4.5 Knuth-Bendix Completion

Completion:

Goal: Given a set E of equations, transform E into an equivalent convergent set R of rewrite rules.
(If R is finite: decision procedure for E.)

How to ensure termination?

Fix a reduction ordering $\succ$ and construct R in such a way that $\rightarrow_R \subseteq \succ$ (i. e., $l \succ r$ for every $l \rightarrow r \in R$).

How to ensure confluence?

Check that all critical pairs are joinable.

Knuth-Bendix Completion: Inference Rules

The completion procedure is itself presented as a set of rewrite rules working on a pair of equations E and rules R: $(E_0; R_0) \Rightarrow (E_1; R_1) \Rightarrow (E_2; R_2) \Rightarrow \ldots$

At the beginning, $E = E_0$ is the input set and $R = R_0$ is empty. At the end, E should be empty; then R is the result.

For each step $(E; R) \Rightarrow (E'; R')$, the equational theories of $E \cup R$ and $E' \cup R'$ agree: $\approx_{E \cup R} = \approx_{E' \cup R'}$.

Notations:

The formula $s \dot{\approx} t$ denotes either $s \approx t$ or $t \approx s$.

$\mathrm{CP}(R)$ denotes the set of all critical pairs between rules in R.

Orient

$$(E \uplus \{s \dot{\approx} t\}; R) \quad \Rightarrow_{KBC} \quad (E; R \cup \{s \rightarrow t\})$$

if $s \succ t$

Note: There are equations $s \approx t$ that cannot be oriented, i. e., neither $s \succ t$ nor $t \succ s$.

Trivial equations cannot be oriented – but we don't need them anyway:

Delete

$$(E \uplus \{s \approx s\}; R) \quad \Rightarrow_{KBC} \quad (E; R)$$

Critical pairs between rules in R are turned into additional equations:

Deduce

$$(E; R) \quad \Rightarrow_{KBC} \quad (E \cup \{s \approx t\}; R)$$

if $\langle s, t\rangle \in \mathrm{CP}(R)$

Note: If $\langle s, t\rangle \in \mathrm{CP}(R)$ then $s \; {}_R\!\leftarrow u \rightarrow_R t$ and hence $R \models s \approx t$.

The following inference rules are not absolutely necessary, but very useful (e. g., to get rid of joinable critical pairs and to deal with equations that cannot be oriented):

Simplify-Eq

$$(E \uplus \{s \dot{\approx} t\}; R) \quad \Rightarrow_{KBC} \quad (E \cup \{u \approx t\}; R)$$

if $s \rightarrow_R u$

Simplification of the right-hand side of a rule is unproblematic.

R-Simplify-Rule

$$(E; R \uplus \{s \rightarrow t\}) \quad \Rightarrow_{KBC} \quad (E; R \cup \{s \rightarrow u\})$$

if $t \rightarrow_R u$

Simplification of the left-hand side may influence orientability and orientation. Therefore, it yields an *equation*:

L-Simplify-Rule

$$(E; R \uplus \{s \rightarrow t\}) \quad \Rightarrow_{KBC} \quad (E \cup \{u \approx t\}; R$$

if $s \rightarrow_R u$ using a rule $l \rightarrow r \in R$ such that $s \sqsupset l$ (see next slide).

For technical reasons, the lhs of $s \rightarrow t$ may only be simplified using a rule $l \rightarrow r$, if $l \rightarrow r$ *cannot* be simplified using $s \rightarrow t$, that is, if $s \sqsupset l$, where the *encompassment quasi-ordering* $\underset{\sim}{\sqsupset}$ is defined by

$$s \underset{\sim}{\sqsupset} l \;\text{ if }\; s|_p = l\sigma \text{ for some } p \text{ and } \sigma$$

and $\sqsupset = \underset{\sim}{\sqsupset} \setminus \underset{\sim}{\sqsubset}$ is the strict part of $\underset{\sim}{\sqsupset}$.

Lemma 4.27 $\sqsupset$ *is a well-founded strict partial ordering.*

Lemma 4.28 *If* $(E; R) \Rightarrow_{KBC} (E'; R')$, *then* $\approx_{E \cup R} = \approx_{E' \cup R'}$.

Lemma 4.29 *If* $(E; R) \Rightarrow_{KBC} (E'; R')$ *and* $\rightarrow_R \subseteq \succ$, *then* $\rightarrow_{R'} \subseteq \succ$.

Knuth-Bendix Completion: Correctness Proof

If we run the completion procedure on a set E of equations, different things can happen:

(1) We reach a state where no more inference rules are applicable and E is not empty. $\Rightarrow$ Failure (try again with another ordering?)

(2) We reach a state where E is empty and all critical pairs between the rules in the current R have been checked.

(3) The procedure runs forever.

In order to treat these cases simultaneously, we need some definitions.

A (finite or infinite sequence) $(E_0; R_0) \Rightarrow_{KBC} (E_1; R_1) \Rightarrow_{KBC} (E_2; R_2) \Rightarrow_{KBC} \ldots$ with $R_0 = \emptyset$ is called a *run* of the completion procedure with input E_0 and $\succ$.

For a run, $E_\infty = \bigcup_{i \geq 0} E_i$ and $R_\infty = \bigcup_{i \geq 0} R_i$.

The sets of *persistent equations or rules* of the run are $E_* = \bigcup_{i \geq 0} \bigcap_{j \geq i} E_j$ and $R_* = \bigcup_{i \geq 0} \bigcap_{j \geq i} R_j$.

Note: If the run is finite and ends with E_n, R_n, then $E_* = E_n$ and $R_* = R_n$.

A run is called *fair*, if $CP(R_*) \subseteq E_\infty$ (i. e., if every critical pair between persisting rules is computed at some step of the derivation).

Goal:

Show: If a run is fair and E_* is empty, then R_* is convergent and equivalent to E_0.

In particular: If a run is fair and E_* is empty, then $\approx_{E_0} = \approx_{E_\infty \cup R_\infty} = \leftrightarrow^*_{E_\infty \cup R_\infty} = \downarrow_{R_*}$.

General assumptions from now on:

$(E_0; R_0) \Rightarrow_{KBC} (E_1; R_1) \Rightarrow_{KBC} (E_2; R_2) \Rightarrow_{KBC} \ldots$
is a fair run.

R_0 and E_* are empty.

A *proof* of $s \approx t$ in $E_\infty \cup R_\infty$ is a finite sequence $(s_0, \dots, s_n)$ such that $s = s_0$, $t = s_n$, and for all $i \in \{1, \dots, n\}$:

(1) $s_{i-1} \leftrightarrow_{E_\infty} s_i$, or

(2) $s_{i-1} \rightarrow_{R_\infty} s_i$, or

(3) $s_{i-1} \;{}_{R_\infty}\!\!\leftarrow s_i$.

The pairs (s_{i-1}, s_i) are called *proof steps.*

A proof is called a *rewrite proof in* R_*, if there is a $k \in \{0, \dots, n\}$ such that $s_{i-1} \rightarrow_{R_*} s_i$ for $1 \leq i \leq k$ and $s_{i-1} \;{}_{R_*}\!\!\leftarrow s_i$ for $k+1 \leq i \leq n$

Idea (Bachmair, Dershowitz, Hsiang):

Define a well-founded ordering on proofs, such that for every proof that is not a rewrite proof in R_* there is an equivalent smaller proof.

Consequence: For every proof there is an equivalent rewrite proof in R_*.

We associate a *cost* $c(s_{i-1}, s_i)$ with every proof step as follows:

(1) If $s_{i-1} \leftrightarrow_{E_\infty} s_i$, then $c(s_{i-1}, s_i) = (\{s_{i-1}, s_i\}, -, -)$, where the first component is a multiset of terms and $-$ denotes an arbitrary (irrelevant) term.

(2) If $s_{i-1} \rightarrow_{R_\infty} s_i$ using $l \rightarrow r$, then $c(s_{i-1}, s_i) = (\{s_{i-1}\}, l, s_i)$.

(3) If $s_{i-1} \;{}_{R_\infty}\!\!\leftarrow s_i$ using $l \rightarrow r$, then $c(s_{i-1}, s_i) = (\{s_i\}, l, s_{i-1})$.

Proof steps are compared using the lexicographic combination of the multiset extension of the reduction ordering $\succ$, the encompassment ordering $\sqsupset$, and the reduction ordering $\succ$.

The cost $c(P)$ of a proof P is the multiset of the costs of its proof steps.

The *proof ordering* $\succ_C$ compares the costs of proofs using the multiset extension of the proof step ordering.

Lemma 4.30 $\succ_C$ *is a well-founded ordering.*

Lemma 4.31 *Let P be a proof in $E_\infty \cup R_\infty$. If P is not a rewrite proof in R_*, then there exists an equivalent proof P' in $E_\infty \cup R_\infty$ such that $P \succ_C P'$.*

Proof. If P is not a rewrite proof in R_*, then it contains

(a) a proof step that is in E_∞, or
(b) a proof step that is in $R_\infty \setminus R_*$, or
(c) a subproof $s_{i-1} \;{}_{R_*}\!\!\leftarrow s_i \rightarrow_{R_*} s_{i+1}$ (peak).

We show that in all three cases the proof step or subproof can be replaced by a smaller subproof:

Case (a): A proof step using an equation $s \doteq t$ is in E_∞. This equation must be deleted during the run.

If $s \approx t$ is deleted using *Orient*:
$\dots s_{i-1} \leftrightarrow_{E_\infty} s_i \dots \quad \Longrightarrow \quad \dots s_{i-1} \rightarrow_{R_\infty} s_i \dots$

If $s \approx t$ is deleted using *Delete*:
$\dots s_{i-1} \leftrightarrow_{E_\infty} s_{i-1} \dots \quad \Longrightarrow \quad \dots s_{i-1} \dots$

If $s \approx t$ is deleted using *Simplify-Eq*:
$\dots s_{i-1} \leftrightarrow_{E_\infty} s_i \dots \quad \Longrightarrow \quad \dots s_{i-1} \rightarrow_{R_\infty} s' \leftrightarrow_{E_\infty} s_i \dots$

Case (b): A proof step using a rule $s \rightarrow t$ is in $R_\infty \setminus R_*$. This rule must be deleted during the run.

If $s \rightarrow t$ is deleted using *R-Simplify-Rule*:
$\dots s_{i-1} \rightarrow_{R_\infty} s_i \dots \quad \Longrightarrow \quad \dots s_{i-1} \rightarrow_{R_\infty} s' \;{}_{R_\infty}\!\!\leftarrow s_i \dots$

If $s \rightarrow t$ is deleted using *L-Simplify-Rule*:
$\dots s_{i-1} \rightarrow_{R_\infty} s_i \dots \quad \Longrightarrow \quad \dots s_{i-1} \rightarrow_{R_\infty} s' \leftrightarrow_{E_\infty} s_i \dots$

Case (c): A subproof has the form $s_{i-1} \;{}_{R_*}\!\!\leftarrow s_i \rightarrow_{R_*} s_{i+1}$.

If there is no overlap or a non-critical overlap:
$\dots s_{i-1} \;{}_{R_*}\!\!\leftarrow s_i \rightarrow_{R_*} s_{i+1} \dots \quad \Longrightarrow \quad \dots s_{i-1} \rightarrow^*_{R_*} s' \;{}^{*}_{R_*}\!\!\leftarrow s_{i+1} \dots$

If there is a critical pair that has been added using *Deduce*:
$\dots s_{i-1} \;{}_{R_*}\!\!\leftarrow s_i \rightarrow_{R_*} s_{i+1} \dots \quad \Longrightarrow \quad \dots s_{i-1} \leftrightarrow_{E_\infty} s_{i+1} \dots$

In all cases, checking that the replacement subproof is smaller than the replaced subproof is routine. □

Theorem 4.32 *Let* $(E_0; R_0) \Rightarrow_{KBC} (E_1; R_1) \Rightarrow_{KBC} (E_2; R_2) \Rightarrow_{KBC} \ldots$ *be a fair run and let* R_0 *and* E_* *be empty. Then*

(1) *every proof in* $E_\infty \cup R_\infty$ *is equivalent to a rewrite proof in* R_**,*

(2) R_* *is equivalent to* E_0*, and*

(3) R_* *is convergent.*

Proof. (1) By well-founded induction on $\succ_C$ using the previous lemma.

(2) Clearly $\approx_{E_\infty \cup R_\infty} = \approx_{E_0}$. Since $R_* \subseteq R_\infty$, we get $\approx_{R_*} \subseteq \approx_{E_\infty \cup R_\infty}$. On the other hand, by (1), $\approx_{E_\infty \cup R_\infty} \subseteq \approx_{R_*}$.

(3) Since $\rightarrow_{R_*} \subseteq \succ$, R_* is terminating. By (1), R_* is confluent. □

4.6 Unfailing Completion

Classical completion:

Try to transform a set E of equations into an equivalent convergent TRS.

Fail, if an equation can neither be oriented nor deleted.

Unfailing completion (Bachmair, Dershowitz and Plaisted):

If an equation cannot be oriented, we can still use *orientable instances* for rewriting.

Note: If $\succ$ is total on ground terms, then every *ground instance* of an equation is trivial or can be oriented.

Goal: Derive a *ground convergent* set of equations.

Let E be a set of equations, let $\succ$ be a reduction ordering.

We define the relation $\rightarrow_{E^\succ}$ by

$$s \rightarrow_{E^\succ} t \quad \text{iff} \quad \begin{array}{l} \text{there exist } (u \approx v) \in E \text{ or } (v \approx u) \in E, \\ p \in \mathrm{pos}(s), \text{ and } \sigma : X \rightarrow \mathrm{T}_\Sigma(X), \\ \text{such that } s|_p = u\sigma \text{ and } t = s[v\sigma]_p \textit{ and } u\sigma \succ v\sigma. \end{array}$$

Note: $\rightarrow_{E^\succ}$ is terminating by construction.

From now on let $\succ$ be a reduction ordering that is total on ground terms.

E is called ground convergent w. r. t. $\succ$, if for all ground terms s and t with $s \leftrightarrow_E^* t$ there exists a ground term v such that $s \rightarrow_{E^\succ}^* v \; {}_{E^\succ}^{*}\!\!\leftarrow t$. (Analogously for $E \cup R$.)

As for standard completion, we establish ground convergence by computing critical pairs.

However, the ordering $\succ$ is not total on non-ground terms. Since $s\theta \succ t\theta$ implies $s \not\preceq t$, we approximate $\succ$ on ground terms by $\not\preceq$ on arbitrary terms.

Let $u_i \mathrel{\dot\approx} v_i$ $(i = 1, 2)$ be equations in E whose variables have been renamed such that $\mathrm{vars}(u_1 \mathrel{\dot\approx} v_1) \cap \mathrm{vars}(u_2 \mathrel{\dot\approx} v_2) = \emptyset$. Let $p \in \mathrm{pos}(u_1)$ be a position such that $u_1|_p$ is not a variable, σ is an mgu of $u_1|_p$ and u_2, and $u_i\sigma \not\preceq v_i\sigma$ $(i = 1, 2)$. Then $\langle v_1\sigma, (u_1\sigma)[v_2\sigma]_p\rangle$ is called a *semi-critical pair* of E with respect to $\succ$.

The set of all semi-critical pairs of E is denoted by $\mathrm{SP}_\succ(E)$.

Semi-critical pairs of $E \cup R$ are defined analogously. If $\rightarrow_R \subseteq \succ$, then $\mathrm{CP}(R)$ and $\mathrm{SP}_\succ(R)$ agree.

Note: In contrast to critical pairs, it may be necessary to consider overlaps of a rule with itself at the top. For instance, if $E = \{f(x) \approx g(y)\}$, then $\langle g(y), g(y')\rangle$ is a non-trivial semi-critical pair.

The *Deduce* rule takes now the following form:

Deduce

$(E; R) \quad \Rightarrow_{UKBC} \quad (E \cup \{s \approx t\}; R)$

if $\langle s, t\rangle \in \mathrm{SP}_{\succ}(E \cup R)$

The other rules are inherited from $\Rightarrow_{KBC}$. The fairness criterion for runs is replaced by

$$\mathrm{SP}_{\succ}(E_* \cup R_*) \subseteq E_\infty$$

(i. e., if every semi-critical pair between persisting rules or equations is computed at some step of the derivation).

Analogously to Thm. 4.32 we obtain now the following theorem:

Theorem 4.33 *Let $(E_0; R_0) \Rightarrow_{UKBC} (E_1; R_1) \Rightarrow_{UKBC} (E_2; R_2) \Rightarrow_{UKBC} \dots$ be a fair run; let $R_0 = \emptyset$. Then*

(1) $E_* \cup R_*$ is equivalent to E_0, and

(2) $E_* \cup R_*$ is ground convergent.

Moreover one can show that, whenever there exists a *reduced* convergent R such that $\approx_{E_0} = {\downarrow_R}$ and $\rightarrow_R \in \succ$, then for every fair *and simplifying* run $E_* = \emptyset$ and $R_* = R$ up to variable renaming.

Here R is called reduced, if for every $l \rightarrow r \in R$, both l and r are irreducible w. r. t. $R \setminus \{l \rightarrow r\}$. A run is called simplifying, if R_* is reduced, and for all equations $u \approx v \in E_*$, u and v are incomparable w. r. t. $\succ$ and irreducible w. r. t. R_*.

Unfailing completion is refutationally complete for equational theories:

Theorem 4.34 *Let E be a set of equations, let $\succ$ be a reduction ordering that is total on ground terms. For any two terms s and t, let $\hat{s}$ and $\hat{t}$ be the terms obtained from s and t by replacing all variables by Skolem constants. Let $eq/2$, $true/0$ and $false/0$ be new operator symbols, such that $true$ and $false$ are smaller than all other terms. Let $E_0 = E \cup \{eq(\hat{s}, \hat{t}) \approx true,\ eq(x, x) \approx false\}$. If $(E_0; \emptyset) \Rightarrow_{UKBC} (E_1; R_1) \Rightarrow_{UKBC} (E_2; R_2) \Rightarrow_{UKBC} \dots$ be a fair run of unfailing completion, then $s \approx_E t$ iff some $E_i \cup R_i$ contains $true \approx false$.*

Outlook:

Combine ordered resolution and unfailing completion to get a calculus for equational clauses:

compute inferences between (strictly) maximal literals as in ordered resolution,
compute overlaps between maximal sides of equations as in unfailing completion

$\Rightarrow$ Superposition calculus.