Satisfiability Checking - WS 2023/2024

Series 6

teaching@ths.rwth-aachen.de
https://ths.rwth-aachen.de/teaching/

Exercise 1

You are given the following code and are asked if the functions `twice` and `twice_flat` are equivalent. Assume that `foo` is some function, model it as an uninterpreted function.

```
int foo(int x) { ... }
int twice(int n) {
        int out = n;
        for (int i = 0; i < 2; i++) {
                out = foo(out);
        }
        return out;
}
int twice_flat(int n) {
        return foo(foo(n));
}
```

1. Create a formula φ_1 modeling `twice`.
2. Create a formula φ_2 modeling `twice_flat`.
3. Create a formula φ_3 stating that there is an input for which the two functions give a different output.
4. Apply Ackermann's reduction to φ_3.

Solution:

$$\begin{aligned}
\varphi_1 :=& out_0 = n \wedge \\
& out_1 = foo(out_0) \wedge \\
& out_2 = foo(out_1) \\
\\
\varphi_2 :=& out_f = foo(foo(n)) \\
\\
\varphi_3 :=& (\varphi_1 \wedge \varphi_2) \wedge (out_2 \neq out_f) \\
\\
\varphi_{UF} :=& (\\
& out_0 = n \wedge \\
& out_1 = foo(out_0) \wedge \\
& out_2 = foo(out_1) \wedge \\
& out_f = foo(foo(n)) \\
&) \wedge (out_2 \neq out_f) \\
\\
\varphi_{flat} :=& (\\
& out_0 = n \wedge \\
& out_1 = f_1 \wedge \\
& out_2 = f_2 \wedge \\
& out_f = f_4 \\
&) \wedge (out_2 \neq out_f) \\
\\
\varphi_{cong} :=& \\
& ((out_0 = out_1) \rightarrow f_1 = f_2) \wedge \\
& ((out_0 = n) \rightarrow f_1 = f_3) \wedge \\
& ((out_0 = f_3) \rightarrow f_1 = f_4) \wedge \\
& ((out_1 = n) \rightarrow f_2 = f_3) \wedge \\
& ((out_1 = f_3) \rightarrow f_2 = f_4) \wedge \\
& ((f_3 = n) \rightarrow f_3 = f_4) \\
\\
\varphi_{reduced} :=& \varphi_{flat} \wedge \varphi_{cong}
\end{aligned}$$

Exercise 2

Let $a_{[l]}, b_{[l]}, c_{[l]}$ be bit vectors of size l in unsigned encoding.

- Give a propositional formula φ' that encodes the following finite-precision bit-vector arithmetic formula for $l = 3$:

$$\varphi : c_{[l]} = a_{[l]} \oplus b_{[l]} \wedge d_{[l]} = a_{[l]} +_U b_{[l]} \wedge e_{[l]} = a_{[l]} \cdot_U b_{[l]}$$

- Give the number of variables and clauses needed to express φ' in CNF.
- Give the space complexity (i.e. the growth of the number of variables and clauses for $l \rightarrow \infty$) of the encoding for $\oplus$, $+$ and $\cdot$ respectively in $\mathcal{O}$-notation.

Solution:

- Encoding for $l = 3$:

$$
\begin{aligned}
\oplus :& \bigwedge_{i=0,1,2} (c_i \iff a_i \oplus b_i) \\
+ :& (d_0 \iff a_0 \oplus b_0) \wedge \\
& (o_0 \iff a_0 \wedge b_0) \wedge \\
& (d_1 \iff a_1 \oplus b_1 \oplus o_0) \wedge (o_1 \iff (a_1 \wedge b_1) \vee (a_1 \wedge o_0) \vee (b_1 \wedge o_0)) \wedge \\
& (d_2 \iff a_2 \oplus b_2 \oplus o_1) \\
\cdot :& (x = 0) \wedge \\
& (a_0 \rightarrow \varphi_+(x, b, y)) \wedge (\neg a_0 \rightarrow x = y) \wedge \\
& (a_1 \rightarrow \varphi_+(y, b << 1, z)) \wedge (\neg a_1 \rightarrow y = z) \wedge \\
& (a_2 \rightarrow \varphi_+(z, b << 2, e)) \wedge (\neg a_2 \rightarrow z = e) \wedge \\
\text{alternative } \cdot_2 :& (e_0 \iff a_0 \wedge b_0) \wedge \\
& (e_1 \iff (a_0 \wedge b_1) \oplus (a_1 \wedge b_0)) \wedge \\
& (e_2 \iff (a_0 \wedge b_2) \oplus (a_1 \wedge b_1) \oplus (a_2 \wedge b_0) \oplus (a_0 \wedge a_1 \wedge b_0 \wedge b_1))
\end{aligned}
$$

- CNF:

$$
\begin{aligned}
\varphi_1 := \alpha \iff \beta \oplus \gamma :& (\neg\alpha \vee \neg\beta \vee \neg\gamma) \wedge (\neg\alpha \vee \beta \vee \gamma) \wedge (\alpha \vee \neg\beta \vee \gamma) \wedge (\alpha \vee \beta \vee \neg\gamma) \\
\varphi_1' := \alpha \iff \beta \oplus 0 :& (\neg\alpha \vee \beta) \wedge (\alpha \vee \neg\beta) \\
\varphi_2 := \alpha \iff \beta \wedge \gamma :& (\neg\alpha \vee \beta) \wedge (\neg\alpha \vee \gamma) \wedge (\alpha \vee \neg\beta \vee \neg\gamma) \\
\varphi_2' := \alpha \iff \beta \wedge 0 :& (\neg\alpha) \\
\varphi_3 := \alpha \iff \beta \oplus \gamma \oplus \delta :& (\neg\alpha \vee \neg\beta \vee \neg\gamma \vee \delta) \wedge (\neg\alpha \vee \neg\beta \vee \gamma \vee \neg\delta) \wedge \\
& (\neg\alpha \vee \beta \vee \neg\gamma \vee \neg\delta) \wedge (\neg\alpha \vee \beta \vee \gamma \vee \delta) \wedge \\
& (\alpha \vee \neg\beta \vee \neg\gamma \vee \neg\delta) \wedge (\alpha \vee \neg\beta \vee \gamma \vee \delta) \wedge \\
& (\alpha \vee \beta \vee \neg\gamma \vee \delta) \wedge (\alpha \vee \beta \vee \gamma \vee \neg\delta) \\
\varphi_3' := \alpha \iff 0 \oplus \gamma \oplus \delta :& (\neg\alpha \vee \neg\gamma \vee \neg\delta) \wedge (\neg\alpha \vee \gamma \vee \delta) \wedge \\
& (\alpha \vee \gamma \vee \delta) \wedge (\alpha \vee \neg\gamma \vee \delta) \wedge (\alpha \vee \gamma \vee \neg\delta) \\
\varphi_3'' := \alpha \iff \beta \oplus 0 \oplus \delta :& (\neg\alpha \vee \neg\beta \vee \neg\delta) \wedge (\neg\alpha \vee \beta \vee \delta) \wedge \\
& (\alpha \vee \beta \vee \delta) \wedge (\alpha \vee \beta \vee \neg\delta) \\
\varphi_3''' := \alpha \iff \beta \oplus \gamma \oplus 0 :& (\neg\alpha \vee \neg\beta \vee \neg\gamma) \wedge (\neg\alpha \vee \beta \vee \gamma) \wedge \\
& (\alpha \vee \beta \vee \gamma) \wedge (\alpha \vee \beta \vee \neg\gamma)
\end{aligned}
$$

$$
\begin{aligned}
\oplus :& \bigwedge_{i=0,1,2} \varphi_1(c_i, a_i, b_i) \\
+ :& \varphi_1(d_0, a_0, b_0) \wedge \\
& \varphi_2(o_0, a_0, b_0) \wedge \\
& \varphi_3(d_1, a_1, b_1, o_0) \wedge \\
& (\neg a_1 \vee \neg b_1 \vee o_1) \wedge (\neg a_1 \vee \neg o_0 \vee o_1) \wedge \\
& (a_1 \vee b_1 \vee \neg o_1) \wedge (a_1 \vee o_0 \vee \neg o_1) \wedge \\
& (\neg b_1 \vee \neg o_0 \vee o_1) \wedge (b_1 \vee o_0 \vee \neg o_1) \wedge \\
& \varphi_3(d_2, a_2, b_2, o_1)
\end{aligned}
$$

$$
\begin{aligned}
\cdot :& (\neg x_0) \wedge (\neg x_1) \wedge (\neg x_2) \wedge \\
& (\neg a_0 \vee \varphi_1(y_0, x_0, b_0)) \wedge \\
& (\neg a_0 \vee \varphi_2(o_0, x_0, b_0)) \wedge \\
& (\neg a_0 \vee \varphi_3(y_1, x_1, b_1, o_0)) \wedge \\
& (\neg a_0 \vee \neg x_1 \vee \neg b_1 \vee o_1) \wedge (\neg a_0 \vee \neg x_1 \vee \neg o_0 \vee o_1) \wedge \\
& (\neg a_0 \vee x_1 \vee b_1 \vee \neg o_1) \wedge (\neg a_0 \vee x_1 \vee o_0 \vee \neg o_1) \wedge \\
& (\neg a_0 \vee \neg b_1 \vee \neg o_0 \vee o_1) \wedge (\neg a_0 \vee b_1 \vee o_0 \vee \neg o_1) \wedge \\
& (\neg a_0 \vee \varphi_3(y_2, x_2, b_2, o_1)) \\
& \\
& (\neg a_1 \vee \varphi_1(z_0, y_0, 0)) \wedge \\
& (\neg a_1 \vee \varphi_2(p_0, y_0, 0)) \wedge \\
& (\neg a_1 \vee \varphi_3(z_1, y_1, b_0, p_0)) \wedge \\
& (\neg a_1 \vee \neg y_1 \vee \neg b_0 \vee p_1) \wedge (\neg a_1 \vee \neg y_1 \vee \neg p_0 \vee p_1) \wedge \\
& (\neg a_1 \vee y_1 \vee b_0 \vee \neg p_1) \wedge (\neg a_1 \vee y_1 \vee p_0 \vee \neg p_1) \wedge \\
& (\neg a_1 \vee \neg b_0 \vee \neg p_0 \vee p_1) \wedge (\neg a_1 \vee b_0 \vee p_0 \vee \neg p_1) \wedge \\
& (\neg a_1 \vee \varphi_3(z_2, y_2, b_1, p_1)) \\
& \\
& (\neg a_2 \vee \varphi_1'(e_0, z_0, 0)) \wedge \\
& (\neg a_2 \vee \varphi_2'(q_0, z_0, 0)) \wedge \\
& (\neg a_2 \vee \varphi_3''(e_1, z_1, 0, q_0)) \wedge \\
& (\neg a_2 \vee \neg z_1 \vee \neg q_0 \vee q_1) \wedge \\
& (\neg a_1 \vee z_1 \vee \neg q_1) \wedge (\neg a_2 \vee z_1 \vee q_0 \vee \neg q_1) \wedge \\
& (\neg a_2 \vee q_0 \vee \neg q_1) \\
& (\neg a_2 \vee \varphi_3(e_2, z_2, b_0, q_1))
\end{aligned}
$$

$$
\begin{aligned}
\text{alternative } \cdot_2 :& \varphi_1(e_0, a_0, b_0) \wedge \\
& (\neg a_0 \vee \neg a_1 \vee \neg b_0 \vee \neg b_1 \vee \neg e_1) \wedge (\neg a_0 \vee a_1 \vee \neg b_1 \vee e_1) \wedge \\
& (\neg a_0 \vee b_0 \vee \neg b_1 \vee e_1) \wedge (a_0 \vee \neg a_1 \vee \neg b_0 \vee e_1) \wedge \\
& (a_0 \vee a_1 \vee \neg e_1) \wedge (a_0 \vee b_0 \vee \neg e_1) \wedge \\
& (\neg a_1 \vee \neg b_0 \vee b_1 \vee e_1) \wedge (a_1 \vee b_1 \vee \neg e_1) \wedge (b_0 \vee b_1 \vee \neg e_1) \\
& \\
& (\neg a_0 \vee \neg a_1 \vee b_0 \vee \neg b_1 \vee \neg b_2 \vee \neg e_2) \wedge \\
& (\neg a_0 \vee a_1 \vee b_0 \vee \neg b_2 \vee e_2) \wedge (\neg a_0 \vee \neg a_2 \vee \neg b_0 \vee \neg b_2 \vee \neg e_2) \wedge \\
& (\neg a_0 \vee \neg a_2 \vee \neg b_0 \vee b_2 \vee e_2) \wedge (\neg a_0 \vee a_2 \vee \neg b_0 \vee \neg b_2 \vee e_2) \wedge \\
& (\neg a_0 \vee a_2 \vee \neg b_0 \vee b_2 \vee \neg e_2) \wedge (\neg a_0 \vee b_0 \vee b_1 \vee \neg b_2 \vee e_2) \wedge \\
& (a_0 \vee \neg a_1 \vee \neg a_2 \vee \neg b_0 \vee \neg b_1 \vee \neg e_2) \wedge (a_0 \vee \neg a_1 \vee a_2 \vee \neg b_1 \vee e_2) \wedge \\
& (a_0 \vee \neg a_1 \vee b_0 \vee \neg b_1 \vee e_2) \wedge (a_0 \vee a_1 \vee \neg a_2 \vee \neg b_0 \vee e_2) \wedge \\
& (a_0 \vee a_1 \vee a_2 \vee \neg e_2) \wedge (a_0 \vee a_1 \vee b_0 \vee \neg e_2) \wedge \\
& (a_0 \vee \neg a_2 \vee \neg b_0 \vee b_1 \vee e_2) \wedge (a_0 \vee a_2 \vee b_1 \vee \neg e_2) \wedge \\
& (a_0 \vee b_0 \vee b_1 \vee \neg e_2) \wedge (\neg a_1 \vee b_0 \vee \neg b_1 \vee b_2 \vee e_2) \wedge \\
& (a_1 \vee b_0 \vee b_2 \vee \neg e_2) \wedge (b_0 \vee b_1 \vee b_2 \vee \neg e_2)
\end{aligned}
$$

	Variables	Clauses	Literals
φ_1	3	4	12
φ_1'	2	2	4
φ_2	3	3	7
φ_2'	1	1	1
φ_3	4	8	32
φ_3'	3	5	15
φ_3''	3	4	12
φ_3'''	3	4	12
$\varphi_\oplus$	9	12	36
φ_+	11	29	61
$\varphi_\cdot$	24	79	337
$\varphi_{\cdot_2}$	6	32	136

- $\oplus$: Variables: $3 \cdot l \in \mathcal{O}(l)$
  Clauses: $4 \cdot l \in \mathcal{O}(l)$
  Literals: $12 \cdot l \in \mathcal{O}(l)$

  $+$: Variables: $3 \cdot l + (l - 1) \in \mathcal{O}(l)$
  Clauses: $7 + 14 \cdot (l - 2) + 8 \in \mathcal{O}(l)$
  Literals: $12 + 7 + (24 + 18) \cdot l + 24 \in \mathcal{O}(l)$

  $\cdot$: Variables: $\mathcal{O}(l^2)$
  Clauses: $\mathcal{O}(l^2)$
  Literals: $\mathcal{O}(l^3)$