A complete tour of completion algorithms

Jean-Pierre Jouannaud
INRIA-LIAMA and Tsinghua Software Chair, Beijing

Symposium in honour of
Pierre-Louis Curien
September 10, 2013

Joint ideas with
Pierre-Louis Curien, PPS
and
Lihong Zhi, AMSS, Beijing
Thanks to
Pierluigi Curioso
for being here.
Ciao Pierluigi
buon compleanno !
Outline

1. Membership Problem
2. Canonical bases
3. Completion methods
4. Conclusion
1. Membership Problem
2. Canonical bases
3. Completion methods
4. Conclusion
1. Membership Problem

2. Canonical bases

3. Completion methods

4. Conclusion
Completion is an algorithm aiming at

- (semi)-decide membership to an equational theory (mkbTT)
- decide membership to a polynomial ideal (Mathematica)
- analyze singularities of a surface at a point (Mapple)
- Solve linear partial differential equations (Numerica)
- explain existing decidability results e.g., Shostak’s combination of decision procedures
- combine several theories together e.g., Toyama’s modular confluence result
- solve equations in complex theories by narrowing
- attack security protocols (CASRUL)
- compute non-linear invariants for numeric programs
- Infer types for functional programming languages
- etc.
**Equations** are pairs of terms written as \( s = t \). An equation is **ground** if \( s, t \) are ground terms.

Given a set of equations \( E := \{ s_i = t_i \} \) the *equational theory* \( =_E \) is reflexive, symmetric, transitive closure of replacement of equals by equals.

**Fact:** Membership to an equational theory is undecidable.
Let $A$ be a commutative ring with identity 1, typically the ring of polynomials $\mathcal{P}_n$ with $n$ undeterminates $X_1, \ldots, X_n$ over the ring of rational numbers $\mathbb{Q}$ taken as *scalars*.

**Definition**: the *ideal* generated by a (possibly finite) subset $I$ of $A$ is the set of polynomials $I_{\text{ideal}} := \{\Sigma_i p_i s_i \mid p_i \in \mathcal{P}_n \text{ and } s_i \in I\}$.

**Rewriting**: with a polynomial $P$ is done by division in the ring, resulting in a remainder.

**Fact**: the ideal generated by a set of polynomials $I := \{p_i\}_i$ *is* the equivalence class of 0 in the equational theory generated by $E := \{p_i = 0\}_i$.

The equation $p = 0$ can be written as $\text{Mon} \rightarrow \text{Tail}$, where $\text{Mon}$ is the *leading* monomial of $p$ $\text{mon} \rightarrow \text{Head}$, where $\text{mon}$ is the *loosing* monomial of $p$. 
There is an \( n \log n \) algorithm for deciding membership to a ground equational theory called congruence closure. [Kozen, Nelsson, Shostak]

When variables are at depth at most one, membership to the equational theory becomes NP-complete. [Comon-Jouannaud]

The ground-AC, ACI, ACZ, ACZI cases are (simply or doubly) exponential. [Marché, Narendran, Rusinowitch, Huynh]

The case of polynomial rings is doubly exponential. [Buchberger]
Outline

1. Membership Problem
2. Canonical bases
3. Completion methods
4. Conclusion
A *rewrite quasi-ordering* $\succeq$ is a *monotonic* quasi-ordering: 

$$u \succeq v \text{ implies } w[u]_p \succeq w[v]_p$$

$$u \simeq v \text{ implies } w[u]_p \simeq w[v]_p$$

A *rewrite ordering* is a rewrite quasi-ordering such that $\simeq$ is the syntactic equality.

An *AC-rewrite ordering* is a rewrite quasi-ordering such that $\simeq$ is $=_\text{AC}$.

A *monomial rewrite ordering* is a rewrite quasi-ordering on monomials such that $\simeq$ is the equational theory $Mon :=$

$$X^\alpha Y^\beta = Y^\beta X^\alpha \quad (X^\alpha Y^\beta)Z^\gamma = X^\alpha(Y^\beta Z^\gamma) \quad X^\alpha X^\beta = X^{\alpha+\beta} \quad X^0 = 1$$

A *polynomial rewrite ordering* is the multiset extension of a monomial ordering to normalized sums of monomials.

A monomial rewrite ordering ($\succ$ or $\succsim$) is called *global* if $X \succ 1$ and *local* if $1 \succsim X$.

There exist *total* orderings in all cases. Global monomial orderings are *well-founded*. Local ones are *ill-founded*. 
A **rewrite quasi-ordering** $\succeq$ is a **monotonic** quasi-ordering:

$u \succ v$ implies $w[u]_p \succ w[v]_p$  
$u \simeq v$ implies $w[u]_p \simeq w[v]_p$

A **rewrite ordering** is a rewrite quasi-ordering such that $\simeq$ is the syntactic equality.

An **AC-rewrite ordering** is a rewrite quasi-ordering such that $\simeq$ is $=_{AC}$.

A **monomial rewrite ordering** is a rewrite quasi-ordering on monomials such that $\simeq$ is the equational theory $Mon :=$

$$X^\alpha Y^\beta = Y^\beta X^\alpha \quad (X^\alpha Y^\beta)Z^\gamma = X^\alpha(Y^\beta Z^\gamma) \quad X^\alpha X^\beta = X^{\alpha+\beta} \quad X^0 = 1$$

A **polynomial rewrite ordering** is the multiset extension of a monomial ordering to normalized sums of monomials.

A monomial rewrite ordering ($\succ$ or $\succsim$) is called **global** if $X \succ 1$ and **local** if $1 \succsim X$.

There exist **total** orderings in all cases. Global monomial orderings are **well-founded**. Local ones are **ill-founded**.
A rewrite quasi-ordering $\succeq$ is a monotonic quasi-ordering:
\[ u \succ v \text{ implies } w[u] \succ w[v] \quad u \sim v \text{ implies } w[u] \sim w[v] \]

A rewrite ordering is a rewrite quasi-ordering such that $\sim$ is the syntactic equality.

An AC-rewrite ordering is a rewrite quasi-ordering such that $\sim =_{AC}$.

A monomial rewrite ordering is a rewrite quasi-ordering on monomials such that $\sim$ is the equational theory $Mon :=$
\[
X^\alpha Y^\beta = Y^\beta X^\alpha \quad (X^\alpha Y^\beta)Z^\gamma = X^\alpha (Y^\beta Z^\gamma) \quad X^\alpha X^\beta = X^{\alpha+\beta} \quad X^0 = 1
\]

A polynomial rewrite ordering is the multiset extension of a monomial ordering to normalized sums of monomials.

A monomial rewrite ordering ($\succeq$ or $\succ$) is called global if $X \succ 1$ and local if $1 \succ X$.

There exist total orderings in all cases. Global monomial orderings are well-founded. Local ones are ill-founded.
Global monomial orderings

Start with an order on undeterminates: \( X_1 \succ \ldots \succ X_n \).
A monomial is written \( X_1^{\alpha_1} \ldots X_n^{\alpha_n} \) with \( \alpha_i \geq 0 \).

**Lexicographic order** \( \succ_{lo} \):
a monomial is interpreted by an \( n \)-tuple \( (\alpha_1, \ldots, \alpha_n) \).
\( n \)-tuples are compared in \( (>\mathbb{N})_{\text{lex}} \).

**Degree reverse lexicographic order** \( \succ_{drlo} \):
a monomial is interpreted by the pair \( (\sum_i \alpha_i, (\alpha_n, \ldots, \alpha_1)) \).
Pairs are compared in \( (>\mathbb{N}, (<\mathbb{N})_{\text{lex}})_{\text{lex}} \).

**Example:**

<table>
<thead>
<tr>
<th>Pair</th>
<th>Interpretation</th>
<th>lexico</th>
<th>Reverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>((X_1^2 X_2, X_1^2 X_3^2))</td>
<td>(((2, 1, 0), (2, 0, 2)))</td>
<td>(\succ_{lo})</td>
<td>(&lt;_{drlo})</td>
</tr>
<tr>
<td>((X_1^2 X_2^2, X_1^2 X_2))</td>
<td>(((2, 2), (2, 1)))</td>
<td>(\succ_{lo})</td>
<td>(\succ_{drlo})</td>
</tr>
<tr>
<td>((X_1^2 X_2^2, X_1^2 X_3^2))</td>
<td>(((2, 2, 0), (2, 0, 2)))</td>
<td>(\succ_{lo})</td>
<td>(&lt;_{drlo})</td>
</tr>
</tbody>
</table>
Hironaka’s local monomial ordering

Local lexicographic order $\succ_{llo}$:
a monomial is interpreted by an $n$-tuple $(\alpha_1, \ldots, \alpha_n)$.
$n$-tuples are compared in $(\langle N \rangle_{\text{lex}}$).

Local degree reverse lexicographic order $\succ_{ldrlo}$:
a monomial is interpreted by the pair $(\Sigma_i \alpha_i, (\alpha_n, \ldots, \alpha_1))$.
Pairs are compared in $(\langle N, (\langle N \rangle_{\text{lex}} \rangle_{\text{lex}}$).

Example:

<table>
<thead>
<tr>
<th>Pair</th>
<th>Interpretation</th>
<th>Local lex</th>
<th>Local reverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(X_1^2 X_2, X_1 X_3^2)$</td>
<td>$((2, 1, 0), (2, 0, 2))$</td>
<td>$\prec_{llo}$</td>
<td>$\succ_{ldrlo}$</td>
</tr>
<tr>
<td>$(X_1^2 X_2, X_1^2 X_2)$</td>
<td>$((2, 2), (2, 1))$</td>
<td>$\prec_{llo}$</td>
<td>$\prec_{ldrlo}$</td>
</tr>
<tr>
<td>$(X_1^2 X_2^2, X_1^2 X_3^2)$</td>
<td>$((2, 2, 0), (2, 0, 2))$</td>
<td>$\prec_{llo}$</td>
<td>$\succ_{ldrlo}$</td>
</tr>
</tbody>
</table>
A set of ground rules $R$ is a \textit{canonical basis} for an equational theory $\equiv_E$ iff

(i) \textbf{computability of normal forms:}
for all $u$ and $S \subseteq R$, $u \downarrow_S$ is computable;

(ii) \textbf{soundness:} $R$ generates the equational theory $\equiv_E$;

(iii) \textbf{inter-irreducibility:}
for all $s \rightarrow t \in R$, $s = s \downarrow_{R \setminus \{s \rightarrow t\}}$ (and $t = t \downarrow_R$)

Main property of (ground) canonical bases:
$s = t \in \equiv_E$ iff $s \downarrow_R = t \downarrow_R$.

Proof: inter-irreducibility implies Church-Rosser by Hindley.

To lift the main property of bases to non-ground ones:
(iv) \textbf{joinability of critical pairs}

\[ r\sigma \leftarrow l\sigma = l\sigma[g\sigma]_p \rightarrow l\sigma[d\sigma]_p \]
A set of ground rules $R$ is a *canonical basis* for an equational theory $\equiv_E$ iff

(i) **computability of normal forms:** for all $u$ and $S \subseteq R$, $u \downarrow_S$ is computable;

(ii) **soundness:** $R$ generates the equational theory $\equiv_E$;

(iii) **inter-irreducibility:** for all $s \rightarrow t \in R$, $s = s \downarrow_{R \setminus \{s \rightarrow t\}}$ (and $t = t \downarrow_R$)

Main property of (ground) canonical bases:
$s = t \in \equiv_E$ iff $s \downarrow_R = t \downarrow_R$.

**Proof:** inter-irreducibility implies Church-Rosser by Hindley.

To lift the main property of bases to non-ground ones:

(iv) **joinability** of critical pairs

\[ r\sigma \leftarrow l\sigma = l\sigma[g\sigma]_p \rightarrow l\sigma[d\sigma]_p \]
Canonicity Property following from (i,ii,iii,iv):

Given $\succ$ well-founded s.t. $\overset{+}{\rightarrow}_R \subseteq \succ$, then $R$ is unique.

Example: canonical set of rules for free groups
Canonical representations of ideals

In the case of polynomial computations, we need to compute modulo the theory $Pol$ extending $Mon$ with $AC(+)$, and distributivity of multiplication over addition.

A set of rules $R$ is a canonical basis for an ideal $=_{E}$ iff

(i) computability of normal forms: for all $u$ and $S \subseteq R$, $u \downarrow_{S}$ is computable;

(ii) soundness: $R$ generates the equational theory $=_{E}$;

(iii) inter-irreducibility: for all $s \rightarrow t \in R$, $s = s \downarrow_{R \setminus \{s \rightarrow t\}}$ (and $t = t \downarrow_{R}$);

(iv) coherence of normal forms: for all $u, v$ such that $u =_{Pol} v$, $u \downarrow_{S} =_{Pol} v \downarrow_{S}$;

To force (iv) and make critical pairs explicit, we add Stickel’s extension rules: given a rule $M \rightarrow P$, we use instead: $Mx \rightarrow Px$. 
In the case of polynomial computations, we need to compute modulo the theory $Pol$ extending $Mon$ with AC(+), and distributivity of multiplication over addition.

A set of rules $R$ is a **canonical basis** for an ideal $=_E$ iff

(i) **computability of normal forms:** for all $u$ and $S \subseteq R$, $u \downarrow_S$ is computable;

(ii) **soundness:** $R$ generates the equational theory $=_E$;

(iii) **inter-irreducibility:** for all $s \rightarrow t \in R$, $s = s \downarrow_{R \setminus \{s \rightarrow t\}}$ (and $t = t \downarrow_R$);

(iv) **coherence of normal forms:** for all $u, v$ such that $u =_{Pol} v$, $u \downarrow_S =_{Pol} v \downarrow_S$;

To force (iv) and make critical pairs explicit, we add Stickel’s **extension rules:** given a rule $M \rightarrow P$, we use instead: $Mx \rightarrow Px$. 
In the case of polynomial computations, we need to compute modulo the theory \( Pol \) extending \( Mon \) with AC(\( + \)), and distributivity of multiplication over addition.

A set of rules \( R \) is a \textit{canonical basis} for an ideal \( \equiv_E \) iff

(i) \textbf{computability of normal forms:} for all \( u \) and \( S \subseteq R \), \( u \downarrow_S \) is computable;

(ii) \textbf{soundness:} \( R \) generates the equational theory \( \equiv_E \);

(iii) \textbf{inter-irreducibility:} for all \( s \rightarrow t \in R \), \( s = s \downarrow_{R \setminus \{s \rightarrow t\}} \) (and \( t = t \downarrow_R \));

(iv) \textbf{coherence of normal forms:} for all \( u, v \) such that \( u =_{Pol} v \), \( u \downarrow_S =_{Pol} v \downarrow_S \);

To force (iv) and make critical pairs explicit, we add Stickel’s \textit{extension rules}: given a rule \( M \rightarrow P \), we use instead: \( Mx \rightarrow Px \).
Example of canonical basis with $\succ_{lo}$

\[
\begin{align*}
X_2^3 x & \rightarrow X_2^2 x \\
X_1 X_2^2 y & \rightarrow X_2^2 y \\
X_1^2 z & \rightarrow X_2^2 z
\end{align*}
\]

is a canonical basis, but

\[
\begin{align*}
X_1^2 X_2 x & \rightarrow X_1^2 x \\
X_1 X_2^2 y & \rightarrow X_2^2 y
\end{align*}
\]

is not since (instantiating $x$ by $X_2$ and $y$ by $X_1$ yields:

\[
\begin{align*}
X_1^2 X_2^2 \\
X_1 X_2^2 \\
X_1^2
\end{align*}
\]

although both define the same ideal.
Example of canonical basis with $\succ_{lo}$

\[
\begin{align*}
X_2^3 x & \rightarrow X_2^2 x \\
X_1 X_2^2 y & \rightarrow X_2^2 y \\
X_1^2 z & \rightarrow X_2^2 z
\end{align*}
\]

is a canonical basis, but

\[
\begin{align*}
X_1^2 X_2 x & \rightarrow X_1^2 x \\
X_1 X_2^2 y & \rightarrow X_2^2 y
\end{align*}
\]

is not since (instantiating $x$ by $X_2$ and $y$ by $X_1$ yields:

\[
\begin{align*}
X_1^2 X_2^2 \\
\downarrow \\
X_1^2
\end{align*}
\]

\[
\begin{align*}
\downarrow \\
X_1^2
\end{align*}
\]

although both define the same ideal.
Example of canonical basis with $\succ_{drlo}$

$$X_1^2 X_2 x \rightarrow X_1^2 x$$
$$X_1^3 y \rightarrow X_1^2 y$$
$$X_2^2 z \rightarrow X_1^2 z$$

is another canonical basis for the same ideal. In particular
Example of canonical basis with $\succ_{ll\sigma}$

\[ X_1^2 x \rightarrow X_1^2 X_2 x \]
\[ X_2^2 y \rightarrow X_1 X_2^2 y \]

is another canonical basis for the same ideal. In particular

\[ X_1^2 X_2^2 \]

\[ X_1^2 X_2^3 \]
\[ \downarrow \]
\[ X_1^3 X_2^3 \]
\[ X_1^3 X_2^3 = \]
\[ X_1^3 X_2^3 \]
\[ X_1^3 X_2^3 \]
**Knuth basis:** uses an arbitrary well-founded order $\succ$ on terms such that $\frac{\star}{R} \subseteq \succ$

**Groebner basis:** uses a global order on polynomials $\succ$ generated by an arbitrary order on the unknowns.

**Janet basis:** same as above, but for non-commutative rings.

**Hironaka basis:** uses a local order on polynomials $\succ$ generated by an arbitrary order on the unknowns.
Computation of normal forms

blind strategy in case of a well-founded order: [Janet, Buchberger, Knuth-Bendix]

specific strategy for computing weak normal forms of polynomials in presence of an ill-founded order: [Hironaka, Mora]

What is a weak R-normal form for $t$?

A term $u$ such that
(i) $t \xrightarrow{*} R u$
(ii) $\forall p, q$ such that $u|_p =_R u|_q$, then $u|_p = u|_q$.

Lemma: Assume weak-normal forms are computable. Then the equational theory is decidable.

[Hironaka, Mora]: polynomials have computable weak normal forms.
Limit ground completion with wfo \( \succ [\text{Knuth-Bendix}] \)

**Input:**
\[
\frac{E}{\emptyset, E}
\]

**Output:**
\[
\frac{S, \emptyset}{S}
\]

**Orient:**
\[
\begin{align*}
S & \quad E \cup \{u = v\} \\
S \cup \{u \to v\}, E & \quad \text{if } u \succ v
\end{align*}
\]

**Delete:**
\[
\begin{align*}
S & \quad E \cup \{u = u\} \\
S, E & \quad \text{if } u \succ u
\end{align*}
\]

**Compose:**
\[
\begin{align*}
S \cup \{u \to v\}, E & \quad S \cup \{u \to v'\}, E \\
S & \quad S \cup \{u \to v'\}, E \quad \text{if } v \overset{S}{\to} v'
\end{align*}
\]

**Simplify:**
\[
\begin{align*}
S \cup \{u \to v\}, E & \quad S, E \cup \{u' = v\} \\
S & \quad S, E \cup \{u' = v\} \quad \text{if } u \overset{S}{\to} u'
\end{align*}
\]

**Termination argument:** the multiset
\[
\{s \mid s = t \in E \lor s \to v \in S \lor u \to s \in S\}
\]
decreases in \( \succ_m \) when any rule but Orient is applied.

**Correctness argument:** equational deductions.
There is one more rule:

**Critical pair:**

\[
\frac{S, E}{S, E \cup \{ s = t \}} \quad \text{if } s = t \in CP(S)
\]

**Theorem [Huet]:** If critical pairs are computed lazily and equations can always be oriented, then the (possibly infinite) limit rewrite system is confluent.

**Proof:** arbitrary proofs are transformed in finite time into persisting rewrite proofs.
Limit AC\(^+\)-completion with wfo \(\succeq_{lo}\) [Buchberger, etc.]

Compute critical pairs associated with extension rules:

\[
\text{Deduce: } \quad S \cup \{lx \rightarrow rx, l'y \rightarrow r'y\}, E \\
S \cup \{l \rightarrow r, l' \rightarrow r'\}, E \cup \{l_2r' = l'_2r\} \\
\text{if } l =_{\text{Mon}} l_1l_2, l' =_{\text{Mon}} l'_1l'_2 \text{ and } l_1 =_{\text{Mon}} l'_1
\]

Termination argument: call \textit{prime factor} in a \textit{monomial} \(m_1 + \ldots + m_n\) a term \(m_i\) not headed by \(+\). We interpret the current state \((S, E)\) by the set of prime factors occurring in rules and equations. \textbf{Orient} and \textbf{Deduce} do not change the set. Full simplification decrease the set. Since all rules but \textbf{Deduce} terminate, we conclude termination as a consequence of Higman’s Lemma applied to the lefthand sides of an infinite sequence of rules.

Correctness argument: soundness + joinability of critical pairs by induction on pairs of terms (ordered with \(\succeq_{\text{mul}}\)).
| **Simplify:** | \[
\frac{S, E \cup \{u = v\}}{S, E \cup \{u \downarrow_S = v \downarrow_S\}}
\]
| \[\text{if} \quad u \downarrow_S \neq v \downarrow_S, \quad u \downarrow_S \neq u \text{ or } v \downarrow_S \neq v\] |
| **Delete:** | \[
\frac{S, E \cup \{u = v\}}{S, E}
\]
| \[\text{if } u \downarrow_S \equiv v \downarrow_S\] |

| **Orient:** | \[
\frac{S, E \cup \{u = v\}}{S \setminus S' \cup \{u \rightarrow v\}, E \cup S'}
\]
| \[u, v \text{ irreducible by } S, \quad u \succ v\] |
| \[S' = \{l' \rightarrow r' \in S | l' \rightarrow \{u \rightarrow v\} l'' \text{ or } r' \rightarrow \{u \rightarrow v\} r''\}\] |

**Termination argument:** multiset of terms compared in the multiset extension of \(\succ\) augmented with encompassement.

**Correctness argument:** \(S\) is a basis for \(\equiv_S\) is an invariant.

**Remark:** Need to add **Deduce** in non-ground case, but the correctness argument applies now without change.
Need to add **Deduce** for extensions as before.

The proof of termination is the same as in $AC^+$-case. The proof of corectness is the same as in the free case.
Working with ill-founded orders is much more difficult for two reasons:

- computing normal forms may not be possible: use weak normal forms.

  Our understanding has not reached the point yet where we would have an abstract formulation of Hironaka’s algorithm for computing weak normal forms.

- ensuring progress of completion cannot rely on the order: see [Jouannaud, van Oostrom] for a solution.
Completion is a very old idea going back to ... 1920?
well-foundedness in completion is challenged!
History has been unfair to Janet!

Janet: 1920
Hironaka: 1964
Buchberger: 1965
Knuth and Bendix: 1970
THANKS

TO THE AUDIENCE

FOR LISTENING TO THIS

COMPLETED TOUR