LPP 2026/27 (063AA, 9CFU)

Programming Languages

Fabio Gadducci

and Laboratory

Vincenzo Ciancia

03 - Unification

Some solutions

1st exercise

Conjectures vs theorems

a natural number ***p*** is **prime**
if it cannot be written as the product of two smaller numbers

n	Is n prime?	$2^n - 1$	Is $2^n - 1$ prime?
2	yes	3	yes
3	yes	7	yes
4	no: $4 = 2 \cdot 2$	15	no: $15 = 3 \cdot 5$
5	yes	31	yes
6	no: $6 = 2 \cdot 3$	63	no: $63 = 7 \cdot 9$
7	yes	127	yes
8	no: $8 = 2 \cdot 4$	255	no: $255 = 15 \cdot 17$
9	no: $9 = 3 \cdot 3$	511	no: $511 = 7 \cdot 73$
10	no: $10 = 2 \cdot 5$	1023	no: $1023 = 31 \cdot 33$

1st exercise

if p is prime
then $2^p - 1$ is prime

Use any mean to prove or disprove the above conjectures

1st exercise

if p is prime
then $2^p - 1$ is prime

$p = 11$ is prime

Use any mean to prove or disprove the above conjectures

1st exercise

if p is prime
then $2^p - 1$ is prime

$p = 11$ is prime

$2^{11} - 1 = 2047$ is not prime

Use any mean to prove or disprove the above conjectures

1st exercise

if p is prime
then $2^p - 1$ is prime

$p = 11$ is prime

$2^{11} - 1 = 2047$ is not prime

$2047 = 23 \cdot 89$

Use any mean to prove or disprove the above conjectures

1st exercise

if p is prime
then $2^p - 1$ is prime

$p = 11$ is prime

$2^{11} - 1 = 2047$ is not prime

$2047 = 23 \cdot 89$

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

$n = a \cdot b$ with $a, b > 1$

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

$n = a \cdot b$ with $a, b > 1$

$2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 =$

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

$n = a \cdot b$ with $a, b > 1$

$2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 =$

$(2^a)^b + (2^a)^{b-1} + \cdots + (2^a)^2 + 2^a$

$\quad - ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

$n = a \cdot b$ with $a, b > 1$

$2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 =$

$(2^a)^b + (2^a)^{b-1} + \cdots + (2^a)^2 + 2^a$

$-((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$

$2^a\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1)$

$-\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

$n = a \cdot b$ with $a, b > 1$

$$2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 =$$

$$(2^a)^b + (2^a)^{b-1} + \cdots + (2^a)^2 + 2^a$$

$$-((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$$

$$2^a\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1)$$

$$-\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$$

$$(2^a - 1)((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1)$$

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

$n = a \cdot b$ with $a, b > 1$

$2^a - 1 > 1$

$((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) > 1$

$2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 =$

$(2^a)^b + (2^a)^{b-1} + \cdots + (2^a)^2 + 2^a$

$-((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$

$2^a\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1)$

$-\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$

$(2^a - 1)((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1)$

Use any mean to prove or disprove the above conjectures

1st exercise

if $n > 1$ is not prime
then $2^n - 1$ is not prime

$n = a \cdot b$ with $a, b > 1$

$2^a - 1 > 1$

$((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) > 1$

$2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1 =$

$(2^a)^b + (2^a)^{b-1} + \cdots + (2^a)^2 + 2^a$

$-((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$

$2^a\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1)$

$-\ ((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1) =$

$(2^a - 1)((2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1)$

Use any mean to prove or disprove the above conjectures

About 1st exercise

$n = 11$ is prime
but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime

About 1st exercise

$n = 11$ is prime
but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime

$n = a \cdot b$ non prime (with $1 < a, b < n$)

About 1st exercise

$n = 11$ is prime
but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime

$n = a \cdot b$ non prime (with $1 < a, b < n$)

$$
\begin{aligned}
p^q - 1 = p^q &+ p^{q-1} + p^{q-2} + \cdots + p \\
&- p^{q-1} - p^{q-2} - \cdots - p - 1
\end{aligned}
$$

About 1st exercise

$n = 11$ is prime
but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime

$n = a \cdot b$ non prime (with $1 < a, b < n$)

$$
\begin{aligned}
p^q - 1 &= p^q + p^{q-1} + p^{q-2} + \cdots + p \\
&\qquad - p^{q-1} - p^{q-2} - \cdots - p - 1 \\
&= (p^{q-1} + p^{q-2} + \cdots + 1)(p - 1)
\end{aligned}
$$

About 1st exercise

$n = 11$ is prime

but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime

$n = a \cdot b$ non prime (with $1 < a, b < n$)

$$\begin{aligned} p^q - 1 &= p^q + p^{q-1} + p^{q-2} + \cdots + p \\ &\quad - p^{q-1} - p^{q-2} - \cdots - p - 1 \\ &= (p^{q-1} + p^{q-2} + \cdots + 1)(p - 1) \end{aligned}$$

$2^{ab} - 1 = (2^a)^b - 1 = ((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1)(2^a - 1)$ is not prime

About 1st exercise

$n = 11$ is prime
but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime

$n = a \cdot b$ non prime (with $1 < a, b < n$)

$$
\begin{aligned}
p^q - 1 &= p^q + p^{q-1} + p^{q-2} + \cdots + p \\
&\quad - p^{q-1} - p^{q-2} - \cdots - p - 1 \\
&= (p^{q-1} + p^{q-2} + \cdots + 1)(p - 1)
\end{aligned}
$$

$2^{ab} - 1 = (2^a)^b - 1 = ((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1)(2^a - 1)$ is not prime

> 1

About 1st exercise

$n = 11$ is prime

but $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime

$n = a \cdot b$ non prime (with $1 < a, b < n$)

$$\begin{aligned} p^q - 1 &= p^q + p^{q-1} + p^{q-2} + \cdots + p \\ &\qquad - p^{q-1} - p^{q-2} - \cdots - p - 1 \\ &= (p^{q-1} + p^{q-2} + \cdots + 1)(p - 1) \end{aligned}$$

$2^{ab} - 1 = (2^a)^b - 1 = \underbrace{((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1)}_{>1}\underbrace{(2^a - 1)}_{>1}$ is not prime

Exercise

Expressions with variables $\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E}$

How to evaluate expressions such as $(x \oplus 4) \otimes y$?

Need some memories $\mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$

machine states $\langle \mathsf{E}, \sigma \rangle$

interpretation function $\mathcal{E}[\![\cdot]\!] : Exp \to (\mathbb{M} \to \mathbb{N})$

Let's redefine the various semantics and properties

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E}$$

$$\mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$(num)\,\frac{}{\langle \mathsf{N}, \sigma \rangle \longrightarrow n}$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$(num)\,\frac{}{\langle \mathsf{N}, \sigma\rangle \longrightarrow n}$$

$$(sum)\,\frac{\langle \mathsf{E}_0, \sigma\rangle \longrightarrow n_0 \quad \langle \mathsf{E}_0, \sigma\rangle \longrightarrow n_1}{\langle \mathsf{E}_0 \oplus \mathsf{E}_1, \sigma\rangle \longrightarrow n}\; n = n_0 + n_1$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$(num)\,\frac{}{\langle \mathsf{N}, \sigma \rangle \longrightarrow n}$$

$$(sum)\,\frac{\langle \mathsf{E}_0, \sigma \rangle \longrightarrow n_0 \quad \langle \mathsf{E}_0, \sigma \rangle \longrightarrow n_1}{\langle \mathsf{E}_0 \oplus \mathsf{E}_1, \sigma \rangle \longrightarrow n}\; n = n_0 + n_1$$

$$(prod)\,\frac{\langle \mathsf{E}_0, \sigma \rangle \longrightarrow n_0 \quad \langle \mathsf{E}_0, \sigma \rangle \longrightarrow n_1}{\langle \mathsf{E}_0 \otimes \mathsf{E}_1, \sigma \rangle \longrightarrow n}\; n = n_0 \times n_1$$

Exercise

$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E}$

$\mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$

$$(num)\,\frac{}{\langle \mathsf{N}, \sigma\rangle \longrightarrow n}$$

$$(var)\,\frac{}{\langle x, \sigma\rangle \longrightarrow \sigma(x)}$$

$$(sum)\,\frac{\langle \mathsf{E}_0, \sigma\rangle \longrightarrow n_0 \quad \langle \mathsf{E}_0, \sigma\rangle \longrightarrow n_1}{\langle \mathsf{E}_0 \oplus \mathsf{E}_1, \sigma\rangle \longrightarrow n}\; n = n_0 + n_1$$

$$(prod)\,\frac{\langle \mathsf{E}_0, \sigma\rangle \longrightarrow n_0 \quad \langle \mathsf{E}_0, \sigma\rangle \longrightarrow n_1}{\langle \mathsf{E}_0 \otimes \mathsf{E}_1, \sigma\rangle \longrightarrow n}\; n = n_0 \times n_1$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad\qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$\mathcal{E}[\![\cdot]\!] : Exp \to (\mathbb{M} \to \mathbb{N})$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad\qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$\mathcal{E}[\![\cdot]\!] : Exp \to (\mathbb{M} \to \mathbb{N})$$

$$\mathcal{E}[\![\mathsf{N}]\!]\color{red}{\sigma} = \color{blue}{n}$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$\mathcal{E}[\![\cdot]\!] : Exp \to (\mathbb{M} \to \mathbb{N})$$

$$\mathcal{E}[\![\mathsf{N}]\!]\sigma = n$$

$$\mathcal{E}[\![\mathsf{E}_0 \oplus \mathsf{E}_1]\!]\sigma = \mathcal{E}[\![\mathsf{E}_0]\!]\sigma + \mathcal{E}[\![\mathsf{E}_1]\!]\sigma$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$\mathcal{E}[\![\cdot]\!] : Exp \to (\mathbb{M} \to \mathbb{N})$$

$$\mathcal{E}[\![\mathsf{N}]\!]\sigma = n$$

$$\mathcal{E}[\![\mathsf{E}_0 \oplus \mathsf{E}_1]\!]\sigma = \mathcal{E}[\![\mathsf{E}_0]\!]\sigma + \mathcal{E}[\![\mathsf{E}_1]\!]\sigma$$

$$\mathcal{E}[\![\mathsf{E}_0 \otimes \mathsf{E}_1]\!]\sigma = \mathcal{E}[\![\mathsf{E}_0]\!]\sigma \times \mathcal{E}[\![\mathsf{E}_1]\!]\sigma$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

$$\mathcal{E}[\![\cdot]\!] : Exp \to (\mathbb{M} \to \mathbb{N})$$

$$\mathcal{E}[\![\mathsf{N}]\!]\sigma = n$$

$$\mathcal{E}[\![\mathsf{E}_0 \oplus \mathsf{E}_1]\!]\sigma = \mathcal{E}[\![\mathsf{E}_0]\!]\sigma + \mathcal{E}[\![\mathsf{E}_1]\!]\sigma$$

$$\mathcal{E}[\![\mathsf{E}_0 \otimes \mathsf{E}_1]\!]\sigma = \mathcal{E}[\![\mathsf{E}_0]\!]\sigma \times \mathcal{E}[\![\mathsf{E}_1]\!]\sigma$$

$$\mathcal{E}[\![x]\!]\sigma = \sigma(x)$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad\qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

termination?

determinacy?

Exercise

$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E}$ $\qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$

termination? $\forall \mathsf{E}.\ \forall \sigma.\ \exists n.\ \langle \mathsf{E}, \sigma \rangle \longrightarrow n$

determinacy?

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad\qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

termination? $\forall \mathsf{E}.\ \forall \sigma.\ \exists n.\ \langle \mathsf{E}, \sigma \rangle \longrightarrow n$

$$\forall \mathsf{E}.\ \forall \sigma.\ \exists n.\ \mathcal{E}[\![\mathsf{E}]\!]\sigma = n$$

determinacy?

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad\qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

termination? $\forall \mathsf{E}.\ \forall \sigma.\ \exists n.\ \langle \mathsf{E}, \sigma \rangle \longrightarrow n$

$\forall \mathsf{E}.\ \forall \sigma.\ \exists n.\ \mathcal{E}[\![\mathsf{E}]\!]\sigma = n$

determinacy?

$$\forall \mathsf{E}, \sigma, n, m.\ \left(\begin{array}{l} \langle \mathsf{E}, \sigma \rangle \longrightarrow n \\ \wedge \\ \langle \mathsf{E}, \sigma \rangle \longrightarrow m \end{array} \right) \Rightarrow n = m$$

Exercise

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \otimes \mathsf{E} \qquad\qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

termination? $\forall \mathsf{E}.\ \forall \sigma.\ \exists n.\ \langle \mathsf{E}, \sigma \rangle \longrightarrow n$

$$\forall \mathsf{E}.\ \forall \sigma.\ \exists n.\ \mathcal{E}[\![\mathsf{E}]\!]\sigma = n$$

determinacy?

$$\forall \mathsf{E}, \sigma, n, m.\ \left(\begin{array}{l} \langle \mathsf{E}, \sigma \rangle \longrightarrow n \\ \wedge \\ \langle \mathsf{E}, \sigma \rangle \longrightarrow m \end{array} \right) \Rightarrow n = m$$

$$\forall \mathsf{E}, \sigma, n, m.\ \left(\begin{array}{l} \mathcal{E}[\![\mathsf{E}]\!]\sigma = n \\ \wedge \\ \mathcal{E}[\![\mathsf{E}]\!]\sigma = m \end{array} \right) \Rightarrow n = m$$

Inference

SOS rule application?

1. a goal

$$(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m$$

SOS rule application?

$$(prod)\,\frac{\mathsf{E}_0 \longrightarrow n_0 \qquad \mathsf{E}_1 \longrightarrow n_1}{\mathsf{E}_0 \otimes \mathsf{E}_1 \longrightarrow n} \; n = n_0 \cdot n_1$$

2. take a rule

$$(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m$$

SOS rule application?

$$(prod)\ \frac{\mathsf{E}_0 \longrightarrow n_0 \qquad \mathsf{E}_1 \longrightarrow n_1}{\boxed{\mathsf{E}_0 \otimes \mathsf{E}_1 \longrightarrow n}}\ n = n_0 \cdot n_1$$

3. unify
(if possible)

$$\mathsf{E}_0 = 1 \oplus 2$$
$$\mathsf{E}_1 = 3 \oplus 4$$
$$n = m$$

$$\boxed{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m}$$

SOS rule application?

$$(prod)\,\frac{1 \oplus 2 \longrightarrow n_0 \quad 3 \oplus 4 \longrightarrow n_1}{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m}\; m = n_0 \cdot n_1$$

4. instantiate

$$\boxed{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m}$$

SOS rule application?

$$(prod)\frac{\boxed{1 \oplus 2 \longrightarrow n_0} \quad \boxed{3 \oplus 4 \longrightarrow n_1}}{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m}\ m = n_0 \cdot n_1$$

5. recursively solve subgoals

$$(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m$$

SOS rule application?

$$(prod)\,\frac{1 \oplus 2 \longrightarrow \boxed{3} \quad 3 \oplus 4 \longrightarrow \boxed{7}}{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m} \; m = \boxed{3 \cdot 7}$$

6. combine results

$$(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow m$$

SOS rule application?

$$(prod)\,\frac{1 \oplus 2 \longrightarrow 3 \quad 3 \oplus 4 \longrightarrow 7}{(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow \boxed{21}}$$

7. return results

$$(1 \oplus 2) \otimes (3 \oplus 4) \longrightarrow \boxed{21}$$

Deduction process

$$(rule\ \ name)\,\frac{premises}{conclusion}\,side\ \ condition$$

goal

Deduction process

$$(rule\ \ name)\,\frac{premises}{conclusion}\,side\ \ condition$$

$$goal$$

Signatures

Unsorted signature

$$(\Sigma, ar)$$

a set of function symbols
(also called operators)

$$\Sigma = \{c, f, g, ...\}$$

arity function
(number of arguments)

$$ar : \Sigma \to \mathbb{N}$$

each function symbol has an arity

Running example

$\Sigma = \{0, \mathsf{succ}, \mathsf{plus}\}$

$ar(0) = 0$	constant
$ar(\mathsf{succ}) = 1$	unary
$ar(\mathsf{plus}) = 2$	binary

Equivalently

$$(\Sigma, ar)$$

let $\Sigma_n \triangleq ar^{-1}(n)$

$$= \{f \in \Sigma \mid ar(f) = n\}$$

a signature is an arity-indexed family of sets of operators

$$\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$$

Running example

$$\Sigma_0 = \{0\}$$

$$\Sigma_1 = \{\mathsf{succ}\}$$

$$\Sigma_2 = \{\mathsf{plus}\}$$

$$\Sigma_n = \varnothing \qquad \text{if } n > 2$$

Terms over a signature

$\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$ a signature

$X = \{x, y, z, ...\}$ an infinite set of variables

$T_{\Sigma,X}$ denotes the set of all terms over Σ, X

$T_{\Sigma,X}$ is the least set such that:

- if $x \in X$, then $x \in T_{\Sigma,X}$
- if $c \in \Sigma_0$, then $c \in T_{\Sigma,X}$
- if $f \in \Sigma_n$ and $t_1, ..., t_n \in T_{\Sigma,X}$, then $f(t_1, ..., t_n) \in T_{\Sigma,X}$

i.e. $T_{\Sigma,X} \ni t ::= \underset{x \in X}{x} \mid \underset{c \in \Sigma_0}{c} \mid \underset{f \in \Sigma_n}{f(t_1, ..., t_n)}$

Vars

$\Sigma = \{\Sigma_n\}_{n\in\mathbb{N}} \quad X = \{x, y, z, ...\} \qquad t \in T_{\Sigma,X}$

$vars(t)$ set of variables that appears in the term *t*

$$vars : T_{\Sigma,X} \to \wp(X)$$

$$vars(x) \triangleq \{x\}$$

$$vars(c) \triangleq \varnothing$$

$$vars(f(t_1, ..., t_n)) \triangleq \bigcup_{i=1}^{n} vars(t_i)$$

Closed terms

a term with no variables is called closed

$$T_\Sigma \triangleq vars^{-1}(\varnothing) = \{t \in T_{\Sigma,X} \mid vars(t) = \varnothing\}$$

(obviously $T_\Sigma \subseteq T_{\Sigma,X}$)

Running example

$$\Sigma_0 = \{\mathsf{0}\}$$

$$\Sigma_1 = \{\mathsf{succ}\}$$

$$\Sigma_2 = \{\mathsf{plus}\}$$

$$\Sigma_n = \varnothing \qquad \text{if } n > 2$$

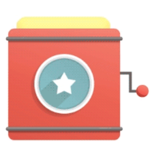
Exercise

let's complete the schema
(obviously $T_\Sigma \subseteq T_{\Sigma,X}$)

t	$t \in ?$	$vars(t)$
0	◉ T_Σ ○ $T_{\Sigma,X}$	$\varnothing$
x	○ T_Σ ◉ $T_{\Sigma,X}$	$\{x\}$
succ(0)	○ T_Σ ○ $T_{\Sigma,X}$	
succ(x)	○ T_Σ ○ $T_{\Sigma,X}$	
succ(plus(0), x)	○ T_Σ ○ $T_{\Sigma,X}$	
plus(succ(x), 0)	○ T_Σ ○ $T_{\Sigma,X}$	
succ(succ(0), plus(x))	○ T_Σ ○ $T_{\Sigma,X}$	
succ(plus(w, z))	○ T_Σ ○ $T_{\Sigma,X}$	
plus(plus(x, succ(y)), plus(0, succ(x)))	○ T_Σ ○ $T_{\Sigma,X}$	

Exercise

let's complete the schema
(obviously $T_\Sigma \subseteq T_{\Sigma,X}$)



t	$t \in ?$	$vars(t)$
0	◉ T_Σ ○ $T_{\Sigma,X}$	$\varnothing$
x	○ T_Σ ◉ $T_{\Sigma,X}$	$\{x\}$
succ(0)	○ T_Σ ○ $T_{\Sigma,X}$	
succ(x)	○ T_Σ ○ $T_{\Sigma,X}$	
succ(plus(0), x)	○ T_Σ ○ $T_{\Sigma,X}$	
plus(succ(x), 0)	○ T_Σ ○ $T_{\Sigma,X}$	
succ(succ(0), plus(x))	○ T_Σ ○ $T_{\Sigma,X}$	
succ(plus(w, z))	○ T_Σ ○ $T_{\Sigma,X}$	
plus(plus(x, succ(y)), plus(0, succ(x)))	○ T_Σ ○ $T_{\Sigma,X}$	

Substitutions

$\rho : X \to T_{\Sigma,X}$ a substitution assigns terms to variables

we only consider substitutions that are identity everywhere, except for a finite number of cases, written

$$\rho = [\underbrace{x_1 = t_1 \, , \, \ldots \, , \, x_n}_{\text{all different}} = t_n] \qquad \rho(x) = \begin{cases} t_i & \text{if } x = x_i \\ x & \text{otherwise} \end{cases}$$

Notation

$\rho : X \to T_{\Sigma,X}$ a substitution assigns terms to variables

overloaded notation for the lifted function $\rho : T_{\Sigma,X} \to T_{\Sigma,X}$

$\rho(t)$ denotes the term obtained by simultaneous application of the substitution to all variable occurrences in *t*

$t\rho$ alternative notation

Example

$$\rho \triangleq [\, x = \mathsf{succ}(y)\ ,\ y = \mathsf{0}]$$

$$t \triangleq \mathsf{plus}(\ \mathsf{plus}(x, y)\ ,\ \mathsf{succ}(x)\ )$$

$$t\rho = \mathsf{plus}(\ \mathsf{plus}(\mathsf{succ}(y), \mathsf{0})\ ,\ \mathsf{succ}(\mathsf{succ}(y))\ )$$

mgt relation

t is more general than t' if $\exists \rho.\ t' = t\rho$

in which case, we also say t' is an instance of t

$\mathsf{plus}(x, \mathsf{succ}(y))$	mgt	$\mathsf{plus}(0, \mathsf{succ}(\mathsf{succ}(z)))$
$\mathsf{plus}(0, x)$	~~mgt~~	$\mathsf{plus}(y, 0)$
$\mathsf{plus}(y, 0)$	~~mgt~~	$\mathsf{plus}(0, x)$
$\mathsf{plus}(0, x)$ $\mathsf{plus}(y, 0)$	mgt	$\mathsf{plus}(0, 0)$

mgt relation

mgt is transitive and reflexive

mgt relation

mgt is transitive and reflexive

if $(t_1 \text{ mgt } t_2)$ and $(t_2 \text{ mgt } t_3)$, then $(t_1 \text{ mgt } t_3)$

mgt relation

mgt is transitive and reflexive

t mgt t

if $(t_1$ mgt $t_2)$ and $(t_2$ mgt $t_3)$, then $(t_1$ mgt $t_3)$

mgt relation

mgt is transitive and reflexive

t mgt t

if (t_1 mgt t_2) and (t_2 mgt t_3), then (t_1 mgt t_3)

there are terms $t \neq t'$ such that (t mgt t') and (t' mgt t)

succ(x) succ(y)

mgt relation

mgt is transitive and reflexive

t mgt t

if (t_1 mgt t_2) and (t_2 mgt t_3), then (t_1 mgt t_3)

there are terms $t \neq t'$ such that (t mgt t') and (t' mgt t)

succ(x) succ(y)

mgt can be extended to substitutions pointwise

ρ mgt ρ' if $\exists \rho''.\ \forall x.\ \rho'(x) = \rho''(\rho(x))$

Unification
(in its simplest form: syntactic, first-order)

Unification problem

Given a set of potential equalities

$$\mathcal{G} = \{\ell_1 \stackrel{?}{=} r_1, ..., \ell_n \stackrel{?}{=} r_n\}$$

where $\ell_1, ..., \ell_n, r_1, ..., r_n \in T_{\Sigma,X}$

can we find a substitution ρ such that

$$\forall i \in [1, n].\ \rho(\ell_i) = \rho(r_i) \quad ?$$

we call such a ρ a solution of $\mathcal{G}$

$$sols(\mathcal{G}) \triangleq \{\rho \mid \forall i \in [1, n].\ \rho(\ell_i) = \rho(r_i)\}$$

Examples

$$\mathcal{G} = \{\mathsf{plus}(x, 0) \stackrel{?}{=} \mathsf{plus}(0, y)\}$$

$$sols(\mathcal{G}) \triangleq \{[x = 0, y = 0]\}$$

$$\mathcal{G} = \{\mathsf{succ}(x) \stackrel{?}{=} \mathsf{succ}(\mathsf{succ}(y))\}$$

$$sols(\mathcal{G}) \triangleq \{[x = \mathsf{succ}(y)], [x = \mathsf{succ}(0), y = 0], ...\}$$

Unification problem

More interestingly, can we solve the following problem?

Given a set of potential equalities

$$\mathcal{G} = \{\ell_1 \stackrel{?}{=} r_1, ..., \ell_n \stackrel{?}{=} r_n\}$$

where $\ell_1, ..., \ell_n, r_1, ..., r_n \in T_{\Sigma,X}$

can we find a most general solution ρ ?

$\rho \in sols(\mathcal{G})$ and

$\forall \rho' \in sols(\mathcal{G}).\ \rho$ mgt ρ'

Unification algorithm

Idea: we iteratively reduce the set $\mathcal{G}$
by solution-preserving tranformations until
either a solution is found
or we can prove there is no solution

$$\mathcal{G} \cdots \mathcal{G}_1 \cdots \mathcal{G}_n \cdots \{x_1 \stackrel{?}{=} t_1, ..., x_k \stackrel{?}{=} t_k\}$$

Solutions may not exist
and even if they exist may not be unique

Termination

$$\mathcal{G} = \{\ell_1 \stackrel{?}{=} r_1, \ldots, \ell_n \stackrel{?}{=} r_n\}$$

$\mathcal{G}$ and $\mathcal{G}'$ are equivalent if $sols(\mathcal{G}) = sols(\mathcal{G}')$

the algorithm terminates successfully when we reach

$\mathcal{G}' = \{x_1 \stackrel{?}{=} t_1, \ldots, x_k \stackrel{?}{=} t_k\}$ equivalent to $\mathcal{G}$

all different

$$\{x_1, \ldots, x_k\} \cap \bigcup_{i=1}^{k} vars(t_i) = \varnothing$$

any such $\mathcal{G}'$ defines a straightforward solution $[x_1 = t_1, \ldots, x_k = t_k]$

Notation

$$\mathcal{G} = \{\ell_1 \stackrel{?}{=} r_1, ..., \ell_n \stackrel{?}{=} r_n\}$$

$$vars(\mathcal{G}) \triangleq \bigcup_{i=1}^{n} (vars(\ell_i) \cup vars(r_i))$$

$$\mathcal{G}\rho \triangleq \{\ell_1\rho \stackrel{?}{=} r_1\rho, ..., \ell_n\rho \stackrel{?}{=} r_n\rho\}$$

Unification algorithm

delete

$\mathcal{G} \cup \{t \stackrel{?}{=} t\}$

becomes

$\mathcal{G}$

Unification algorithm

delete

$$\mathcal{G} \cup \{t \stackrel{?}{=} t\}$$

becomes

$$\mathcal{G}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

Unification algorithm

delete

$$\mathcal{G} \cup \{t \stackrel{?}{=} t\}$$

becomes

$$\mathcal{G}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

swap

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$$

becomes

$$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$$

Unification algorithm

delete

$$\mathcal{G} \cup \{t \stackrel{?}{=} t\}$$

becomes

$$\mathcal{G}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

swap

$$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} x\}$$

becomes

$$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, \ldots, t_m)\}$$

decompose

$$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} f(u_1, \ldots, u_m)\}$$

becomes

$$\mathcal{G} \cup \{t_1 \stackrel{?}{=} u_1, \ldots, t_m \stackrel{?}{=} u_m\}$$

Unification algorithm

delete

$$\mathcal{G} \cup \{t \stackrel{?}{=} t\}$$

becomes

$$\mathcal{G}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

swap

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$$

becomes

$$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$$

decompose

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} f(u_1, ..., u_m)\}$$

becomes

$$\mathcal{G} \cup \{t_1 \stackrel{?}{=} u_1, ..., t_m \stackrel{?}{=} u_m\}$$

occur-check

$$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$$

fails if $x \in vars(f(t_1, ..., t_m))$

Unification algorithm

delete

$$\mathcal{G} \cup \{t \stackrel{?}{=} t\}$$

becomes

$$\mathcal{G}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

swap

$$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} x\}$$

becomes

$$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, \ldots, t_m)\}$$

decompose

$$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} f(u_1, \ldots, u_m)\}$$

becomes

$$\mathcal{G} \cup \{t_1 \stackrel{?}{=} u_1, \ldots, t_m \stackrel{?}{=} u_m\}$$

occur-check

$$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, \ldots, t_m)\}$$

fails if $x \in vars(f(t_1, \ldots, t_m))$

conflict

$$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} g(u_1, \ldots, u_h)\}$$

fails if $f \neq g$ or $m \neq h$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, \mathsf{0})\}$$

decompose

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} f(u_1, ..., u_m)\}$$

becomes

$$\mathcal{G} \cup \{t_1 \stackrel{?}{=} u_1, ..., t_m \stackrel{?}{=} u_m\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

decompose

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} f(u_1, ..., u_m)\}$$

becomes

$$\mathcal{G} \cup \{t_1 \stackrel{?}{=} u_1, ..., t_m \stackrel{?}{=} u_m\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y \, , \; x \stackrel{?}{=} 0\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\ ,\ x \stackrel{?}{=} 0\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} 0\}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y \,,\, x \stackrel{?}{=} 0\}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

$$\{\mathsf{succ}(0) \stackrel{?}{=} y \,,\, x \stackrel{?}{=} 0\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\; x \stackrel{?}{=} 0\}$$

$$\{\mathsf{succ}(0) \stackrel{?}{=} y\,,\; x \stackrel{?}{=} 0\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\ ,\ x \stackrel{?}{=} 0\}$$

$$\{\mathsf{succ}(0) \stackrel{?}{=} y\ ,\ x \stackrel{?}{=} 0\}$$

swap

$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$

becomes

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, 0)\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y \,,\; x \stackrel{?}{=} 0\}$$

$$\{\mathsf{succ}(0) \stackrel{?}{=} y \,,\; x \stackrel{?}{=} 0\}$$

swap

$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$

becomes

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$

$$\{y \stackrel{?}{=} \mathsf{succ}(0) \,,\; x \stackrel{?}{=} 0\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, \mathsf{0})\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\ ,\ x \stackrel{?}{=} \mathsf{0}\}$$

$$\{\mathsf{succ}(\mathsf{0}) \stackrel{?}{=} y\ ,\ x \stackrel{?}{=} \mathsf{0}\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{0})\ ,\ x \stackrel{?}{=} \mathsf{0}\}$$

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, \mathsf{0})\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\; x \stackrel{?}{=} \mathsf{0}\}$$

$$\{\mathsf{succ}(\mathsf{0}) \stackrel{?}{=} y\,,\; x \stackrel{?}{=} \mathsf{0}\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{0})\,,\; x \stackrel{?}{=} \mathsf{0}\}$$

success!

Example

$$\{\mathsf{plus}(\mathsf{succ}(x), x) \stackrel{?}{=} \mathsf{plus}(y, \mathsf{0})\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\ ,\ x \stackrel{?}{=} \mathsf{0}\}$$

$$\{\mathsf{succ}(\mathsf{0}) \stackrel{?}{=} y\ ,\ x \stackrel{?}{=} \mathsf{0}\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{0})\ ,\ x \stackrel{?}{=} \mathsf{0}\}$$

success! $\rho = [y = \mathsf{succ}(\mathsf{0})\ ,\ x = \mathsf{0}]$

Example

$$\{\mathsf{plus}(0, x) \stackrel{?}{=} \mathsf{succ}(y)\}$$

Example

$$\{\mathsf{plus}(0, x) \stackrel{?}{=} \mathsf{succ}(y)\} \quad \mathsf{plus} \neq \mathsf{succ}$$

Example

$$\{\mathsf{plus}(0, x) \stackrel{?}{=} \mathsf{succ}(y)\}$$ plus $\neq$ succ

conflict

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} g(u_1, ..., u_h)\}$$

fails if $f \neq g$ or $m \neq h$

Example

$$\{\mathsf{plus}(0, x) \stackrel{?}{=} \mathsf{succ}(y)\}$$ plus $\neq$ succ

conflict

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} g(u_1, ..., u_h)\}$$

fails if $f \neq g$ or $m \neq h$

failure!

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\ ,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

swap

$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$

becomes

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

swap

$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$

becomes

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

Example

$$\{\mathsf{succ}(x) \overset{?}{=} y\,,\ \mathsf{succ}(y) \overset{?}{=} x\}$$

$$\{\mathsf{succ}(x) \overset{?}{=} y\,,\ x \overset{?}{=} \mathsf{succ}(y)\}$$

eliminate

$$\mathcal{G} \cup \{x \overset{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \overset{?}{=} t\}$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y \,,\, \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y \,,\, x \stackrel{?}{=} \mathsf{succ}(y)\}$$

eliminate

$$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$$

becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$

$$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y \,,\, x \stackrel{?}{=} \mathsf{succ}(y)\}$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\, \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\, x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y\,,\, x \stackrel{?}{=} \mathsf{succ}(y)\}$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

swap

$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$

becomes

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

swap

$$\mathcal{G} \cup \{f(t_1, ..., t_m) \stackrel{?}{=} x\}$$

becomes

$$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{succ}(y))\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{succ}(y))\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{succ}(y))\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\} \quad y \in vars(\mathsf{succ}(\mathsf{succ}(y)))$$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{succ}(y))\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$y \in \mathit{vars}(\mathsf{succ}(\mathsf{succ}(y)))$

occur-check

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$

fails if $x \in \mathit{vars}(f(t_1, ..., t_m))$

Example

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ \mathsf{succ}(y) \stackrel{?}{=} x\}$$

$$\{\mathsf{succ}(x) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{\mathsf{succ}(\mathsf{succ}(y)) \stackrel{?}{=} y\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$$\{y \stackrel{?}{=} \mathsf{succ}(\mathsf{succ}(y))\,,\ x \stackrel{?}{=} \mathsf{succ}(y)\}$$

$y \in vars(\mathsf{succ}(\mathsf{succ}(y)))$

occur-check

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, ..., t_m)\}$
fails if $x \in vars(f(t_1, ..., t_m))$

failure!

Exercise

$$\{\mathsf{plus}(x, \mathsf{succ}(x)) \stackrel{?}{=} \mathsf{plus}(0, y)\ ,\ \mathsf{plus}(y, z) \stackrel{?}{=} \mathsf{plus}(z, w)\}$$

delete

$\mathcal{G} \cup \{t \stackrel{?}{=} t\}$
becomes
$\mathcal{G}$

eliminate

$\mathcal{G} \cup \{x \stackrel{?}{=} t\}$
becomes if $x \in vars(\mathcal{G}) \setminus vars(t)$
$\mathcal{G}[x = t] \cup \{x \stackrel{?}{=} t\}$

swap

$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} x\}$
becomes
$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, \ldots, t_m)\}$

decompose

$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} f(u_1, \ldots, u_m)\}$
becomes
$\mathcal{G} \cup \{t_1 \stackrel{?}{=} u_1, \ldots, t_m \stackrel{?}{=} u_m\}$

occur-check

$\mathcal{G} \cup \{x \stackrel{?}{=} f(t_1, \ldots, t_m)\}$
fails if $x \in vars(f(t_1, \ldots, t_m))$

conflict

$\mathcal{G} \cup \{f(t_1, \ldots, t_m) \stackrel{?}{=} g(u_1, \ldots, u_h)\}$
fails if $f \neq g$ or $m \neq h$