A Taste of Rewrite Systems

Nachum Dershowitz
Department of Computer Science, University of Illinois, Urbana IL 61801, USA

Abstract. This survey of the theory and applications of rewriting with equations discusses the existence and uniqueness of normal forms, the Knuth-Bendix completion procedure and its variations, as well as rewriting-based (functional and logic) programming and (equational, first-order, and inductive) theorem proving. Ordinary, associative-commutative, and conditional rewriting are covered. Current areas of research are summarized and an extensive bibliography is provided.

0 Menu

Equational reasoning is an important component in symbolic algebra, automated deduction, high-level programming languages, program verification, and artificial intelligence. Reasoning with equations involves deriving consequences of given equations and finding values for variables that satisfy a given equation.

Rewriting is a very powerful method for dealing with equations. Directed equations, called “rewrite rules”, are used to replace equals by equals, but only in the indicated direction. The theory of rewriting centers around the concept of “normal form”, an expression that cannot be rewritten any further. Computation consists of rewriting to a normal form; when the normal form is unique, it is taken as the value of the initial expression. When rewriting equal terms always leads to the same normal form, the set of rules is said to be “convergent” and rewriting can be used to check for equality.

This chapter gives a brief survey of the theory of rewriting and its applications to issues in programming languages and automated deduction. Section 1 offers a few motivating examples as appetizer. The “bread and butter” concepts come next: Sect. 2 addresses the question of existence of normal forms; Sect. 3 addresses their uniqueness. Section 4 describes a brew for constructing convergent systems. The main course is a choice of Sect. 5, a method for proving validity of equations, and, Sect. 6, a method for solving equations. As side dishes, Sections 7 and 8 consider extensions of rewriting to handle associative-commutative function symbols and conditional equations. Dessert is Sect. 9, which applies conditional and unconditional rewriting to programming, while, the pièce de résistance, Sect. 10, shows how rewriting is used to facilitate deductive and inductive proofs. Finally, over coffee, Sect. 11 mentions some current areas of research. An extensive bibliography for further reading (the “check”) is attached.
1 Rewriting

We begin our rewriting feast with the following three puzzles:

**Puzzle 1 Hercules and Hydra.** Hydra is a bush-like creature with multiple heads. Each time Hercules hacks off a head of hers, Hydra sprouts many new branches identical to—and adjacent to—the weakened branch that used to hold the severed head. But whenever he chops off a head coming straight out of the ground, no new branches result. Suppose Hydra starts off as a lone stalk ten branches tall. The question is: Does Hercules ever defeat Hydra?

**Puzzle 2 Chameleon Island.** The chameleons on this strange island come in three colors, red, yellow, and green, and wander about continuously. Whenever two chameleons of different colors meet, they both change to the third color. Suppose there are 15 red chameleons, 14 yellow, and 13 green. Can their haphazard meetings lead to a stable state, all sharing the same color?

**Puzzle 3 Grecian Urn.** An urn contains 150 black beans and 75 white. Two beans are removed at a time; if they’re the same color, a black one is placed in the urn; if they’re different, the white one is returned. The process is repeated as long as possible. Is the color of the last bean in the urn predetermined and, if so, what is it?

All three puzzles give rules for going from one state to another. The first two concern the possibility of getting from some starting state to a final state; the last asks how the final state is related to the initial state.

In general, a rewrite system consists of a set of rules for transforming terms. Hercules and Hydra can be expressed pictorially as in Fig. 1.

![Fig. 1. Hercules versus Hydra.](image)

Chameleon Island can be expressed by three rules:

\[
\begin{align*}
\text{red yellow} & \rightarrow \text{green green} \\
\text{green yellow} & \rightarrow \text{red red} \\
\text{red green} & \rightarrow \text{yellow yellow ,}
\end{align*}
\]

with the added proviso that chameleons can rearrange themselves at will.

The Grecian Urn may be expressed as the following system of four rules, one per possible pair of beans:

\[
\begin{align*}
\text{black black} & \rightarrow \text{black} \\
\text{white white} & \rightarrow \text{black} \\
\text{black white} & \rightarrow \text{white} \\
\text{white black} & \rightarrow \text{white .}
\end{align*}
\]

In the sequel, we will solve these puzzles by applying techniques from the theory of rewriting. But, first, let’s take a look at some more prosaic examples of rewrite systems.
Example 1 (Insertion Sort). The following is a program to arrange a list of numbers in non-increasing order by inserting elements one by one into position:

\[
\begin{align*}
\text{max}(0, x) & \rightarrow x \\
\text{max}(x, 0) & \rightarrow x \\
\text{max}(s(x), s(y)) & \rightarrow s(\text{max}(x, y)) \\
\text{min}(0, x) & \rightarrow 0 \\
\text{min}(x, 0) & \rightarrow 0 \\
\text{min}(s(x), s(y)) & \rightarrow s(\text{min}(x, y)) \\
\text{sort}(\text{nil}) & \rightarrow \text{nil} \\
\text{sort}(\text{cons}(x, y)) & \rightarrow \text{insert}(x, \text{sort}(y)) \\
\text{insert}(x, \text{nil}) & \rightarrow \text{cons}(x, \text{nil}) \\
\text{insert}(x, \text{cons}(y, z)) & \rightarrow \text{cons}(\text{max}(x, y), \text{insert}(\text{min}(x, y), z)) .
\end{align*}
\]

Lists are represented in “cons” notation and numbers in successor (unary) notation. We would like to ascertain that every term constructed from sort, cons, nil, s, and 0 leads to a unique term, not containing sort, nor the auxiliary symbols, insert, max, and min. \(\square\)

As in the previous example, both sides of a rule \(l \rightarrow r\) can contain variables which refer to arbitrary terms. A rule is used to rewrite any subterm that is an instance of the left-hand side \(l\). That is, \(u[l]\) rewrites to \(u[r]\), where \(\sigma\) is a substitution of terms for variables of the rule (the same term substituted for each occurrence of the same variable). \(u[]\) is the “context” in which the instance \(l\) of \(l\) occurs as a subterm, and \(u[r]\) is \(u[l]\) with that subterm replaced by the right-hand side after its variables have had the same substitution \(\sigma\) applied. Such a rewrite step is written \(u[l] \rightarrow u[r]\) or, backwards, as \(u[r] \rightarrow u[l]\). Rules are applied nondeterministically, since, in general, more than one rule can be applied, and any one rule may apply at more than one position within a term.

Rewrite systems have long been used as decision procedures for validity in equational theories, that is, for truth of an equation in all models of the theory.

Example 2 (Loops). Consider the following system of a dozen rules:

\[
\begin{align*}
x'x & \rightarrow e \\
x/x & \rightarrow e \\
e \cdot x & \rightarrow x \\
x \cdot e & \rightarrow x \\
e \backslash x & \rightarrow x \\
x/e & \rightarrow x
\end{align*}
\]

Each rule follows by algebraic manipulation from some combination of the following five axioms for algebraic structures called “loops”:

\[
\begin{align*}
x'x & = y \\
x/x & = y \\
y/x & = y
\end{align*}
\]

and the definition \(y/x = e\). To use the rewrite system to decide whether an arbitrary equation is a valid identity for all loops (in which case it can be proved by purely equational reasoning), we need to ascertain that any two terms equal in the same theory have the same normal forms. \(\square\)

Rewrite systems can also be used to “interpret” other programming languages.

Example 3 (Interpreter). The state of a machine with three integer-valued registers can be represented as a triple \((x, y, z)\). The semantics of its instruction set can be defined by the rules for the interpreter shown in Fig. 2. The penultimate rule, for example, can clearly be applied ad infinitum. The question is what strategy of rule application, if any, will lead to a normal form whenever there is one. \(\square\)
Fig 2. Three-register machine interpreter.

\[
\begin{align*}
\text{eval(set0} & \ n, \langle x, \ y, \ z \rangle) \rightarrow \langle n, \ y, \ z \rangle \\
\text{eval(set1} & \ n, \langle x, \ y, \ z \rangle) \rightarrow \langle x, \ n, \ z \rangle \\
\text{eval(set2} & \ n, \langle x, \ y, \ z \rangle) \rightarrow \langle x, \ y, \ n \rangle \\
\text{eval(inc0} & \langle x, \ y, \ z \rangle) \rightarrow \langle s(x), \ y, \ z \rangle \\
\text{eval(inc1} & \langle x, \ y, \ z \rangle) \rightarrow \langle x, \ s(y), \ z \rangle \\
\text{eval(inc2} & \langle x, \ y, \ z \rangle) \rightarrow \langle x, \ y, \ s(z) \rangle \\
\text{eval(dec0} & \langle s(x), \ y, \ z \rangle) \rightarrow \langle x, \ y, \ z \rangle \\
\text{eval(dec1} & \langle x, \ s(y), \ z \rangle) \rightarrow \langle x, \ y, \ z \rangle \\
\text{eval(dec2} & \langle x, \ y, \ s(z) \rangle) \rightarrow \langle x, \ y, \ z \rangle \\
\text{eval(ifpos0} & \ p, \langle 0, \ y, \ z \rangle) \rightarrow \langle 0, \ y, \ z \rangle \\
\text{eval(ifpos1} & \ p, \langle s(x), \ y, \ z \rangle) \rightarrow \text{eval}(p, \langle s(x), \ y, \ z \rangle) \\
\text{eval(ifpos1} & \ p, \langle x, \ 0, \ z \rangle) \rightarrow \langle x, \ 0, \ z \rangle \\
\text{eval(ifpos1} & \ p, \langle x, \ s(y), \ z \rangle) \rightarrow \text{eval}(p, \langle x, \ s(y), \ z \rangle) \\
\text{eval(ifpos2} & \ p, \langle x, \ y, \ 0 \rangle) \rightarrow \langle x, \ y, \ 0 \rangle \\
\text{eval(ifpos2} & \ p, \langle x, \ y, \ s(z) \rangle) \rightarrow \text{eval}(p, \langle x, \ y, \ s(z) \rangle) \\
\text{whilepos0} & \ p \rightarrow \text{ifpos0} (p, \text{whilepos0} p) \\
\text{whilepos1} & \ p \rightarrow \text{ifpos1} (p, \text{whilepos1} p) \\
\text{whilepos2} & \ p \rightarrow \text{ifpos2} (p, \text{whilepos2} p) \\
\text{eval}(p, q, u) & \rightarrow \text{eval}(q, \text{eval}(p, u)) .
\end{align*}
\]

Two important properties a rewrite system may possess are termination and confluence. We address these in the following two sections.

2 Termination

Definition 1 Termination. A rewrite system is terminating if there are no infinite derivations \( t_1 \rightarrow t_2 \rightarrow \cdots \).

The rules for the Chameleon Puzzle are not terminating; to wit, \( \text{red yellow yellow} \rightarrow \text{green green yellow} \rightarrow \text{green red red} \rightarrow \text{yellow yellow red} \), which rearranges to \( \text{red yellow yellow} \), from which point the same three steps may be repeated over and over again. On the other hand, each step in the Grecian Urn Puzzle decreases the number of beans, so it always terminates. The Loop system also terminates, since it always shortens the length of the expression, but, as pointed out above, our interpreter does not.

Termination is an undecidable property of rewrite systems. Nonetheless, the following general method is very often helpful in termination proofs:

Definition 2 Termination Function. A termination function takes a term as argument and is of one of the following types:

- a function that returns the outermost function symbol of a term, with symbols ordered by some precedence (a "precedence" is a well-founded partial ordering of symbols);
- a function that extracts the immediate subterm at a specified position (which position, can depend on the outermost function symbol of the term);
- a function that extracts the immediate subterm of a specified rank (the kth largest in the path ordering defined recursively below);
- a homomorphism from terms to some well-founded set of values;
- a monotonic homomorphism, having the strict subterm property, from terms to some well-founded set (a homomorphism is monotonic with respect to the well-founded ordering if the value it assigns to a term \( f(\ldots s \ldots) \) is greater than or equivalent to that of \( f(\ldots t \ldots) \) whenever the value of \( s \) is greater than \( t \); it has the strict subterm property if the value of \( f(\ldots t \ldots) \) is always strictly greater than that of its subterm \( t \)).
- a strictly monotonic homomorphism, having the strict subterm property, from terms to some well-founded set (it is strictly monotonic if the value of \( f(\ldots s \ldots) \) is strictly greater than that of \( f(\ldots t \ldots) \) whenever \( s \) is of greater value than \( t \)); or
- a constant function.

Simple examples of homomorphisms from terms to the natural numbers are size (number of function symbols, including constants), depth (maximum nesting of function symbols), and weight (sum of integral weights of function symbols). Size and weight are strictly monotonic; depth is monotonic.

**Definition 3 Path Ordering.** Let \( \tau_0, \ldots, \tau_{i-1} \ (i \geq 0) \) be monotonic homomorphisms, all but possibly \( \tau_{i-1} \) strict, and let \( \tau_i, \ldots, \tau_k \) be any other kinds of termination functions. The induced path ordering \( \succ \) is as follows:

\[
s = f(s_1, \ldots, s_m) \succeq g(t_1, \ldots, t_n) = t
\]

if either of the following hold:

1. \( s_i \succeq t \) for some \( i \), \( i = 1, \ldots, m \); or
2. \( s \succ t \) and \( (\tau_i(s), \ldots, \tau_k(s)) \) is lexicographically greater than or equal to \( (\tau_i(t), \ldots, \tau_k(t)) \), where function symbols are compared according to their precedence, homomorphic images are compared in the corresponding well-founded ordering, and subterms are compared recursively in \( \succ \).

A tuple \( (x_1, \ldots, x_m) \) is lexicographically greater than \( (y_1, \ldots, y_n) \) if (a) \( x_i \) is greater than \( y_i \) for some \( i \) \((1 \leq i \leq n)\) and \( x_j \) is equivalent to \( y_j \) for all \( j \) up to, but not including, \( i \), or if (b) the \( x_i \) and \( y_i \) are equivalent for all \( i \) up to and including \( n \) and also \( m > n \). We say that \( s \succ t \) if \( s \succeq t \), but \( s \nprec t \).

This ordering mixes and matches syntactic considerations (the first three types of termination functions) with semantic considerations (the others).

**Theorem 4 [19].** A rewrite system terminates if \( l \sigma \succ r \sigma \) in a path ordering \( \succ \) for all rules \( l \rightarrow r \) and substitutions \( \sigma \), and also \( \tau_0(l \sigma) = \tau_0(r \sigma) \) for each of the nonmonotonic homomorphisms among its termination functions.

The proof of this theorem is based on Kruskal's Tree Theorem and the fact that \( s \rightarrow t \) and \( s \succ t \) imply \( f(s_1, \ldots, s_n) \succ f(t_1, \ldots, t_m) \), for all terms \( s, t, \ldots \) and function symbols \( f \).

The path ordering encompasses many of the orderings described in the literature. The simplest, and perhaps most generally useful, version of this ordering, called the lexicographic path ordering, uses a precedence for \( \tau_i \) and the \( i \)th subterm for the remaining \( \tau_j \) (or any other permutation of all the subterms). The precedence typically encapsulates the dependency of some function definitions on others. The resultant path ordering is "syntactic" in that it depends only on the relative order of the function symbols appearing in the terms being compared. Terms \( s \) and \( t \) are compared by first comparing their outermost function symbols; if they're equal, then subterms are compared recursively, in order; if the outermost symbol of \( s \) is larger, all that needs to be shown is that \( s \) is larger than \( t \)'s subterms; otherwise, the only way \( s \) can be larger than \( t \) is if one of its subterms is.

To prove that Insertion Sort terminates, note that five of the rules show a decrease for \( \succ \) by virtue of clause (1) of the definition of the path ordering, regardless of what we choose for the \( \tau_i \). For the recursive rules of \( \text{max} \) and \( \text{min} \), we can use the precedence \( \text{max} \) and \( \text{min} \) greater than \( s \) as \( \tau_i \). For the base case of \( \text{insert} \), we let \( \text{insert} \succ \text{cons} \) in the precedence. For the recursive rule of \( \text{sort} \), we let \( \text{sort} \succ \text{insert} \), and have \( \tau_i \) give the sole argument of \( \text{sort} \). Finally, for the recursive rule of \( \text{insert} \), we make \( \text{insert} \succ \text{max}, \text{min} \) in the precedence, and have \( \tau_i \) return the second argument of \( \text{insert} \).

Another important class of orderings, the polynomial path orderings, uses a polynomial interpretation for \( \tau_i \). The interpretation associates a (multivariate) monotonic integer polynomial with each function symbol and constant, which is extended to a homomorphism to give meaning to terms. The remaining \( \tau_i \) select subterms as before. For example, Loops may be shown terminating by letting each binary symbol take the sum
of its arguments. This “semantic” ordering acts like the lexicographic path ordering when the polynomials are all of degree 0 (constants). The advantage of polynomials over other classes of interpretations is that tools are available to help compute inequalities.

To show that Hercules invariably defeats Hydra, we need to show that after each chop and regrowth, Hydra is smaller than before. To this end, we let nodes have variable arity. This multiset path ordering, in effect, uses a precedence for \(\pi_0\) and has \(\pi_i\) give the \(i\)th largest subterm. The precedence for Hydra makes branching nodes larger than heads. Replacing a branch with any number of smaller branches is a decrease in this ordering.

3 Confluence

We will use \(s \rightarrow t\) to mean \(s \rightarrow t\) or \(t \rightarrow s\). We say \(s\) derives \(t\) and write \(s \rightarrow^* t\) if \(s \rightarrow \ldots \rightarrow t\) in zero or more steps. We say that \(s\) and \(t\) are convertible, symbolized \(s \equiv^* t\), if \(s \rightarrow \ldots \rightarrow t\) in zero or more steps, and that \(s\) and \(t\) are joinable, or that \(s \equiv t\) has a rewrite proof, if \(s\) and \(t\) derive the same term.

The following two definitions are easily shown equivalent:

**Definition 5 Church-Rosser Property.** A rewrite system is Church-Rosser if terms are joinable whenever they are convertible. (See Fig. 3(a).)

**Definition 6 Confluence.** A rewrite system is confluent if terms are joinable whenever they are derivable from the same term. (See Fig. 3(b).)

![Fig. 3. Confluence Properties.](image)

Terminating confluent systems are called convergent or complete. Often, we are only interested in confluence for ground (variable-free) terms.

A weaker form of confluence is the following:

**Definition 7 Local Confluence.** A rewrite system is locally confluent if two terms are joinable whenever they are both obtainable by rewriting (in one step) from the same term. (See Fig. 3(c).)

The following, sometimes referred to as the “Diamond Lemma”, connects local and global confluence:
Theorem 8 [20]. A terminating rewrite system is Church-Rosser if and only if it is locally confluent.

A rewrite system is locally confluent if (but not only if) no left-hand side unifies with a non-variable subterm (except itself) of any left-hand side, taking into account that variables appearing in two rules (or in two instances of the same rule) are always treated as disjoint. To get confluence for nonterminating systems we have an additional requirement:

**Definition 9 Orthogonal System.** A rewrite system is orthogonal if no left-hand side unifies with a renamed non-variable subterm of any other left-hand side or with a renamed proper subterm of itself, and no variable appears more than once on any left-hand side.

The importance of orthogonal systems stems from the following result:

**Theorem 10 [22].** Every orthogonal system is confluent.

In particular, our erstwhile interpreter is confluent.

**Example 4 Combinatory Logic.** Combinatory Logic is a prime example of a (nonterminating) orthogonal system (juxtaposition and $\langle,\rangle$ are binary operators):

$$
\begin{align*}
Ix & \rightarrow x \\
(Kx)y & \rightarrow x \\
((Sx)y)z & \rightarrow (xz)(yz).
\end{align*}
$$

This system can be used to implement any recursive function. The combinators $K$ and $S$ were dubbed “kestrel” and “starling” by Smullyan; $I$ is the identity combinator. □

**Example 5 Cartesian Closed Categories.** The following non-orthogonal, non-confluent system is used in the compilation of functional languages (juxtaposition represents the binary composition operator):

$$
\begin{align*}
Ix & \rightarrow x \\
xI & \rightarrow x \\
xy & \rightarrow x(yz) \\
(x,y)z & \rightarrow xz, yz \\
F(x,y) & \rightarrow x \\
E(Cx,y) & \rightarrow xy \\
S(x,y) & \rightarrow y \\
(Cx)y & \rightarrow C(xy,F,S).
\end{align*}
$$

The combinators $E$ and $C$ stand for “evaluation” and “Currying”, respectively; $I$ is the identity morphism; $F$ and $S$ project the components of pairs $\langle,\rangle$. □

For terminating confluent systems, any rewriting strategy will lead to the unique normal form of any given term; for nonterminating orthogonal systems, we defer to the discussion in Sect. 9. Also, for terminating systems, there is a stronger result, relating confluence to joinability in a finite number of cases:

**Definition 11 Critical Pair.** If $l \rightarrow r$ and $s \rightarrow t$ are two rewrite rules (with variables made distinct) and $\mu$ is a most general unifier of $l$ and a nonvariable subterm $s'$ of $s$, then the equation $t\mu = s\mu[r\mu]$, where $r\mu$ has replaced $s'\mu = (l\mu)$ in $s\mu$, is a critical pair.

A finite rewrite system has a finite number of critical pairs.

**Theorem 12 [28][25].** A rewrite system is locally confluent if and only if all its critical pairs are joinable. Therefore, a terminating system is confluent (hence, convergent) if and only if all its critical pairs are joinable.

Insertion Sort has one trivially joinable critical pair, 0=0, formed from either the first two rules, or the fourth and fifth.
Example 6 Fragment of Group Theory. Each of the rules

\[
\begin{array}{ll}
0 + x & \rightarrow x \\
-x + x & \rightarrow 0 \\
-x & \rightarrow 0 \\
-x + (x + y) & \rightarrow y \\
x + ((-x) + y) & \rightarrow y
\end{array}
\]

follows from some combination of the following three axioms:

\[
\begin{align*}
x + 0 & = x \\
0 + x & = x \\
(-x) + (x + y) & = y
\end{align*}
\]

This system has numerous critical pairs, all of which are joinable. For example, the rules \(x + (-x) \rightarrow 0\) and \(x + ((-x) + y) \rightarrow y\) form a critical pair \(x + 0 = -(x)\), both sides of which reduce, via other rules, to \(x\). □

Definition 13 Encompassment. A term \(s\) encompasses a term \(t\) if a subterm of \(s\) is an instance of \(t\). We write \(s \triangleright t\) if \(s\) encompasses \(t\), but not vice-versa.

Definition 14 Reduced System. A system \(R\) is reduced if, for each rule \(l \rightarrow r\) in \(R\), the right-hand side \(r\) is irreducible (unrewritable) and if \(l \triangleright l'\), for the left-hand side \(l\), then \(l'\) is irreducible (proper subterms of \(l\) are in normal form, as is any term more general than \(l\)).

The above Fragment is reduced, but the Interpreter isn’t.

Definition 15 Canonical System. A rewrite system is canonical if it is confluent, terminating, and reduced.

The following interesting fact was observed by a number of people:

Theorem 16 [29]. Suppose two canonical (not necessarily finite) rewrite systems have the same equational theory (that is, their convertibility relations are the same) and when combined are still terminating. Then the two must be identical up to renaming of variables.

Two interesting results with practical repercussions are:

Theorem 17 [27]. The union of two confluent rewrite systems sharing no function symbols (or constants) is also confluent.

Theorem 18 [94]. The union of two convergent rewrite systems sharing no function symbols (or constants), and in which no variable appears more than once on any left-hand side, is also convergent.

4 Completion

To construct confluent systems, a method is used, called completion, which turns critical pairs into rewrite rules. Completion uses an ordering to orient equations and to allow use of unoriented equations to simplify. This ordering should be a reduction ordering, defined as follows:

Definition 19 Reduction Ordering. A well-founded partial ordering \(\succ\) on terms is a reduction ordering if \(s \succ t\) implies \(u[s] \succ u[t]\), for any context \(u[\cdot]\) and substitution \(\sigma\).
The path ordering is not necessarily a reduction ordering, but its major special cases, including the lexicographic and multiset path orderings, are.

The encompassment ordering also plays a role in most versions of completion. It is used to determine which of two rules is more general, and hence preferred.

In our version of completion, not only rules, but also equations, are used to rewrite with. A term $u[\sigma]$, containing an instance of $l$ of an equation $l = r$ or $r = l$, may be rewritten to $u[r\sigma]$ whenever $u[\sigma]$ is greater than $u[r\sigma]$ in the given reduction ordering.

We require a broader notion of critical pair:

**Definition 20 Ordered Critical Pair.** Given a reduction ordering $\succ$, if $l = r$ and $s = t$ are two (not necessarily distinct) equations (with variables distinct), $\mu$ is a most general unifier of $l$ and a nonvariable subterm of $s$, and $s\mu$ is not necessarily smaller than either $t\mu$ or $sp[r\mu]$, then the equation $t\mu = sp[r\mu]$ is a (ordered) critical pair formed from those equations. (Term $s$ is not necessarily smaller than term $t$ if there is a substitution $\sigma$ such that $s\sigma \succ t\sigma$.)

Completion maintains a set of unoriented equations $E$ and a set of rules $R$ oriented according to the given reduction ordering $\succ$. These sets are manipulated in the following six ways:

**Deduce:** Add a critical pair of $R$ and/or $E$ to $E$.

**Simplify:** Use a rule in $R$ to rewrite either side of an equation $s = t$ in $E$. Or use an equation $l = r$ in $E$ (or use $r = l$ in $E$) to rewrite $s$ (or $t$), provided $l$ strictly encompasses $s$ (or $t$).

**Delete:** Remove an equation from $E$ whose sides are identical.

**Orient:** Remove an equation $s = t$ (or $t = s$) from $E$ such that $s \succ t$. Add the rule $s \rightarrow t$ to $R$.

**Compose:** Use $R$ or $E$ to rewrite the right-hand side of an existing rule.

**Collapse:** Use a rule $l \rightarrow r$ in $R$ or equation $l = r$ in $E$ to rewrite the left-hand side $s$ of a rule in $R$, provided $l$ strictly encompasses $s$. Remove the rewritten rule from $R$ and place it as an equation in $E$.

One simple version of completion mixes the above inference steps according to the following strategy:

$$(((\text{Simplify} \cup \text{Delete})^*; (\text{Orient}; \text{Compose}^*; \text{Collapse}^*))^*; \text{Deduce})^*.$$  

In words: simplify and delete equations as much as possible before orienting. Use the newly oriented equation to fully compose right-hand sides and collapse left-hand sides of all non-reduced existing rules; then, go back and simplify over again. When there are no equations left to orient, generate one new critical pair, and repeat the whole process.

Different versions of completion differ in which equations they orient first and in how they keep track of critical pairs that still need to be deduced. They, in fact, often skip some critical pairs. A version of completion is **fair** if it does not altogether avoid processing any relevant critical pair. Running completion with a fair strategy can have one of three outcomes: it might converge on a finite system that is a decision procedure for the initial set of equations; it might reach a point in which all (ordered) critical pairs have been considered and all have rewrite proofs—using rules and equations; or it might loop and generate an infinite number of rules and/or equations.

**Theorem 21 [43][40].** For any fair completion strategy, if at some point all critical pairs between persisting rules have been considered and no equation persists forever in $E$, then the (finite or infinite) set of rules persisting in $R$ is convergent.
This means that eventually both sides of any identity in the theory of the initial set of equations will become joinable.

**Example 7 Abelian Groups I.** Completion, given

\[
\begin{align*}
    x \cdot 1 &= x \\
    x \cdot (y \cdot z) &= (x \cdot y) \cdot z \\
    x \cdot x^- &= 1,
\end{align*}
\]

and a lexicographic path ordering (in which \( \succ \succ \succ \succ \) and \( \cdot \) looks at its left argument first) will generate the following decision procedure for free Abelian (commutative) groups:

\[
\begin{array}{c|c}
  1^- & 1 \\
  x \cdot 1 & x \\
  x \cdot (y \cdot z) & x \cdot (y \cdot z) \\
  1 \cdot x & x \cdot (y \cdot z) \\
  (x^-)^- & x \cdot (x^- \cdot z) \\
  x \cdot x^- & (y \cdot x)^- \\
\end{array}
\]

Those equations used in both directions have a two-headed arrow. To decide validity of an equation \( s = t \), the lexicographic path ordering is extended to a total ordering that includes any constants appearing in \( s \) or \( t \). The double-headed rules are then used only in a direction that reduces in this ordering. The equation is valid if and only if both \( s \) and \( t \) have the same normal form.

**Definition 22 Completal Simplification Ordering.** A reduction ordering is a completal simplification ordering if it can be extended to a reduction ordering that is total on ground terms (in which any two distinct terms—made up of function symbols and constants occurring in the given equations—are comparable).

Such orderings have the property that every term is strictly greater than its proper subterms. Examples include the empty ordering, the lexicographic path ordering with a partial or total precedence, and the polynomial path ordering.

**Theorem 23 [33][40].** Suppose \( R \) is a finite convergent system for axioms \( E \) and \( \succ \) is a completal simplification ordering for which all rules in \( R \) decrease. Any fair completion strategy will generate a finite convergent system for \( E \) (not necessarily identical to \( R \)).

If \( R \) is canonical and the strategy performs all compositions and collapses, then, by Theorem 16, completion will actually produce \( R \).

The efficiency of completion depends on the number of critical pairs deduced. In general, an equation \( s = t \) is redundant if there exist proofs \( Q_i \) of equations \( u_i = u_i, i = 1, \ldots, n \), such that \( u_0 = s \), \( u_{n+1} = t \), \( u > u_0, \ldots, u_{n+1} \), and the proof \( s \leftarrow u \rightarrow t \) from which the critical pair was formed is greater than each of the \( Q_i \) in some well-founded ordering \( \gg \) on equational proofs. (The proof ordering \( \gg \) must have the property that a proof decreases by replacing a subproof with one involving terms that are all smaller vis-à-vis the reduction ordering \( \succ \) supplied to completion.)

The following can be shown by induction with respect to \( \gg \):

**Theorem 24 [40].** For any fair completion strategy, if at some point all non-redundant critical pairs between persisting rules have been considered and no equation persists forever in \( E \), then the (finite or infinite) set of rules persisting in \( R \) is convergent.

For the Group Fragment, the critical pair \( y = (-0) + y \), obtained by rewriting \( (-0) + (0 + y) \) with \( 0 + x \rightarrow x \) and \( (0 + x) + (x + y) \rightarrow y \), is redundant since \( (-0) + (0 + y) \) is greater than each of the terms in the alternative proof \( y \leftarrow 0 + y \leftarrow (-0) + y \).

Various techniques have been used in practice to check for redundancy. In particular, a critical pair can be ignored if the variable part of either of the rules involved becomes reducible. Experimental results that give some indication of the utility of such redundancy criteria have been reported, particularly in the associative-commutative case described in the next section.
5 Validity

In addition to its use for generating canonical systems to serve as decision procedures for the given axioms, completion may also be used as an equational theorem prover. Classical forward reasoning systems work from the axioms, “expanding” the set of established formulæ by inferring new ones from old ones. Completion may be viewed as an inference engine that also “contracts” formulæ by constantly rewriting them, making forward reasoning practical. The potentially infinite set of rules and equations generated by completion are used to simplify the two sides of the equation in question. Rules are used in the indicated direction only, while equations are used in whichever direction reduces the term it is applied to in the given ordering. An identity is proved when both sides reduce via rules and equations to the identical term.

For completeness of this theorem-proving methodology, we require a completable ordering.

Theorem 25 [75][44][33]. Suppose $s \equiv t$ is a theorem of $E$. For any fair completion strategy starting with $E$ and a completable simplification ordering, at some point $s$ and $t$ will rewrite to the identical term using the generated rules and equations.

The word problem in arbitrary equational theories can always be semi-decided in this way. With an empty ordering, completion amounts to ordinary paramodulation of unit equations; with more of an ordering, completion can be more effective, by reducing the number of allowed inferences and increasing the amount of simplification that may be performed without loss of completeness.

Example 8 Distributive Lattices. With axioms:

\[
\begin{align*}
x \land x &= x \\
x \land y &= y \land x \\
x \lor x &= x \\
x \lor y &= y \lor x \\
(x \land y) \land z &= x \land (y \land z) \\
(x \lor y) \lor z &= x \lor (y \lor z) \\
(x \lor y) \land x &= x \\
(x \land y) \lor x &= x \\
x \lor (y \land z) &= (x \land y) \lor (x \land y),
\end{align*}
\]

and a lexicographic path ordering that makes meet bigger than join, completion eventually generates:

\[
x \land (y \lor z) \to (x \lor y) \land (x \lor y).
\]

The above method can be refined to ignore critical pairs that have different rewrite proofs, each depending on the relative ordering of terms substituted for variables.

6 Satisfiability

We turn now from questions of validity to satisfiability.

If ground terms are joinable whenever they are convertible, we say the system is ground confluent. If it is, in addition, terminating, then it’s ground convergent.

Definition 26 Ground Convergence. A system is ground convergent if every ground (variable-free) term always rewrites to a unique normal form.

Ground convergence is a reasonable property to expect from a rewrite system, like Insertion Sort, used as a program. Such programs compute the value of a ground term by rewriting it to its unique normal form.

Definition 27 Narrowing. A term $s$ narrows to a term $t$, symbolized $s \leadsto t$, if $t = s[t/\mu]$, for some non-variable subterm $s'$ of $s$, renamed rule $t \leadsto r$ in $R$, and most general unifier $\mu$ of $s'$ and $t$.

By $\leadsto^*$ we denote the reflexive-transitive closure of this narrowing relation.
Theorem 28 [48]. If $R$ is a rewrite system, $\sigma$ is an irreducible substitution (that is, $x\sigma$ is irreducible for all variables $x$), and $s\sigma \rightarrow^* t$, then there exists a term $u$ such that $s \sim^* u$ and $u$ is at least as general as $t$.

A term $u$ is at least as general as a term $t$ if there is a substitution $\tau$ such that $t\tau = u$.

Thus, narrowing can be used with such systems to solve equational goals; a solution is a substitution $\sigma$ for which $s\sigma$ has normal form $t$. Narrowing a goal $eval(p, (x, 0, 0))$ with the Interpreter, where $p$ is some fixed program, will find all inputs $x$ that lead to various final triples. The unifiers of each step are composed to get the solution to the original goal.

Theorem 29 [8]. If $R$ is a ground convergent rewrite system and $s\sigma \rightarrow^* t$, then there exist terms $u$ and $v$ such that $s \sim^* u$, $t \rightarrow^* v$, and $u$ is at least as general as $v$.

Example 9 List Append. With the program

\[
\begin{align*}
\text{append}(\text{nil}, y) & \rightarrow y \\
\text{append}(\text{cons}(x, z), y) & \rightarrow \text{cons}(x, \text{append}(z, y))
\end{align*}
\]

the goal $\text{append}(x, y)$ generates all lists $x$ and the result of appending them to $y$. For example, $\text{append}(x, y) \sim y$ with $x \leftarrow \text{nil}$.

Without convergence, reducible solutions are lost. Variations on narrowing include: normal narrowing in which terms are rewritten to normal form before narrowing; basic narrowing in which the substitution part of prior narrowings is not subsequently narrowed; top-down narrowing in which terms are decomposed from top down to identify necessary narrowings; left-to-right narrowing in which the leftmost possible narrowing is performed at each step; other restrictions obtain all solutions only in special cases.

7 Associativity and Commutativity

Many axioms are difficult to handle by rewriting. We could not, for example, include the non-terminating rule $x + y \rightarrow y + x$ in a rewrite-system decision procedure. Instead, we can restrict application of the rule to commute only in the direction that decreases the term in some given ordering. For example, we might allow $2 + 1$ to be replaced by $1 + 2$, but not vice-versa, as done in Sect. 5. Another approach is to use commutativity only to enable the application of other rules. For example, we would apply a rule $x + 0 \rightarrow x$ to $0 + 1$, as well as to $1 + 0$. In the associative-commutative (AC) case, this means that $u[s] \rightarrow u[\text{let}]$ whenever $s$ is equal under AC to an instance $\sigma$ of the left-hand side of some rule $l \rightarrow r$ (that is, $s$ and $\sigma$ may have arguments to AC symbols permuted). Thus, AC-matching must be used to detect applicability of rules in this case for AC-rewriting.

To better handle these problematic identities, reasonably efficient special-purpose completion procedures have been designed. For instance, the completion procedure given in the previous section may be modified in the following ways to handle AC symbols:

1. An equation $s = t$ is oriented only if $s' \succ t'$ for any AC variants $s'$ of $s$ and $t'$ of $t$. This ensures that each AC-rewrite reduces the term it is applied to.
2. AC-unification is used to generate critical pairs instead of ordinary unification. This means that we look at the set of most general substitutions that allow a left-hand side to be AC-equivalent to a non-variable subterm of another left-hand side, and get a critical pair for each such ambiguously rewritable term.
3. AC-rewriting is used for composition, collapsing, and simplification.
4. Any equation between AC-variants is deleted.
5. An additional expansion operation is needed: whenever a new equation $f(s, t) = r$ is formed, where $f$ is an AC symbol and $f(s, t) \neq r$, an extended equation $f(s, f(t, z)) = f(r, \text{cons}(z))$ is added, too, for some new variable $z$. This ensures that $f(s, t) = r$ can be used even when rearrangement is needed to get an instance of its left-hand side.
Recall that the Chameleons do not terminate. But if we turn any of the rules around, they do! Though the result is not confluent, AC completion can be used to generate a confluent system of rules and equations: Start off with the three rules as unoriented equations, and use an ordering with red > yellow > green. The oriented equations are:

\[
\begin{align*}
\text{red yellow} & \rightarrow \text{green green} \\
\text{red red} & \rightarrow \text{green yellow} \\
\text{red green} & \rightarrow \text{yellow yellow}.
\end{align*}
\]

Notice how the second rule acts contrary to the "real" chameleons. The extended rules are:

\[
\begin{align*}
\text{yellow (red z)} & \rightarrow \text{green (green z)} \\
\text{red (red z)} & \rightarrow \text{green (yellow z)} \\
\text{green (red z)} & \rightarrow \text{yellow (yellow z)},
\end{align*}
\]

and their commutative variants. The green red and extended yellow red rules produce an critical pair yellow (yellow yellow) = green (green green), which gets oriented from left to right:

\[
\text{yellow (yellow yellow)} \rightarrow \text{green (green green)}.
\]

The complete system reduces the initial state and the monochrome states to distinct normal forms. (Which?) Since the system is Church-Rosser, there is no way to get from the initial arrangement of chameleons to one in which they are of uniform color, no matter which way any of the rules are used.

**Example 10 Abelian Groups II.** The AC-completion procedure, given

\[
\begin{align*}
x \cdot 1 & = x \\
x \cdot x^- & = 1,
\end{align*}
\]

where \(\cdot\) is AC, and a polynomial ordering in which \(\tau_0(x \cdot y) = \tau_0(x) + \tau_0(y) + 1, \tau_0(x^-) = 2\tau_0(x), \) and \(\tau_0(1) = 1,\) generates the following decision procedure for Abelian groups:

\[
\begin{align*}
1^- & \rightarrow 1 \\
(x^-)^- & \rightarrow x \\
(x \cdot x^-)^- & \rightarrow x^- \cdot y^- \\
x \cdot x^- & \rightarrow 1 \\
(x \cdot (x^- \cdot z))^- & \rightarrow z.
\end{align*}
\]

The last rule is a composed version of the extension \(x \cdot (x^- \cdot z) \rightarrow 1 \cdot z\) of \(x \cdot x^- \rightarrow 1.\) This extended rule, together with with \((y_0 \cdot x_0)^- \rightarrow x_0^- \cdot y_0^-\), forms a critical pair

\[
(x_2 \cdot z_1)(x_2 \cdot (x_1 \cdot x_2)^- \cdot z_2)^- = (z_1 \cdot z_2)^-
\]

via AC-unifier \(x \leftrightarrow x_1 \cdot x_2, z \leftrightarrow z_1 \cdot z_2, y_0 \leftrightarrow x_1 \cdot z_1,\) and \(x_0 \leftrightarrow x_2 \cdot x^- \cdot z_2.\) Both sides reduce to \(z_2^- \cdot z_1^-\).

With this system, both sides of any identity reduce by AC-rewriting to AC-equivalent terms.

The Greecian Urn may also be viewed as an AC-rewriting system. Beans are rearranged until the pair to be removed are adjacent. Extended with rules \(l \ z \rightarrow r \ z\) for each original bean rule, \(; \rightarrow r\), this is system is confluent. For instance, \(\text{black white} \rightarrow \text{white}\) and the extended rule \(\text{white white} \ z \rightarrow \text{black z}\), rewrite a \(\text{black white white}\) bean arrangement to \(\text{white white}\) and \(\text{black black}\), respectively, both of which rewrite to \(\text{black}\). This means that the normal form is independent of the order in which rules are applied. If there are an even number of white beans, they can be paired and reduced to black, and then all the black beans reduce to one; if there are an odd number, the leftover white bean swallows all remaining blacks.
Example 11 Ring Idempotents. The ring axioms
\[
\begin{align*}
x + 0 &= x & x(y + z) &= (xy) + (xz) \\
x + (-x) &= 0 & (y + z)x &= (yx) + (zx) \\
x + y &= y + x & (x + y) + z &= x + (y + z)
\end{align*}
\]
plus
\[
\begin{align*}
ba &= a \\
bb &= b \\
cc &= c \\
(a + b + c(a + b + c) &= a + b + c.
\end{align*}
\]

can be completed, with an appropriate ordering, to a convergent AC system that includes the rules
\[
\begin{align*}
ba &\rightarrow \neg(ab) + \neg(bc) + \neg(cb) + \neg(ac) + \neg(ca) \\
bc &\rightarrow abc + acb + cab + cba + abc + ab + ac + cb + ba + ca + bc.
\end{align*}
\]

The normal forms of this system include (besides inverses and sums) all monomials (the order of factors matters) not containing \(ba\), \(bb\), \(cc\), \(ba\), or \(bc\).

\[\square\]

8 Conditional Rewriting

A conditional rewrite system is a collection of rules of the form
\[
u_1 = v_1 \land \cdots \land u_n = v_n \mid l \rightarrow r,
\]
meaning that terms \(u[\sigma]\), containing an instance of left-hand side \(l\), rewrite to \(v[\sigma]\) only when all the conditions \(u_\sigma = v_\sigma\) hold. The most popular operational semantics for such a system require both sides of each condition to rewrite to the same normal form before an instance of \(l\) may be rewritten.

Example 12 Conditional Append. To get the flavor of this expanded notion of rewriting, consider the system
\[
\begin{align*}
null(nil) &\rightarrow true \\
null(cons(x, y)) &\rightarrow false \\
car(cons(x, y)) &\rightarrow x \\
cdr(cons(x, y)) &\rightarrow y \\
null(x) = false &\rightarrow append(x, y) \rightarrow cons(car(x), append(cdr(x), y))
\end{align*}
\]
and its derivation
\[
append(cons(a, cons(b, nil)), cons(c, nil)) \rightarrow^* cons(a, cons(b, cons(c, nil))).
\]

\[\square\]

Definition 30. A conditional rewrite system is orthogonal if each variable occurs at most once in a left-hand side of each rule, one side of each condition in each rule is a ground normal form, and no left-hand side unifies with a renamed non-variable subterm of any other left-hand side or with a proper subterm of itself.

Theorem 31 [56]. Every orthogonal conditional rewrite system is confluent.

This definition of orthogonality could be weakened to allow overlaps when the conjunction of the conditions of the overlapping rules cannot be satisfied by the rules of the system. This is the case with the Conditional Append example, since only the last two rules overlap, but \(null(nil)\) can never be \(false\).

For non-orthogonal systems, another approach is required. Under certain circumstances terminating systems are confluent if all their critical pairs are joinable, but we need a suitable notion of critical pair:
**Definition 32** Conditional Critical Pair. Let $R$ be a conditional rewrite system. The conditional equation $c\mu \land p\mu \Rightarrow sp[\rho]\mu \Rightarrow t\mu$ is a conditional critical pair of $R$ if $c \vdash l \rightarrow r$ and $p \mid s \rightarrow t$ are conditional rules of $R$, $l$ unifies via most general unifier $\mu$ with a nonvariable subterm of $s$ and $c\mu \land p\mu$ is satisfiable in $R$.

**Theorem 33** [59]. If no left-hand side unifies with a nonvariable proper subterm of a left-hand side, and if every critical pair is joinable, then the system is confluent.

A conditional critical pair $p \Rightarrow s=t$ is joinable if $s\sigma$ and $t\sigma$ are joinable for all $\sigma$ satisfying $p$.

**Definition 34** Decreasing Systems. A conditional system is decreasing if there exists a well-founded ordering $\gg$ containing the rewrite relation $\rightarrow$ and which satisfies two additional requirements: (a) $\gg$ has the subterm property $f(\ldots, s, \ldots) \gg s$, and (b) $l\sigma \gg t\sigma$ for each rule $c \mid l \rightarrow r$ and substitution $\sigma$.

Decreasing systems exactly capture the finiteness of recursive evaluation of terms. The notion needs to be extended, however, to cover systems (important in logic programming) with variables in conditions that do not also appear in the left-hand side.

**Theorem 35** [57][59]. A decreasing system is confluent (hence, convergent) if and only if there is a rewrite proof of $s\sigma=t\sigma$ for each critical pair $c \Rightarrow s=t$ and substitution $\sigma$ such that $c\sigma$ holds.

Conditional Append is decreasing.

**Example 13** Stack. The following is a decreasing conditional rewrite system:

\[
\begin{align*}
\text{top}(\text{push}(x, y)) & \rightarrow x \quad \text{pop}(\text{push}(x, y)) \rightarrow y \\
\text{empty}!(\text{empty}) & \rightarrow \text{true} \\
\text{empty}!(\text{push}(x, y)) & \rightarrow \text{false} \\
\text{empty}!(x) & = \text{false} \mid \text{push(top(x), pop(x))} \rightarrow x.
\end{align*}
\]

\[\square\]

Completion has been extended to conditional equations, with "ordered" conditional critical pairs turned into rules only if they are decreasing.

9 Programming

Rewrite systems are readily used as a programming language. If one requires of the programmer that all programs be terminating, then rewriting may be used as is to compute normal forms. With ground confluence, one is assured of their uniqueness.

Many programs (interpreters, for example) do not always terminate. Still, we would want to compute normal forms whenever they exist. Confluent systems have at most one normal form per input term. To find the unique normal form for orthogonal systems, we use the following strategy for choosing the point at which to apply a rule:

**Definition 36** Outermost Rewriting. A rewriting step $s \rightarrow t$ is outermost if no rule applies at a symbol closer to the root symbol (in the tree representation of terms).

**Theorem 37** [64]. For any orthogonal system, if no outermost step is perpetually ignored, the normal form—if there is one—will be reached.
Outermost rewriting of expressions is used to compute normal forms in Combinatory Logic.

In this way, orthogonal systems provide a simple, pattern-directed (first-order) functional programming language, in which the orthogonal conditional operator

\[
\begin{align*}
if(\text{true}, x, y) & \rightarrow x \\
if(\text{false}, x, y) & \rightarrow y
\end{align*}
\]

can also conveniently be incorporated. Various strategies have been developed for efficient computation in special cases. Moreover, orthogonal systems lend themselves easily to parallel evaluation schemes.

Conditional equations provide a natural bridge between functional programming, based on equational semantics, and logic-programming, based on Horn clauses. Interpreting definite Horn clauses \( p \lor q_1 \lor \cdots \lor q_n \) as conditional rewrite rules, \( q_1 = \text{true} \land \cdots \land q_n = \text{true} \mid p \rightarrow \text{true} \) gives a system satisfying the constraints of Theorem 33, because predicate symbols are never nested in the "head" (\( p \)) of a clause. Furthermore, all critical pairs are joinable, since all right-hand sides are the same (\text{true}).

Solving existential queries for conditional equations corresponds to the logic-programming capability of resolution-based languages like Prolog. Goals of the form \( s \rightarrow t \) can be solved by a linear restriction of paramodulation akin to narrowing (for unconditional equations) and to the SLD-strategy in Horn-clause logic. If \( s \) and \( t \) are unifiable, then the goal is satisfied by any instance of their most general unifier. Alternatively, if there is a (renamed) conditional rule \( c \mid l \rightarrow r \) such that \( l \) unifies with a nonvariable (selected) subterm of \( s \) via most general unifier \( \mu \), then the conditions in \( c\mu \) are solved, say via substitution \( \rho \), and the new goal becomes \( s\mu \rightarrow t\mu \).

Suppose we wish to solve

\[
\text{append}(x, y) \rightarrow x
\]

using Conditional Append. To apply the conditional rule, we need first to solve \( \text{null}(x) = \text{false} \) using the (renamed) rule \( \text{null}(\text{cons}(u, v)) \rightarrow \text{false} \), thereby narrowing the original goal to

\[
\text{cons(car(\text{cons}(u, v)), \text{append}(\text{cdr(\text{cons}(u, v)), y))))} \rightarrow \text{cons}(u, v).
\]

Straightforward rewriting reduces this to

\[
\text{cons}(u, \text{append}(v, y)) \rightarrow \text{cons}(u, v),
\]

to which the first rule for append applies (letting \( v \) be \text{nil} \)), giving a new goal \( \text{cons}(u, y) \rightarrow \text{cons}(u, v) \). Since the two terms are now unifiable, this process has produced the solution \( x \leftarrow \text{cons}(u, \text{nil}) \) and \( y \leftarrow \text{nil} \).

For ground confluent conditional systems, any equationally satisfiable goal can be solved by the method outlined above. Some recent proposals for logic programming languages, incorporating equality, adopt such an operational mechanism.

Simplification via terminating rules is a very powerful feature, particularly when defined function symbols are allowed to be arbitrarily nested in left-hand sides (which is permitted with orthogonal rules). Assuming ground convergence, any strategy can be used for simplification, and completeness of the goal-solving process is preserved. One way negation can be handled is by incorporating negative information in the form of rewrite rules which are then used to simplify subgoals to \text{false}. Combined with eager simplification, this approach has the advantage of allowing unsatisfiable goals to be pruned, thereby avoiding some potentially infinite paths. Various techniques are also available to help avoid some superfluous paths that cannot lead to solutions.

\section{10 Theorem Proving}

We have already seen how completion is used to prove validity of equations in equational theories (that is, truth in all models) and also how narrowing and related methods can be used to solve equational goals in conditional and unconditional theories. In this section we will see how to handle the non-equational case.
Completion can be used to prove validity of Horn clauses in Horn theories by writing each clause \( \neg q \lor p \) as an equation \( p \land q \Rightarrow q \), and each unit clause \( p \) as \( p = \text{true} \). The completeness of completion for equational reasoning means that an equational proof will be found for any atomic formula, the validity of which follows from a given set of clauses, all expressed as just indicated (plus the Boolean equation \( \text{true} \land x = x \)).

One approach to extending rewriting methods to the full first-order predicate calculus is to add inference rules for restricted forms of paramodulation to refutational theorem provers. An ordering of terms and formulae is used to restrict inferences and to allow simplification.

Alternatively, one can apply completion to the full first-order case by employing Boolean algebra. The following AC system does the trick:

\[
\begin{align*}
x \lor \text{true} & \rightarrow \text{true} & x \equiv \text{true} & \rightarrow x \\
x \lor \text{false} & \rightarrow x & (x \equiv y) \lor z & \rightarrow (x \lor z) \equiv (y \lor z) \\
x \lor y & \rightarrow y \lor x & x \lor (y \lor z) & \rightarrow (x \lor y) \lor z \\
x \equiv y & \rightarrow y \equiv x & x \equiv (y \lor z) & \rightarrow (x \equiv y) \equiv z \\
x \lor x & \rightarrow x & x \lor x \lor y & \rightarrow x \lor y \\
x \equiv x & \rightarrow \text{true} & x \equiv x \equiv y & \rightarrow y ,
\end{align*}
\]

where \( \lor \) is "inclusive or" and \( \equiv \) is "equivalent". With this system, all propositional tautologies reduce to \( \text{true} \) and contradictions, to \( \text{false} \). To prove validity of a formula, one Skolemizes its negation (and renames variables) to obtain a universally quantified formula, and expresses it using the above connectives. Then, were the original formula \( \text{true} \), there would be an equational proof of the contradiction \( \text{true} = \text{false} \). Completion can be used to discover such a proof.

As a very simple example, consider the theorem

\[
\exists x p(x) \land \forall x (p(x) \lor p(f(x)))) \Rightarrow \exists x p(f(f(x))) .
\]

Its Skolemized negation is equivalent to the following equations:

\[
\begin{align*}
p(f(f(x))) &= \text{false} \\
p(a) &= \text{true} \\
p(x) \lor p(f(x)) &= p(f(x)) ,
\end{align*}
\]

where \( a \) is a Skolem constant. These equations entail the contradiction:

\[
\begin{align*}
\text{true} &= \text{true} \lor [p(f(a)) \lor p(f(f(a)))] = p(a) \lor [p(f(a)) \lor p(f(f(a)))] = p(f(a)) \lor p(f(f(a))) = p(f(f(a))) = \text{false} .
\end{align*}
\]

For program verification, one often needs to prove that an equation or formula holds in the standard (initial) model, rather than in all models. Such proofs typically require the use of induction. Rewriting techniques have been applied to inductive proofs of equations, establishing \( s = t \) in the standard model of the axioms by proving that \( s \sigma \) and \( t \sigma \) are joinable for all substitutions \( \sigma \) of ground terms constructed from function symbols and constants appearing in the axioms. For example, the equation \( \text{append}(x, \text{nil}) = x \) is true for all lists \( x \), but is not true in all other models of the List Append axioms. The equation \( \text{black} x = x \) is true for all strings of beans \( x \), but does not follow equationally from AC and the Grecian Um rules.

**Definition 38** Cover Set. Let \( R \) be a rewrite system and \( \rightarrow \) be a reduction ordering containing its rewriting relation \( \rightarrow \). A cover set \( S \) for conjecture \( c \) is a set of equations such that every ground instance \( c \sigma \) is equal (in the equational theory of \( R \)) to an instance \( \epsilon \sigma \) of an equation \( \epsilon \) in \( S \), such that \( c \sigma \succeq \epsilon \sigma \).

**Definition 39** Rewriting Induction. Let \( R \) be a rewrite system and \( \rightarrow \) be a reduction ordering containing its rewriting relation \( \rightarrow \). Let \( c \) be a conjecture and \( S \), its cover set. Rewriting induction is the rule of inference which allows one to conclude that every ground instance of \( c \) is true for \( R \) by showing that each case \( \epsilon \) in \( S \) follows (equationally) from \( R \) and instances \( \epsilon \sigma \) of the hypothesis that are smaller than \( \epsilon \) vis-a-vis \( \rightarrow \).
In practice, a conjecture \( s = t \) is proved by expanding it into cases \( s \sigma_1 = t \sigma_1, \ldots, s \sigma_n = t \sigma_n \), for some "covering" substitutions \( \sigma_1, \ldots, \sigma_n \), rewriting each case to be proved at least once using \( R \), then attempting to construct rewrite proofs for them, freely using the inductive hypothesis \( s = t \). The rewrite step guarantees that all instances of the hypothesis used in the rewrite proofs are smaller than the case of the conjecture under consideration. For ground convergent systems, narrowing at a particular position in a term is often a convenient method of generating cover sets and taking the requisite first step.

**Theorem 40** [89]. **Rewriting induction is sound.**

**Example 14** Reversal of Lists. Consider the following canonical system for reversing lists:

\[
\begin{align*}
\text{reverse}(\text{nil}) & \rightarrow \text{nil} \\
\text{reverse}(\text{cons}(x, y)) & \rightarrow \text{append}(\text{reverse}(y), \text{cons}(x, \text{nil})) \\
\text{append}(\text{nil}, x) & \rightarrow x \\
\text{append}(x, \text{nil}) & \rightarrow x \\
\text{append}(\text{cons}(x, y), z) & \rightarrow \text{cons}(x, \text{append}(y, z)) \\
\text{append}(\text{cons}(x, y), z) & \rightarrow \text{append}(x, \text{append}(y, z)),
\end{align*}
\]

and suppose one wishes to prove that

\[
\text{reverse}(\text{append}(x, y)) = \text{append}(\text{reverse}(y), \text{reverse}(x)).
\]

All cases are covered by \( x \mapsto \text{nil} \) and \( x \mapsto \text{cons}(x_1, x_2) \), since ground terms containing \( \text{reverse} \) or \( \text{append} \) reduce to lists built of \( \text{cons} \) and \( \text{nil} \). The corresponding two instances of the conjecture form a cover set. For \( x = \text{nil} \), we need \( \text{reverse}(y) = \text{reverse}(y) \), which is trivially the case. For \( x = \text{cons}(x_1, x_2) \), we need to show

\[
\begin{align*}
\text{append}(\text{reverse}(\text{append}(x_2, y)), \text{cons}(x_1, \text{nil})) & = \\
\text{append}(\text{reverse}(y), \text{append}(\text{reverse}(x_2), \text{cons}(x_1, \text{nil}))).
\end{align*}
\]

The left side rewrites by hypothesis to

\[
\text{append}(\text{append}(\text{reverse}(y), \text{reverse}(x_2)), \text{cons}(x_1, \text{nil})),
\]

which rewrites to the right-hand side. \( \square \)

In more complicated cases, additional lemmata may need to be added to \( R \) along the way. Completion can help find them.

Unlike traditional inductive proof methods, rewriting induction is guaranteed to disprove a false conjecture. (Of course, no method can prove all true ones.)

**Definition 41** Ground Reducibility. A term \( s \) is ground reducible with respect to a rewrite system if all its ground instances \( s^g \) are rewriteable.

**Theorem 42** [80][84]. Ground reducibility is decidable for finite rewrite systems, but undecidable for AC systems.

**Theorem 43** [34][88][37]. An equation \( c \) is not an inductive theorem of a ground convergent rewrite system \( R \) if and only if deducing critical pairs by unifying left-hand sides of rules in \( R \) on the larger (rather, not necessarily smaller) side of conjectures derived in this way from \( c \) produces a equation \( u = v \) such that the larger of \( u \) and \( v \) is ground irreducible by \( R \), or else \( u \) and \( v \) are distinct, but neither is ground reducible.

The set of critical pairs between \( R \) and \( c \) is always a (generous) cover set, unless \( c \) is obviously not an inductive theorem, as described in the above theorem. Simplification by rules and lemmas may be incorporated into the proof procedure.
11 Future Research

Rewriting is an active field of theoretical and applied research. Current research topics include the following:

Typed Rewriting Under reasonable assumptions, virtually everything we have done extends to the multisorted case. Adding subsorts allows functions to be completely defined without having to introduce error elements for when they are applied outside their intended domains. But deduction in such "order-sorted" algebras presents some difficulties. The most popular approach is to insist that the sort of the right-hand side is always contained in that of the left.

AC termination The methods we have described for proving termination of ordinary rewriting are of only limited applicability when associativity and commutativity are built into the rewriting process. Special techniques have been devised to handle this case, which is of great practical importance.

Higher-order rewriting In the previous sections, we worked with first-order terms only. Since the typed lambda calculus is terminating and confluent, some researchers have been looking at ways of combining it with higher-order rewriting in such a way as to preserve convergence, thereby endowing rewriting with higher-order capabilities.

Hierarchical systems From the point of view of software engineering, it is important that properties of rewrite programs, like termination and confluence, be modular. That is, we would like to be able to combine two terminating systems, or two convergent systems, and to have the same properties hold for the combined system. This is not true in general, not even when one system makes no reference to the function symbols and constants used in the other. Finding useful cases when systems may safely be combined is a current area of study.

Concurrency Confluent systems, in general, and orthogonal systems, in particular, are natural candidates for parallel processing, since rewrites at different positions are more or less independent of each other. Work is being undertaken on language and implementation issues raised by this possibility.

Infinite rewriting Rewriting can be extended to apply to structures other than the finite terms we have considered. Indeed, graph rewriting has important applications, since graphs allow one to represent structure-sharing, as well as infinite terms.

First-order theorem proving In Sect. 10, we saw how to simulate resolution-like inference equationally. A productive area of research is the application of ideas from rewriting to more traditional refutational theorem provers. Using orderings on terms and formulas helps restrict deduction and increase the amount of simplification and redundancy elimination that can be incorporated without forfeiting completeness.

Acknowledgments

I thank Jieh Hsiang for his comments. This work was supported in part by the National Science Foundation under Grants CCR-90-07195 and CCR-90-24271 and by a Lady Davis fellowship at the Hebrew University of Jerusalem.

Selected Bibliography

The hundred items in this bibliography were chosen from among English language references on rewriting. They are divided into sections, corresponding to Sections 1-11 above, and are listed chronologically within section. (Beware that chronology oftentimes does not reflect the dependency of ideas, particularly as only the
most polished versions are listed here.) Included are most books and surveys, plus many articles that were historically important, represent major stepping stones, or present the current state of research. Surveys are starred. Related topics, including the Lambda Calculus, Combinatory Logic, unification theory, and resolution theorem proving, have been omitted, as have descriptions of implementations. Several new books and surveys are in the offing.

1. **Rewriting**


2. **Termination**


3. Confluence


4. Completion


5. Validity


6. Satisfiability


7. AC-Completion


8. Conditional Rewriting


9. Programming


10. Theorem Proving


11. Future Research


