First order rewriting

Xavier Urbain

2024-2025

Equality (decision)

Group theory

$$\begin{array}{rcl} x \cdot e & = & x \\ x \cdot x^{-1} & = & e \\ (x \cdot y) \cdot z & = & x \cdot (y \cdot z) \end{array}$$

$e \cdot x = x \cdot e$ OK

Using equations. . .

$$\begin{aligned} e \cdot x &= e \cdot (x \cdot e) = e \cdot (x \cdot (x^{-1} \cdot (x^{-1})^{-1})) = e \cdot ((x \cdot x^{-1}) \cdot (x^{-1})^{-1}) \\ &= e \cdot (e \cdot (x^{-1})^{-1}) = (e \cdot e) \cdot (x^{-1})^{-1} = e \cdot (x^{-1})^{-1} \\ &= (x \cdot x^{-1}) \cdot (x^{-1})^{-1} = x \cdot (x^{-1} \cdot (x^{-1})^{-1}) = x \cdot e \end{aligned}$$

First order

Monosorted

Signature : $(\mathcal{F}, \tau)$ $\qquad S$

- $\mathcal{F}$: set of symbols
- τ : function $\mathcal{F} \to \mathbb{N}$,
  n : arity of f $\qquad \underbrace{S \times \cdots \times S}_{n} \to S$

Arity 0 : constants

First order

Signature $(\mathcal{F}, \tau)$,

X : set of variables $\qquad$ + fresh one

$\mathcal{T}(\mathcal{F}, X)$: smallest set such that

- $x \in X$ term
- $f \in \mathcal{F}$, $\tau(f) = n$, $\quad t_1 \ldots t_n$ terms
  then $f(t_1, \ldots, t_n)$ term

Ground terms : $\mathcal{T}(\mathcal{F}, \varnothing)$

First order - subterms

Terms seen as trees $\rightsquigarrow$ positions Λ = root
... as functions from positions to $\mathcal{F} \cup X$

$\mathbb{N}_+^*$ sequences over $\mathbb{N}_+$ Concat p and q : $p \cdot q$

$p \leq_{\text{pref}} q$ iff $\exists r \in \mathbb{N}_+^*, p \cdot r = q$ p prefix of q

Subterm of t at position p, $t|_p = \{q \in \mathbb{N}_+^* \mid p \cdot q \in \mathcal{P}\text{os}(t)\}$ $t|_p(q) = t(p \cdot q)$
Subterm relation : $t \rhd s$ if $\exists p \neq \Lambda$ such that $t|_p = s$ (proper subterm)

For $t|_p$ $(p \in \mathcal{P}\text{os}(t))$ and u, Replacement $t[u]_p$, defined by :
$\{q \in \mathbb{N}_+^* \mid q \in \mathcal{P}\text{os}(t) \wedge p \not\leq_{\text{pref.}} q\} \cup \{p \cdot q \mid q \in \mathcal{P}\text{os}(u)\}$

$$t[u]_p(q) = t(q) \qquad \text{if } q \in \mathcal{P}\text{os}(t) \wedge p \not\leq_{\text{pref.}} q$$
$$t[u]_p(p \cdot q) = u(q)$$

First order

Substitution : application $X \to \mathcal{T}(\mathcal{F}, X)$
Usually : identity except on a finite set

Notation postfix : $\sigma(x) \rightsquigarrow x\sigma$
Extended to terms by unique $H_\sigma : \mathcal{T}(\mathcal{F}, X) \to \mathcal{T}(\mathcal{F}, X)$

- $H_\sigma(x) = x$ if x not in σ's domain
- $H_\sigma(x) = x\sigma$ if x in σ's domain
- $H_\sigma(f(s_1, \ldots, s_m)) = f(H_\sigma(s_1), \ldots, H_\sigma(s_m))$ if $f(s_1, \ldots, s_m) \in \mathcal{T}(\mathcal{F}, X)$

Notation abuse : substitution $\rightsquigarrow$ extended substitution

Ground substitution if $X \to \mathcal{T}(\mathcal{F}, \varnothing)$
Rk. Term with variables : seen as all its ground instances

First order

More general ? subsumption : $s \geq t$ iff $\exists \sigma,\ s\sigma = t$
σ more general than τ iff $\exists \theta,\ \sigma\theta = \tau$

Renaming : equivalence relation akin to α-conversion

$$\sigma = \{x_1 \mapsto y_1, \cdots, x_n \mapsto y_n\} \qquad y_i \text{ pairwise distincts}$$

Matching : for s t terms, finding σ such that $s\sigma = t$

Unification : for s t terms, finding σ such that $s\sigma = t\sigma$

- Decidable (1st order, e.g. Robinson)
- If unifiable : unique most general unifier (vanilla)

A hint of semantics

Monosorted
For $(\mathcal{F}, \tau)$ a signature, $\mathcal{F}$-algebra :

- Support $A \neq \varnothing$
- Application $f_A : A^n \to A$
  for all $f \in \mathcal{F}, \tau(f) : n$ $\mathcal{T}(\mathcal{F}, X)$ $\mathcal{F}$-algebra

For A B $\mathcal{F}$-algebras, homomorphism from A to B :
application $h : A \to B$ such that for all $f, \tau(f) = n$

$$\forall a_1, \cdots, a_n \in A, \quad h(f_A(a_1, \cdots, a_n)) = f_B(h(a_1), \cdots, h(a_n))$$

A-assignment : homomorphism from $\mathcal{T}(\mathcal{F}, X)$ to A

Congruence (equi. relation compatible with A) $\rightsquigarrow$ Quotient

A hint of semantics

Multisorted

For $(\mathcal{S}, \mathcal{F}, \tau)$ a sorted signature, $\mathcal{F}$-algebra :

- Support $A \neq \emptyset$ for each $s \in \mathcal{S}$
- Application $f_A : A_{s_1} \times \cdots \times A_{s_n} \to A_s$
  for all $f \in \mathcal{F}, f : s_1 \times \cdots \times s_n \to s$ $\quad$ $\mathcal{T}(\mathcal{F}, X)$ $\mathcal{F}$-algebra

For A B $\mathcal{F}$-algebras, homomorphism from A to B :

set of applications $h_s : A_s \to B_s$ such that for all $f : s_1 \times \cdots s_n \to s$

$$\forall a_1, \cdots, a_n \in A, \quad h_s(f_A(a_1, \cdots, a_n)) = f_B(h_{s_1}(a_1), \cdots, h_{s_n}(a_n))$$

A-assignment : homomorphism from $\mathcal{T}(\mathcal{F}, X)$ to A

Congruence (equi. relation compatible with A) $\rightsquigarrow$ Quotient

Equational reasoning

Equation : pair of terms of same sort, $s = t$ $\quad$ set of equations E

Model : A $\mathcal{F}$-algebra, $A \vDash E$ if $\forall s = t \in E$, $\forall A$-assignment σ, $s\sigma = t\sigma$

$=_E$ smallest congruence on $\mathcal{T}(\mathcal{F}, X)$ such that $\forall \sigma, \forall s = t \in E, s\sigma =_E t\sigma$

Quotient : $\mathcal{T}(\mathcal{F}, X)/ =_E$ $\quad \rightsquigarrow \quad$ $\mathcal{F}$-algebra, and $\mathcal{T}(\mathcal{F}, X)/ =_E \vDash E$

$s = t$ an equation, word problem related to $s = t$: $\quad E \vDash^{?} s = t$

Equational theory (of E) : $\{s = t \mid E \vDash s = t\}$

To solve it : equational reasoning

Equational reasoning

$$\frac{}{s = s} \quad \text{Reflexivity}$$

$$\frac{s = t}{t = s} \quad \text{Symmetry}$$

$$\frac{s = t \qquad t = u}{s = u} \quad \text{Transitivity}$$

$$\frac{s = t}{u[s\sigma]_p = u[t\sigma]_p} \quad \text{Replacement}$$

Starting from E, uses of : *Refl., Symmetry, Transitivity, Replacement*

If derivation : $E \vdash s = t$

Equational reasoning

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(x \cdot I(x)) = e}{e = (x \cdot I(x))}}{e \cdot I(I(x)) = (x \cdot I(x)) \cdot I(I(x))} \qquad \dfrac{(x \cdot y) \cdot z = x \cdot (y \cdot z)}{(x \cdot I(x)) \cdot I(I(x)) = x \cdot (I(x) \cdot I(I(x)))}}{e \cdot I(I(x)) = x \cdot (I(x) \cdot I(I(x)))} \qquad \dfrac{x \cdot I(x) = e}{x \cdot (I(x) \cdot I(I(x))) = x \cdot e}}{e \cdot I(I(x)) = x \cdot e} \qquad x \cdot e = x}{e \cdot I(I(x)) = x}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(x \cdot e) = x}{x = (x \cdot e)}}{x \cdot I(I(y)) = (x \cdot e) \cdot I(I(y))} \qquad \dfrac{\dfrac{(x \cdot y) \cdot z = x \cdot (y \cdot z)}{(x \cdot e) \cdot I(I(y)) = x \cdot (e \cdot I(I(y)))} \qquad \dfrac{\dfrac{\vdots}{e \cdot I(I(x)) = x}}{x \cdot (e \cdot I(I(y))) = x \cdot y}}{(x \cdot e) \cdot I(I(y)) = x \cdot y}}{x \cdot I(I(y)) = x \cdot y}}{e \cdot I(I(x)) = e \cdot x}}{e \cdot x = e \cdot I(I(x))} \qquad \dfrac{\vdots}{e \cdot I(I(x)) = x}}{e \cdot x = x}$$

[(Birkoff)] if at least a ground term (per sort),

$E \vDash s = t \quad \Leftrightarrow \quad E \vdash s = t \quad \Leftrightarrow \quad s =_E t$

A view on $=_E$, equational step

$=_E$ a bit rich $\rightsquigarrow$ smaller relation $\leftrightarrow_E$

smallest reflexive pre-congruence that contains E $(=_E : \leftrightarrow^\star_E)$

$s \leftrightarrow_E t$: $\exists u = v \in E,\ \sigma$ substitution,

$$s = s[u\sigma]_p \quad t = s[v\sigma]_p$$

Notation $s \longleftrightarrow^p_{u=v,\sigma} t$

A view on $=_E$, equational step

Group theory, E :

$$\begin{array}{llcl} (U) & x \cdot e & = & x \\ (I) & x \cdot I(x) & = & e \\ (A) & (x \cdot y) \cdot z & = & x \cdot (y \cdot z) \end{array}$$

$$\begin{array}{l} e \cdot x \longleftrightarrow^2_N e \cdot (x \cdot e) \longleftrightarrow^{22}_I e \cdot (x \cdot (I(x) \cdot I(I(x)))) \\ \longleftrightarrow^2_A e \cdot ((x \cdot I(x)) \cdot I(I(x))) \longleftrightarrow^{21}_I e \cdot (e \cdot I(I(x))) \\ \longleftrightarrow^\Lambda_A (e \cdot e) \cdot I(I(x)) \longleftrightarrow^1_N e \cdot I(I(x)) \longleftrightarrow^1_I (x \cdot I(x)) \cdot I(I(x)) \\ \longleftrightarrow^\Lambda_A x \cdot (I(x) \cdot I(I(x))) \longleftrightarrow^2_I \quad x \cdot e \end{array}$$

Unification problem

Definition

$T(\mathcal{F}, X)$ term algebra. Unification problem :

- $\top$,
- $\bot$,
- $s_1 = t_1 \wedge \ldots \wedge s_n = t_n$.

Every substitution solution of $\top$.
No substitution solution of $\bot$.
σ solution of $s_1 = t_1 \wedge \ldots \wedge s_n = t_n$ if for all $i = 1, \ldots, n$, $s_i\sigma \equiv t_i\sigma$.

Set of solutions of P : $\mathrm{U}(P)$.

Unification problem, example

$f(x, a) = f(f(b, y), y) \wedge y = a$

Question : is there any σ such that
$f(x, a)\sigma \equiv f(f(b, y), y)\sigma$ AND $y\sigma \equiv a$?

Here yes, though not always the case

Unification problem, *mgu*

Theorem.

$T(\mathcal{F}, X)$ term algebra, P unification problem.

- $\mathsf{U}(P) = \varnothing$,
- $\mathsf{U}(P) \neq \varnothing$, main solution (most general) σ unique (up to renaming).
  σ Most General Unifier *mgu*(P).

Proof : translation to equivalent and easier problem.

Definition

P_1, P_2 unification problems over $T(\mathcal{F}, X)$.
P_1 and P_2 equivalents if $\mathsf{U}(P_1) = \mathsf{U}(P_2)$.

Unification problem, *mgu*

Theorem.

$T(\mathcal{F}, X)$ term algebra, P unification problem.

- $\mathsf{U}(P) = \varnothing$,
- $\mathsf{U}(P) \neq \varnothing$, main solution (most general) σ unique (up to renaming).
  σ Most General Unifier *mgu*(P).

Proof : translation to equivalent and easier problem.

Definition

P unification problem sur $T(\mathcal{F}, X)$. P solved form :

- $\top$,
- $\bot$,
- $x_1 = t_1 \wedge \ldots \wedge x_n = t_n$ where x_i pairwise distincts, outside t_j.

Solved forms, solutions

Proposition.

$P \equiv x_1 = t_1 \wedge \ldots \wedge x_n = t_n$ solved form, $\theta = \{x_1 := t_1, \ldots, x_n := t_n\}$
Then $\mathsf{U}(P) = \{\theta\sigma \mid \sigma \text{ substitution}\}$

Proof : for σ solution, $\sigma = \theta\sigma$.

- $x = x_i \in \mathsf{Dom}(\theta)$ $\quad x\theta\sigma \equiv x_i\theta\sigma = (x_i\theta)\sigma = t_i\sigma = x_i\sigma = x\sigma$.
- $x \neq x_i \in \mathsf{Dom}(\theta)$ $\quad x\theta\sigma = (x\theta)\sigma = x\sigma$.

For σ : $x_i\theta\sigma = (x_i\theta)\sigma = t_i\sigma = t_i\theta\sigma$ hence $\theta\sigma$ solution.

Definition

For P equivalent to solved form $x_1 = t_1 \wedge \ldots \wedge x_n = t_n$,
mgu$(P) = \{x_1 := t_1, \ldots, x_n := t_n\}$.

$f(x, a) = f(f(b, y), y) \wedge y = a$ equivalent to $x = f(b, a) \wedge y = a$,
mgu$(P) = \{x := f(b, a), y := a\}$.

Transformation rules 1/2

Trivial
$$\frac{s = s}{\top}$$

Decompose
$$\frac{f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)}{s_1 = t_1 \wedge \ldots \wedge s_n = t_n}$$

Incompat.
$$\frac{f(s_1, \ldots, s_n) = g(t_1, \ldots, t_m)}{\bot} \quad \text{if } f \neq g$$

Union
$$\frac{x = y \wedge P}{x = y \wedge P\{x := y\}} \quad \text{if } x, y \in \mathsf{Var}(P)$$

Rules de transformation 2/2

Replace $\dfrac{x = s \wedge P}{x = s \wedge P\{x := s\}}$ if $x \in \mathrm{Var}(P) \setminus \mathrm{Var}(s)$ and $s \notin X$.

Fusion $\dfrac{x = s \wedge x = t}{x = s \wedge s = t}$ if $x \in X$, $s, t \notin X$ and $|s| \leq |t|$.

Occur. check $\dfrac{x_1 = t_1[x_2]_{p_1} \wedge \ldots x_n = t_n[x_1]_{p_n}}{\perp}$ if $p_1 \cdot \ldots \cdot p_n \neq \Lambda$

Rules : properties

Set of rules U defines an algorithm

Theorem.
Transformation correct.
I.e., if $P_0 \to_U P_1$ then P_0, P_1 equivalent.

Theorem.
$\to_U$ well-founded.
I.e., no infinite chain $P_0 \to_U P_1 \to_U \cdots \to_U P_n \to_U P_{n+1} \to_U \cdots$

Theorem.
Transformation complete.
I.e., when U not applicable, then P solved form.

Rules : termination

Proof : $\to_U$ included into $>$ well-founded.

$$(I_1(P), I_2(P), I_3(P)) \quad (\geq_1, \geq_2, \geq_3)_{\mathrm{lex}} \quad (I_1(Q), I_2(Q), I_3(Q))$$

In fact : $I \uparrow$ $\qquad$ $I \uparrow$

$$P \qquad \geq \qquad Q$$

Definition

$\leq_1, \ldots, \leq_n$ over non empty $D_1, \ldots, D_n$.

Lexicographic composition : disjoint union $\simeq$ and $<$:

$$\begin{array}{lcll} (x_1, \ldots, x_n) & \simeq & (y_1, \ldots, y_n) & \text{if } \forall i = 1, \ldots n \;\; x_i \simeq_i y_i \\ (x_1, \ldots, x_n) & < & (y_1, \ldots, y_n) & \text{if } \exists j \in \{1, \ldots, n\} \; \forall i = 1, \ldots j-1 \\ & & & \quad x_i \simeq_i y_i \;\; \wedge \;\; x_j <_j y_j \end{array}$$

Rules : termination

Proof : $\to_U$ included into $>$ well-founded.

$$(I_1(P), I_2(P), I_3(P)) \quad (\geq_1, \geq_2, \geq_3)_{\mathrm{lex}} \quad (I_1(Q), I_2(Q), I_3(Q))$$

In fact : $I \uparrow$ $\qquad$ $I \uparrow$

$$P \qquad \geq \qquad Q$$

Definition

Multiset extension :(reflexive) transitive closure of $\leq^1_{mul} = \simeq^1_{mul} \cup <^1_{mul}$

$$\begin{array}{l} M \cup \{x\} \simeq^1_{mul} M \cup \{y\} \text{ if } x \simeq y \\ M \cup \{y_1, \ldots, y_n\} <^1_{mul} M \cup \{x\} \text{ if } \forall j \in \{1, \ldots, n\} \;\; y_j < x \end{array}$$

Rules : termination

Proof : $\rightarrow_U$ included into $>$ well-founded.

$$(I_1(P), I_2(P), I_3(P)) \quad (\geq_1, \geq_2, \geq_3)_{\text{lex}} \quad (I_1(Q), I_2(Q), I_3(Q))$$

In fact : $I \uparrow$ $\qquad$ $I \uparrow$

$P \qquad \geq \qquad Q$

Definition

x variable solved if one occurrence in $P \equiv x = t \wedge P'$

$I_1(P)$ = number of variables not solved in P.

$\geq_1$ usual ordering on $\mathbb{N}$.

Union	$>_1$
Replace	$>_1$
Remainder	$\geq_1$

Rules : termination

Proof : $\rightarrow_U$ included into $>$ well-founded.

$$(I_1(P), I_2(P), I_3(P)) \quad (\geq_1, \geq_2, \geq_3)_{\text{lex}} \quad (I_1(Q), I_2(Q), I_3(Q))$$

In fact : $I \uparrow$ $\qquad$ $I \uparrow$

$P \qquad \geq \qquad Q$

Definition

Size of $s = t$: $\max(|s|, |t|)$.

$I_2(P)$ = multiset of sizes in P.

$\geq_2$ multiset extention usual ordering on $\mathbb{N}$.

Union	$>_1$	
Replace	$>_1$	
Triv., Dec., Incomp., Occ.	$\geq_1$	$>_2$
Fusion	$\geq_1$	$\geq_2$

Rules : termination

Proof : $\rightarrow_U$ included into $>$ well-founded.

$$(I_1(P), I_2(P), I_3(P)) \quad (\geq_1, \geq_2, \geq_3)_{\text{lex}} \quad (I_1(Q), I_2(Q), I_3(Q))$$

In fact : $I \uparrow$ $\qquad$ $I \uparrow$

$P \qquad \geq \qquad Q$

Definition

$I_3(P)$ = number of equations with member $\in X$.

$\geq_3$ usual ordering on $\mathbb{N}$.

Union	$>_1$		
Remplace	$>_1$		
Triv., Dec., Incomp., Occ.	$\geq_1$	$>_2$	
Fusion	$\geq_1$	$\geq_2$	$>_3$

Rules : completeness

Proof : P with U not applicable, different from $\top$ and $\bot$.

Neither Decompose nor Incompat. hence $P \equiv x_1 = t_1 \wedge \ldots \wedge x_n = t_n$.

No Fusion hence x_i pairwise distincts.

If (at least) two occurrences of x_i in P :

- $t_i \rhd x_i$ impossible : no Occur. check.
- x_i being t_i impossible : no Trivial.
- $t_j \rhd x_i, i \neq j$ impossible : no Remplace.

Rules : completeness

If (at least) two occurrences of x_i in P (cont.) :

- x_i being t_j, $j \neq i$ hence j^{th} equation : $x_j = x_i$.
  - $t_i \notin X$ impossible : no Remplace with x_i.
  - $t_i \in X$, appearing outside i^{th} equation impossible : no Union.
  - $t_i \in X, t_i \equiv x_i'$, uniquely in i^{th} equation :

$$P \equiv x_1 = t_1 \wedge \ldots \wedge x_{i-1} = t_{i-1} \wedge x_i' = x_i \wedge x_{i+1} = t_{i+1} \wedge \ldots \wedge x_n = t_n$$

Corollary.

P unification problem,

- $\mathsf{U}(P) = \varnothing$ or
- $\mathsf{U}(P) \neq \varnothing$ with *mgu* unique (up to renaming).

Examples

$\mathcal{F} = \{f, g, a, b\}$, with f binary, g unary, a and b constants, $X = \{x, y, z\}$.

$\mathsf{U}(f(a,b) = f(a,a)) = \varnothing$

$$\begin{array}{rc} & f(a,b) = f(a,a) \\ \text{Decompose} & \\ & a = a \wedge b = a \\ \text{Trivial} & \\ & b = a \\ \text{Incompat.} & \\ & \perp \end{array}$$

Examples

$\mathcal{F} = \{f, g, a, b\}$, with f binary, g unary, a and b constants, $X = \{x, y, z\}$.

$\mathsf{U}(f(x,y) = f(z,z)) = \{x := z, y := z\}$

$$\text{Decompose}\ \frac{f(x,y) = f(z,z)}{x = z \wedge y = z}$$

Examples

$\mathcal{F} = \{f, g, a, b\}$, with f binary, g unary, a and b constants, $X = \{x, y, z\}$.

$\mathsf{U}(f(x, f(a,y)) = f(f(b,z), x)) = \varnothing$

$$\begin{array}{rc} & f(x, f(a,y)) = f(f(b,z), x) \\ \text{Decompose} & \\ & x = f(b,z) \wedge f(a,y) = x \\ \text{Fusion} & \\ & x = f(b,z) \wedge f(a,y) = f(b,z) \\ \text{Decompose} & \\ & x = f(b,z) \wedge a = b \wedge y = z \\ \text{Incompat.} & \\ & \perp \end{array}$$

Examples

$\mathcal{F} = \{f, g, a, b\}$, with f binary, g unary, a and b constants, $X = \{x, y, z\}$.

$\mathsf{U}(f(f(a,y), f(y,z)) = f(x,x)) = \{x := f(a,a), y := a, z := a\}$

$$
\begin{array}{rc}
 & f(f(a,y), f(y,z)) = f(x,x) \\
\text{Decompose} & \\
 & f(a,y) = x \wedge f(y,z) = x \\
\text{Fusion} & \\
 & f(a,y) = x \wedge f(y,z) = f(a,y) \\
\text{Decompose} & \\
 & f(a,y) = x \wedge y = a \wedge z = y \\
\text{Replace} & \\
 & f(a,a) = x \wedge y = a \wedge z = a
\end{array}
$$

Examples

$\mathcal{F} = \{f, g, a, b\}$, with f binary, g unary, a and b constants, $X = \{x, y, z\}$.

$\mathsf{U}(f(x, f(x,z)) = f(f(y,z), y)) = \emptyset$

$$
\begin{array}{rc}
 & f(x, f(x,z)) = f(f(y,z), y) \\
\text{Decompose} & \\
 & x = f(y,z) \wedge f(x,z) = y \\
\text{Occur. check} & \\
 & \bot
\end{array}
$$