\
op &: = \ \mid\ \leq\ \mid\ < \\
sum &: term \mid sum + term \\
term &: identifier \mid constant \mid constant\ \ identifier
\end{aligned}
$$

$$2z_1 + 3z_2 \leq 5 \wedge z_2 + 5z_2 - 10z_3 \geq 6 \wedge z1 + z3 = 3$$

Домен

- Целые числа
- Рациональные числа

Домен

- Целые числа - целочисленное линейное программирование
- Рациональные числа - симлекс метод

Логика битовых векторов

$$
\begin{aligned}
formula &: formula \wedge formula \mid \neg formula \mid (\, formula \,) \mid atom \\
atom &: term \; rel \; term \mid Boolean\text{-}Identifier \mid term[\, constant \,] \\
rel &: < \;\mid\; = \\
term &: term \; op \; term \mid identifier \mid \;\sim term \mid constant \mid atom \,?\, term : term \mid \\
&\quad\; term[\, constant : constant \,] \mid ext(\, term \,) \\
op &: + \mid \; - \; \mid \; \cdot \; \mid / \mid \; << \; \mid \; >> \; \mid \& \mid \; | \; \mid \oplus \mid \circ
\end{aligned}
$$

Мотивация

$$(x - y > 0) \iff (x > y)$$

Мотивация

$(x - y > 0) \iff (x > y)$

```
unsigned char number = 200;
number = number + 100;
printf("Sum: %d\n", number);
```

$$(x - y > 0) \iff (x > y)$$

```
unsigned char number = 200;
number = number + 100;
printf("Sum: %d\n", number);
```

$$
\begin{array}{r}
11001000 = 200 \\
+\,01100100 = 100 \\
\hline
= 00101100 = 44
\end{array}
$$

Определения

$\lambda i \in \{0, \ldots, l-1\}.\, f(i)$

Определения

$\lambda i \in \{0, \ldots, l-1\}.\, f(i)$

$b : \{0, \ldots, l-1\} \longrightarrow \{0, 1\}$

Определения

$$\lambda i \in \{0, \ldots, l-1\}.\, f(i)$$

$$b : \{0, \ldots, l-1\} \longrightarrow \{0, 1\}$$

$$|_{[l]} \;:\, (bvec_l \times bvec_l) \longrightarrow bvec_l$$

$$a \,|\, b \doteq \;\lambda i.\, (a_i \vee b_i)$$

Определения

$$\lambda i \in \{0, \ldots, l-1\}.\, f(i)$$
$$b : \{0, \ldots, l-1\} \longrightarrow \{0, 1\}$$
$$|_{[l]} \; : (bvec_l \times bvec_l) \longrightarrow bvec_l$$
$$a \,|\, b \doteq \; \lambda i.\, (a_i \vee b_i)$$
$$\langle\cdot\rangle_U : bvec_l \longrightarrow \{0, \ldots, 2^l - 1\}\;,$$
$$\langle b\rangle_U \doteq \; \textstyle\sum_{i=0}^{l-1} b_i \cdot 2^i.$$

Определения

$$\lambda i \in \{0, \ldots, l-1\}.\, f(i)$$

$$b : \{0, \ldots, l-1\} \longrightarrow \{0, 1\}$$

$$|_{[l]} \; : (bvec_l \times bvec_l) \longrightarrow bvec_l$$

$$a \,|\, b \doteq \; \lambda i.\, (a_i \vee b_i)$$

$$\langle\cdot\rangle_U : bvec_l \longrightarrow \{0, \ldots, 2^l - 1\} \; ,$$

$$\langle b\rangle_U \doteq \; \textstyle\sum_{i=0}^{l-1} b_i \cdot 2^i.$$

$$\langle\cdot\rangle_S : bvec_l \longrightarrow \{-2^{l-1}, \ldots, 2^{l-1} - 1\} \; ,$$

$$\langle b\rangle_S := -2^{l-1} \cdot b_{l-1} + \textstyle\sum_{i=0}^{l-2} b_i \cdot 2^i \; .$$

Определения

$$
\begin{aligned}
a_{[l]} +_U b_{[l]} = c_{[l]} &\iff \langle a \rangle_U + \langle b \rangle_U = \langle c \rangle_U \mod 2^l\,, \\
a_{[l]} -_U b_{[l]} = c_{[l]} &\iff \langle a \rangle_U - \langle b \rangle_U = \langle c \rangle_U \mod 2^l\,, \\
a_{[l]} +_S b_{[l]} = c_{[l]} &\iff \langle a \rangle_S + \langle b \rangle_S = \langle c \rangle_S \mod 2^l\,, \\
a_{[l]} -_S b_{[l]} = c_{[l]} &\iff \langle a \rangle_S - \langle b \rangle_S = \langle c \rangle_S \mod 2^l\,.
\end{aligned}
$$

$$
-a_{[l]} = b_{[l]} \iff -\langle a \rangle_S = \langle b \rangle_S \mod 2^l\,.
$$

Определения

$$
\begin{aligned}
a_{[l]U} < b_{[l]U} &\iff \langle a\rangle_U < \langle b\rangle_U \ , \\
a_{[l]S} < b_{[l]S} &\iff \langle a\rangle_S < \langle b\rangle_S \ , \\
a_{[l]U} < b_{[l]S} &\iff \langle a\rangle_U < \langle b\rangle_S \ , \\
a_{[l]S} < b_{[l]U} &\iff \langle a\rangle_S < \langle b\rangle_U \ .
\end{aligned}
$$

Определения

$$
\begin{aligned}
a_{[l]} \cdot_U b_{[l]} = c_{[l]} &\iff \langle a\rangle_U \cdot \langle b\rangle_U = \langle c\rangle_U \mod 2^l \,, \\
a_{[l]} /_U b_{[l]} = c_{[l]} &\iff \langle a\rangle_U / \langle b\rangle_U = \langle c\rangle_U \mod 2^l \,, \\
a_{[l]} \cdot_S b_{[l]} = c_{[l]} &\iff \langle a\rangle_S \cdot \langle b\rangle_S = \langle c\rangle_S \mod 2^l \,, \\
a_{[l]} /_S b_{[l]} = c_{[l]} &\iff \langle a\rangle_S / \langle b\rangle_S = \langle c\rangle_S \mod 2^l \,.
\end{aligned}
$$

Определения

$$ext_{[m]U}(a_{[l]}) = b_{[m]U} \iff \langle a \rangle_U = \langle b \rangle_U \ ,$$
$$ext_{[m]S}(a_{[l]}) = b_{[m]S} \iff \langle a \rangle_S = \langle b \rangle_S \ .$$

Определения

$$a_{[l]} \ll b_U = \lambda i \in \{0, \ldots, l-1\}. \begin{cases} a_{i-\langle b \rangle_U} & : i \geq \langle b \rangle_U \\ 0 & : \text{otherwise} \end{cases}$$

$$a_{[l]U} \gg b_U = \lambda i \in \{0, \ldots, l-1\}. \begin{cases} a_{i+\langle b \rangle_U} & : i < l - \langle b \rangle_U \\ 0 & : \text{otherwise} . \end{cases}$$

$$a_{[l]S} \gg b_U = \lambda i \in \{0, \ldots, l-1\}. \begin{cases} a_{i+\langle b \rangle_U} & : i < l - \langle b \rangle_U \\ a_{l-1} & : \text{otherwise} . \end{cases}$$

Алгоритм

Algorithm 6.2.1: BV-FLATTENING

Input: A formula φ in bit-vector arithmetic
Output: An equisatisfiable Boolean formula $\mathcal{B}$

function BV-FLATTENING
  $\mathcal{B}{:=}e(\varphi)$; ▷ the propositional skeleton of φ
  for each $t_{[l]} \in T(\varphi)$ **do**
    for each $i \in \{0, \ldots, l-1\}$ **do**
      set $e(t)_i$ to a new Boolean variable;
  for each $a \in At(\varphi)$ **do**
    $\mathcal{B}{:=}\mathcal{B} \wedge$ BV-CONSTRAINT(e, a);
  for each $t_{[l]} \in T(\varphi)$ **do**
    $\mathcal{B}{:=}\mathcal{B} \wedge$ BV-CONSTRAINT(e, t);
  return $\mathcal{B}$;

Замены

$$\bigwedge_{i=0}^{l-1} (C_i \iff e(t)_i)$$

$$\bigwedge_{i=0}^{l-1} ((a_i \vee b_i) \iff e(t)_i)$$

Замены

$$\bigwedge_{i=0}^{l-1} (C_i \iff e(t)_i)$$

Замены

$$\begin{aligned} sum(a,b,cin) &\doteq (a \oplus b) \oplus cin\ , \\ carry(a,b,cin) &\doteq (a \wedge b) \vee ((a \oplus b) \wedge cin) \end{aligned}$$

$$c_i \doteq \begin{cases} cin & : i = 0 \\ carry(x_{i-1}, y_{i-1}, c_{i-1}) & : otherwise \end{cases}$$

$$\begin{aligned} add(x,y,cin) &\doteq \langle result, cout \rangle\ , \\ result_i &\doteq sum(x_i, y_i, c_i) \quad for\ i \in \{0, \ldots, l-1\} \\ cout &\doteq c_n\ . \end{aligned}$$

$$\bigwedge_{i=0}^{l-1} (add(a,b,0).result_i \iff e(t)_i)$$

Замены

$$\bigwedge_{i=0}^{l-1} a_i = b_i \iff e(t)$$

$$\langle a \rangle_U < \langle b \rangle_U \iff \neg add(a, \sim b, 1).cout$$

$$\langle a \rangle_S < \langle b \rangle_S \iff (a_{l-1} \iff b_{l-1}) \oplus add(a,\ b, 1).cout$$

Замены

$$ls(a_{[l]}, b_{[n]U}, -1) \doteq a\ ,$$

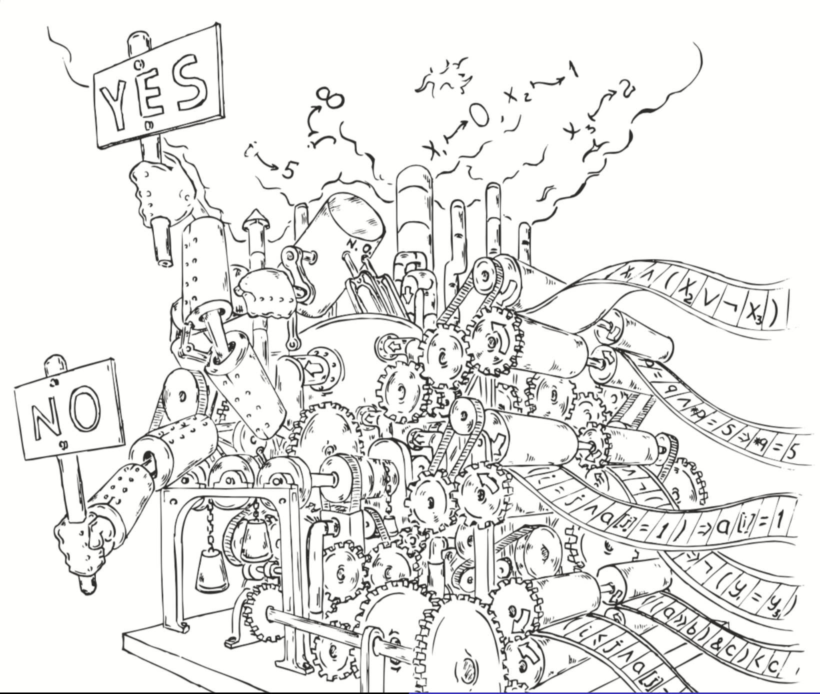
$$ls(a_{[l]}, b_{[n]U}, s) \doteq$$

$$\lambda i \in \{0, \ldots, l-1\}. \begin{cases} (ls(a, b, s-1))_{i-2^s} & : i \geq 2^s \wedge b_s \\ (ls(a, b, s-1))_i & : \neg b_s \\ 0 & : \text{otherwise}\ . \end{cases}$$

Замены

$$
\begin{aligned}
mul(a, b, -1) &\doteq 0, \\
mul(a, b, s) &\doteq mul(a, b, s-1) + (b_s ? (a << s) : 0)
\end{aligned}
$$

$$
\begin{aligned}
b \neq 0 &\implies e(t) \cdot b + r = a \\
b \neq 0 &\implies r < b\,.
\end{aligned}
$$


YES
NO
N.O.