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

\[ \{\forall, \exists\} > \neg > \land > \lor > \{\leftarrow, \rightarrow\} > \leftrightarrow \]

- 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.

\[
\mathcal{E}_1 \quad (X \cdot Y) \cdot Z \approx X \cdot (Y \cdot Z) \quad \text{(associativity)}
\]

\[
1 \cdot X \approx X \quad \text{(left unit)}
\]

\[
X \cdot 1 \approx X \quad \text{(right unit)}
\]

\[
X^{-1} \cdot X \approx 1 \quad \text{(left inverse)}
\]

\[
X \cdot X^{-1} \approx 1 \quad \text{(right inverse)}
\]
Axioms of Equality

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

  \[
  \begin{align*}
  X & \approx X \quad \text{(reflexivity)} \\
  X \approx Y & \rightarrow Y \approx X \quad \text{(symmetry)} \\
  X \approx Y \land Y \approx Z & \rightarrow X \approx Z \quad \text{(transitivity)} \\
  \bigwedge_{i=1}^{n} X_i \approx Y_i & \rightarrow f(X_1, \ldots, X_n) \approx f(Y_1, \ldots, Y_n) \quad \text{(f–substitutivity)} \\
  \bigwedge_{i=1}^{n} X_i \approx Y_i \land r(X_1, \ldots, X_n) & \rightarrow r(Y_1, \ldots, Y_n) \quad \text{(r–substitutivity)}
  \end{align*}
  \]

- **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
    \[
    \{ t \approx t \mid t \text{ is a ground term} \}
    \cup \{ a \approx b, \ b \approx a \}
    \cup \{ g(a, a) \approx g(b, a), \ g(a, a) \approx g(a, b), \ g(a, a) \approx g(b, b), \ldots \}
    \]
- 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

- $L[s]$ literal which contains an occurrence of the term $s$
- $L[s/t]$ literal obtained from $L$ by replacing an occurrence of $s$ by $t$

- **Paramodulation**

\[
\frac{[L_1[s], L_2, \ldots, L_n]}{[L_1[s/r], L_2, \ldots, L_m]} \quad \frac{[l \approx r, L_{n+1}, \ldots, L_m]}{\theta = \text{mgu}(s, l)}
\]

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

- **Remember**

\[
E \cup E_\approx \models \forall s \approx t \quad \iff \quad \land_{E \cup E_\approx} \rightarrow \forall s \approx t \text{ is valid}
\]
\[
\iff \quad \neg (\land_{E \cup E_\approx} \rightarrow \forall s \approx t) \text{ is unsatisfiable}
\]
\[
\iff \quad E \cup E_\approx \cup \{\neg \forall s \approx t\} \text{ is unsatisfiable}
\]
\[
\iff \quad E \cup E_\approx \cup \{\exists s \not\approx t\} \text{ is unsatisfiable}
\]

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

\[ \varepsilon_1 \cup \{ X \approx X, \ X \cdot X \approx 1 \} \models (\forall X, Y) \ X \cdot Y \approx Y \cdot X \]

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( a \cdot b \not\approx b \cdot a )</td>
<td>initial query</td>
<td>( \cdot )</td>
<td>( \cdot )</td>
<td>hypothesis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>( 1 \cdot X_1 \approx X_1 )</td>
<td>left unit</td>
<td>( a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot (X_4 \cdot X_4)) )</td>
<td>( \cdot )</td>
<td>associativity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>( X_2 \approx X_2 )</td>
<td>reflexivity</td>
<td>( a \cdot b \not\approx ((X_3 \cdot b) \cdot (a \cdot X_4)) )</td>
<td>( a \cdot b \not\approx (a \cdot 1) \cdot b )</td>
<td>hypothesis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>( X_1 \approx 1 \cdot X_1 )</td>
<td>pm(2,3)</td>
<td>( \cdot )</td>
<td>( \cdot )</td>
<td>right unit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>( a \cdot b \not\approx (1 \cdot b) \cdot a )</td>
<td>pm(1,4)</td>
<td>( a \cdot b \not\approx (a \cdot 1) \cdot b )</td>
<td>( \cdot )</td>
<td>hypothesis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>( X_3 \cdot X_3 \approx 1 )</td>
<td>pm(6,7)</td>
<td>( n )</td>
<td>( n' )</td>
<td>( a \cdot b \not\approx a \cdot b )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>( X_4 \approx X_4 )</td>
<td>pm(5,8)</td>
<td>( n' )</td>
<td>( X_5 \approx X_5 )</td>
<td>reflexivity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>( 1 \approx X_3 \cdot X_3 )</td>
<td>right unit</td>
<td>( n'' )</td>
<td>[]</td>
<td>res ((n, n'))</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Example in Shorthand Notation

\[ \varepsilon_1 \cup \{ X \approx X, \ X \cdot X \approx 1 \} \models (\forall X, Y) \ X \cdot Y \approx Y \cdot X \]

<table>
<thead>
<tr>
<th>Step</th>
<th>Equation</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( a \cdot b \not\approx b \cdot a )</td>
<td>initial query</td>
</tr>
<tr>
<td>2</td>
<td>( 1 \cdot X_1 \approx X_1 )</td>
<td>left unit</td>
</tr>
<tr>
<td>3</td>
<td>( X_2 \approx X_2 )</td>
<td>reflexivity</td>
</tr>
<tr>
<td>4</td>
<td>( X_1 \approx 1 \cdot X_1 )</td>
<td>pm(2,3)</td>
</tr>
<tr>
<td>5</td>
<td>( a \cdot b \not\approx (1 \cdot b) \cdot a )</td>
<td>pm(1,4)</td>
</tr>
<tr>
<td>6</td>
<td>( X_3 \cdot X_3 \approx 1 )</td>
<td>hypothesis</td>
</tr>
<tr>
<td>7</td>
<td>( X_4 \approx X_4 )</td>
<td>hypothesis</td>
</tr>
<tr>
<td>8</td>
<td>( 1 \approx X_3 \cdot X_3 )</td>
<td>pm(6,7)</td>
</tr>
<tr>
<td>9</td>
<td>( a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot a )</td>
<td>pm(5,8)</td>
</tr>
</tbody>
</table>

\[ a \cdot b \not\approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot 1) \]

- hypothesis
- associativity
- right unit
- reflexivity
- res \((n, n')\)
The Example in Shorthand Notation Again

\[ b \cdot a \approx (1 \cdot b) \cdot a \quad \text{left unit} \]

\[ \approx ((X_3 \cdot X_3) \cdot b) \cdot a \quad \text{hypothesis} \]

\[ \approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot 1) \quad \text{right unit} \]

\[ \approx ((X_3 \cdot X_3) \cdot b) \cdot (a \cdot (X_4 \cdot X_4)) \quad \text{hypothesis} \]

\[ \approx (X_3 \cdot ((X_3 \cdot b) \cdot (a \cdot X_4))) \cdot X_4 \quad \text{associativity} \]

\[ \approx (a \cdot 1) \cdot b \quad \text{hypothesis} \]

\[ \approx a \cdot b \quad \text{right unit} \]

- 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
    - $L_1 [s]$ 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.
- $s[u]$ denotes a term $s$ which contains an occurrence of $u$.
- $s[u/v]$ 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: $s[u] \rightarrow_{\mathcal{R}} t$ iff there exist $l \rightarrow r \in \mathcal{R}$ and $\theta$ such that $u = l\theta$ and $t = s[u/r\theta]$.
- Example: $\mathcal{R}_3 = \{ \text{append}([\ ], X) \rightarrow X, \text{append}([X|Y], Z) \rightarrow [X|\text{append}(Y, Z)] \}$

$$\text{append}([1, 2], [3, 4]) \rightarrow_{\mathcal{R}_3} [1|\text{append}([2], [3, 4])]$$
$$\rightarrow_{\mathcal{R}_3} [1, 2|\text{append}([\ ], [3, 4])]$$
$$\rightarrow_{\mathcal{R}_3} [1, 2, 3, 4]$$
Matching problem
Given terms $u$ and $l$, does there exist a substitution $\theta$ 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

\[ \rightarrow^* \text{ denotes the reflexive and transitive closure of } \rightarrow \]

- \[ \text{append}([1, 2], [3, 4]) \rightarrow^*_3 [1, 2, 3, 4] \]

\[ s \leftrightarrow R \text{ iff } s \leftarrow R \text{ or } s \rightarrow R \]

- Let \( R_4 = \{ a \rightarrow b, c \rightarrow b \} \),
  then \( a \rightarrow R_4 b \leftarrow R_4 c \) and, consequently, \( a \leftrightarrow R_4 b \leftrightarrow R_4 c \)

\[ \leftrightarrow^* \text{ denotes the reflexive and transitive closure of } \leftrightarrow \]

- \( a \leftrightarrow^* R_4 c \)

We sometimes simply write \( \rightarrow \) or \( \leftrightarrow \) instead of \( \rightarrow R \) or \( \leftrightarrow R \), respectively.
Let \( \mathcal{R} \) be a term rewriting system

\[ \mathcal{E}_\mathcal{R} := \{ l \approx r \mid l \rightarrow r \in \mathcal{R} \} \cup \mathcal{E}_\approx \]

For \( \mathcal{R}_4 = \{ a \rightarrow b, c \rightarrow b \} \) we obtain \( \mathcal{E}_{\mathcal{R}_4} = \{ a \approx b, c \approx b \} \cup \mathcal{E}_\approx \)

**Theorem 2**

(i) \( s \stackrel{*}{\rightarrow}_\mathcal{R} t \) implies \( s \approx_{\mathcal{E}_\mathcal{R}} t \)

(ii) \( s \approx_{\mathcal{E}_\mathcal{R}} t \) iff \( s \leftrightarrow_{\mathcal{R}} t \)

**Proof**

\( g(X, a) \rightarrow_{\mathcal{R}_4} g(X, b) \) 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 \( g(X, a) \rightarrow_{\mathcal{R}_4} g(X, b) \leftarrow_{\mathcal{R}_4} g(X, c) \)
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 \textit{append}([1, 2], [3.4]) wrt \( \mathcal{R}_3 \)

- Normal forms are not necessarily unique. Consider

\[
\mathcal{R}_5 = \{ \begin{align*}
\text{neg}(\text{neg}(X)) & \rightarrow X, \\
\text{neg}(\text{or}(X, Y)) & \rightarrow \text{and}(\text{neg}(X), \text{neg}(Y)), \\
\text{neg}(\text{and}(X, Y)) & \rightarrow \text{or}(\text{neg}(X), \text{neg}(Y)), \\
\text{and}(X, \text{or}(Y, Z)) & \rightarrow \text{or}(\text{and}(X, Y), \text{and}(X, Z)), \\
\text{and}(\text{or}(X, Y), Z) & \rightarrow \text{or}(\text{and}(Y, Z), \text{and}(Z, X))
\end{align*} \}
\]

\text{and}(\text{or}(X, Y), \text{or}(U, V)) has the normal forms
\text{or}((\text{and}(Y, U), \text{and}(U, X)), \text{or}(\text{and}(Y, V), \text{and}(V, X))) \text{ and } \text{or}((\text{and}(Y, U), \text{and}(Y, V)), \text{or}((\text{and}(V, X), \text{and}(X, U))) \text{ wrt } \mathcal{R}_5
Confluent Term Rewriting Systems

- $s \downarrow_{\mathcal{R}} t$ iff there exists $u$ such that $s \rightarrow_{\mathcal{R}} u \leftarrow_{\mathcal{R}} t$
- $s \uparrow_{\mathcal{R}} t$ iff there exists $u$ such that $s \leftarrow_{\mathcal{R}} u \rightarrow_{\mathcal{R}} t$

Consider $\mathcal{R}_6 = \{ b \rightarrow a, b \rightarrow c \}$. 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 $s \downarrow_{\mathcal{R}} t$

- $\mathcal{R}_7 = \mathcal{R}_6 \cup \{ a \rightarrow c \}$ is confluent

- $\mathcal{R}$ is Church-Rosser iff for all terms $s$ and $t$ we find $s \leftrightarrow_{\mathcal{R}} t$ iff $s \downarrow_{\mathcal{R}} t$

Theorem 3 $\mathcal{R}$ is Church-Rosser iff $\mathcal{R}$ is confluent

Remember $s \rightarrow_{\mathcal{R}} t$ iff $s \approx_{E_{\mathcal{R}}} t$

- 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:
  - $L_1[\pi]$ 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 $\succ$ be a partial order on the set of terms, i.e., $\succ$ 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 $\theta$
  - replacement property if $s \succ t$ then $u[s] \succ u[s/t]$

- 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 $\theta$ 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 $f(X, Y)' = 2X + Y$
  - $g(X, Y)' = X + Y$

  - Define $s \succ t$ iff $s' > t'$
  - 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 $\theta$ and $l \rightarrow r \in \mathcal{R}$ such that $u = l\theta$
- Let $l_1 \rightarrow r_1 \in \mathcal{R}$ and $l_2 \rightarrow r_2 \in \mathcal{R}$ be applicable to $t \leadsto$ 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) \( \mathcal{R}_8 = \{a \rightarrow c, \ b \rightarrow c\} \)

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

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

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

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

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

Let
\[ l_1 \rightarrow r_1, \; l_2 \rightarrow r_2 \]
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 \( \theta \)

Then, the pair \( \langle (l_1 [u/r_2]) \theta, \; r_1 \theta \rangle \) is said to be critical

It is obtained by superimposing \( l_1 \) with \( l_2 \)

Superimposing \( (X \cdot Y) \cdot Z \rightarrow X \) with \( g(a) \cdot f(b) \rightarrow c \)
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 $s \rightarrow t$ or $t \rightarrow s$ to $\mathcal{R}$

▷ This is called completion

▷ The equational theory remains unchanged
Completion Procedure

- Given a terminating \( R \) together with a termination ordering \( \triangleright \)
  1. If for all critical pairs \( \langle s, t \rangle \) of \( R \) we find that \( s \downarrow_{R} t \)
     then return “success”; \( R \) is canonical
  2. If \( R \) 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 \( s \triangleright t \) then add the rule \( s \rightarrow t \) to \( R \) and goto 1
        - If \( t \triangleright s \) then add the rule \( t \rightarrow s \) to \( R \) and goto 1
        - If neither \( s \triangleright t \) nor \( t \triangleright s \) then return “fail”

- The completion procedure may either succeed or fail or loop
- During completion the ordering \( \triangleright \) may be extended to a more powerful one
- The completion procedure may be extended to unfailing completion
Completion: An Example

Consider

\[ R_{11} = \{ c \rightarrow b, f \rightarrow b, f \rightarrow a, e \rightarrow a, e \rightarrow d \} \]

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 \( b \rightarrow a \) and \( d \rightarrow a \)

We obtain

\[ R'_{11} = \{ c \rightarrow b, f \rightarrow b, f \rightarrow a, e \rightarrow a, e \rightarrow d, b \rightarrow a, d \rightarrow a \} \]

\( R'_{11} \) is canonical

\( s \approx_{E_R} t \) iff \( s \approx_{E_{R'}} t \)

All proofs for \( s \approx_{E_{R'_{11}}} t \) are in so-called valley form
Unification Theory

- **Idea** We want to build equational axioms into the unification computation

- **E-unification problem** consists of an equational theory $E$ and two terms $s$ and $t$, and is the question whether $E \cup E \models \exists s \approx t$ holds

  - A substitution $\theta$ is a solution of the $E$-unification problem iff $s\theta \approx E t\theta$
  
  - In this case $\theta$ is called $E$-unifier for $s$ and $t$
  
  - If $E = \emptyset$ then $E$-unification is unification

- Consider $E = \{f(X) \approx X\}$ and let $s = g(f(a), a)$ and $t = g(Y, Y)$.

  - $\{Y \mapsto a\}$ is an $E$-unifier for $s$ and $t$

  - The unification problem $\{s \approx t\}$ is unsolvable

- Substitutions $\eta$ and $\theta$ are $E$-equal on a set $\mathcal{V}$ of variables ($\theta \approx_E \eta[\mathcal{V}]$) iff $X\eta \approx_E X\theta$ for all $X \in \mathcal{V}$

  - Reconsider $E = \{f(X) \approx X\}$

  - $\{Y \mapsto a\}$ and $\{Y \mapsto f(a)\}$ are $E$-equal on $\{X, Y\}$
\(\varepsilon\)-Instances

- Substitution \(\eta\) is an \(\varepsilon\)-instance of \(\theta\) on a set \(\mathcal{V}\) of variables (\(\eta \leq_{\varepsilon} \theta[\mathcal{V}]\)) (or \(\theta\) is more general than \(\eta\) wrt \(\varepsilon\) and \(\mathcal{V}\)) iff there exists a substitution \(\tau\) such that \(X\eta \approx_{\varepsilon} X\theta\tau\) for all \(X \in \mathcal{V}\).

- \(\eta\) is a strict \(\varepsilon\)-instance of \(\theta\) (\(\eta <_{\varepsilon} \theta[\mathcal{V}]\)) iff \(\eta \leq_{\varepsilon} \theta[\mathcal{V}]\) and \(\eta \not\approx_{\varepsilon} \theta[\mathcal{V}]\).

- If neither \(\eta \leq_{\varepsilon} \theta[\mathcal{V}]\) nor \(\theta \leq_{\varepsilon} \eta[\mathcal{V}]\) then \(\theta\) and \(\eta\) 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

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

- $\mathcal{E} = \{f(X, Y) \approx f(Y, X)\}$
  - $\theta_1$ 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 \( \theta_3 = \{ X \mapsto f(g(a, b), g(a, b)), \ Y \mapsto a \} \)

\[
\begin{align*}
f(X, g(a, b))\theta_3 &= f(f(g(a, b), g(a, b)), g(a, b)) \\
&\approx_{\mathcal{E}} f(g(a, b), f(g(a, b), g(a, b))) \\
&= f(g(Y, b), X)\theta_3
\end{align*}
\]

- \( \theta_1 \) and \( \theta_3 \) 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 \( \theta_1 \) and \( \theta_3 \) 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 $S$ of $\mathcal{E}$-unifiers for $s$ and $t$
  - $S \subseteq \mathcal{U}_\mathcal{E}(s, t)$ and
  - for all $\eta \in \mathcal{U}_\mathcal{E}(s, t)$ there exists $\theta \in S$ such that $\eta \leq_\mathcal{E} \theta[\text{var}(s) \cup \text{var}(t)]$
- Minimal complete set $S$ of $\mathcal{E}$-unifiers for $s$ and $t$
  - complete set and
  - for all $\theta, \eta \in S$ we find $\eta \leq_\mathcal{E} \theta[\text{var}(s) \cup \text{var}(t)]$ implies $\theta = \eta$
- Complete sets of $\mathcal{E}$-unifiers for $s$ and $t$ are often denoted by $c\mathcal{U}_\mathcal{E}(s, t)$
- Minimal complete sets of $\mathcal{E}$-unifiers for $s$ and $t$ are often denoted by $\mu\mathcal{U}_\mathcal{E}(s, t)$
- 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 $\theta \equiv_\mathcal{E} \eta[\forall]$ iff $\eta \leq_\mathcal{E} \theta[\forall]$ and $\theta \leq_\mathcal{E} \eta[\forall]$
- $\mu\mathcal{U}_\mathcal{E}(s, t)$ is unique up to $\equiv_\mathcal{E} [\text{var}(s) \cup \text{var}(t)]$ 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 $\Rightarrow$ Exercise.
  - $\theta$ and $\eta$ 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 $\mathcal{R} = \{f(a, X) \rightarrow X, \ g(f(X, Y)) \rightarrow g(Y)\}$

**Claim** $\mu \mathcal{U}_{\mathcal{E}_{\mathcal{R}}} (g(X), g(a))$ does not exist

- $\mathcal{R}$ is canonical $\leadsto$ Exercise
- Define $\sigma_0 = \{X \mapsto a\}$
- $\sigma_1 = \{X \mapsto f(X_1, a)\} = \{X \mapsto f(X_1, X\sigma_0)\}$
- $\vdots$
- $\sigma_i = \{X \mapsto f(X_i, X\sigma_{i-1})\}$

- Let $S = \{\sigma_i \mid i \geq 0\}$
- $S$ is a $cU_{\mathcal{E}_{\mathcal{R}}} (g(X), g(a))$ $\leadsto$ 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 $\sigma_{i-1} \leq_{\mathcal{E}_{\mathcal{R}}} \sigma_i[\{X\}]$
Proof of Theorem 7 Continued

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

- The unification type of $E$ is
  - unitary iff a set $\mu U_E(s, t)$ exists for all $s, t$ and has cardinality 0 or 1
  - finitary iff a set $\mu U_E(s, t)$ exists for all $s, t$ and is finite
  - infinitary iff a set $\mu U_E(s, t)$ exists for all $s, t$, and there are $u$ and $v$ such that $\mu U_E(u, v)$ is infinite
  - zero iff there are $s, t$ such that $\mu U_E(s, t)$ does not exist
Unification procedures

- **ɛ-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 ɛ-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

<table>
<thead>
<tr>
<th>Equational System</th>
<th>Unification Type</th>
<th>Unification decidable?</th>
<th>Complexity of the decision problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{E}_A$</td>
<td>infinitary</td>
<td>yes</td>
<td>NP-hard</td>
</tr>
<tr>
<td>$\mathcal{E}_C$</td>
<td>finitary</td>
<td>yes</td>
<td>NP-complete</td>
</tr>
<tr>
<td>$\mathcal{E}_{AC}$</td>
<td>finitary</td>
<td>yes</td>
<td>NP-complete</td>
</tr>
<tr>
<td>$\mathcal{E}_{AG}$</td>
<td>unitary</td>
<td>yes</td>
<td>polynomial</td>
</tr>
<tr>
<td>$\mathcal{E}_{AI}$</td>
<td>zero</td>
<td>yes</td>
<td>NP-hard</td>
</tr>
<tr>
<td>$\mathcal{E}_{CR1}$</td>
<td>zero</td>
<td>no</td>
<td>–</td>
</tr>
<tr>
<td>$\mathcal{E}<em>{DL}$, $\mathcal{E}</em>{DR}$</td>
<td>unitary</td>
<td>yes</td>
<td>polynomial</td>
</tr>
<tr>
<td>$\mathcal{E}_D$</td>
<td>infinitary</td>
<td>no</td>
<td>NP-hard</td>
</tr>
<tr>
<td>$\mathcal{E}_{DA}$</td>
<td>infinitary</td>
<td>?</td>
<td>polynomial</td>
</tr>
<tr>
<td>$\mathcal{E}_{BR}$</td>
<td>unitary</td>
<td>yes</td>
<td>NP-complete</td>
</tr>
</tbody>
</table>
Additional Remarks

- **\( \mathcal{E} \)-matching problem**
  \[ \mathcal{E} \cup \mathcal{E} \models \exists \theta \ s \approx \_ \_ \_ \ t \theta \]

- **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** $s[u] \rightarrow_R t$ iff there are $l \rightarrow r \in R$ and $\theta$ such that $u = l\theta$ and $t = s[u/r\theta]$

► Now consider $\mathcal{E}_R \models \exists s \approx t$

▷ **Narrowing** $s[u] \Rightarrow_R t$ iff there are $l \rightarrow r \in R$ and $\theta$ such that $u\theta = l\theta$ and $t = (s[u/r])\theta$

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 $\text{var}(l) \supseteq \text{var}(r)$ 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

- \{e_1, e_2, \ldots \} \quad \text{or} \quad \emptyset

- X \in_k \mathcal{M} \quad \text{iff} \quad X \text{ occurs precisely } k \text{ times in } \mathcal{M}

- \mathcal{M}_1 \equiv \mathcal{M}_2 \quad \text{iff} \quad \text{for all } X \text{ we find } X \in_k \mathcal{M}_1 \text{ iff } X \in_k \mathcal{M}_2

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

- X \in_m \mathcal{M}_1 \setminus \mathcal{M}_2 \quad \text{iff} \quad \text{there exist } k, l \geq 0 \text{ such that }
  \begin{align*}
  & \text{either } X \in_k \mathcal{M}_1, X \in_l \mathcal{M}_2, k > l \text{ and } m = k - l \\
  & \text{or } X \in_k \mathcal{M}_1, X \in_l \mathcal{M}_2, k \leq l \text{ and } m = 0
  \end{align*}

- X \in_m \mathcal{M}_1 \cap \mathcal{M}_2 \quad \text{iff} \quad \text{there exist } k, l \geq 0 \text{ such that }
  \begin{align*}
  & X \in_k \mathcal{M}_1, X \in_l \mathcal{M}_2 \text{ and } m = \min\{k, l\}
  \end{align*}

- \mathcal{M}_1 \preceq \mathcal{M}_2 \quad \text{iff} \quad \mathcal{M}_1 \cap \mathcal{M}_2 \equiv \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 $\mathcal{E}_{AC1} = \{ X \circ (Y \circ Z) \approx (X \circ Y) \circ Z, X \circ Y \approx Y \circ X, X \circ 1 \approx X \}$
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
  - \( \cdot^\prime \) (from the set of fluent terms into the set of multisets of fluents)
    \[
    t^\prime = \begin{cases}
      \emptyset & \text{if } t = 1 \\
      \{ t \} & \text{if } t \text{ is a fluent} \\
      u^\prime \cup v^\prime & \text{if } t = u \circ v
    \end{cases}
    \]

  - \( \cdot^-\) (from the set of multisets of fluents into the set of fluent terms)
    \[
    \mathcal{M}^{-\prime} = \begin{cases}
      1 & \text{if } \mathcal{M} \models \emptyset \\
      s \circ \mathcal{N}^{-\prime} & \text{if } \mathcal{M} \models \{ s \} \cup \mathcal{N}
    \end{cases}
    \]
Matching and Unification Problems

► Submultiset matching problem
Does there exist a $\theta$ such that $M\theta \subseteq N$, where $N$ is ground?

► Submultiset unification problem
Does there exist a $\theta$ such that $M\theta \subseteq N\theta$?

► Fluent matching problem
Does there exist a $\theta$ 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 $\theta$ 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**
  \[(s \circ X)\theta \approx_{AC1} t \iff (s\theta)^I \subseteq t^I \text{ and } (X\theta)^I \doteq t^I \setminus (s\theta)^I\]

- **Equivalence of unification problems**
  \[(s \circ X)\theta \approx_{AC1} t\theta \iff (s\theta)^I \subseteq (t\theta)^I \text{ and } (X\theta)^I \doteq (t\theta)^I \setminus (s\theta)^I\]

- **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 $\exists \theta \ (s \circ X) \theta \approx_{AC1} t$?
(where $t$ is ground and $X$ does not occur in $s$)

Output: A solution $\theta$ of the fluent matching problem, if it is solvable;
        failure, otherwise

1. $\theta = \varepsilon$
2. if $s \approx_{AC1} 1$ then return $\theta \{ X \mapsto t \}$
3. don’t-care non-deterministically select a fluent $u$ from $s$ and remove $u$ from $s$
4. don’t-know non-deterministically select a fluent $v$ from $t$ such that
   there exists a substitution $\eta$ with $u\eta = v$
5. if such a fluent exists then apply $\eta$ to $s$, delete $v$ from $t$ and let $\theta := \theta\eta$,
     otherwise stop with failure
6. goto 2