Space and Congruence Compression of Proofs

Andreas Fellner

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

computer languages

European Master in Computational Logic

Master Thesis Presentation
Vienna, 23^{rd} of September 2014

Example

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Example

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Unsatisfiable!

Example

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Unsatisfiable!

Proof

Equality is transitive, therefore from $f(a) = a$, $a = b$ and $b = f(b)$ follows $f(a) = f(b)$, which contradicts $f(a) \neq f(b)$

Example

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Unsatisfiable!

Proof

Equality is transitive, therefore from $f(a) = a$, $a = b$ and $b = f(b)$ follows $f(a) = f(b)$, which contradicts $f(a) \neq f(b)$

A different Proof

$f(.)$ is a function, therefore from $a = b$ follows $f(a) = f(b)$, which contradicts $f(a) \neq f(b)$

Definitions

Definitions

Ground Terms

- Constants $a, b, c, \ldots$
- Compound Terms $f(t_1, \ldots, t_n)$

Definitions

Ground Terms

- Constants $a, b, c, \ldots$
- Compound Terms $f(t_1, \ldots, t_n)$

Congruence Relation

- Reflexive: $t = t$
- Symmetric: $s = t \Rightarrow t = s$
- Transitive: $t_1 = t_2 \ldots t_{m-1} = t_m \Rightarrow t_1 = t_m$
- Compatible: $\forall_i : t_i = s_i \Rightarrow f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$

Definitions

Ground Terms

- Constants $a, b, c, \ldots$
- Compound Terms $f(t_1, \ldots, t_n)$

Congruence Relation

- Reflexive: $t = t$
- Symmetric: $s = t \Rightarrow t = s$
- Transitive: $t_1 = t_2 \ldots t_{m-1} = t_m \Rightarrow t_1 = t_m$
- Compatible: $\forall_i : t_i = s_i \Rightarrow f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$

Congruence Closure R^* of R

- Smallest Congruence Relation containing R

Definitions

Ground Terms

- Constants $a, b, c, \ldots$
- Compound Terms $f(t_1, \ldots, t_n)$

Congruence Relation

- Reflexive: $t = t$
- Symmetric: $s = t \Rightarrow t = s$
- Transitive: $t_1 = t_2 \ldots t_{m-1} = t_m \Rightarrow t_1 = t_m$
- Compatible: $\forall_i : t_i = s_i \Rightarrow f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$

Congruence Closure R^* of R

- Smallest Congruence Relation containing R

Explanation for $s = t$

- Set of equations E, such that $(s, t) \in E^*$

Example continued

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Example continued

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Explanation for $f(a) = f(b)$

$\{\ f(a) = a,\ a = b\ ,\ b = f(b)\ \}$

Example continued

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Explanation for $f(a) = f(b)$

$\{ \quad a = b\ , b = f(b)\ \}$

Example continued

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Explanation for $f(a) = f(b)$

$\{ \qquad a = b \qquad \}$

Example continued

Knowledge

1. $f(a) = a$
2. $a = b$
3. $b = f(b)$
4. $f(a) \neq f(b)$

Explanation for $f(a) = f(b)$

$\{ \quad a = b \quad \}$

Short explanation $\rightsquigarrow$ short proof

Short Explanation Decision Problem

Given a set of input equations E, a target equation $s = t$ and $k \in \mathbb{N}$, does there exist an explanation $E' \subseteq E$ of $s = t$ with $|E'| \leq k$?

Short Explanation Decision Problem

Given a set of input equations E, a target equation $s = t$ and $k \in \mathbb{N}$, does there exist an explanation $E' \subseteq E$ of $s = t$ with $|E'| \leq k$?

NP-complete

NP-completeness proof sketch

From a propositional logic formula Φ obtain ...

- a set of equations E_Φ
- a target equation $s_\Phi = t_\Phi$
- $k_\Phi \in \mathbb{N}$

such that ...

Φ is satisfiable if and only if there is an explanation $E' \subseteq E_\Phi$ of $s_\Phi = t_\Phi$ with $|E'| \leq k_\Phi$

NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Translation to equations

NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Translation to equations

$t_1(\hat{x}_1)$

$\hat{c}_1 - t_1(\hat{x}_2)$

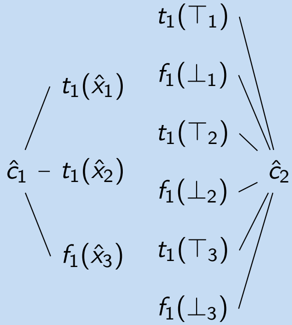
$f_1(\hat{x}_3)$

NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Translation to equations

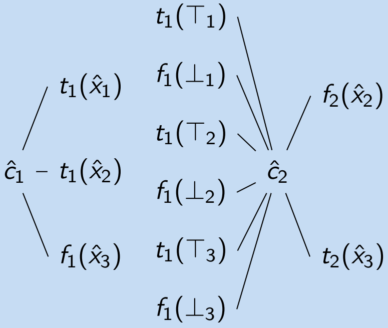


NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Translation to equations

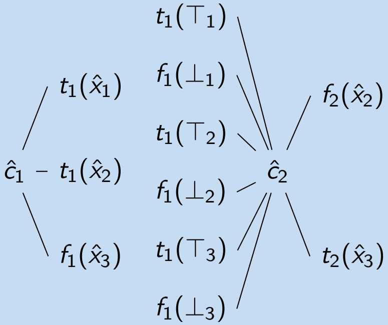


NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Translation to equations

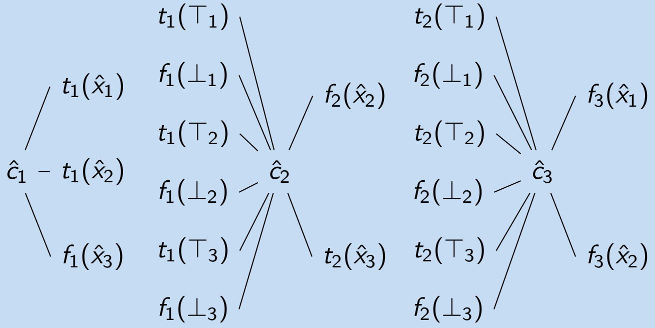


NP-completeness proof sketch example

Formula

$$(x_1 \lor x_2 \lor \neg x_3) \land (\neg x_2 \lor x_3) \land (\neg x_1 \lor \neg x_2)$$

Translation to equations

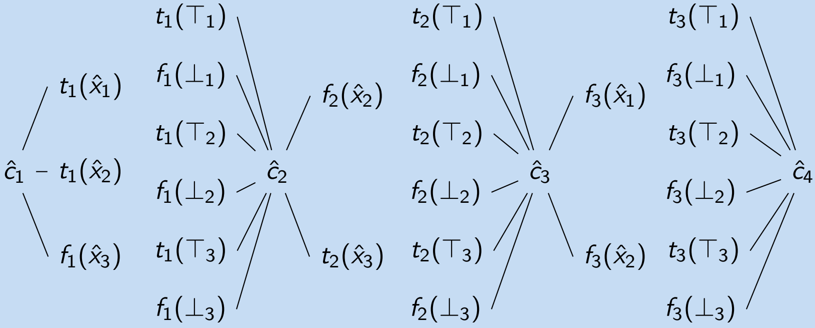


NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Translation to equations

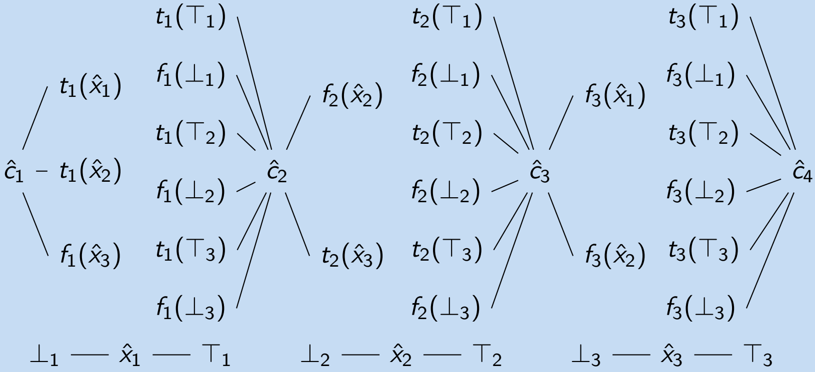


NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Translation to equations



NP-completeness proof sketch example

Formula

$$(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2)$$

Small subset corresponding to satisfying assignment

$\hat{c}_1 - t_1(\hat{x}_1) \quad t_1(\top_1) - \hat{c}_2 - f_2(\hat{x}_2) \quad f_2(\bot_2) - \hat{c}_3 - f_3(\hat{x}_2) \quad f_3(\bot_2) - \hat{c}_4$

$\hat{x}_1 \;—\; \top_1 \qquad \bot_2 \;—\; \hat{x}_2 \qquad \hat{x}_3 \quad \top_3$

Motivation

The Complang Style

- Nicer colors
- Fewer boxes
- More room for your content!

An overall great style for your presentation!

A Listing

Example

```
void bubble_sort(int* a, int n) {
  int i,j;
  for (i = 0; i < n; i++) {
    for (j = 0; j < i; j++) {
      if (a[i] > a[j]) SWAP(a[i],a[j]);
    }
  }
}
```

Thank You

Thank you for using the complang style!

Bug reports & feature requests:
`adrian@complang.tuwien.ac.at`