

Abstract Canonical Presentations[★]

Nachum Dershowitz¹

*School of Computer Science
Tel-Aviv University
P.O. Box 39040
Ramat Aviv, Tel Aviv 69978
Israel*

Claude Kirchner

*INRIA & LORIA
615, rue du Jardin Botanique
B.P. 101
54602 Villers-lès-Nancy Cedex
France*

Abstract

Solving goals—like proving properties, deciding word problems or resolving constraints—is *much* easier with some presentations of the underlying theory than with others. Typically, what have been called “completion processes”, in particular in the study of equational logic, involve finding appropriate presentations of a given theory to more easily solve a given class of problems.

We provide a general proof-theoretic setting that relies directly on the fundamental concept of “good”, that is, normal-form proofs, itself defined using well-founded orderings on proof objects. This foundational framework allows for abstract definitions of canonical presentations and very general characterizations of saturation and redundancy criteria.

Key words: Canonicity, proof orderings, redundancy, saturation, canonical rewriting, completion

*One good definition
is worth three theorems.*

—Alfred Adler, “Mathematics and creativity”
(*The New Yorker*, 1972)

1 Introduction

It is common, when defining a theory axiomatically, to ask whether the chosen axioms—like Euclid’s axiom of parallels—are independent. Dependent axioms are superfluous from the point of view of the theory (set of theorems), so such redundancies can be removed without impacting the theory. One speaks then of independent sets of equations, or of alternative presentations of algebras.

For formal, non-computational purposes, one often seeks small, elegant axiomatizations, but there are competing measures of smallness—such as fewest axioms or minimal overall size, let alone of elegance. And there is no theoretical reason to expect there to be a unique smallest way of presenting a theory. At the other extreme, the full deductively-closed theory is, of course, unique, but is almost invariably infinite and unsuitable as a presentation. Our goal here is to provide criteria for the identification of ideal, canonical presentations, using more subtle preferences than mere size.

Mathematics also involves solving equations, or, more generally, sets of constraints. In such a context, one cares about the *form* of formulæ. The process of solving transforms a defining set for the problem into formulæ that are in *solved form*; see [Comon and Kirchner, 2001]. In Gaussian elimination, for example, one begins with a set of linear equalities involving unknowns, and infers solved forms assigning numerical values to each unknown, or most general relations between variables. This corresponds to the point of view that arithmetic is a cheap form of inference, while equation solving is relatively hard. Thus, once one has derived a solved form, it is an easy matter to check whether other linear equalities follow.

* This paper is a revised and extended version of one presented in 2002 by the first author at the Clifford Lectures in Mathematical Logic for Computer Science at Tulane University and by the second author at the UNIF workshop [Dershowitz and Kirchner, 2002], and which appeared in the Proceedings of the Symposium on Logic in Computer Science [Dershowitz and Kirchner, 2003].

Email addresses: `Nachum.Dershowitz@cs.tau.ac.il` (Nachum Dershowitz),
`Claude.Kirchner@loria.fr` (Claude Kirchner).

¹ Supported in part by the Israel Science Foundation (grant no. 254/01).

Good Presentations

In these examples, as in many others, one is given an axiomatic presentation, and sets up a goal of inferring certain formulæ: theorems in Euclidean geometry, in one case; solutions of equations, in the other. In both cases, some presentations of the underlying theory are better suited for the task at hand than others. So, one needs to *define* the “best” axiomatic presentation for any given problem-solving task. To that end, we compare presentations in terms of the quality of proofs they allow. Our work is, therefore, based on a concept of “good” proofs and our goal is to ground the theory of good proofs.

The archetypical instance of this paradigm consists in finding a rewriting-based decision procedure for the uniform word problem in a given equational theory. In this context, the best proofs are rewrite (“valley”) proofs and the best presentation is a terminating Church-Rosser (“convergent”) rewrite system (see [Baader and Nipkow, 1998, Dershowitz and Plaisted, 2001, “Terese” (M. Bezem, J. W. Klop and R. de Vrijer, eds.), 2002]).

Good presentations, good proofs and good inferences are clearly related, but what is the best starting point for developing an æsthetic, unified and useful understanding of them? We promote the thesis that the ideal starting point is the concept of proof orderings. Proof quality is measured via a well-founded proof ordering on the set of all proofs: the smaller in the ordering, the better.

Good Proofs

Consider a naïve example: Suppose we have an equational theory defined by the axioms $a = b$ and $b = c$. Then $a = b = c = b = c$ and $a = b = c$ are both valid proofs of $a = c$, but, clearly, the second is better than the first, as it is shorter, and non-circuitous. More generally, in proof theory, one assigns ordinals to proofs and shows that under certain circumstances there exists a “critical” subformula that can be replaced in a way that reduces the ordinal of the proof. These proof-theoretical concepts have been extended to dynamically changing proof systems (see [Dershowitz and Okada, 1988]). Here we generalize the proof-ordering method, as used in term rewriting for establishing properties of rewrite-system completion procedures [Bachmair and Dershowitz, 1994], to an abstract setting of arbitrary proof systems, supplied with an arbitrary ordering of proofs.

As a simple example of where these considerations are leading, imagine some axiom $p(x)$. It would be quite natural to consider it virtually cost-free to instantiate an axiom like this in an inference $\frac{p(x)}{p(t)}$, proving the “corollary” $p(t)$. So, were one to charge for axioms by their size, a generic subproof of the above form would be cheaper than direct use of the corollary, $p(t)$, for any

big term t . Thus, for a good presentation, there would be no advantage in including such trivial consequences of the axiom.

Good Inferences

How can we tell a machine to go about finding good proofs? Much of the research in automated deduction consists in finding the best inference system for finding the best proofs or best presentations. In addition to correctness and completeness, two other notions are essential here: saturation and redundancy. Since the search spaces are in general huge and their structure unknown a priori, one controls the application of locally defined inference rules by applying rules only up to saturation of the formula set (to insure termination) and up to redundancy (to reduce search). Thus, the dominant point of view in the deduction community is to seek out good inferences and maintain control over them.

Completion processes have been devised in various different contexts, but in rather similar fashion. These include: standard Knuth-Bendix completion [1970], equational completion [Huet, 1980, Peterson and Stickel, 1981, Jouanaud and Kirchner, 1986], completion in specific algebras (like order-sorted ones [Gnaedig, Kirchner, and Kirchner, 1988]), inductionless induction (initiated by Musser; see [Kapur and Musser, 1987]), ordered completion [Lankford, 1975, Bachmair, Dershowitz, and Plaisted, 1989, Hsiang and Rusinowitch, 1991], completion for semantic unification [Dershowitz, 1989, Doggaz and Kirchner, 1991], to mention a few. The formalization of the completion mechanism, as well as its correctness and completeness, has been intensively studied, beginning with the seminal work of Gérard Huet [1981] and especially since the introduction of proof orderings in [Bachmair, Dershowitz, and Hsiang, 1986]. The universality of “completion” in automated deduction is further evident in the syntheses of completion and Gröbner basis generation initiated by Bruno Buchberger [Buchberger, 1987], as in, for example, [Kandri-Rody, Kapur, and Winkler, 1989].

We provide abstract definitions of saturation and redundancy that are applicable in these, and many other, frameworks.

Canonical Presentations

An interesting feature of the complete set of reductions produced by Knuth-Bendix completion [1970] and the Gröbner bases produced by Buchberger’s algorithm [1965, 1985] is that they are unique, regardless of nondeterministic choices made along the way [Dershowitz, Marcus, and Tarlecki, 1988, Metivier, 1983]. In other words, “best presentations” are unique for a given ordering of proofs (usually built from a given term ordering). Our abstract notions lead

similarly to canonicity.

Overview

Since we aim to be foundational, starting from a very simple, abstract and universal setting, we define a number of abstract properties of *presentations*, that is, of arbitrary sets of formulæ. Fixing inference and the ordering, we characterize the unique *canonical presentation* for a theory in several ways:

- (1) Lemmata that can appear as premises in minimal proofs (Definition 25)
- (2) Smallest saturated set (Theorem 44)
- (3) Simplest presentation (Theorem 55)
- (4) Non-redundant formulæ (Corollary 62)
- (5) Reduced saturated set (Proposition 63)
- (6) Conclusions of trivial proofs (Corollary 69)

These characterization of the canonical presentation for a theory are boxed thus in the following sections.

A collateral contribution of this work is abstract formal definitions of redundancy, saturation, canonicity, completeness, simplicity, and triviality, all of which are fundamental notions in the design, study and analysis of proof search methods.

The next section defines the basics. Section 3 uses proof orderings to define the canonical presentation and Section 4 explains how to reduce presentations. Section 5 introduces the central concept of saturation. Redundancy and its elimination are the subject of Section 6. By introducing a notion of sub-proof, Section 7 provides an additional, more practical characterization of the canonical presentation. We conclude with a brief discussion of related and future works.

2 Ordered Proof Systems

We begin with the following structure, which we call an *ordered proof system*, and which consists of the following five components:

- *Proofs* \mathbb{P} ;
- *Formulæ* \mathbb{A} ;
- *Premises* $Pm : \mathbb{P} \rightarrow 2^{\mathbb{A}}$ (provides the set of assumptions used by a proof p , usually denoted $[p]^{Pm}$);

- *Conclusion* $Cl : \mathbb{P} \rightarrow \mathbb{A}$ (provides the formula a proof p allows to prove, usually denoted $[p]_{Cl}$);
- *Well-founded proof ordering* $\geq : \mathbb{P} \times \mathbb{P} \rightarrow 2$.

The crucial point here is the proof ordering, which may be partial. As usual, we use $>$ for $\geq \cap \neq$. We assume for convenience that the proof ordering only compares proofs with the same conclusion ($p \geq q \Rightarrow [p]_{Cl} = [q]_{Cl}$), rather than mention this condition each time we have cause to compare proofs. (In Section 7, we explore the implications of an additional subproof relation.)

As we develop a foundational framework, we do not need to make any assumptions whatsoever as to the way formulæ and proofs are described. Therefore, the formal system used to define the proofs could be inference-based (like for equational logic [Taylor, 1979]) or the sequent calculus [Girard, Lafont, and Taylor, 1989]), or grammar-based, or anything else. Of course, the syntax of all proofs should not be confused with the description of “good” proofs. An inference-based description of the latter is the subject of [Bonacina and Dershowitz, 2003].

We will use the term *presentation* to mean a set of formulæ, and *justification* to mean a set of proofs. We reserve the term *theory* for the deductive closure of a presentation.

Example 1 (Ground Resolution) *Consider a propositional ordered binary resolution calculus: Formulæ are finite sets of literals; proofs are finite unordered unary-binary trees, with formulæ for leaves and literals labelling internal nodes. Propositional constants are (arbitrarily) linearly ordered and proofs are compared using the corresponding recursive path ordering [Dershowitz, 1982].*

On the concrete level, for a literal ℓ , $\bar{\ell}$, its negation, and L, L' , clauses, a binary node ℓ corresponds to the application of binary resolution (called identical resolution in [Dowek, Hardin, and Kirchner, 2003]), labelled by the name of the literal being resolved:

$$\frac{\ell \vee L \quad \bar{\ell} \vee L'}{L \vee L'} (\ell)$$

Then, given the presentation $B = \{a \vee \bar{b}, b \vee c, \bar{a} \vee \bar{c}, a\}$, we have for example the following two proofs of b :

$$\frac{\frac{b \vee c \quad \bar{a} \vee \bar{c} (c)}{\bar{a} \vee b} \quad a (a)}{b} (a) \qquad \frac{a \quad \frac{\bar{a} \vee \bar{c} (a)}{\bar{c}} (a)}{b} \quad b \vee c (c)$$

Comparing them, assuming the precedence $a < b < c$, we see that the first is

smaller:

$$c(\mathbf{a}(a, \bar{a} \vee \bar{c}), b \vee c) >_{m\text{po}} \mathbf{a}(c(b \vee c, \bar{a} \vee \bar{c}), a)$$

We will now prove elementary results based on the ordered proof system notion. We start by extending the mappings Pm and Cl to sets of proofs in the standard fashion:

Definition 2

$$\begin{aligned} [P]^{Pm} &\stackrel{!}{=} \bigcup_{p \in P} [p]^{Pm} \\ [P]_{Cl} &\stackrel{!}{=} \{[p]_{Cl} : p \in P\} \end{aligned}$$

Then trivially: $[\emptyset]^{Pm} = [\emptyset]_{Cl} = \emptyset$.

It follows immediately from the definitions that Pm and Cl are monotonic:

Lemma 3 (Monotonicity of Pm and Cl) For all justifications P and Q :

$$P \subseteq Q \Rightarrow [P]^{Pm} \subseteq [Q]^{Pm} \quad (1)$$

$$P \subseteq Q \Rightarrow [P]_{Cl} \subseteq [Q]_{Cl} \quad (2)$$

Definition 4 (Proofs) For all presentations A , the set of all proofs using some of the premises in A is defined as:

$$Pf(A) \stackrel{!}{=} \{p \in \mathbb{P} : [p]^{Pm} \subseteq A\}$$

For a specific conclusion $c \in \mathbb{A}$, we sometimes write:

$$Pf_c(A) \stackrel{!}{=} \{p \in Pf(A) : [p]_{Cl} = c\}$$

Lemma 5 For all presentations A :

$$[Pf(A)]^{Pm} \subseteq A$$

Proof. We have $[Pf(A)]^{Pm} = \bigcup_{p \in Pf(A)} [p]^{Pm} \subseteq A$ by definition of $Pf(A)$. \square

It follows from these definitions that justifications are monotonic:

Lemma 6 (Monotonicity of Pf) For all presentations A and B and formulæ c :

$$\begin{aligned} A \subseteq B &\Rightarrow Pf_c(A) \subseteq Pf_c(B) \\ A \subseteq B &\Rightarrow Pf(A) \subseteq Pf(B) \end{aligned}$$

Proof. Note that $[p]^{Pm} \subseteq A \subseteq B$ for all $p \in Pf(A)$; thus $p \in Pf(B)$. \square

Lemma 7 For all justifications P :

$$P \subseteq Pf([P]^{Pm})$$

Proof. By monotonicity of Pm , we have $p \in P \Rightarrow [p]^{Pm} \subseteq [P]^{Pm} \Rightarrow p \in Pf([P]^{Pm})$. \square

Remark 8 Because of Lemmata 5 and 7 presentations and justifications are related by the Galois connection formed by Pf and Pm with respect to subset.

From the previous definitions, it is easy to see that proofs need only what they use, that is:

Lemma 9 For all presentations A ,

$$Pf([Pf(A)]^{Pm}) = Pf(A)$$

Proof. By Lemma 5 and monotonicity of Pf , $Pf([Pf(A)]^{Pm}) \subseteq Pf(A)$. By Lemma 7, $Pf(A) \subseteq Pf([Pf(A)]^{Pm})$. \square

We can now define the notion of a “theory” generated by a presentation:

Definition 10 (Theories)

- The theory (or deductive closure) of a presentation A :

$$Th A \stackrel{!}{=} [Pf(A)]_{cl} \tag{3}$$

- A presentation A is a basis for a theory θ if

$$Th A = \theta$$

- A presentation A is deductively closed if

$$Th A = A$$

- Presentations A and B are equivalent if they allow exactly the same theorems:

$$A \equiv B \stackrel{!}{=} Th A = Th B$$

Definition 11 (Consequence) *The consequence relation \vdash has the following natural definition:*

$$A \vdash c \stackrel{!}{=} \exists p. [p]^{Pm} = A \wedge [p]^{Cl} = c$$

This is extended to multiple conclusions as

$$A \vdash B \stackrel{!}{=} \forall c \in B. A \vdash c$$

Most of our results depend on the following standard properties of Tarskian consequence relations:

Postulate A (Reflexivity) *For all formulæ a :*

$$\{a\} \vdash a$$

Postulate B (Closure) *For all presentations A :*

$$Th Th A \subseteq Th A$$

We will assume that these postulates hold for all proof systems considered in this paper.

Useful basic properties of proof systems follow from these postulates.

Proposition 12 (Monotonicity) *For all presentations A and B :*

$$A \subseteq B \Rightarrow Th A \subseteq Th B$$

Proof. This follows from monotonicity of Pf and Cl . \square

Proposition 13 (Reflexivity) *For all formulæ a :*

$$A \subseteq Th A$$

Proposition 14 (Transitivity) *For all presentations A , B and C ,*

$$Th A \supseteq B \wedge Th B \supseteq C \Rightarrow Th A \supseteq C$$

Proof. By Monotonicity we have $Th\ Th\ A \supseteq Th\ B$. By Closure we get $Th\ A \supseteq Th\ Th\ A \supseteq Th\ B \supseteq C$. \square

A presentation and its theory contain the same information in the sense that they allow to prove exactly the same theorems:

Lemma 15 *A presentation A and its theory $Th\ A$ support exactly the same theorems:*

$$Th\ A \equiv A$$

Proof. For all presentations A , by Reflexivity, $A \subseteq Th\ A$, and by Monotonicity, $Th\ A \subseteq Th\ Th\ A$. Finally, Closure allows one to conclude that $Th\ Th\ A = Th\ A$, or $Th\ A \equiv A$. \square

Lemma 16 *For all presentations A :*

$$[Pf(A)]^{Pm} = A$$

Proof. We have one direction already in Lemma 5. For the other, consider any formula a in A . By the Reflexivity Postulate, $\{a\} \vdash a$. So there is a proof $p \in Pf(\{a\}) \subseteq Pf(A)$ with premise and conclusion a . By monotonicity of Pm , $a \in [p]^{Pm} \subseteq [Pf(A)]^{Pm}$, as required. \square

Finally, we get that larger presentations mean larger justifications and vice-versa:

Lemma 17 *For all presentations A and B :*

$$A \subseteq B \Leftrightarrow Pf(A) \subseteq Pf(B) \tag{4}$$

$$A = B \Leftrightarrow Pf(A) = Pf(B) \tag{5}$$

Proof. We have one direction of (4) by monotonicity of Pf . Suppose $a \in A$. There is, by Reflexivity, a proof $p \in Pf_a(a) \subseteq Pf_a(A) \subseteq Pf_a(B)$ with a as both premise and conclusion. Hence, $a \in B$, yielding the other direction.

The second equivalence follows immediately. \square

3 Canonical Presentations

Proof orderings allow for minimal proofs, central to our development of a theory of canonical inference. Recall that by definition, $q < p$ only holds for proofs p and q with the same conclusion. Of course there could be incomparable proofs with same conclusion.

Definition 18 (Minimal Proofs) *The minimal proofs in a justification P are denoted as follows:*

$$\mu P \stackrel{!}{=} \{p \in P : \neg \exists q \in P. q < p\}$$

Obviously, for all justifications P ,

$$\mu P \subseteq P \tag{6}$$

Note that the notion of minimal proofs is *not* monotonic, as clearly $P \subseteq Q$ does not in general imply that $\mu P \subseteq \mu Q$.

Well-foundedness of the proof ordering means that minimal proofs exist and suffice:

Lemma 19 *For all presentations A :*

$$Th A = [\mu Pf(A)]_{Cl}$$

Proof. Minimal proofs are proofs, i.e. $Pf(A) \supseteq \mu Pf(A)$ (by 6). So by monotonicity of Cl , we get $[Pf(A)]_{Cl} \supseteq [\mu Pf(A)]_{Cl}$.

Suppose $p \in Pf_c(A)$. Since \geq is well-founded, there exists a minimal $q \in Pf_c(A)$, $q \leq p$. Hence $c \in [\mu Pf(A)]_{Cl}$. \square

Definition 20 (Flattening) *Those premises employed in minimal proofs are denoted:*

$$A^b \stackrel{!}{=} [\mu Pf(A)]^{Pm}$$

Lemma 21 *Flattening a presentation gives less formulæ:*

$$A^b \subseteq A$$

Proof. By monotonicity of Pm and Lemma 5, we get $A^b = [\mu Pf(A)]^{Pm} \subseteq [Pf(A)]^{Pm} \subseteq A$. \square

The following lemma is useful:

Lemma 22 $\mu Q \subseteq P \wedge \mu P \subseteq Q \Leftrightarrow \mu P = \mu Q$

Proof. The right-to-left direction is easy (by 6). For the other, suppose $p \in \mu P$. By assumption, $p \in Q$. Consider any $q \in \mu Q$ such that $q \leq p$. By assumption, q is also in P . But p is minimal in P . Hence, $p = q \in \mu Q$. \square

Now that we know how to define good proofs, we can understand how much one can restrict a presentation without jeopardizing the theory.

Definition 23 (Normal Form Proof) *A proof p is in normal form if it belongs to the set of minimal proofs that allow the use of all theorems as lemmata: $p \in \mu Pf(Th A)$*

Normal form proofs are denoted as follows:

$$Nf(A) \stackrel{\dagger}{=} \mu Pf(Th A)$$

Considering only normal-form proofs does not restrict the theory, as we have:

Lemma 24

$$Th A = [Nf(A)]_{Cl}$$

Proof. By definition $Th A = [Pf(A)]_{Cl}$; applying this to $Th A$ we get $Th Th A = [Pf(Th A)]_{Cl}$. By Lemmata 15 and 19, we have

$$Th A = Th Th A = [Pf(Th A)]_{Cl} = [Nf(A)]_{Cl}$$

\square

Our main definition is:

Definition 25 (Canonical Presentation) *The canonical presentation A^\sharp of a presentation A is the flattened theory of A :*

$$A^\sharp \stackrel{!}{=} [Th A]^b$$

Inlining the previous definitions rephrases that the canonical presentation contains those formulæ that appear as premises of all possible valid minimal proofs:

$$A^\sharp = [Th A]^b = [\mu Pf(Th A)]^{Pm} = [Nf(A)]^{Pm} \quad (7)$$

4 Reduced Systems

In a classical way (cf. the Smyth [1977] powerdomain construction), proof orderings can be lifted to sets of proofs as follows:

Definition 26 (Better Proof Sets) *Justification Q is better than justification P if:*

$$P \sqsupseteq Q \stackrel{!}{\equiv} \forall p \in P. \exists q \in Q. p \geq q$$

Justifications are similar if:

$$P \simeq Q \stackrel{!}{\equiv} P \sqsupseteq Q \sqsupseteq P$$

Proposition 27 *Better (\sqsupseteq) is a quasi-order.*

It follows from the definitions that these relations are compatible: $P \simeq Q \sqsupseteq R \simeq S$ implies $P \sqsupseteq S$.

Proposition 28 *For all justifications P and Q :*

$$P \sqsupseteq \mu P \quad (8)$$

$$P \subseteq Q \Rightarrow P \sqsupseteq Q \quad (9)$$

$$P \sqsupseteq Q \Rightarrow [P]_{cl} \subseteq [Q]_{cl} \quad (10)$$

$$P \sqsupseteq Q \Leftrightarrow \mu P \sqsupseteq \mu Q \quad (11)$$

Proof. Well-foundedness ensures that minimal proofs exist, therefore (8) holds.

Implication (9) holds trivially.

Line (10) holds since $q < p$ only holds for proofs p, q with the same conclusion.

Suppose $P \sqsupseteq Q$. Trivially, $\mu P \sqsupseteq P$; by (8), $Q \sqsupseteq \mu Q$; so $\mu P \sqsupseteq \mu Q$. For the other direction of (11): $P \sqsupseteq \mu P \sqsupseteq \mu Q \sqsupseteq Q$. \square

Proposition 29 *For all presentations A and B :*

$$Pf(A) \sqsupseteq Pf(B) \Rightarrow Th A \subseteq Th B \quad (12)$$

$$A \subseteq B \Rightarrow Pf(A) \sqsupseteq Pf(B) \quad (13)$$

$$B \subseteq A \wedge Pf(A) \sqsupseteq Pf(B) \Rightarrow A \equiv B \quad (14)$$

Proof. Line (12) is a consequence of (10); (13) is a consequence of the monotonicity of Pf ; (14) follows from the two previous ones. \square

Proposition 30 *The relation \sqsupseteq is a partial ordering on minimal proofs.*

Proof. The relation is transitive (Proposition 27). Antisymmetry holds since, assuming $\mu P \sqsupseteq \mu Q \sqsupseteq \mu P$ and $p \in \mu P$, there must be a $q \in \mu Q$ and $p' \in \mu P$ such that $p \geq q \geq p'$. Hence $p' = p = q$. By symmetry, $\mu P = \mu Q$. \square

Lemma 31 *Minimal proofs use the premises of minimal proofs:*

$$\mu Pf(A^b) = \mu Pf(A)$$

Proof. Suppose $p \in \mu Pf_c(A)$ for some c . Then $[p]^{Pm} \subseteq A^b$ and $p \in Pf_c(A)^b$. Were there a $q \in Pf_c(A)^b \subseteq Pf(A)$ such that $q < p$, p would not be minimal in $Pf(A)$.

For the other direction, suppose $p \in \mu Pf_c(A)^b \subseteq Pf(A)$, but p is not minimal in $Pf(A)$. In other words, there is some $q \in Pf_c(A)$ such that $p > q$. There must be some $r \in \mu Pf_c(A) \subseteq \mu Pf(A^b)$ such that $q \geq r$. This contradicts the minimality of p in $Pf(A)^b$. \square

A presentation A is said to be *reduced* (or *flat*) if $A = A^b$.

Lemma 32 *What is reduced cannot be further reduced:*

$$A^{bb} = A^b$$

Proof. Apply Pm to both sides of Lemma 31. \square

Theorem 33 *A reduced system can prove as much as the initial one:*

$$A^b \equiv A$$

Proof. By Lemmata 19 and 31,

$$Th A^b = [Pf(A)^b]_{Cl} = [\mu Pf(A)^b]_{Cl} = [\mu Pf(A)]_{Cl} = [Pf(A)]_{Cl} = Th A$$

\square

Theorem 34 *The sharpening function \sharp is canonical with respect to the equivalence of presentations. That is:*

$$A^\sharp \equiv A \tag{15}$$

$$A \equiv B \Leftrightarrow A^\sharp = B^\sharp \tag{16}$$

$$A^{\sharp\sharp} = A^\sharp \tag{17}$$

Proof. For (15), by Theorem 33 and Lemma 15, we get $A^\sharp = [Th A]^b \equiv Th A \equiv A$.

For (16), suppose $A \equiv B$, that is, $Th A = Th B$. By substitution of equals in the definitions: $A^\sharp = (Th A)^b = (Th B)^b = B^\sharp$.

Conversely, if $A^\sharp = B^\sharp$, by (15), $A \equiv A^\sharp = B^\sharp \equiv B$.

For (17), letting B be A^\sharp in (16), $A \equiv A^\sharp$ iff $A^\sharp = A^{\sharp\sharp}$, and (15) gives the left side. \square

Finally, since, by Lemma 32, we have $(A^\sharp)^b = (Th A)^{bb} = (Th A)^b = A^\sharp$,

Lemma 35 *The canonical presentation A^\sharp cannot be further reduced:*

$$(A^\sharp)^b = A^\sharp \tag{18}$$

5 Saturated Presentations

There are two manners in which a presentation can be said to suffice for normal form proofs:

Definition 36 (Completeness) *A presentation A is complete if every theorem has a normal form proof, that is, if*

$$Th A \subseteq [Pf(A) \cap Nf(A)]_{cl}$$

or, equivalently,

$$Th A = [Pf(A) \cap Nf(A)]_{cl}$$

Definition 37 (Saturation) *A presentation A is saturated — denoted $Satur A$ — if it supports all possible normal form proofs:*

$$Nf(A) \subseteq Pf(A)$$

It follows from Lemma 22 that:

Lemma 38 *A presentation A is saturated iff*

$$\mu Pf(A) = Nf(A)$$

A presentation is complete if it is saturated, but proving the converse (Proposition 43 below) requires an additional hypothesis:

Definition 39 *Minimal proofs are unique if for all $A \subseteq \mathbb{A}$ and $c \in \mathbb{A}$ it is the case that*

$$|\mu Pf_c(A)| \leq 1$$

Proposition 40 *If minimal proofs are unique, then all of A^b is needed:*

$$B \subsetneq A^b \Rightarrow Th B \subsetneq Th A$$

for all presentations A and B .

Proof. By Lemma 21 and monotonicity of Th :

$$B \subsetneq A^b \subseteq A \Rightarrow Th B \subseteq Th A$$

Let $a \in A^b \setminus B = [\mu Pf(A \setminus B)]^{Pm}$. Then there is a $p \in \mu Pf(A) \setminus Pf(B)$, which, by uniqueness, has a conclusion $[p]_{cl} \notin [Pf(B)]_{cl} = Th B$. \square

The following is useful:

Lemma 41 For all presentations A :

$$\mu Pf(A) \cap Nf(A) = Pf(A) \cap Nf(A)$$

Proof. Since $\mu Pf(A) \subseteq Pf(A)$, we need only to show that $Pf(A) \cap Nf(A) \subseteq \mu Pf(A)$. Suppose $p \in Pf(A) \setminus \mu Pf(A)$. Then there is a $q \in \mu Pf(A) \subseteq Pf(A) \subseteq Pf(Th A)$ (by Reflexivity) such that $p > q$. But then $p \notin \mu Pf(Th A) = Nf(A)$. \square

Theorem 42 A presentation A is saturated iff it contains its own canonical presentation A^\sharp :

$$\text{Satur } A \Leftrightarrow A^\sharp \subseteq A$$

Proof. As $A^\sharp \subseteq B \Leftrightarrow Nf(A) \subseteq Pf(B)$, and by the definition of saturated, we need to show that $\mu Pf(A) = Nf(A)$ iff $Nf(A) \subseteq Pf(A)$. By Reflexivity and monotonicity of Pf : $Pf(A) \subseteq Pf(Th A)$. So, for any minimal proof $p \in \mu Pf_c(A) \subseteq Pf_c(Th A)$ there must be a $q \in \mu Pf_c(Th A) = Nf_c A \subseteq Pf_c(A)$ such that $p \geq q$. By minimality, $p = q \in Nf(A)$. In other words, $\mu Pf(A) \subseteq Nf(A)$. So if $\mu Pf(A) = Nf(A)$, then, $Nf(A) = \mu Pf(A) \subseteq Pf(A)$.

Suppose now that $Nf(A) \subseteq Pf(A)$. By Lemma 41:

$$\begin{aligned} Nf(A) \subseteq Pf(A) &\Leftrightarrow Nf(A) = Nf(A) \cap Pf(A) = Nf(A) \cap \mu Pf(A) \\ &\Leftrightarrow Nf(A) \subseteq \mu Pf(A) \end{aligned}$$

\square

When we enforce equality instead of the one-sided inclusion of the previous theorem, that is, when we consider presentations that are their own canonical presentation, we arrive at the concept of canonical presentations: A presentation A is *canonical* if $A = A^\sharp$.

Proposition 43 A presentation is complete if it is saturated. If minimal proofs are unique, then a presentation is saturated iff it is complete.

Proof. If $c \in Th A$, then (by Lemma 24) there is a proof $q \in Nf(A)$ of c . If A is saturated, then (by Theorem 42) $[q]^{Pm} \subseteq [Nf(A)]^{Pm} = A^\sharp \subseteq A$, and $q \in (Pf(A) \cap Nf(A))$, as required for completeness.

For the other direction, by completeness and Lemma 41, for all $c \in Th A$, $\mu Pf_c(A) \cap Nf_c A \neq \emptyset$. By uniqueness of minimal proofs, $|\mu Pf_c(A)|, |Nf_c A| \leq 1$. Hence, A is saturated, with $\mu Pf_c(A) = Nf_c A$ for all c . \square

We can now state a second characterization of canonical presentations:

Theorem 44 *The canonical presentation A^\sharp is the smallest saturated set:*

$$\boxed{\begin{array}{l} \text{Satur} \quad A^\sharp \\ A \equiv B \Rightarrow [\text{Satur } B \Leftrightarrow A^\sharp \subseteq B] \end{array}}$$

Thus, the canonical presentation is minimal in the sense that no equivalent proper subset of A^\sharp is saturated.

Corollary 45 *If A is saturated, then every equivalent superset also is:*

$$\text{Satur } A \wedge A \equiv B \wedge A \subseteq B \Rightarrow \text{Satur } B$$

Example 46 (Ground Resolution — Continued) *Consider again the resolution calculus: The canonical presentation for $A = \{a \vee \bar{b}, b \vee c, \bar{a} \vee \bar{c}\}$ includes, in addition, $\{b \vee \bar{a}, a \vee c, \bar{b} \vee \bar{c}\}$. The canonical basis of $B = A \cup \{a\}$ is just $\{a, b, \bar{c}\}$. The canonical basis of $B \cup \{c\}$ is the empty clause.*

6 Redundancy

Formulæ that when removed from a presentation do not hurt proof quality will be termed “redundant”. The concept of redundancy lies at the heart of efficient theorem proving: one seeks to perform inferences on non-redundant formulæ so as to avoid redundancy propagation, whose cost could be prohibitive.

This “better than” quasi-ordering on proofs is lifted to a “simpler than” quasi-ordering on (equivalent) sets of formulæ, as follows:

Definition 47 (Simpler Presentation) *Presentation B is said to be simpler than an equivalent presentation A when B provides better proofs than does A :*

$$A \succsim B \stackrel{!}{\equiv} Th A = Th B \wedge Pf(A) \sqsupseteq Pf(B)$$

Presentations are similar if their proofs are:

$$A \approx B \stackrel{!}{\equiv} Pf(A) \simeq Pf(B)$$

Reflexivity and transitivity are inherited from \equiv and \sqsubseteq . Therefore:

Proposition 48 *The relation \succsim is a quasi-ordering.*

We get easily that:

Lemma 49

$$A \approx B \Leftrightarrow \mu Pf(A) = \mu Pf(B)$$

Lemma 50 *Presentation A is saturated iff $Th A \approx A$.*

Proof. It is always the case that $A \succsim Th A \succsim A^\sharp$. If A is saturated, then $A \supseteq A^\sharp$ and, therefore, $Th A \succsim A^\sharp \succsim A$. For the other direction, suppose $p \in Nf(A)$. Since A is similar, there must be a proof $q \in Pf(A) \subseteq Pf(Th A)$, such that $q \leq p$. But $q \not\leq p$, so $p \in Pf(A)$. It follows that $Nf(A) \subseteq Pf(A)$, and A is saturated. \square

Proposition 51 *For all presentations A and B :*

$$A \subseteq B \wedge Th A = Th B \Rightarrow A \succsim B \tag{19}$$

$$A \subseteq B \wedge Pf(B) \sqsupseteq Pf(A) \Rightarrow A \approx B \tag{20}$$

Proof. Line (19) is a consequence of (11) and the definitions. If $A \subseteq B$ and $Pf(B) \sqsupseteq Pf(A)$, as on the left of (20), then $Pf(A) \simeq Pf(B)$, again by (11). Hence, their theories are the same, and, by definition, $A \approx B$. \square

Proposition 52 *The relation \succsim is a quasi-ordering and \approx is its associated equivalence relation.*

Lemma 53 *For all presentations A , B and C :*

$$C \subseteq B \wedge A \succsim A \setminus B \Rightarrow A \approx A \setminus C$$

Proof. We apply (20): We are given that $Pf(A) \sqsupseteq Pf(A \setminus B)$ and, by monotonicity of Pf , we have $Pf(A \setminus B) \sqsupseteq Pf(A \setminus C)$. \square

Canonical presentations are indeed simpler:

Proposition 54

$$A \approx A^b \tag{21}$$

$$A \succsim A^\sharp \tag{22}$$

Proof. To see that $A \approx A^b$, note that, by Theorem 33, the two theories are equal. Thus, by Lemma 21 and the first fact, $A^b \succsim A$. Applying Lemma 31 and Proposition 28, we get that $A \succsim A^b$, since

$$Pf(A) \sqsupseteq \mu Pf(A) = \mu Pf(A^b) \sqsupseteq Pf(A^b)$$

For the second claim: By Lemma 5,

$$A^\sharp = [\mu Pf(Th A)]^{Pm} \subseteq [Pf(Th A)]^{Pm} \subseteq Th A$$

Thus,

$$\mu Pf(A^\sharp) \subseteq Pf(A^\sharp) \subseteq Pf(Th A)$$

Also, by Lemma 7,

$$\mu Pf(Th A) \subseteq Pf([\mu Pf(Th A)]^{Pm}) = \mu Pf(A^\sharp) \subseteq Pf(A^\sharp)$$

By Lemma 22,

$$\mu Pf(A^\sharp) = \mu Pf(Th A)$$

so

$$Pf(Th A) \sqsupseteq \mu Pf(Th A) = \mu Pf(A^\sharp) \sqsupseteq Pf(A^\sharp)$$

In other words, $Th A \succsim A^\sharp$. By the Reflexivity Postulate and (11), we have $A \succsim Th A$, so, by transitivity of \succsim , we are done. \square

Theorem 55 *A canonical presentation A^\sharp is the simplest:*

$$A \equiv B \Rightarrow B \succsim A^\sharp$$

Definition 56 (Redundancy) *A set R of formulæ is (globally) redundant with respect to a presentation A when:*

$$A \cup R \approx A \setminus R$$

The set of all (individually) redundant formulæ of a given presentation A is denoted $Red A$:

$$Red A \stackrel{\dagger}{=} \{r \in A : A \approx A \setminus \{r\}\}$$

Theorem 57 *The set of individually redundant formulæ is globally redundant:*

$$A \approx A \setminus Red A$$

Proof. Let $A' = A \setminus Red A \subseteq A$. We show that $Pf(A) \supseteq Pf(A')$ and conclude using (20). Consider some proof $p_1 \in Pf_c(A) \setminus Pf(A')$. Since there is a redundant $r \in [p_1]^{Pm} \cap Red A$, there must be a proof $p_2 \in Pf_c((A \setminus \{r\})) \subseteq Pf(A)$ such that $p_1 \geq p_2$. But $[p_2]^{Pm} \neq [p_1]^{Pm}$, so $p_1 > p_2$. If $p_2 \notin Pf(A')$, then there would also be a $p_3 \in Pf(A)$, such that $p_2 > p_3$. Since the proof ordering is well-founded, this cannot go on forever, so there is, in fact, a proof $p_n \in Pf_c(A')$ such that $p_1 \geq p_n$. \square

Theorem 58 *Redundant formulæ are not needed:*

$$A^b = A \setminus Red A$$

Proof. If $a \notin A^b = [\mu Pf(A)]^{Pm}$, then $Pf(A) \supseteq Pf(A \setminus \{a\})$. Thus, $A \simeq A \setminus \{a\}$ and $a \in Red A$.

On the other hand, let $a \in A^b \subseteq A$, that is, $a \in [p]^{Pm}$ for some $p \in \mu Pf(A)$. Suppose $a \in Red A$, in other words, $A \simeq A' = A \setminus \{a\}$. So, there must be a proof $q \leq p$ such that $[q]^{Pm} \subseteq A'$. Since, then, $q \neq p$, we have $q < p$. Hence, $p \notin \mu Pf(A)$, a contradiction. Thus, $a \notin Red A$. \square

It follows from Lemma 38 that

Corollary 59 *Similar presentations are either both saturated or neither is.*

For any two justifications $P \subseteq Q$, it is always the case that $P \cap \mu Q \subseteq \mu P$. So:

Lemma 60 *For any presentation A :*

$$Pf(A) \cap \mu Pf(Th A) \subseteq \mu Pf(A) \tag{23}$$

$$Pf(A) \cap \mu Pf(Th A) = \mu Pf(A) \cap \mu Pf(Th A) \tag{24}$$

Hence:

Lemma 61 *Similar presentations are either both complete or neither is.*

Proof. If $A \approx B$, then, by definition, $Th B = Th A$, and, by Lemma 49, $\mu Pf(A) = \mu Pf(B)$. So, if A is complete, we get:

$$\begin{aligned} Th B &= Th A = [Pf(A) \cap Nf(A)]_{cl} = [\mu Pf(A) \cap Nf(A)]_{cl} \\ &= [\mu Pf(B) \cap Nf(B)]_{cl} = [Pf(B) \cap Nf(B)]_{cl} \end{aligned}$$

□

Corollary 62 *The canonical presentation A^\sharp is the theory without redundancies:*

$\begin{aligned} A^\sharp &= Th A \setminus Red Th A \\ Red A^\sharp &= \emptyset \end{aligned}$
--

Lemma 57 is another corollary.

Proposition 63

<p><i>A presentation is canonical iff it is saturated and reduced.</i></p>
--

Proof. One direction follows immediately from Theorem 44 and Corollary 62. For the other direction, let A be saturated and reduced. We aim to show that $A = A^\sharp$. By Proposition 54, $A \simeq A^\sharp$ and the two presentations are equivalent. If A is saturated, then by Theorem 42, $A \supseteq A^\sharp$. By (19), for any $r \in A \setminus A^\sharp$, $A \simeq A^\sharp \simeq A \setminus \{r\}$. But $Red A = \emptyset$, since A is reduced, so it cannot be that $r \in A$. In other words, $A \setminus A^\sharp = \emptyset$, and A is canonical. □

7 Subproofs

In the operational quest for the best proofs, a fundamental step is to perform localized searches for bad subproofs, which could stand improvement. To that end, we now impose additional structure on proofs: a well-founded *subproof*

(partial) order \triangleright . We extend this notation to sets of proofs:

$$P \triangleright Q \stackrel{\dagger}{=} \forall q \in Q. \exists p \in P. p \triangleright q$$

and use \trianglerighteq for its reflexive closure.

Definition 64 (Proper Subproofs) *We also use the following notation for the set of all subproofs:*

$$\Sigma P \stackrel{\dagger}{=} \{p \in \mathbb{P} : \exists q \in P. q \trianglerighteq p\}$$

Definition 65 *A proof is deemed trivial when its conclusion depends only on itself, that is, if $[p]^{Pm} = \{[p]_{CI}\}$, and it is its own only subproof.*

We denote by \hat{a} such a trivial proof of $a \in \mathbb{A}$ and by \hat{A} , the set of trivial proofs of each $a \in A$.

We will hereinafter assume three things about subproofs:

Postulate C (Triviality) *Assumptions are subproofs:*

$$p \trianglerighteq \widehat{[p]^{Pm}}$$

for all proofs p .

Postulate D (Subproof) *Subproofs use a subset of the assumptions:*

$$p \trianglerighteq q \Rightarrow [p]^{Pm} \supseteq [q]^{Pm}$$

for all proofs p and q .

Most significantly,

Postulate E (Replacement) *Decreasing a subproof, decreases the whole proof:*

$$p \triangleright q > q' \Rightarrow \exists p' \in Pf([p]^{Pm} \cup [q']^{Pm}). p > p' \triangleright q'$$

for all proofs p , q and q' .

Note that this postulate is weaker than the cut rule

$$\frac{A \vdash B \quad B \vdash c}{A \vdash c}$$

in that it only guarantees a proof of $A \vdash c$ when the proofs of $A \vdash B$ are

smaller than the trivial subproofs \widehat{B} appearing in the proofs of $B \vdash c$.

As a consequence of Triviality, every formula admits a trivial proof:

Proposition 66 *Every formula a has a trivial proof $\widehat{a} \in Pf(\{a\})$.*

Proof. By the Reflexivity Postulate, there is a proof p of a such that $[p]^{Pm} = \{a\}$. By Triviality, $p \supseteq \widehat{a}$. \square

As a consequence of Replacement, all subproofs of minimal proofs are minimal:

Proposition 67 *For all presentations A ,*

$$\Sigma \mu Pf(A) = \mu Pf(A)$$

Theorem 68 *Minimal trivial proofs are irredundant:*

$$A^b = [\mu Pf(A) \cap \widehat{A}]_{Cl}$$

for all presentations A .

Proof. Suppose $a \in A^b$. Then, there is, by the Trivia Postulate, some proof $p \in \mu Pf(A^b)$, such that $p \supseteq \widehat{a}$. Were \widehat{a} not minimal, then by the Replacement Postulate, neither would p be minimal. So, $\widehat{A}^b \subseteq \mu Pf(A)$. Clearly $\widehat{A}^b \subseteq \widehat{A}$. Hence, $A^b = [\widehat{A}^b]_{Cl} \subseteq [\mu Pf(A) \cap \widehat{A}]_{Cl}$.

For the other direction, suppose $c \in [\mu Pf(A) \cap \widehat{A}]_{Cl}$. Then

$$c \in [\mu Pf(A) \cap \widehat{A}]^{Pm} \subseteq [\mu Pf(A)]^{Pm} = A^b$$

\square

Substituting the definition of A^\sharp :

Corollary 69 *The canonical presentation A^\sharp is the set of conclusions of all trivial normal-form proofs:*

$$\begin{array}{l} A^\sharp = [Nf(A) \cap \widehat{Th A}]_{Cl} \\ \widehat{A}^\sharp = Nf(A) \cap \widehat{Th A} \end{array}$$

8 Discussion

We have designed an abstract framework for canonical reasoning without assuming anything about the context other than the existence of a well-founded ordering of entities named “proofs”. We have striven to attain the highest degree of abstraction possible—yet derive nontrivial result—by maximizing the potential of a fruitful definition of “good proofs”.

We have suggested that proof orderings, rather than formula orderings, take center stage in theorem proving with contraction (simplification and deletion of formulæ). Given a proof ordering that distinguishes “good proofs” from “bad proofs”, it makes sense to define completeness of a set of formulæ as the claim that all theorems enjoy a smallest (“best”, “normal form”) proof. Then, an inference system is complete if it has the ability to generate all formulæ needed for such ideal proofs. Abstract conditions for inference of complete and saturated presentations, based on the definitions herein, as well as example applications, such as paramodulation and ground completion, are explored in [Bonacina and Dershowitz, 2003].

Both saturation and redundancy have been defined in terms of the proof ordering. This appears to be flexible, since it allows small proofs to use large assumptions. Given a formula ordering, one can, of course, choose to compare proofs by simply comparing the multiset of their assumptions. The definition of redundancy in [Bachmair and Ganzinger, 1991], namely, that an inference is redundant if its conclusion can be inferred from smaller formulæ, coincides with ours when proofs are measured first by their maximal assumption. Our definition accords with the one given by Bonacina and Hsiang [1995, Def. 3.3]—a sentence is redundant if adding it to the set of assumptions does not decrease any minimal proof. (See [Bonacina, 1992, Chap. 2].)

The concept of saturation in theorem proving, in which superfluous deductions are not necessary for completeness, was suggested by Rusinowitch [1989, pp. 99–100] in the context of a Horn-clause resolution calculus. In our terminology: A presentation was said to be saturated when all inferrible formulæ are syntactically subsumed by formulæ in the presentation. (See also [Rusinowitch, 1991].) This concept was refined by Bachmair and Ganzinger [1991, 2001] and Nieuwenhuis and Rubio [2001, pp. 29–42]. These more recent works deem a set saturated if every possible inference is redundant, but use the more general notions of redundancy.

Finally, it bears mentioning that, thanks to the Curry-deBruijn-Howard morphism, one can view a proof p as a term whose type is precisely its conclusion $[p]_{CI}$. Considering proof orderings would then be related to the definition of a suitable ordering on higher-order terms, as studied, for example, in [Jouan-

naud and Rubio, 1999], or, for dependently typed terms, in [Cirstea, Kirchner, and Liquori, 2001, Barthe, Cirstea, Kirchner, and Liquori, 2003, Virga, 1999].

Acknowledgements

This paper benefited greatly from comments and suggestions by Maria-Paola Bonacina, Guillaume Burel, Mitch Harris and anonymous referees.

References

- Baader, F., Nipkow, T., 1998. *Term Rewriting and all That*. Cambridge University Press. 3
- Bachmair, L., Dershowitz, N., 1994. Equational inference, canonical proofs, and proof orderings. *Journal of Association for Computing Machinery* 41 (2), 236–276. 3
- Bachmair, L., Dershowitz, N., Hsiang, J., June 1986. Orderings for equational proofs. In: *Proceedings 1st IEEE Symposium on Logic in Computer Science* (Cambridge, MA). pp. 346–357. 4
- Bachmair, L., Dershowitz, N., Plaisted, D. A., 1989. Completion without failure. In: Aït-Kaci, H., Nivat, M. (Eds.), *Resolution of Equations in Algebraic Structures 2: Rewriting Techniques*. Academic Press, New York, pp. 1–30. 4
- Bachmair, L., Ganzinger, H., 1991. Completion of first-order clauses with equality by strict superposition (Extended abstract). In: Okada, M., Kaplan, S. (Eds.), *Proceedings 2nd International Workshop on Conditional and Typed Term Rewriting Systems* (Montreal, Canada, June 1990). Vol. 516 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, pp. 162–180. 25
- Bachmair, L., Ganzinger, H., 2001. Resolution theorem proving. In: Robinson, A., Voronkov, A. (Eds.), *Handbook of Automated Reasoning*. Vol. I. Elsevier Science, Ch. 2, pp. 19–99. 25
- Barthe, G., Cirstea, H., Kirchner, C., Liquori, L., Jan. 2003. Pure Patterns Type Systems. In: *Principles of Programming Languages - POPL2003*, New Orleans, USA. ACM, pp. 250–261. 26
- Bonacina, M. P., December 1992. Distributed automated deduction. Ph.D. thesis, Department of Computer Science, State University of New York at Stony Brook. 25
- Bonacina, M.-P., Dershowitz, N., 2003. Abstract canonical inference. *ACM Transactions on Computational Logic* to appear. 6, 25
- Bonacina, M. P., Hsiang, J., 1995. Towards a foundation of completion proce-

- dures as semidecision procedures. *Theoretical Computer Science* 146, 199–242. 25
- Buchberger, B., 1965. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Dissertation, Univ. Innsbruck, Austria. 4
- Buchberger, B., 1985. *Multidimensional Systems Theory*. Reidel, Bose, N.K. Ed., Ch. Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, pp. 184–232. 4
- Buchberger, B., 1987. History and basic features of the critical-pair / completion approach. *Journal of Symbolic Computation* 3 (1 & 2), 3–38. 4
- Cirstea, H., Kirchner, C., Liquori, L., Apr. 2001. The Rho cube. In: Honsell, F. (Ed.), *Proc. Foundations of Software Science and Computation Structures*. Lecture Notes in Computer Science. Genova, Italy, pp. 166–180. 26
- Comon, H., Kirchner, C., 2001. Constraint solving on terms. *Lecture Notes in Computer Science* 2002. 2
- Dershowitz, N., March 1982. Orderings for term-rewriting systems. *Theoretical Computer Science* 17 (3), 279–301. 6
- Dershowitz, N., 1989. Completion and its applications. In: Aït-Kaci, H., Nivat, M. (Eds.), *Resolution of Equations in Algebraic Structures, Volume 2: Rewriting Techniques*. Academic Press inc., pp. 31–86. 4
- Dershowitz, N., Kirchner, C., Jul. 2002. Abstract canonical inference systems. In: *Proceedings of the UNIF’02 workshop*.
- Dershowitz, N., Kirchner, C., Jun. 2003. Abstract saturation-based inference. In: Kolaitis, P. (Ed.), *Proceedings of 18th IEEE Symposium on Logic in Computer Science*. IEEE, Ottawa, Ontario, pp. 65–74.
- Dershowitz, N., Marcus, L., Tarlecki, A., August 1988. Existence, uniqueness and construction of rewrite systems. *SIAM Journal of Computing* 17 (4), 629–639. 4
- Dershowitz, N., Okada, M., 1988. Proof-theoretic techniques and the theory of rewriting. In: *Proceedings 3rd IEEE Symposium on Logic in Computer Science, Edinburgh (UK)*. IEEE, pp. 104–111. 3
- Dershowitz, N., Plaisted, D. A., 2001. Rewriting. In: Robinson, A., Voronkov, A. (Eds.), *Handbook of Automated Reasoning*. Vol. I. Elsevier Science, Ch. 9, pp. 535–610. 3
- Doggaz, N., Kirchner, C., 1991. Completion for unification. *Theoretical Computer Science* 85 (1), 231–251. 4
- Dowek, G., Hardin, T., Kirchner, C., Nov 2003. Theorem proving modulo. *Journal of Automated Reasoning* 31 (1), 33–72. 6
- Girard, J.-Y., Lafont, Y., Taylor, P., 1989. *Proofs and Types*. Vol. 7 of Cambridge Tracts in Theoretical Computer Science. Cambridge University Press. 6
- Gnaedig, I., Kirchner, C., Kirchner, H., 1988. Equational completion in ordered algebras. In: Dauchet, M., Nivat, M. (Eds.), *Proceedings 13th Colloquium on Trees in Algebra and Programming*. Vol. 299 of Lecture Notes in Computer Science. Springer-Verlag, pp. 165–184. 4

- Grätzer, G., 1979. *Universal Algebra*, 2nd Edition. Springer-Verlag. 28
- Hsiang, J., Rusinowitch, M., July 1991. Proving refutational completeness of theorem proving strategies. The transfinite semantic tree method. *J. of the Association for Computing Machinery* 38 (3), 559–587. 4
- Huet, G., Oct. 1980. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the ACM* 27 (4), 797–821, preliminary version in 18th Symposium on Foundations of Computer Science, IEEE, 1977. 4
- Huet, G., August 1981. A complete proof of correctness of the Knuth–Bendix completion algorithm. *Journal of Computer and System Sciences* 23 (1), 11–21, also as: Rapport 25, INRIA, 1980. 4
- Jouannaud, J.-P., Kirchner, H., 1986. Completion of a set of rules modulo a set of equations. *SIAM Journal of Computing* 15 (4), 1155–1194. 4
- Jouannaud, J.-P., Rubio, A., 1999. The higher-order recursive path ordering. In: Longo, G. (Ed.), *Proc. 14th Annual Symposium on Logic in Computer Science*. IEEE, Trento, Italy, pp. 402–411. 25
- Kandri-Rody, A., Kapur, D., Winkler, F., 1989. Knuth-Bendix procedures and Buchberger algorithm—A synthesis. In: *Proc. 20th International Symposium on Symbolic and Algebraic Computation* (Portland, Oregon). pp. 55–67. 4
- Kapur, D., Musser, D. R., 1987. Proof by consistency. *Artificial Intelligence* 13 (2), 125–157. 4
- Knuth, D. E., Bendix, P. B., 1970. Simple word problems in universal algebras. In: Leech, J. (Ed.), *Computational Problems in Abstract Algebra*. Pergamon Press, Oxford, pp. 263–297. 4
- Lankford, D. S., December 1975. Canonical inference. Memo ATP-32, Automatic Theorem Proving Project, University of Texas, Austin, TX. 4
- Metivier, Y., January 1983. About the rewriting systems produced by the Knuth-Bendix completion algorithm. *Information Processing Letters* 16 (1), 31–34. 4
- Nieuwenhuis, R., Rubio, A., 2001. Paramodulation-based theorem proving. In: Robinson, A., Voronkov, A. (Eds.), *Handbook of Automated Reasoning*. Vol. I. Elsevier Science, Ch. 7, pp. 371–443. 25
- Peterson, G., Stickel, M., 1981. Complete sets of reductions for some equational theories. *J. of the Association for Computing Machinery* 28 (2), 233–264. 4
- Rusinowitch, M., 1989. *Démonstration Automatique: Techniques de Réécriture*. Science Informatique. InterEditions, Paris. 25
- Rusinowitch, M., 1991. Theorem-proving with resolution and superposition. *J. Symbolic Computation* 11, 21–50. 25
- Smyth, M. B., 1977. Powerdomains. *J. of Computer and Systems Science* 16, 23–36. 13
- Taylor, W., 1979. Equational logic. *Houston Journal of Mathematics* 5, 1–51, appears also in [Grätzer, 1979], Appendix 4. 6
- “Terese” (M. Bezem, J. W. Klop and R. de Vrijer, eds.), 2002. *Term Rewriting*

Systems. Cambridge University Press. 3
Virga, R., Sep. 1999. Higher-order rewriting with dependent types. Ph.D.
thesis, Department of Mathematical Sciences, Carnegie Mellon University,
available as Technical Report CMU-CS-99-167. 26