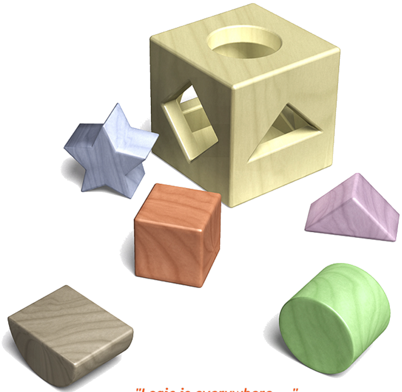
Equational Logic

Steffen Hölldobler
International Center for Computational Logic
Technische Universität Dresden
Germany

- **Equational Systems**
- **Paramodulation**
- **Term Rewriting Systems**
- **Unification Theory**
- **Application: Multisets**



"Logic is everywhere ..."

Equational Systems

- Consider a first order language with the following precedence hierarchy

$$\{\forall, \exists\} > \neg > \wedge > \vee > \{\leftarrow, \rightarrow\} > \leftrightarrow$$

- Let $\approx$ be a binary predicate symbol written infix
- An equation is an atom of the form $s \approx t$
- An equational system $\mathcal{E}$ is a finite set of universally closed equations
- Notation Universal quantifiers are usually omitted

$$\begin{array}{lll} \mathcal{E}_1 & (X \cdot Y) \cdot Z \approx X \cdot (Y \cdot Z) & \text{(associativity)} \\ & 1 \cdot X \approx X & \text{(left unit)} \\ & X \cdot 1 \approx X & \text{(right unit)} \\ & X^{-1} \cdot X \approx 1 & \text{(left inverse)} \\ & X \cdot X^{-1} \approx 1 & \text{(right inverse)} \end{array}$$

Axioms of Equality

- **The equality relation enjoys some typical properties expressed by the following universally closed axioms of equality $\mathcal{E}_{\approx}$**

$$
\begin{array}{lr}
X \approx X & \text{(reflexivity)} \\
X \approx Y \rightarrow Y \approx X & \text{(symmetry)} \\
X \approx Y \wedge Y \approx Z \rightarrow X \approx Z & \text{(transitivity)} \\
\bigwedge_{i=1}^{n} X_i \approx Y_i \rightarrow f(X_1, \ldots, X_n) \approx f(Y_1, \ldots, Y_n) & \text{(f–substitutivity)} \\
\bigwedge_{i=1}^{n} X_i \approx Y_i \wedge r(X_1, \ldots, X_n) \rightarrow r(Y_1, \ldots, Y_n) & \text{(r–substitutivity)}
\end{array}
$$

- **Note**
  - **Substitutivity axioms are defined for each function symbol f and each relation symbol r in the underlying alphabet**
  - **Universal quantifiers have been omitted**

Equality and Logical Consequence

- We are interested in computing logical consequences of $\mathcal{E} \cup \mathcal{E}_{\approx}$
  - $\mathcal{E}_1 \cup \mathcal{E}_{\approx} \models (\exists X)\, X \cdot a \approx 1$?
  - $\mathcal{E}_1 \cup \mathcal{E}_{\approx} \cup \{X \cdot X \approx 1\} \models (\forall X, Y)\, X \cdot Y \approx Y \cdot X$?
- One possibility is to apply resolution
  - There are 10^{21} resolution steps needed to solve the examples
  - $\mathcal{E} \cup \mathcal{E}_{\approx}$ causes an extremely large search space
- Idea Remove troublesome formulas from $\mathcal{E} \cup \mathcal{E}_{\approx}$ and build them into the deductive machinery
  - Use additional rule of inference like paramodulation
  - Build the equational theory into the unification computation

Least Congruence Relation

- $\mathcal{E} \cup \mathcal{E}_{\approx}$ is a set of definite clauses
- There exists a least model for $\mathcal{E} \cup \mathcal{E}_{\approx}$
- Example
  - Let the only function symbols be the constants a, b and the binary g
  - Let $\mathcal{E}_2 = \{a \approx b\}$
  - The least model of $\mathcal{E}_2 \cup \mathcal{E}_{\approx}$ is

$$\begin{aligned} &\{t \approx t \mid t \text{ is a ground term}\} \\ &\cup \{a \approx b,\ b \approx a\} \\ &\cup \{g(a, a) \approx g(b, a),\ g(a, a) \approx g(a, b),\ g(a, a) \approx g(b, b), \ldots\} \end{aligned}$$

- Define $s \approx_{\mathcal{E}} t$ iff $\mathcal{E} \cup \mathcal{E}_{\approx} \models \forall\, s \approx t$
  - $g(a, a) \approx_{\mathcal{E}_2} g(a, b)$
  - $g(X, a) \approx_{\mathcal{E}_2} g(X, b)$
  - $\approx_{\mathcal{E}}$ is the least congruence relation on terms generated by $\mathcal{E}$

Paramodulation

- $L\lceil s\rceil$ literal which contains an occurrence of the term s
  $L\lceil s/t\rceil$ literal obtained from L by replacing an occurrence of s by t
- **Paramodulation**

$$\frac{[L_1\lceil s\rceil, L_2, \ldots, L_n] \qquad [l \approx r, L_{n+1}, \ldots, L_m]}{[L_1\lceil s/r\rceil, L_2, \ldots, L_m]\theta} \; \theta = \mathrm{mgu}(s, l)$$

- **Notation** Instead of $\neg s \approx t$ we write $s \not\approx t$
- **Remember**

$$\begin{array}{lll} \mathcal{E} \cup \mathcal{E}_\approx \models \forall\, s \approx t & \text{iff} & \bigwedge_{\mathcal{E} \cup \mathcal{E}_\approx} \to \forall\, s \approx t \text{ is valid} \\ & \text{iff} & \neg(\bigwedge_{\mathcal{E} \cup \mathcal{E}_\approx} \to \forall\, s \approx t) \text{ is unsatisfiable} \\ & \text{iff} & \mathcal{E} \cup \mathcal{E}_\approx \cup \{\neg\forall\, s \approx t\} \text{ is unsatisfiable} \\ & \text{iff} & \mathcal{E} \cup \mathcal{E}_\approx \cup \{\exists\, s \not\approx t\} \text{ is unsatisfiable} \end{array}$$

- **Theorem 1** $\mathcal{E} \cup \mathcal{E}_\approx \cup \{\exists\, s \not\approx t\}$ is unsatisfiable iff there is a refutation of $\mathcal{E} \cup \{X \approx X\} \cup \{\exists\, s \not\approx t\}$ wrt paramodulation, resolution and factoring

An Example

$$\mathcal{E}_1 \cup \{X \approx X,\ X \cdot X \approx 1\} \models (\forall X, Y)\, X \cdot Y \approx Y \cdot X$$

1	$a \cdot b \not\approx b \cdot a$	initial query			$\cdot$	hypothesis
2	$1 \cdot X_1 \approx X_1$	left unit			$a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot (X_4 \cdot X_4))$	
3	$X_2 \approx X_2$	reflexivity			$\cdot$	associativity
4	$X_1 \approx 1 \cdot X_1$	pm(2,3)			$a \cdot b \not\approx (X_3 \cdot ((X_3 \cdot b) \cdot (a \cdot X_4))) \cdot X_4$	
5	$a \cdot b \not\approx (1 \cdot b) \cdot a$	pm(1,4)			$\cdot$	hypothesis
6	$X_3 \cdot X_3 \approx 1$	hypothesis			$a \cdot b \not\approx (a \cdot 1) \cdot b$	
7	$X_4 \approx X_4$	reflexivity			$\cdot$	right unit
8	$1 \approx X_3 \cdot X_3$	pm(6,7)		n	$a \cdot b \not\approx a \cdot b$	
9	$a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot a$	pm(5,8)		n'	$X_5 \approx X_5$	reflexivity
	$\cdot$	right unit		n''	$[\,]$	res (n, n')
	$a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot 1)$					

The Example in Shorthand Notation

$$\mathcal{E}_1 \cup \{X \approx X,\ X \cdot X \approx 1\} \models (\forall X, Y)\, X \cdot Y \approx Y \cdot X$$

1	$a \cdot b \not\approx b \cdot a$	initial query			$\cdot$	hypothesis
2	$1 \cdot X_1 \approx X_1$	left unit			$a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot (X_4 \cdot X_4))$	
3	$X_2 \approx X_2$	reflexivity			$\cdot$	associativity
4	$X_1 \approx 1 \cdot X_1$	pm(2,3)			$a \cdot b \not\approx (X_3 \cdot ((X_3 \cdot b) \cdot (a \cdot X_4))) \cdot X_4$	
5	$a \cdot b \not\approx (1 \cdot b) \cdot a$	pm(1,4)			$\cdot$	hypothesis
6	$X_3 \cdot X_3 \approx 1$	hypothesis			$a \cdot b \not\approx (a \cdot 1) \cdot b$	
7	$X_4 \approx X_4$	reflexivity			$\cdot$	right unit
8	$1 \approx X_3 \cdot X_3$	pm(6,7)		n	$a \cdot b \not\approx a \cdot b$	
9	$a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot a$	pm(5,8)		n'	$X_5 \approx X_5$	reflexivity
	$\cdot$	right unit		n''	$[\,]$	res (n, n')
	$a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot 1)$					

The Example in Shorthand Notation Again

$$
\begin{array}{rcll}
b \cdot a & \approx & (1 \cdot b) \cdot a & \text{left unit} \\
 & \approx & ((X_3 \cdot X_3) \cdot b) \cdot a & \text{hypothesis} \\
 & \approx & ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot 1) & \text{right unit} \\
 & \approx & ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot (X_4 \cdot X_4)) & \text{hypothesis} \\
 & \approx & (X_3 \cdot ((X_3 \cdot b) \cdot (a \cdot X_4))) \cdot X_4 & \text{associativity} \\
 & \approx & (a \cdot 1) \cdot b & \text{hypothesis} \\
 & \approx & a \cdot b & \text{right unit}
\end{array}
$$

- **Now, the search space is 10^{11} instead of 10^{21} steps**
  - **Symmetry can be simulated, which leads to cycles**
  - **All terms s occurring in L_1 are candidates**
  - **$L_1\lceil s \rceil$ may be a variable and can be unified with any term**
- **There are still many redundant and useless steps**
- **Idea Use equations only from left to right $\rightsquigarrow$ term rewriting systems**

Term Rewriting Systems

- An expression of the form $s \rightarrow t$ is called rewrite rule
- A term rewriting system is a finite set of rewrite rules
- In the sequel, $\mathcal{R}$ shall denote a term rewriting system
- $s\lceil u \rceil$ denotes a term s which contains an occurrence of u

  $s\lceil u/v \rceil$ denotes the term obtained from s by replacing an occ. of u by v
- The rewrite relation $\rightarrow_{\mathcal{R}}$ on terms is defined as follows: $s\lceil u \rceil \rightarrow_{\mathcal{R}} t$ iff there exist $l \rightarrow r \in \mathcal{R}$ and θ such that $u = l\theta$ and $t = s\lceil u/r\theta \rceil$
- Example

$$\mathcal{R}_3 = \{ \begin{array}{lcl} append([\,], X) & \rightarrow & X, \\ append([X|Y], Z) & \rightarrow & [X|append(Y, Z)] \; \} \end{array}$$

$$\begin{array}{lcl} append([1,2],[3,4]) & \rightarrow_{\mathcal{R}_3} & [1|append([2],[3,4])] \\ & \rightarrow_{\mathcal{R}_3} & [1,2|append([\,],[3,4])] \\ & \rightarrow_{\mathcal{R}_3} & [1,2,3,4] \end{array}$$

Matching

- **Matching problem**
  Given terms u and l, does there exist a substitution θ such that $u = l\theta$ **?**
  If such a substitution exists, then it is called a **matcher**
- If a matching problem is solvable, then there exists a most general matcher
- If can be computed by a variant of the unification algorithm, where variables occurring in u are treated as (different new) constant symbols
- Whereas unification is in the complexity class $\mathcal{P}$, matching is in $\mathcal{NC}$

Closures

- $\stackrel{*}{\rightarrow}_{\mathcal{R}}$ denotes the reflexive and transitive closure of $\rightarrow_{\mathcal{R}}$
  - $\mathit{append}([1,2],[3,4]) \stackrel{*}{\rightarrow}_{\mathcal{R}_3} [1,2,3,4]$
- $s \leftrightarrow_{\mathcal{R}} t$ iff $s \leftarrow_{\mathcal{R}} t$ or $s \rightarrow_{\mathcal{R}} t$
  - Let $\mathcal{R}_4 = \{a \rightarrow b,\ c \rightarrow b\}$,
    then $a \rightarrow_{\mathcal{R}_4} b \leftarrow_{\mathcal{R}_4} c$ and, consequently, $a \leftrightarrow_{\mathcal{R}_4} b \leftrightarrow_{\mathcal{R}_4} c$
- $\stackrel{*}{\leftrightarrow}_{\mathcal{R}}$ denotes the reflexive and transitive closure of $\leftrightarrow_{\mathcal{R}}$
  - $a \stackrel{*}{\leftrightarrow}_{\mathcal{R}_4} c$
- We sometimes simply write $\rightarrow$ or $\leftrightarrow$ instead of $\rightarrow_{\mathcal{R}}$ or $\leftrightarrow_{\mathcal{R}}$, respectively

Term Rewriting Systems and Equational Systems

- Let $\mathcal{R}$ be a term rewriting system
- $\mathcal{E}_{\mathcal{R}} := \{l \approx r \mid l \to r \in \mathcal{R}\} \cup \mathcal{E}_{\approx}$
  - For $\mathcal{R}_4 = \{a \to b,\ c \to b\}$ we obtain $\mathcal{E}_{\mathcal{R}_4} = \{a \approx b, c \approx b\} \cup \mathcal{E}_{\approx}$
- Theorem 2 (i) $s \xrightarrow{*}_{\mathcal{R}} t$ implies $s \approx_{\mathcal{E}_{\mathcal{R}}} t$
  (ii) $s \approx_{\mathcal{E}_{\mathcal{R}}} t$ iff $s \overset{*}{\leftrightarrow}_{\mathcal{R}} t$
- Proof $\leadsto$ Exercise
  - $g(X, a) \to_{\mathcal{R}_4} g(X, b)$ and $g(X, a) \approx_{\mathcal{E}_{\mathcal{R}_4}} g(X, b)$
  - $g(X, a) \approx_{\mathcal{E}_{\mathcal{R}_4}} g(X, c)$ and $g(X, a) \to_{\mathcal{R}_4} g(X, b) \leftarrow_{\mathcal{R}_4} g(X, c)$

Reducibility and Normal Forms

- s is reducible wrt $\mathcal{R}$ iff there exists t such that $s \rightarrow_{\mathcal{R}} t$
  - otherwise it is irreducible
- t is a normal form of s wrt $\mathcal{R}$ iff $s \stackrel{*}{\rightarrow}_{\mathcal{R}} t$ and t is irreducible
  - $[1, 2, 3, 4]$ is the normal form of $append([1, 2], [3.4])$ wrt $\mathcal{R}_3$
- Normal forms are not necessarily unique. Consider

$$
\begin{array}{rlcl}
\mathcal{R}_5 = \{ & \mathrm{neg}(\mathrm{neg}(X)) & \rightarrow & X, \\
& \mathrm{neg}(or(X, Y)) & \rightarrow & and(\mathrm{neg}(X), \mathrm{neg}(Y)), \\
& \mathrm{neg}(and(X, Y)) & \rightarrow & or(\mathrm{neg}(X), \mathrm{neg}(Y)), \\
& and(X, or(Y, Z)) & \rightarrow & or(and(X, Y), and(X, Z)), \\
& and(or(X, Y), Z) & \rightarrow & or(and(Y, Z), and(Z, X)) \quad \}
\end{array}
$$

$and(or(X, Y), or(U, V))$ has the normal forms
$or(or(and(Y, U), and(U, X)), or(and(Y, V), and(V, X)))$ and
$or(or(and(Y, U), and(Y, V)), or(and(V, X), and(X, U)))$ wrt $\mathcal{R}_5$

Confluent Term Rewriting Systems

- $s \downarrow_{\mathcal{R}} t$ iff there exists u such that $s \xrightarrow{*}_{\mathcal{R}} u \xleftarrow{*}_{\mathcal{R}} t$
- $s \uparrow_{\mathcal{R}} t$ iff there exists u such that $s \xleftarrow{*}_{\mathcal{R}} u \xrightarrow{*}_{\mathcal{R}} t$
  - Consider $\mathcal{R}_6 = \{b \to a,\ b \to c\}$. Then $a \not\downarrow_{\mathcal{R}_6} c$, but $a \uparrow_{\mathcal{R}_6} c$
- $\mathcal{R}$ is **confluent** iff for all terms s and t we find $s \uparrow_{\mathcal{R}} t$ implies $s \downarrow_{\mathcal{R}} t$
  - $\mathcal{R}_7 = \mathcal{R}_6 \cup \{a \to c\}$ is confluent
- $\mathcal{R}$ is **Church-Rosser** iff for all terms s and t we find $s \overset{*}{\leftrightarrow}_{\mathcal{R}} t$ iff $s \downarrow_{\mathcal{R}} t$
- **Theorem 3** $\mathcal{R}$ is Church-Rosser iff $\mathcal{R}$ is confluent
- **Remember** $s \overset{*}{\leftrightarrow}_{\mathcal{R}} t$ iff $s \approx_{\mathcal{E}_{\mathcal{R}}} t$
  - If a term rewriting system is confluent,
    then rewriting has only to be applied in one direction, viz. from left to right !

Canonical Term Rewriting Systems

- $\mathcal{R}$ is **terminating** iff it has no infinite rewriting sequences
  - The question whether $\mathcal{R}$ is terminating is undecidable
- $\mathcal{R}$ is **canonical** iff $\mathcal{R}$ is confluent and terminating
  - If $\mathcal{R}$ is canonical, then $s \approx_{\mathcal{E}_\mathcal{R}} t$ iff $s \downarrow_\mathcal{R} t$
  - If $\mathcal{R}$ is canonical, then $\mathcal{E}_\mathcal{R}$ is decidable
- Given $\mathcal{E}$. If $\approx_\mathcal{E} = \approx_{\mathcal{E}_\mathcal{R}}$ for some canonical term rewriting system $\mathcal{R}$, then the application of paramodulation can be restricted:
  - $L_1\lceil\pi\rceil$ may not be a variable
  - Symmetry can no longer be simulated
  - Equations, i.e., rewrite rules, are only applied from left to right
  - Further restrictions concerning $\pi \in \mathcal{P}_{L_1}$ are possible
  - This restricted form of paramodulation is called **narrowing**

Termination

- **Is a given term rewriting system $\mathcal{R}$ terminating?**
- Let $\succeq$ be a partial order on the set of terms,
  i.e., $\succeq$ is reflexive, transitive, and antisymmetric
  - $s \succ t$ **iff** $s \succeq t$ and $s \neq t$
  - $s \succ t$ is **well-founded** **iff** there is no infinite sequence $s_1 \succ s_2 \succ \ldots$
- **Idea** Search for a well-founded ordering $\succ$ such that $s \rightarrow_{\mathcal{R}} t$ implies $s \succ t$
- A **termination ordering** $\succ$ is a well-founded, transitive, and antisymmetric relation on the set of terms satisfying the following properties:
  - **full invariance property** if $s \succ t$ then $s\theta \succ t\theta$ for all θ
  - **replacement property** if $s \succ t$ then $u\lceil s\rceil \succ u\lceil s/t\rceil$
- **Theorem 4**
  Let $\mathcal{R}$ be a term rewriting system and $\succ$ a termination ordering.
  If for all rules $l \rightarrow r \in \mathcal{R}$ we find that $l \succ r$ then $\mathcal{R}$ is terminating

Termination Orderings: Two Examples

- Let $|s|$ denote the length of the term s
  $s \succ t$ iff for all grounding substitutions θ we find that $|s\theta| > |t\theta|$
  - $f(X, Y) \succ g(X)$
  - $f(X, Y)$ and $g(X, X)$ can not be ordered
- Polynomial ordering assign to each function symbol a polynomial with coefficients taken from $\mathbb{N}^+$
  - Let $\begin{array}{rcl} f(X, Y)^I & = & 2X + Y \\ g(X, Y)^I & = & X + Y \end{array}$
  - Define $s \succ t$ iff $s^I > t^I$
  - Then, $f(X, Y) \succ g(X, X)$
- There are many other termination orderings!
- $\succ'$ is more powerful than $\succ$ iff $s \succ t$ implies $s \succ' t$ but not vice versa

Confluence

- **Is a given terminating term rewriting system confluent?**
- **$\mathcal{R}$ is locally confluent**
  iff for all terms r, s, t we find: If $t \leftarrow_{\mathcal{R}} r \rightarrow_{\mathcal{R}} s$ then $s \downarrow_{\mathcal{R}} t$
- **Theorem 5** **Let $\mathcal{R}$ be a terminating term rewriting system.**
  $\mathcal{R}$ is confluent iff it is locally confluent

Local Confluence

- **Is a given terminating term rewriting system locally confluent?**
- **A subterm u of t is called a redex**
  iff there exists θ and $l \to r \in \mathcal{R}$ such that $u = l\theta$
- **Let $l_1 \to r_1 \in \mathcal{R}$ and $l_2 \to r_2 \in \mathcal{R}$ be applicable to t $\rightsquigarrow$ two redeces**
  - **Case analysis**

    (a) They are disjoint

    (b) one redex is a subterm of the other one and corresponds to a variable position in the left-hand-side of the other rule

    (c) one redex is a subterm of the other one but does not correspond to a variable position in the left-hand-side of the other rule (the redeces overlap)

Example

- Let $t = (g(a) \cdot f(b)) \cdot c$

(a) $\mathcal{R}_8 = \{a \to c,\ b \to c\}$

- a and b are disjoint redeces in t
- $\mathcal{R}_8$ is locally confluent

(b) $\mathcal{R}_9 = \{a \to c,\ g(X) \to f(X)\}$

- a and $g(a)$ are redeces in t
- a corresponds to the variable position in $g(X)$
- $\mathcal{R}_9$ is locally confluent

(c) $\mathcal{R}_{10} = \{(X \cdot Y) \cdot Z \to X,\ g(a) \cdot f(b) \to c\}$

- $(g(a) \cdot f(b)) \cdot c$ and $g(a) \cdot f(b)$ are overlapping redeces in t
- This is the problematic case!

Critical Pairs

- Let
  - $l_1 \to r_1,\ l_2 \to r_2$ be two new variants of rules in $\mathcal{R}$
  - u be a non-variable subterm of l_1 and
  - u and l_2 be unifiable with mgu θ
- Then, the pair $\langle (l_1\lceil u/r_2\rceil)\theta,\ r_1\theta\rangle$ is said to be critical
- It is obtained by superimposing l_1 with l_2
  - Superimposing $(X \cdot Y) \cdot Z \to X$ with $g(a) \cdot f(b) \to c$
    yields the critical pair $\langle c \cdot Z, g(a)\rangle$
- Theorem 6 A term rewriting system $\mathcal{R}$ is locally confluent
  iff for all critical pairs $\langle s, t\rangle$ of $\mathcal{R}$ we find $s \downarrow_{\mathcal{R}} t$

Completion

- Can a terminating and non-confluent $\mathcal{R}$ be turned into a confluent one?
- Two term rewriting systems $\mathcal{R}$ and $\mathcal{R}'$ are equivalent iff $\approx_{\mathcal{E}_\mathcal{R}} = \approx_{\mathcal{E}_{\mathcal{R}'}}$
- Idea if $\langle s, t \rangle$ is a critical pair then add either $s \to t$ or $t \to s$ to $\mathcal{R}$
  - This is called completion
  - The equational theory remains unchanged

Completion Procedure

- **Given a terminating $\mathcal{R}$ together with a termination ordering $\succ$**
  1. **If for all critical pairs $\langle s, t\rangle$ of $\mathcal{R}$ we find that $s \downarrow_{\mathcal{R}} t$ then return "success"; $\mathcal{R}$ is canonical**
  2. **If $\mathcal{R}$ has a critical pair whose elements do not rewrite to a common term, then transform the elements of the critical pair to some normal form. Let $\langle s, t\rangle$ be the normalized critical pair:**
     - **If $s \succ t$ then add the rule $s \to t$ to $\mathcal{R}$ and goto 1**
     - **If $t \succ s$ then add the rule $t \to s$ to $\mathcal{R}$ and goto 1**
     - **If neither $s \succ t$ nor $t \succ s$ then return "fail"**
- **The completion procedure may either succeed or fail or loop**
- **During completion the ordering $\succ$ may be extended to a more powerful one**
- **The completion procedure may be extended to unfailing completion**

Completion: An Example

- Consider
$$\mathcal{R}_{11} = \{c \to b,\ f \to b,\ f \to a,\ e \to a,\ e \to d\}$$
- Let $f \succ e \succ d \succ c \succ b \succ a$
- The critical pairs are $\langle b, a\rangle$ and $\langle d, a\rangle$
- They can be oriented into the new rules $b \to a$ and $d \to a$
- We obtain
$$\mathcal{R}'_{11} = \{c \to b,\ f \to b,\ f \to a,\ e \to a,\ e \to d,\ b \to a,\ d \to a\}$$
- $\mathcal{R}'_{11}$ is canonical
- $s \approx_{\mathcal{E}_\mathcal{R}} t \quad \text{iff} \quad s \approx_{\mathcal{E}_{\mathcal{R}'}} t$
- All proofs for $s \approx_{\mathcal{E}_{\mathcal{R}'_{11}}} t$ are in so-called valley form

Unification Theory

- **Idea** We want to build equational axioms into the unification computation
- An **$\mathcal{E}$-unification problem** consists of an equational theory $\mathcal{E}$ and two terms s and t, and is the question whether $\mathcal{E} \cup \mathcal{E}_{\approx} \models \exists\, s \approx t$ holds
  - A substitution θ is a **solution** of the $\mathcal{E}$-unification problem **iff** $s\theta \approx_{\mathcal{E}} t\theta$
  - In this case θ is called **$\mathcal{E}$-unifier** for s and t
  - If $\mathcal{E} = \emptyset$ then $\mathcal{E}$-unification is unification
  - Consider $\mathcal{E} = \{f(X) \approx X\}$ and let $s = g(f(a), a)$ and $t = g(Y, Y)$.
    - $\{Y \mapsto a\}$ is an $\mathcal{E}$-unifier for s and t
    - The unification problem $\{s \stackrel{\cdot}{\approx} t\}$ is unsolvable
- Substitutions η and θ are **$\mathcal{E}$-equal** on a set $\mathcal{V}$ of variables ($\theta \approx_{\mathcal{E}} \eta[\mathcal{V}]$) **iff** $X\eta \approx_{\mathcal{E}} X\theta$ for all $X \in \mathcal{V}$
  - Reconsider $\mathcal{E} = \{f(X) \approx X\}$
    - $\{Y \mapsto a\}$ and $\{Y \mapsto f(a)\}$ are $\mathcal{E}$-equal on $\{X, Y\}$

$\mathcal{E}$-Instances

- Subsitution η is an $\mathcal{E}$-instance of θ on a set $\mathcal{V}$ of variables ($\eta \leq_{\mathcal{E}} \theta[\mathcal{V}]$)
  (or θ is more general than η wrt $\mathcal{E}$ and $\mathcal{V}$)
  iff there exists a substitution τ such that $X\eta \approx_{\mathcal{E}} X\theta\tau$ for all $X \in \mathcal{V}$
- η is a strict $\mathcal{E}$-instance of θ ($\eta <_{\mathcal{E}} \theta[\mathcal{V}]$) iff $\eta \leq_{\mathcal{E}} \theta[\mathcal{V}]$ and $\eta \not\approx_{\mathcal{E}} \theta[\mathcal{V}]$
- If neither $\eta \leq_{\mathcal{E}} \theta[\mathcal{V}]$ nor $\theta \leq_{\mathcal{E}} \eta[\mathcal{V}]$
  then θ and η are said to be incomparable on $\mathcal{V}$

Examples

- Consider $\mathcal{E} \cup \mathcal{E}_{\approx} \models (\exists X, Y)\, f(X, g(a, b)) \approx f(g(Y, b), X)$
- $\mathcal{E} = \emptyset$
  - Unification problem is decidable
  - Most general unifier is unique modulo variable renaming

$$\theta_1 = \{X \mapsto g(a, b),\ Y \mapsto a\}$$

- $\mathcal{E} = \{f(X, Y) \approx f(Y, X)\}$
  - θ_1 is a solution and so is $\theta_2 = \{Y \mapsto a\}$

$$f(X, g(a, b))\theta_2 = f(X, g(a, b)) \approx_{\mathcal{E}} f(g(a, b), X) = f(g(Y, b), X)\theta_2$$

  - $\theta_1 \leq_{\mathcal{E}} \theta_2[\{X, Y\}]$
  - There are at most finitely many most general unifiers in this case

Examples Continued

- Reconsider $\mathcal{E} \cup \mathcal{E}_{\approx} \models (\exists X, Y)\, f(X, g(a, b)) \approx f(g(Y, b), X)$
- $\mathcal{E} = \{f(X, f(Y, Z)) \approx f(f(X, Y), Z))\}$
  - $\theta_1 = \{X \mapsto g(a, b),\ Y \mapsto a\}$ is a solution
  - So is $\theta_3 = \{X \mapsto f(g(a, b), g(a, b)),\ Y \mapsto a\}$

$$\begin{array}{rcl} f(X, g(a, b))\theta_3 & = & f(f(g(a, b), g(a, b)), g(a, b)) \\ & \approx_{\mathcal{E}} & f(g(a, b), f(g(a, b), g(a, b))) \\ & = & f(g(Y, b), X)\theta_3 \end{array}$$

  - θ_1 and θ_3 are incomparable on $\{X, Y\}$
  - $\theta_4 = \{X \mapsto f(g(a, b), f(g(a, b), g(a, b))), Y \mapsto a\}$ is yet another solution incomparable to θ_1 and θ_3 on $\{X, Y\}$
  - In general, there may be infinitely many most general unifiers in this case
- $\mathcal{E} = \{f(X, f(Y, Z)) \approx f(f(X, Y), Z)),\ f(X, Y) \approx f(Y, X)\}$
  - There are at most finitely many most general unifiers in this case

Sets of $\mathcal{E}$-Unifiers

- Given an $\mathcal{E}$-unification problem $\mathcal{E} \cup \mathcal{E}_{\approx} \models \exists\, s \approx t$
- $\mathcal{U}_{\mathcal{E}}(s, t)$ denotes the set of all $\mathcal{E}$-unifiers of s and t
- Complete set $\mathcal{S}$ of $\mathcal{E}$-unifiers for s and t
  - $\mathcal{S} \subseteq \mathcal{U}_{\mathcal{E}}(s, t)$ and
  - for all $\eta \in \mathcal{U}_{\mathcal{E}}(s, t)$ there exists $\theta \in \mathcal{S}$ such that $\eta \leq_{\mathcal{E}} \theta[\mathit{var}(s) \cup \mathit{var}(t)]$
- Minimal complete set $\mathcal{S}$ of $\mathcal{E}$-unifiers for s and t
  - complete set and
  - for all $\theta, \eta \in \mathcal{S}$ we find $\eta \leq_{\mathcal{E}} \theta[\mathit{var}(s) \cup \mathit{var}(t)]$ implies $\theta = \eta$
- Complete sets of $\mathcal{E}$-unifiers for s and t are often denoted by $cU_{\mathcal{E}}(s, t)$
- Minimal complete sets of $\mathcal{E}$-unifiers for s and t are often denoted by $\mu U_{\mathcal{E}}(s, t)$
- If $c\mathcal{U}_{\mathcal{E}}(s, t)$ is finite and $\leq_{\mathcal{E}}$ is decidable then there exists $\mu\mathcal{U}_{\mathcal{E}}(s, t)$
- Let $\theta \equiv_{\mathcal{E}} \eta[\mathcal{V}]$ iff $\eta \leq_{\mathcal{E}} \theta[\mathcal{V}]$ and $\theta \leq_{\mathcal{E}} \eta[\mathcal{V}]$
- $\mu\mathcal{U}_{\mathcal{E}}(s, t)$ is unique up to $\equiv_{\mathcal{E}} [\mathit{var}(s) \cup \mathit{var}(t)]$ if it exists

Another Example

- Let the constant a and the binary f be the only function symbols
- Let $\mathcal{E} = \{f(X, f(Y, Z)) \approx f(f(X, Y), Z)\}$
- Consider $\mathcal{E} \cup \mathcal{E}_{\approx} \models \exists\, f(X, a) \approx f(a, Y)$
  - $\theta = \{X \mapsto a,\ Y \mapsto a\}$ is a solution
  - $\eta = \{X \mapsto f(a, Z),\ Y \mapsto f(Z, a)\}$ is another solution
  - $\{\theta, \eta\}$ is a complete set of $\mathcal{E}$-unifiers $\rightsquigarrow$ Exercise
  - θ and η are incomparable under $\geq_{\mathcal{E}}$
  - The set $\{\theta, \eta\}$ is minimal

On the Existence of Minimal Complete Sets of $\mathcal{E}$-Unifiers

- **Theorem 7** Minimal complete sets of $\mathcal{E}$-unifiers do not always exist
- **Proof** Let $\mathcal{R} = \{f(a, X) \to X,\ g(f(X, Y)) \to g(Y)\}$
- **Claim** $\mu\mathcal{U}_{\mathcal{E}_\mathcal{R}}(g(X), g(a))$ does not exist
  - $\mathcal{R}$ is canonical $\rightsquigarrow$ Exercise
  - Define
$$\begin{array}{lcl} \sigma_0 & = & \{X \mapsto a\} \\ \sigma_1 & = & \{X \mapsto f(X_1, a)\} = \{X \mapsto f(X_1, X\sigma_0)\} \\ \vdots & & \\ \sigma_i & = & \{X \mapsto f(X_i, X\sigma_{i-1})\} \end{array}$$
  - Let $\mathcal{S} = \{\sigma_i \mid i \geq 0\}$
  - $\mathcal{S}$ is a $cU_{\mathcal{E}_\mathcal{R}}(g(X), g(a))$ $\rightsquigarrow$ Exercise
  - With $\rho_i = \{X_i \mapsto a\}$ we find $X\sigma_i\rho_i = f(a, X\sigma_{i-1}) \approx_{\mathcal{E}_\mathcal{R}} X\sigma_{i-1}$
  - Hence, $\sigma_{i-1} \leq_{\mathcal{E}_\mathcal{R}} \sigma_i[\{X\}]$
  - Because $X\sigma_i = f(X_i, X\sigma_{i-1}) \not\approx_{\mathcal{E}_\mathcal{R}} X\sigma_{i-1}$ we find $\sigma_i \not\approx_{\mathcal{E}_\mathcal{R}} \sigma_{i-1}$
  - Thus $\sigma_{i-1} <_{\mathcal{E}_\mathcal{R}} \sigma_i[\{X\}]$

Proof of Theorem 7 Continued

- **Remember** $\mathcal{R} = \{f(a, X) \to X,\ g(f(X, Y)) \to g(Y)\}$
  - Assume $\mathcal{S}'$ is a $\mu\mathcal{U}_{\mathcal{E}_\mathcal{R}}(g(X), g(a))$
  - Because $\mathcal{S}$ is complete we find that for all $\theta \in \mathcal{S}'$ there exists $\sigma_i \in \mathcal{S}$ such that $\theta \leq_{\mathcal{E}_\mathcal{R}} \sigma_i[\{X\}]$
  - Because $\sigma_i <_{\mathcal{E}_\mathcal{R}} \sigma_{i+1}[\{X\}]$ we obtain $\theta <_{\mathcal{E}_\mathcal{R}} \sigma_{i+1}[\{X\}]$
  - Because $\mathcal{S}'$ is complete we find that there exists $\sigma \in \mathcal{S}'$ such that $\sigma_{i+1} \leq_{\mathcal{E}_\mathcal{R}} \sigma[\{X\}]$
  - Hence $\theta <_{\mathcal{E}_\mathcal{R}} \sigma[\{X\}]$
  - Thus $\mathcal{S}'$ is not minimal $\leadsto$ **Contradiction**

Unification Types

- The unification type of $\mathcal{E}$ is

unitary	iff	a set $\mu\mathcal{U}_{\mathcal{E}}(s, t)$ exists for all s, t and has cardinality 0 or 1
finitary	iff	a set $\mu\mathcal{U}_{\mathcal{E}}(s, t)$ exists for all s, t and is finite
infinitary	iff	a set $\mu\mathcal{U}_{\mathcal{E}}(s, t)$ exists for all s, t, and there are u and v such that $\mu\mathcal{U}_{\mathcal{E}}(u, v)$ is infinite
zero	iff	there are s, t such that $\mu\mathcal{U}_{\mathcal{E}}(s, t)$ does not exist

Unification procedures

- $\mathcal{E}$-unification procedure
  - input: $s \approx t$
  - output: subset of $\mathcal{U}_{\mathcal{E}}(s, t)$
  - is complete iff for all s, t the output is a $c\mathcal{U}_{\mathcal{E}}(s, t)$
  - is minimal iff for all s, t the output is a $\mu\mathcal{U}_{\mathcal{E}}(s, t)$
- Universal $\mathcal{E}$-unification procedure
  - input: $\mathcal{E}$ and $s \approx t$
  - output: subset of $\mathcal{U}_{\mathcal{E}}(s, t)$
  - is complete iff for all $\mathcal{E}$ and s, t the output is a $c\mathcal{U}_{\mathcal{E}}(s, t)$
  - is minimal iff for all $\mathcal{E}$ and s, t the output is a $\mu\mathcal{U}_{\mathcal{E}}(s, t)$

Typical Questions

- **Given $\mathcal{E}$**
- **Is it decidable whether an $\mathcal{E}$-unification problem is solvable?**
- **What is the unification type of $\mathcal{E}$?**
- **How can we obtain an efficient $\mathcal{E}$-unification algorithm or, preferably, a minimal $\mathcal{E}$-unification procedure?**

Classes of $\mathcal{E}$-Unification Problems

- The class of an $\mathcal{E}$-unification problem $\mathcal{E} \cup \mathcal{E}_{\approx} \models \exists\, s \approx t$ is called
  - elementary iff s and t contain only symbols occurring in $\mathcal{E}$
  - with constants iff s and t may contain additional so-called free constants
  - general iff s and t may contain add. function symbols of arbitrary arity

Unification with Constants: Some Examples

Equational System	Unification Type	Unification decidable?	Complexity of the decision problem
$\mathcal{E}_{A}$	infinitary	yes	NP-hard
$\mathcal{E}_{C}$	finitary	yes	NP-complete
$\mathcal{E}_{AC}$	finitary	yes	NP-complete
$\mathcal{E}_{AG}$	unitary	yes	polynomial
$\mathcal{E}_{AI}$	zero	yes	NP-hard
$\mathcal{E}_{CR1}$	zero	no	–
$\mathcal{E}_{DL}, \mathcal{E}_{DR}$	unitary	yes	polynomial
$\mathcal{E}_{D}$	infinitary	?	NP-hard
$\mathcal{E}_{DA}$	infinitary	no	–
$\mathcal{E}_{BR}$	unitary	yes	NP-complete

Additional Remarks

- **$\mathcal{E}$-matching problem**
  $\mathcal{E} \cup \mathcal{E}_{\approx} \models \exists\theta\ s \approx_{\mathcal{E}} t\theta$
- **Combination problem**
  Can the results and unification algorithms for $\mathcal{E}_1$ and $\mathcal{E}_2$ be combined for $\mathcal{E}_1 \cup \mathcal{E}_2$?
- **Universal $\mathcal{E}$-unification problem**
  $\mathcal{E}$-unification problem, where the equational system is part of the input

Canonical Term Rewriting Systems Revisited

- Let R be a canonical term rewriting system
- So far, we were able to answer questions of the form $\mathcal{E}_R \models \forall\, s \approx t$
  - Rewriting $s\lceil u\rceil \rightarrow_{\mathcal{R}} t$ iff there are $l \rightarrow r \in \mathcal{R}$ and θ such that $u = l\theta$ and $t = s\lceil u/r\theta\rceil$
- Now consider $\mathcal{E}_R \models \exists\, s \approx t$
  - Narrowing $s\lceil u\rceil \Rightarrow_{\mathcal{R}} t$ iff there are $l \rightarrow r \in \mathcal{R}$ and θ such that $u\theta = l\theta$ and $t = (s\lceil u/r\rceil)\theta$ where u is a non-variable subterm of s
  - Please compare narrowing to rewriting and paramodulation!
  - Theorem 8
    Let $\mathcal{R}$ be a canonical term rewriting system with $var(l) \supseteq var(r)$ for all $l \rightarrow r \in \mathcal{R}$. Then narrowing and resolution is sound and complete
  - A complete universal $\mathcal{E}$-unification procedure for canonical theories $\mathcal{E}$ can be built upon narrowing and resolution

Applications

- databases
- information retrieval
- computer vision
- natural language processing
- knowledge based systems
- text manipulation systems
- planning and scheduling systems
- pattern directed programming languages
- logic programming systems
- computer algebra systems
- deduction systems
- non-classical reasoning systems

Multisets

- $\dot{\{} e_1, e_2, \ldots \dot{\}}$ or $\dot{\emptyset}$
- $X \in_k \mathcal{M}$ iff X occurs precisely k times in $\mathcal{M}$

  $\mathcal{M}_1 \doteq \mathcal{M}_2$ iff for all X we find $X \in_k \mathcal{M}_1$ iff $X \in_k \mathcal{M}_2$

  $X \in_m \mathcal{M}_1 \dot{\cup} \mathcal{M}_2$ iff there exist $k, l \geq 0$ such that $X \in_k \mathcal{M}_1$, $X \in_l \mathcal{M}_2$ and $k + l = m$

  $X \in_m \mathcal{M}_1 \dot{\setminus} \mathcal{M}_2$ iff there exist $k, l \geq 0$ such that either $X \in_k \mathcal{M}_1$, $X \in_l \mathcal{M}_2$, $k > l$ and $m = k - l$ or $X \in_k \mathcal{M}_1$, $X \in_l \mathcal{M}_2$, $k \leq l$ and $m = 0$

  $X \in_m \mathcal{M}_1 \dot{\cap} \mathcal{M}_2$ iff there exist $k, l \geq 0$ such that $X \in_k \mathcal{M}_1$, $X \in_l \mathcal{M}_2$ and $m = \mathtt{min}\{k, l\}$

  $\mathcal{M}_1 \dot{\subseteq} \mathcal{M}_2$ iff $\mathcal{M}_1 \dot{\cap} \mathcal{M}_2 \doteq \mathcal{M}_1$

Fluent Terms

- Consider an alphabet with variables $\mathcal{V}$ and set $\mathcal{F}$ of function symbols which contains the binary $\circ$ (written infix) and the constant 1
- Let $\mathcal{F}^- = \mathcal{F} \setminus \{\circ, 1\}$
- The non-variable elements of $\mathcal{T}(\mathcal{F}^-, \mathcal{V})$ are called fluents
- The set of fluent terms is the smallest set satisfying the following conditions
  - 1 is a fluent term
  - Each fluent is a fluent term
  - If s and t are fluent terms then $s \circ t$ is a fluent term as well
- Let

$$\mathcal{E}_{AC1} = \{ \begin{array}{l} X \circ (Y \circ Z) \approx (X \circ Y) \circ Z \\ X \circ Y \approx Y \circ X \\ X \circ 1 \approx X \end{array} \}$$

Multisets vs. Fluent Terms

- In the sequel let
  - t be a fluent term and
  - $\mathcal{M}$ be a multiset of fluents
- Consider the following mappings
  - $\cdot^I$ (from the set of fluent terms into the set of multisets of fluents)

$$t^I = \begin{cases} \dot{\emptyset} & \text{if } t = 1 \\ \dot{\{}t\dot{\}} & \text{if } t \text{ is a fluent} \\ u^I \dot{\cup} v^I & \text{if } t = u \circ v \end{cases}$$

  - $\cdot^{-I}$ (from the set of multisets of fluents into the set of fluent terms)

$$\mathcal{M}^{-I} = \begin{cases} 1 & \text{if } \mathcal{M} \doteq \dot{\emptyset} \\ s \circ \mathcal{N}^{-I} & \text{if } \mathcal{M} \doteq \dot{\{}s\dot{\}} \dot{\cup} \mathcal{N} \end{cases}$$

Matching and Unification Problems

- **Submultiset matching problem**
  Does there exist a θ such that $\mathcal{M}\theta \dot{\subseteq} \mathcal{N}$, where $\mathcal{N}$ is ground?
- **Submultiset unification problem**
  Does there exist a θ such that $\mathcal{M}\theta \dot{\subseteq} \mathcal{N}\theta$?

- **Fluent matching problem**
  Does there exist a θ such that $(s \circ X)\theta \approx_{AC1} t$,
  where t is ground and X does not occur in s?
- **Fluent unification problem**
  Does there exist a θ such that $(s \circ X)\theta \approx_{AC1} t\theta$,
  where X does not occur in s or t?

Submultiset versus Fluent Unification Problems

- **Equivalence of matching problems**

$$(s \circ X)\theta \approx_{AC1} t \quad \text{iff} \quad (s\theta)^I \mathrel{\dot{\subseteq}} t^I \quad \text{and} \quad (X\theta)^I \doteq t^I \mathbin{\dot{\setminus}} (s\theta)^I$$

- **Equivalence of unification problems**

$$(s \circ X)\theta \approx_{AC1} t\theta \quad \text{iff} \quad (s\theta)^I \mathrel{\dot{\subseteq}} (t\theta)^I \quad \text{and} \quad (X\theta)^I \doteq (t\theta)^I \mathbin{\dot{\setminus}} (s\theta)^I$$

- **Theorem 9** Fluent matching and fluent unification problems are
  - decidable
  - finitary and
  - there always exists a minimal complete set of matchers and unifiers

Fluent Matching Algorithm

Input A fluent matching problem $\exists\theta\ (\boldsymbol{s} \circ \boldsymbol{X})\theta \approx_{AC1} \boldsymbol{t}$?
(where $\boldsymbol{t}$ is ground and $\boldsymbol{X}$ does not occur in $\boldsymbol{s}$)

Output A solution θ of the fluent matching problem, if it is solvable;
failure, otherwise

1 $\theta = \varepsilon$

2 **if** $\boldsymbol{s} \approx_{AC1} 1$ **then return** $\theta\{\boldsymbol{X} \mapsto \boldsymbol{t}\}$

3 **don't-care non-deterministically select a fluent** $\boldsymbol{u}$ **from** $\boldsymbol{s}$ **and remove** $\boldsymbol{u}$ **from** $\boldsymbol{s}$

4 **don't-know non-deterministically select a fluent** $\boldsymbol{v}$ **from** $\boldsymbol{t}$ **such that there exists a substitution** η **with** $\boldsymbol{u}\eta = \boldsymbol{v}$

5 **if such a fluent exists then apply** η **to** $\boldsymbol{s}$**, delete** $\boldsymbol{v}$ **from** $\boldsymbol{t}$ **and let** $\theta := \theta\eta$**, otherwise stop with failure**

6 **goto 2**