LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Übung 3 – Konfluenz

Formale Techniken in der Software-Entwicklung

Christian Kroiß

Equational theory

Definition: Let E be a set of Σ-identities.

1. The identity $s \approx t$ is a **semantic consequence** of E ($E \models s \approx t$) iff it holds in all models of E.

2. The relation
$$\approx_E := \{(s,t) \in T(\Sigma,V) \times T(\Sigma,V) | E \models s \approx t\}$$
is called the **equational theory** induced by E.

But is $s \approx_E t$ decidable?

Theorem: If E is finite and $\rightarrow_E$ is convergent (confluent and terminating), then $\approx_E$ is decidable. (See [1])

- So we have to check whether $\rightarrow_E$ (and therefore our module) is terminating and confluent.

- Proving termination
  - Next lecture (at least a sketch)

Proving confluence:

- Confluence is decidable for a finite and terminating term rewriting system due to **the Critical Pair Theorem:**

A TRS is locally confluent iff all its critical pairs are joinable.

Unification is the process of solving the satisfiability problem:

given E, s and t, find a substitution σ such that $\sigma s \approx_E \sigma t$.

σ is called **unifier** of s and t or a solution of the equation $s =^? t$.

Unification

$f(x) =^? f(a)$ has exactly one unifier $\{x \mapsto a\}$.

$x =^? f(y)$ has many unifiers:
$\{x \mapsto f(y)\}, \{x \mapsto f(a), y \mapsto a\}, \dots$.

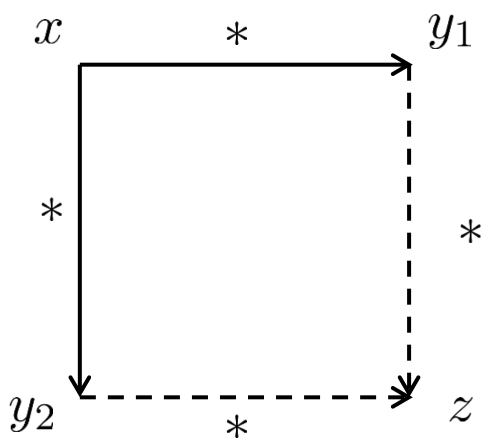
$f(x) =^? g(y)$ has no unifier.

$x =^? f(x)$ has no unifier.

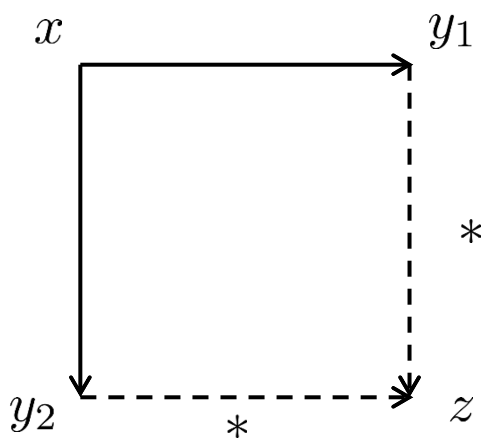
Most general unifier

A substitution σ is called the **most general unifier (mgu)** of E if for every other unifier σ' of E there is a substitution δ with

$$\sigma' = \delta\sigma \; .$$



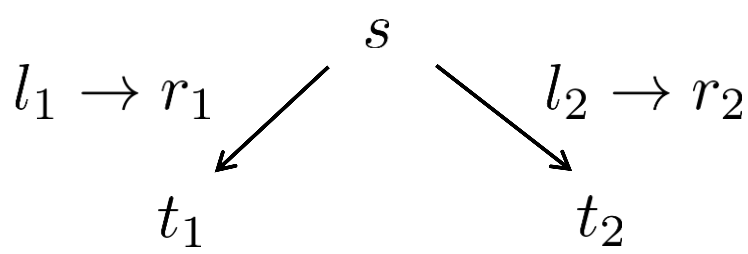
confluence



local confluence

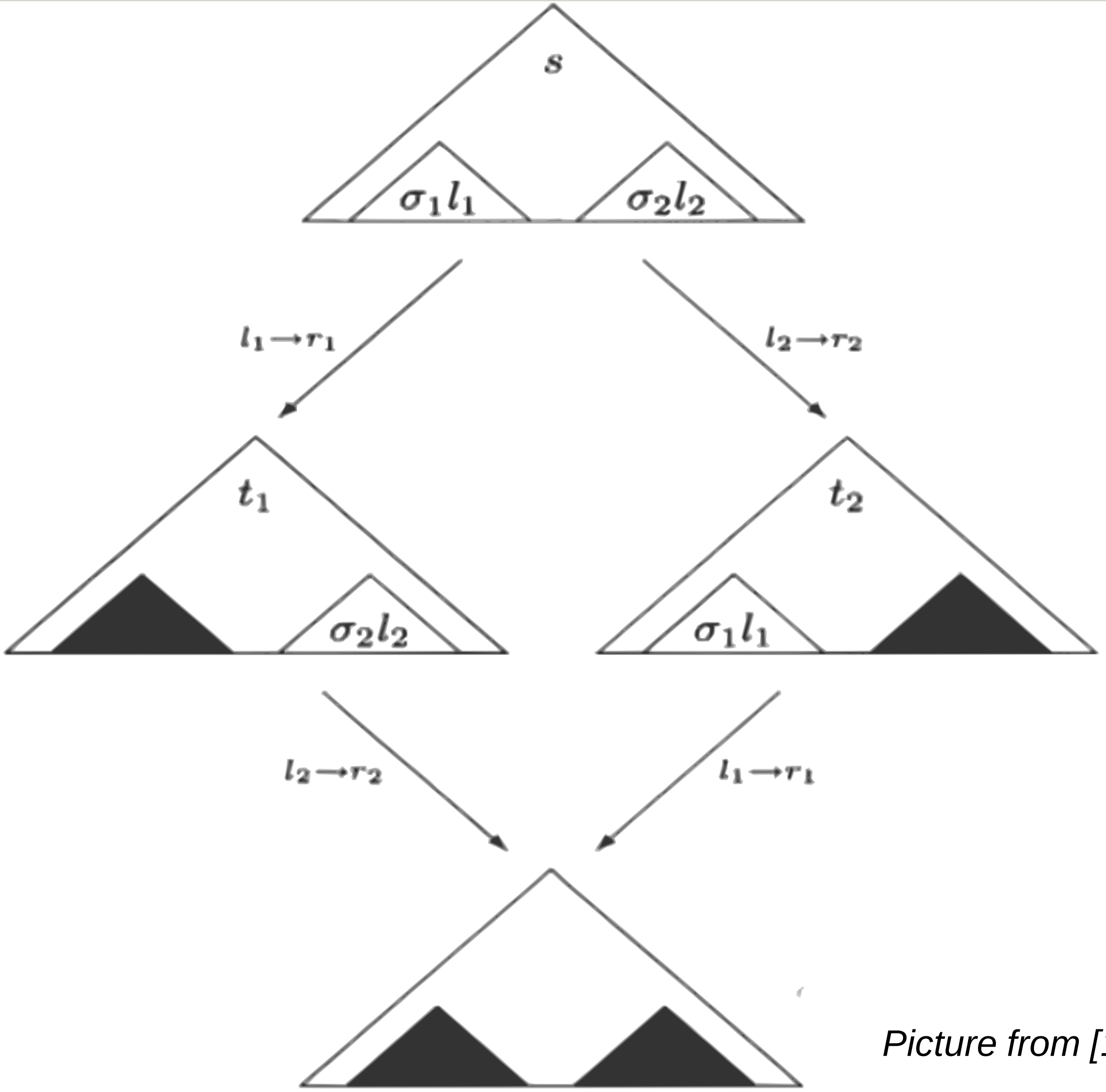
Newman's Lemma: a terminating relation is confluent if it is locally confluent.

Critical pairs



There are rules $l_i \to r_i \in R$, positions $p_i \in Pos(s)$ and substitutions σ_i such that $s|_{p_i} = \sigma_i l_i$ and $t_i = s[\sigma_i r_i]_{p_i}, i = 1, 2$.

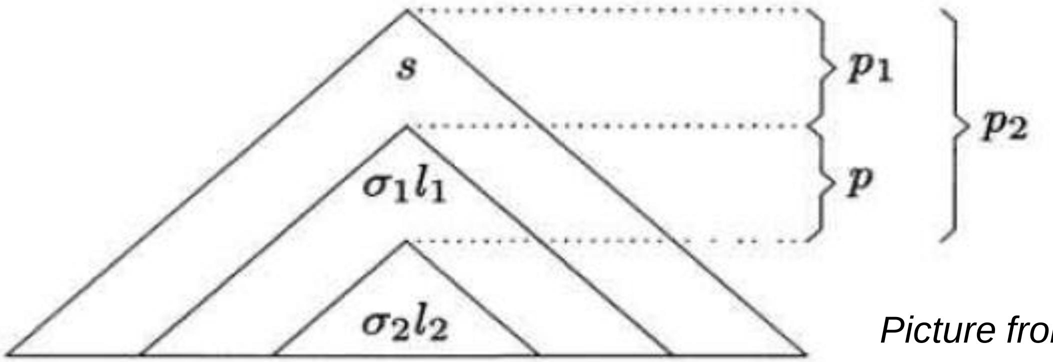
Critical pairs



No overlap

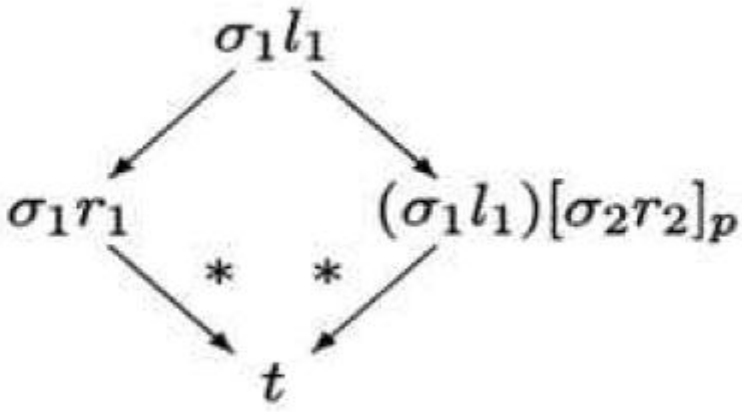
Picture from [1]

Critical pairs

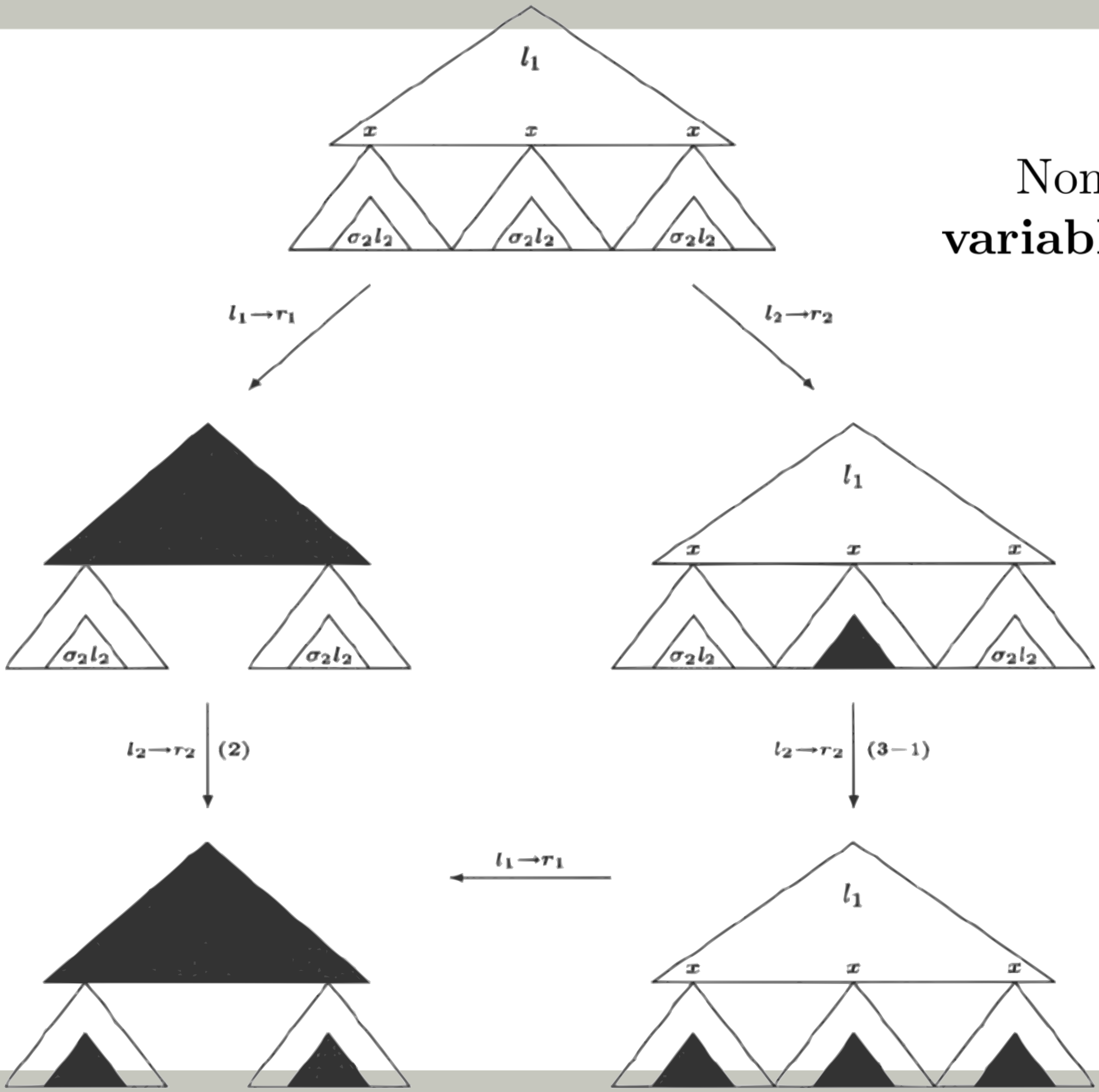


Picture from [1]

Overlap: p_1 is a prefix of p_2, i.e. $p_2 = p_1 p$ for some p which could be empty .



Critical pairs



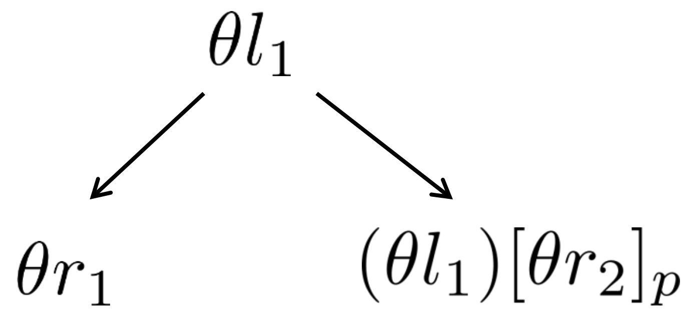
Non-critical overlap: $\sigma_2 l_2$ is at a **variable position** of l_1 .

Picture from [1]

Critical Pairs

Definition: Let $l_i \to r_i, i = 1, 2,$ be two rules whose variables have been renamed such that $Var(l_1, r_1) \cap Var(l_2, r_2) = \emptyset$.
Let $p \in Pos(l_1)$ be such that $l_1|_p$ is not a variable and let θ be an mgu of $l_1|_p =^? l_2$.

This determines a **critical pair** $\langle \theta r_1, (\theta l_1)[\theta r_2]_p \rangle$:



Critical Pair Lemma:

If $s \to_R t_i, i = 1, 2$, then $t_1 \downarrow t_2$ or $t_i = s[u_i]_p, i = 1, 2$, where $\langle u_1, u_2 \rangle$ or $\langle u_2, u_1 \rangle$ is an instance of a critical pair of R .

Critical pair theorem:
A TRS is locally confluent iff all its critical pairs are joinable.

➔ A terminating TRS is confluent iff all its critical pairs are joinable.

Example

(1) $f(f(x,y),z) \to f(x,f(y,z))$

(2) $f(i(x_1),x_1) \to e$

mgu: $\{x \mapsto i(x_1), y \mapsto x_1\}$

$$f(f(i(x_1),x_1),z)$$

$$\swarrow \qquad\qquad \searrow$$

$$f(i(x_1),f(x_1,z)) \qquad\qquad f(e,z)$$

References

[1] Baader, F., & Nipkow, T. (1999). Term rewriting and all that. Cambridge: Cambridge University Press.