Automated Theorem Proving

Lecture 11: Completion

Prof. Dr. Jasmin Blanchette

based on slides by Dr. Uwe Waldmann

Winter Term 2024/25

4.6 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.)

Knuth–Bendix Completion: Idea

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.

Note: Every critical pair $\langle s, t \rangle$ can be *made* joinable by adding $s \rightarrow t$ or $t \rightarrow s$ to R.

(Actually, we first add $s \approx t$ to E and later try to turn it into a rule that is contained in $\succ$; this gives us more freedom.)

Knuth–Bendix Completion: Inference Rules

The completion procedure is presented as a set of inference rules working on a set of equations E and a set of rules R:
$E_0, R_0 \vdash E_1, R_1 \vdash E_2, R_2 \vdash \cdots$.

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 $E, R \vdash E', R'$, the equational theories of $E \cup R$ and $E' \cup R'$ agree: $\approx_{E \cup R} = \approx_{E' \cup R'}$.

Knuth–Bendix Completion: Inference Rules

Notations:

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

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

Knuth–Bendix Completion: Inference Rules

Orient:

$$\frac{E \cup \{s \,\dot{\approx}\, t\}, \quad R}{E, \quad R \cup \{s \to t\}} \qquad \text{if } s \succ t$$

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

Knuth–Bendix Completion: Inference Rules

Trivial equations cannot be oriented—but we do not need them anyway:

Delete:

$$\frac{E \cup \{s \approx s\}, \quad R}{E, \quad R}$$

Knuth–Bendix Completion: Inference Rules

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

Deduce:

$$\frac{E, \quad R}{E \cup \{s \approx t\}, \quad R} \qquad \text{if } \langle s, t\rangle \in \mathrm{CP}(R).$$

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

Knuth–Bendix Completion: Inference Rules

The following inference rules are not strictly necessary, but are very useful (e.g., to eliminate joinable critical pairs and to cope with equations that cannot be oriented):

Simplify-Eq:

$$\frac{E \cup \{s \mathrel{\dot{\approx}} t\}, \quad R}{E \cup \{u \approx t\}, \quad R} \qquad \text{if } s \to_R u.$$

Knuth–Bendix Completion: Inference Rules

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

R-Simplify-Rule:

$$\frac{E, \quad R \cup \{s \to t\}}{E, \quad R \cup \{s \to u\}} \qquad \text{if } t \to_R u.$$

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

L-Simplify-Rule:

$$\frac{E, \quad R \cup \{s \to t\}}{E \cup \{u \approx t\}, \quad R} \qquad \begin{array}{l}\text{if } s \to_R u \text{ using a rule } l \to r \in R \\ \text{such that } s \sqsupset l \text{ (see next slide).}\end{array}$$

Knuth–Bendix Completion: Inference Rules

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 $\sqsupseteq$ is defined by

$$s \sqsupseteq l \quad \text{if} \quad s|_p = l\sigma \text{ for some } p \text{ and } \sigma$$

and $\sqsupset \, = \, \sqsupseteq \setminus \sqsubseteq$ is the strict part of $\sqsupseteq$.

Lemma 4.6.1:

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

Knuth–Bendix Completion: Inference Rules

Lemma 4.6.2:
If $E, R \vdash E', R'$, then $\approx_{E \cup R} = \approx_{E' \cup R'}$.

Lemma 4.6.3:
If $E, R \vdash E', R'$ and $\rightarrow_R \subseteq \succ$, then $\rightarrow_{R'} \subseteq \succ$.

Knuth–Bendix Completion: Inference Rules

Note: Like in ordered resolution, simplification should be preferred to deduction:

- Simplify/delete whenever possible.
- Otherwise, orient an equation if possible.
- Last resort: compute critical pairs.

Knuth–Bendix Completion: Example

We apply the Knuth–Bendix procedure to the set of equations

$$add(zero, zero) \approx zero \quad (1) \qquad add(x, succ(y)) \approx succ(add(x, y)) \quad (2)$$

$$add(succ(x), y) \approx succ(add(x, y)) \quad (3)$$

using the lpo with the precedence $add \succ succ \succ zero$.

We first apply "Orient" to (1)–(3), resulting in the rewrite rules

$$add(zero, zero) \rightarrow zero \quad (4) \qquad add(x, succ(y)) \rightarrow succ(add(x, y)) \quad (5)$$

$$add(succ(x), y) \rightarrow succ(add(x, y)) \quad (6)$$

Knuth–Bendix Completion: Example

$$add(zero, zero) \to zero \quad (4) \qquad add(x, succ(y)) \to succ(add(x, y)) \quad (5)$$
$$add(succ(x), y) \to succ(add(x, y)) \quad (6)$$

Then we apply "Deduce" between (5) and a renamed copy of (6):

$$succ(add(succ(x), y)) \approx succ(add(x, succ(y))) \quad (7)$$

We can now apply "Simplify-Eq" to both sides of (7) using (6) and (5):

$$succ(succ(add(x, y))) \approx succ(succ(add(x, y))) \quad (8)$$

This last equation is trivial and can be deleted using "Delete."

All critical pairs have been checked.
The resulting term rewrite system is $\{(4), (5), (6)\}$.

Knuth–Bendix Completion: Correctness Proof

What can happen if we run the completion procedure on a set E of equations?

(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.

To treat these cases simultaneously, we need some definitions.

Knuth–Bendix Completion: Correctness Proof

A (finite or infinite sequence) $E_0, R_0 \vdash E_1, R_1 \vdash E_2, R_2 \vdash \cdots$ with $R_0 = \emptyset$ is called a run of the completion procedure with input E_0 and $\succ$.

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

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

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

Knuth–Bendix Completion: Correctness Proof

A run is called fair if $CP(R_\infty) \subseteq E_\cup$
(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 $\approx_{E_0} = \approx_{E_\cup \cup R_\cup} = \leftrightarrow^*_{E_\cup \cup R_\cup} = \downarrow_{R_\infty}$.

Knuth–Bendix Completion: Correctness Proof

General assumptions from now on:

$E_0, R_0 \vdash E_1, R_1 \vdash E_2, R_2 \vdash \cdots$ is a fair run.

R_0 and E_∞ are empty.

Knuth–Bendix Completion: Correctness Proof

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

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

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

(3) $s_{i-1} \leftarrow_{R_\cup} s_i$.

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

A proof is called a rewrite proof in R_∞
if there is a $k \in \{0, \ldots, n\}$ such that $s_{i-1} \rightarrow_{R_\infty} s_i$ for $1 \leq i \leq k$
and $s_{i-1} \leftarrow_{R_\infty} s_i$ for $k+1 \leq i \leq n$

Knuth–Bendix Completion: Correctness Proof

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_∞.

Knuth–Bendix Completion: Correctness Proof

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

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

(3) If $s_{i-1} \leftarrow_{R_\cup} s_i$ 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 $\succ$.

Knuth–Bendix Completion: Correctness Proof

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 4.6.4:
$\succ_C$ is a well-founded ordering.

Knuth–Bendix Completion: Correctness Proof

Lemma 4.6.5:
Let P be a proof in $E_\cup \cup R_\cup$. If P is not a rewrite proof in R_∞, then there exists an equivalent proof P' in $E_\cup \cup R_\cup$ such that $P \succ_\mathrm{c} P'$.

Proof:
If P is not a rewrite proof in R_∞, then it contains

(a) a proof step that is in $E_\cup$, or
(b) a proof step that is in $R_\cup \setminus R_\infty$, or
(c) a subproof $s_{i-1} \leftarrow_{R_\infty} s_i \rightarrow_{R_\infty} s_{i+1}$ (peak).

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

Knuth–Bendix Completion: Correctness Proof

Case (a): A proof step using an equation $s \mathrel{\dot{\approx}} t$ is in $E_\cup$.
This equation must be deleted during the run.

If $s \mathrel{\dot{\approx}} t$ is deleted using *Orient*:

$$\dots s_{i-1} \leftrightarrow_{E_\cup} s_i \dots \qquad \Longrightarrow \qquad \dots s_{i-1} \rightarrow_{R_\cup} s_i \dots$$

If $s \mathrel{\dot{\approx}} t$ is deleted using *Delete*:

$$\dots s_{i-1} \leftrightarrow_{E_\cup} s_{i-1} \dots \qquad \Longrightarrow \qquad \dots s_{i-1} \dots$$

If $s \mathrel{\dot{\approx}} t$ is deleted using *Simplify-Eq*:

$$\dots s_{i-1} \leftrightarrow_{E_\cup} s_i \dots \qquad \Longrightarrow \qquad \dots s_{i-1} \rightarrow_{R_\cup} s' \leftrightarrow_{E_\cup} s_i \dots$$

Knuth–Bendix Completion: Correctness Proof

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

If $s \rightarrow t$ is deleted using *R-Simplify-Rule*:

$$\ldots s_{i-1} \rightarrow_{R_\cup} s_i \ldots \quad \Longrightarrow \quad \ldots s_{i-1} \rightarrow_{R_\cup} s' \leftarrow_{R_\cup} s_i \ldots$$

If $s \rightarrow t$ is deleted using *L-Simplify-Rule*:

$$\ldots s_{i-1} \rightarrow_{R_\cup} s_i \ldots \quad \Longrightarrow \quad \ldots s_{i-1} \rightarrow_{R_\cup} s' \leftrightarrow_{E_\cup} s_i \ldots$$

Knuth–Bendix Completion: Correctness Proof

Case (c): A subproof has the form $s_{i-1} \leftarrow_{R_\infty} s_i \rightarrow_{R_\infty} s_{i+1}$.

If there is no overlap or a noncritical overlap:

$$\ldots s_{i-1} \leftarrow_{R_\infty} s_i \rightarrow_{R_\infty} s_{i+1} \ldots \implies \ldots s_{i-1} \rightarrow^*_{R_\infty} s' \leftarrow^*_{R_\infty} s_{i+1} \ldots$$

If there is a critical pair that has been added using “Deduce”:

$$\ldots s_{i-1} \leftarrow_{R_\infty} s_i \rightarrow_{R_\infty} s_{i+1} \ldots \implies \qquad \ldots s_{i-1} \leftrightarrow_{E_\cup} s_{i+1} \ldots$$

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

Knuth–Bendix Completion: Correctness Proof

Theorem 4.6.6:
Let $E_0, R_0 \vdash E_1, R_1 \vdash E_2, R_2 \vdash \cdots$ be a fair run and let R_0 and E_∞ be empty. Then

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

(2) R_∞ is equivalent to E_0, and

(3) R_∞ is convergent.

Knuth–Bendix Completion: Correctness Proof

Proof:

(1) By well-founded induction on $\succ_{\mathrm{C}}$ using the previous lemma.

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

(3) Since $\to_{R_\infty} \subseteq \succ$, R_∞ is terminating.
By (1), R_∞ is confluent. $\square$

4.7 Unfailing Completion

Classical completion:

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

Fail if an equation can be neither 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.

Unfailing Completion

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

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

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

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

Unfailing Completion

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 $s \rightarrow_{E^\succ}^* v \leftarrow_{E^\succ}^* t$.

(Analogously for $E \cup R$.)

Unfailing Completion

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

However, the ordering $\succ$ is not total on nonground terms.

Since $s\theta \succ t\theta$ implies $s \not\preceq t$, we approximate $\succ$ on ground terms by $\not\preceq$ on arbitrary terms.

Unfailing Completion

Let $u_i \mathrel{\dot{\approx}} v_i$ $(i = 1, 2)$ be equations in E whose variables have been renamed such that $\mathrm{var}(u_1 \mathrel{\dot{\approx}} v_1) \cap \mathrm{var}(u_2 \mathrel{\dot{\approx}} v_2) = \emptyset$.
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 semicritical pair of E with respect to $\succ$.

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

Semicritical pairs of $E \cup R$ are defined analogously.

Unfailing Completion

Note: In contrast to critical pairs, it may be necessary to consider overlaps of an equation with itself at the top.

For instance, if $E = \{f(x) \approx g(y)\}$, then $\langle g(y), g(y') \rangle$ is a semicritical pair.

Unfailing Completion

The "Deduce" rule now takes the following form:

Deduce:

$$\frac{E, \quad R}{E \cup \{s \approx t\}, \quad R} \qquad \text{if } \langle s, t \rangle \in \mathrm{SP}_{\succ}(E \cup R).$$

Moreover, the fairness criterion for runs is replaced by

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

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

Unfailing Completion

Unfailing completion is refutationally complete for equational theories:

Theorem 4.7.1:
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 $E_0, \emptyset \vdash E_1, R_1 \vdash E_2, R_2 \vdash \cdots$ is a fair run of unfailing completion, then $s \approx_E t$ if and only if some $E_i \cup R_i$ contains $true \approx false$.

Unfailing Completion

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.