Abstract Canonical Inference Systems

Nachum Dershowitz, Claude Kirchner

Abstract Canonical Inference Systems

Nachum Dershowitz
School of Computer Science
Tel-Aviv University
P.O.B. 39040
Ramat Aviv, Tel-Aviv 69978
Israel
phone: +972-3-640-5356
fax: +972-3-640-5948
email: Nachumd@tau.ac.il

Claude Kirchner
LORIA & INRIA
615, rue du Jardin Botanique
B.P. 101
54602 Villers-lès-Nancy Cedex
France
phone: +33-3-8359-3011
fax: +33-3-8327-8319
email: Claude.Kirchner@loria.fr

Version: July 2002

Abstract

We provide a general proof theoretical setting under which the so-called "completion processes" (as used for equational reasoning) can be modeled, understood, studied, proved and generalized. This framework—based on a well-founded ordering on proofs—allows us to derive saturation processes and redundancy criteria abstractly.

1 Motivation

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 consequences) and can be removed. Similarly, one speaks of independent sets of equations, or alternative presentations of algebras. In these cases, one is comparing sets of formulæ based on number or total size.

We also speak of solving equations, or, more generally, sets of constraints. In such a context, we are interested in the form of the axioms in the set. The process of solving transforms a defining set into axioms in *solved form* (see [7]). In Gaussian elimination, for example, one begins with a set of linear equalities involving unknown constants, and one is looking to infer solved forms assigning numerical values to each unknown. 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 solution, it is easy to check whether other linear equalities follow.

In proof theory, one assigns ordinals to proofs and shows that under certain circumstances there exists a *maximal formula* in a proof that can be replaced in a way that reduces the ordinal of the proof. These proof-theoretical concepts can be extended to dynamically changing proof systems (see [10]).

An interesting feature of the complete sets of reductions produced by Knuth's completion procedure [16] and the Gröbner basis generated by Buchberger's algorithm [6] is that they are unique up to the ordering used [9, 17].

In this paper, we generalize the proof-ordering method used in term-rewriting [5] to an abstract setting of arbitrary proof systems, supplied with an ordering of proofs. Fixing inference and the ordering, but letting axioms vary, we define the set of *canonical* axioms in four ways:

1. Theorems that can appear as assumptions in minimal proofs
2. Non-redundant theorems
3. Conclusions of trivial proofs
4. Limit of a completion process

The only related—but substantially less general—work we can think of is [1].

The form of the paper is rather axiomatic as we stress the full exposition of the formal development and of the proofs, at the expense of motivations that can be found in particular in the usual completion processes as described e.g. in standard literature on rewriting [2, 11].

2 Proof Systems

Let us begin with the following structure, which we will call an *ordered proof system*:

- $\mathbb{P}$ Proofs;
- $\mathbb{A}$ Formulas;
- $\Gamma : \mathbb{P} \to 2^{\mathbb{A}}$ Assumptions;

- $\Delta : \mathbb{P} \to \mathbb{A}$ Conclusion;
- $\geq : \mathbb{P}^2 \to 2$ Well-founded proof ordering.

The proof ordering may be partial. As usual, we use $>$ for $\geq \cap \neq$. We extend Γ and Δ to sets (of proofs), in the standard fashion:

Definition 1

$$\Gamma\, P = \bigcup_{p \in P} \Gamma\, p \tag{1}$$

$$\Delta\, P = \bigcup_{p \in P} \{\Delta\, p\} \tag{2}$$

Definition 2 (Theories) *The set of all the proofs of the formula c, starting from a set of formulæ A:*

$$\Pi(A \vdash c) = \{p \in \mathbb{P} \mid \Gamma\, p = A, \Delta\, p = c\} \tag{3}$$

The set of all proofs using the set of assumptions A:

$$\Pi\, A = \{p \in \mathbb{P} \mid \Gamma\, p \subseteq A\} \tag{4}$$

The theory *of a set of assumptions A:*

$$\Theta A = \Delta\, \Pi\, A \tag{5}$$

It follows from these definitions that Γ, Δ, Π and Θ are monotonic:

Proposition 3 *For all sets of formulæ A and B and sets of proofs P and Q:*

$$\Gamma\, \emptyset = \Delta\, \emptyset = \emptyset \tag{6}$$

$$\Gamma\, \Pi\, A \subseteq A \tag{7}$$

$$P \subseteq Q \Rightarrow \Gamma\, P \subseteq \Gamma\, Q \tag{8}$$

$$P \subseteq Q \Rightarrow \Delta\, P \subseteq \Delta\, Q \tag{9}$$

$$A \subseteq B \Rightarrow \Pi\, A \subseteq \Pi\, B \tag{10}$$

$$A \subseteq B \Rightarrow \Theta A \subseteq \Theta B \tag{11}$$

Proof:

- (6), (8) and (9) are clear from the definitions.
- For (7), $\Gamma\,\Pi\,A = \bigcup_{p\in\Pi\,A}\Gamma\,p \subseteq A$ by definition of $\Pi\,A$.
- For (10), $\forall p \in \Pi\,A, \Delta\,p \subseteq A \subseteq B$ thus $p \in \Pi\,B$.
- Then (11) is a consequence of (9) and (10).

□

Lemma 4

$$\Pi\,\Gamma\,\Pi\,A \quad = \quad \Pi\,A$$

Proof: By (7,10), $\Pi\,\Gamma\,\Pi\,A \subseteq \Pi\,A$.

Suppose $p \in \Pi\,A$. Then $\Gamma\,p \in \Gamma\,\Pi\,A$ by (8) and $p \in \Pi\,\Gamma\,\Pi\,A$, by definition. □

We consider sets of formulæ to be equivalent when they allow one to prove exactly the same theorems. This defines an equivalence relation on $2^{\mathbb{A}}$:

Definition 5 (Equivalence)

$$A \equiv B \quad\Leftrightarrow\quad \Theta A = \Theta B$$

Corollary 6 *Only what is used in proofs is needed:*

$$A \quad\equiv\quad \Gamma\,\Pi\,A$$

Proof:

$$\Theta A = \Delta\,\Pi\,A = \Delta\,\Pi\,\Gamma\,\Pi\,A = \Theta\Gamma\,\Pi\,A$$

□

Definition 7 (Minimal Proofs)

$$\begin{array}{rcl} \mu P & = & \{p \in P \,|\, \neg\exists q \in P.\ \Delta\,q = \Delta\,p \wedge q < p\} \\ \coprod A & = & \mu\Pi\,A \end{array}$$

Well-foundedness of the proof ordering means that:

Proposition 8 *One can prove as much using minimal proofs as with ordinary ones:*

$$(\Theta A \ =)\ \Delta\,\Pi\,A \quad = \quad \Delta\ \coprod\ A$$

Proof: $\Delta\,\Pi\,A \supseteq \Delta\ \amalg\ A$: by monotonicity of Δ and since minimal proofs are proofs, i.e. $\Pi\,A \supseteq \amalg\,A$.

$\Delta\,\Pi\,A \subseteq \Delta\ \amalg\ A$: for all $c \in \Delta\,\Pi\,A$, there exists p such that $p \in \Pi(A \vdash c)$. Since $\geq$ is well-founded, there exists p' minimal, smaller than p that proves the same thing: $p' \in \Pi(A \vdash c)$, therefore $c \in \Delta\ \amalg\ A$. $\square$

Lemma 9 *Minimal proofs use the assumptions of minimal proofs:*

$$\amalg\,\Gamma\,\Pi\,A \quad = \quad \amalg\,A$$

3 Reduced Systems

Definition 10 *Those assumptions employed in minimal proofs are denoted*

$$A^\flat \quad = \quad \Gamma\ \amalg\ A$$

Definition 11 (Reduced) *A set A of formulæ is* reduced *if*

$$A \quad = \quad A^\flat\ (=\ \Gamma\ \amalg\ A)$$

Lemma 12

$$A^\flat \quad \subseteq \quad A$$

Proof: By definition of $\amalg$, $\amalg\,A \subseteq \Pi\,A$ and by monotonicity of Γ and Proposition 3.7 we get $A^\flat = \Gamma\ \amalg\ A \subseteq \Gamma\,\Pi\,A \subseteq A$. $\square$

Lemma 13 *What is reduced cannot be further reduced:*

$$A^{\flat\,\flat} \quad = \quad A^\flat$$

Lemma 14 *A reduced system can prove as much as the initial one:*

$$A^\flat \quad \equiv \quad A$$

Proof: By Lemma 12 and Proposition 8

$$\Theta A^\flat = \Delta\,\Pi\,\Gamma\ \amalg\ A = \Delta\ \amalg\ \Gamma\ \amalg\ A = \Delta\ \amalg\ A = \Theta A$$

$\square$

Up to now we made no assumption on the proof system but their well-foundedness. To get closer to the ordered proof systems we are usually using and which are of main interest, we are assuming from now on three standard things about proofs:

Postulate A (Monotonicity)

$$\Pi(A \vdash c) \neq \emptyset \quad \Rightarrow \quad \Pi(A \cup B \vdash c) \neq \emptyset$$

Postulate B (Reflexivity)

$$\Pi(\{a\} \vdash a) \quad \neq \quad \emptyset$$

Postulate C (Closure)

$$\Theta\Theta A \quad \subseteq \quad \Theta A$$

The name of the postulates are abbreviated C, R, M when clear from the context. Note that these three postulates are not consequences of the previous definitions as there exist ordered proof systems that do not verify them. Closure typically is a consequence of the cut rule.

The first immediate but important consequence of the reflexivity postulate is that the theory generated by a set of formulæ A contains A, i.e. $A \subseteq \Theta A$. Since by definition $\Theta A = \Delta\,\Pi\,A$ and by Proposition 8 we get that $A \subseteq \Delta\ \Pi\ A$. Applying this to ΘA itself we get:

Lemma 15

$$\Theta A \quad \subseteq \quad \Delta\ \Pi\ \Theta A$$

We refer to proofs in $\Pi\,\Theta A$ as being in *normal-form*.

Definition 16 (Trivial Proof) *A proof p is* trivial *if $\Gamma\,p = \{\Delta\,p\}$.*

Every formula admits a trivial proof, by reflexivity. We denote by $\widehat{a}$ such a trivial proof of $a \in \mathbb{A}$ and by $\widehat{A}$ the set of trivial proofs of each $a \in A$.

Reflexivity strengthens Lemma 4 to:

Lemma 17

$$\Gamma\,\Pi\,A \quad = \quad A$$

Proof: $\Gamma\,\Pi\,A \subseteq A$ by (7).

$\Gamma\,\Pi\,A \supseteq A$ since for all $a \in A$, by reflexivity there exists $p \in \Pi(\{a\} \vdash a)$ and thus $a \in \Gamma\,\Pi\,A$. □

Lemma 18 *A set of formulæ A and its full theory ΘA support exactly the same theorems:*

$$\Theta\Theta A = \Theta A \quad (or \quad \Theta A \equiv A)$$

Proof: By reflexivity, $A \subseteq \Theta A$. By (11), $\Theta A \subseteq \Theta\Theta A$. By closure, the theories are equal. $\square$

Also by reflexivity:

Lemma 19 *The set of proofs are the same iff the set of their assumptions are the same.*

$$\Pi\, A = \Pi\, B \quad \Leftrightarrow \quad A = B$$

4 Canonical Systems

Definition 20 (Saturation) *A set A of formulæ is* saturated *if it supports all possible minimal proofs:*

$$A \quad \supseteq \quad [\Theta A]^\flat$$

Our main definition is:

Definition 21 (Canonical Basis) *The formulæ that appear as assumptions of minimal proofs:*

$$\boxed{\quad A^\sharp \quad = \quad [\Theta A]^\flat \quad}$$

Lemma 22

$$(A^\sharp)^\flat \quad = \quad A^\sharp$$

Proof: By Lemma 13 we get: $(A^\sharp)^\flat \;=\; (\Theta A)^{\flat\flat} \;=\; (\Theta A)^\flat \;=\; A^\sharp$. $\square$

Definition 23 (Canonical Set) *A set A of formulæ is* canonical *if*

$$A \quad = \quad A^\sharp \; (= \; [\Theta A]^\flat)$$

Theorem 24 *The canonical basis is a basis:*

$$\boxed{\quad A^\sharp \quad \equiv \quad A \quad}$$

Proof: By Lemmata 14 and 18, we get $A^\sharp = [\Theta A]^\flat \equiv \Theta A \equiv A$. $\square$

Lemma 25

$$A \equiv B \quad \Leftrightarrow \quad A^\sharp = B^\sharp$$

Proof: Suppose $A \equiv B$, that is, $\Theta A = \Theta B$. By substitution of equals in the definitions:

$$A^\sharp = (\Theta A)^\flat = (\Theta B)^\flat = B^\sharp$$

Suppose $A^\sharp = B^\sharp$. By Lemma 14:

$$\Theta A \equiv (\Theta A)^\flat = A^\sharp = B^\sharp = (\Theta B)^\flat \equiv \Theta B$$

$\square$

Corollary 26

$$\boxed{A^{\sharp\sharp} \quad = \quad A^\sharp}$$

Proof: $A \equiv B$ iff $A^\sharp = B^\sharp$ by Lemma 25. Let B be $A^\sharp$, then $A \equiv A^\sharp$ iff $A^\sharp = A^{\sharp\sharp}$ and Theorem 24 gives the left side. $\square$

Corollary 27

$$\amalg\, A^\sharp \quad = \quad \amalg\, \Theta A$$

Proof: By Theorem 24

$$\amalg\, A^\sharp \quad = \quad \amalg\ (\Theta A)^\flat \quad = \quad \amalg\ \Gamma\ \amalg\ \Theta A \quad = \quad \amalg\ \Theta A^\sharp \quad = \quad \amalg\ \Theta A$$

$\square$

Definition 28 (Better Proofs) *Q is* strictly better *than P:*

$$P \sqsupset Q \quad \Leftrightarrow \quad \forall p \in P.\ \exists q \in Q.\ \Delta\, q = \Delta\, p \wedge p > q \tag{12}$$

Q is better *than P:*

$$P \sqsupseteq Q \quad \Leftrightarrow \quad \forall p \in P.\ \exists q \in Q.\ \Delta\, q = \Delta\, p \wedge p \geq q \tag{13}$$

Note that the quasi-order $\sqsupseteq$ is *not* the reflexive closure of $\sqsupset$.

On account of well-foundedness:

Proposition 29

$$\begin{array}{rcccl} & & & & P \sqsupseteq \mu P \\ P \subseteq Q & \Rightarrow & P \sqsupseteq Q & \Rightarrow & \Delta\, P \subseteq \Delta\, Q \\ & & A \subseteq B & \Rightarrow & \Pi\, A \sqsupseteq \Pi\, B \end{array}$$

Proof: By definition of the minimality of μP. $\square$

Corollary 30

$$A \subseteq B \wedge A \equiv B \Rightarrow A \succsim B$$

A set of axioms B is a simpler basis than A when both can prove the same things, but the proofs made from B are better:

Definition 31 (Simpler Basis) *B is* simpler *than A:*

$$A \succsim B \quad \Leftrightarrow \quad A \equiv B \ \wedge \ \Pi\, A \sqsupseteq \Pi\, B$$

Reflexivity and transitivity are immediate:

Lemma 32 $\succsim$ *is a quasi-ordering.*

Lemma 33

$$\boxed{\quad A \ \succsim \ A^\sharp \quad}$$

Proof: By Theorem 24, A and $A^\sharp$ have the same theory. Let $p \in \Pi(B \vdash c)$ with $B \subseteq A$. Let q be the smallest proof of c in $\Pi\,\Theta A$. By definition, $q \in \Pi\,\Theta A$, and, therefore, $\Gamma\, q \subseteq A^\sharp$. $\square$

Theorem 34 *A canonical basis is the simplest:*

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

Proof: Assuming $A \equiv B$ and using Lemmata 33 and 25, $B \succsim B^\sharp = A^\sharp$. $\Box$

Definition 35 (Redundancy) *The* redundant *formulæ in A are:*

$$\rho A \quad = \quad \{r \in \mathbb{A} \,|\, A \succsim A \setminus \{r\}\} \tag{14}$$

Lemma 36 *When there exists redundant formulæ, without them we can prove as much, but the proofs are strictly better:*

$$A \quad \succsim \quad A \setminus \rho A$$

Proof: Let $A' = A \setminus \rho A$. Consider a proof $p_1 \in \Pi\, A \setminus \Pi\, A'$. Since there is a redundant $r \in \Gamma\, p_1 \cap \rho A$, there must be a proof $p_2 \in \Pi\,(A \setminus \{r\}) \subseteq \Pi\, A$ such that $p_1 \geq p_2$ and $\Delta\, p_1 = \Delta\, p_2$. But $\Gamma\, p_2 \neq \Gamma\, p_1$, so $p_1 > p_2$. If $p_2 \notin \Pi\, A'$, then there would also be a $p_3 \in \Pi\, A$, 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 $p_n \in \Pi\, A'$ such that $p_n \leq p_1$ and $\Delta\, p_n = \Delta\, p_1$.

This shows that (1) $\Theta A \subseteq \Theta A'$ and since the converse is true by monotonicity, we get $A \equiv A'$ and (2) since we assume that the set of redundant formulæ is non empty, we get that $A \sqsupset A'$. $\Box$

Theorem 37 *Redundant formulæ are not needed:*

$$A^\flat \quad = \quad A \setminus \rho A$$

Proof: If $a \notin A^\flat = \Gamma\ \amalg\ A$, then $A \succsim A \setminus \{a\}$. Thus, $a \in \rho A$.

Let $a \in A^\flat$, that is, $a \in \Gamma\, p$ for some $p \in \amalg\, A$. Let $A' = A \setminus \{a\}$. Suppose $a \in \rho A$, in other words, $A \succsim A'$. There must be a proof $q \leq p$ with $\Delta\, q = \Delta\, p$ such that $\Gamma\, q \subseteq A'$. Since, then, $q \neq p$, we have $q < p$. Hence, $p \notin \amalg\, A$. Thus, $A^\flat \subseteq A'$. $\Box$

Corollary 38

$$\boxed{A^\sharp \quad = \quad A^\sharp \setminus \rho A^\sharp}$$

Proof: By Theorem 37 and Lemma 22. $\Box$

5 Inference

Definition 39 (Deduction) *A* deduction mechanism $\leadsto$ *is a mapping from sets of formulæ to sets of formulæ.* $A \leadsto B$ *is a* deduction step *of a deduction mechanism* $\leadsto$ *if* $(A, B) \in \ \leadsto$.

Definition 40 (Soundness) *A deduction mechanism* $\leadsto$ *is* sound *if*

$$A \leadsto A' \quad \Rightarrow \quad \Theta A \supseteq \Theta A'$$

We only consider sound mechanisms:

Definition 41 (Derivation) *A* derivation *is a chain of sound deductions:*

$$A_0 \leadsto A_1 \leadsto \cdots \leadsto A_i \leadsto \cdots$$

Definition 42 (Persistent Formulæ) *The* limit A_∞ *of a derivation* $\{A_i\}_i$ *is its persistent formulæ:*

$$A_\infty = \limsup_{i \to \infty} A_i \ = \ \bigcup_j \bigcap_{i>j} A_i$$

We are interested in the ability to derive minimal proofs:

Definition 43 (Completeness) *A derivation* $\{A_i\}_i$ *is* complete *if every theorem of* A_0 *eventually admits a persistent normal-form proof:*

$$\Theta A_0 \quad \subseteq \quad \Delta \, (\Pi \, A_\infty \cap \amalg \, \Theta A_0)$$

This means that there is at least one minimal proof per theorem, but not that all minimal proofs are supported.

Proposition 44 *For a complete derivation* $\{A_i\}_i$

$$\Theta A_0 \quad \subseteq \quad \Theta A_\infty$$

Proof:

$$\Theta A_0 \ \subseteq \ \Delta \, (\Pi \, A_\infty \cap \amalg \, \Theta A_0) \ \subseteq \ \Delta \, \Pi \, A_\infty \ = \ \Theta A_\infty$$

□

Definition 45 (Simplifying) *A deduction mechanism* $\rightsquigarrow$ *is* simplifying *if it proves as much and the proofs only get better:*

$$\begin{aligned} A \rightsquigarrow A' &\Rightarrow \Theta A = \Theta A' \\ A \rightsquigarrow A' &\Rightarrow \Pi\, A \sqsupseteq \Pi\, A' \end{aligned}$$

This is denoted

$$\rightsquigarrow \quad \subseteq \quad \succsim$$

Since the proof ordering is well-founded:

Lemma 46 *A sufficient condition for a simplifying derivation* $\{A_i\}_i$ *to be complete is that each non-normal-form proof becomes eventually strictly better:*

$$\textstyle\bigcup_i \Pi\, A_i \setminus \amalg\, \Theta A_0 \quad \sqsupset \quad \bigcup_i \Pi\, A_i$$

Proof: Let $p_i \in \Pi\, A_i$ be a proof of $c \in \Theta A_i$. Since the derivation is simplifying, there are proofs $p_j \in \Pi\, A_j$ of c such that $p_i \geq p_{i+1} \geq \cdots$. By well-foundedness, from some point on these are all the same proof q. Thus, $\Gamma\, q \subset A_\infty$ and $q \in \Pi\, A_\infty$. If $q \in \amalg\, \Theta A_0$ then $c \in \Delta\, (\Pi\, A_\infty \cap \amalg\, \Theta A_0$ and we are done. Otherwise, the sufficient condition implies that for some k, there is a proof $q_k \in \Pi\, A_k$ of c such that $p_i \geq q > q_k$. Completeness follows by induction on proofs. $\Box$

Corollary 47 *If a deduction mechanism is simplifying then* $\Theta A_0 \subseteq \Theta A_\infty$.

Definition 48 (Finitely-Based Proofs) *An ordered proof system has* finitely-based proofs *if they use only a finite number of assumptions, i.e.* $|\Gamma\, p| < \infty$ *for all* $p \in \mathbb{P}$.

From now on, we will presume finitely-based proofs:

Postulate D

$$p \in \mathbb{P} \Rightarrow |\Gamma\, p| < \infty$$

Lemma 49 *Proofs are* continuous *i.e.*

$$\limsup_{i\to\infty} \Pi\, A_i \quad = \quad \Pi\, A_\infty \ (= \Pi\, \limsup_{i\to\infty} A_i)$$

for any derivation $\{A_i\}_i$ *of a simplifying deduction mechanism.*

Proof: For any $p \in \bigcap_{j>i} \Pi\, A_j$, we have $\Gamma\, p \subseteq A_j$ for all $j > i$. Thus, $\Gamma\, p \subseteq A_\infty$ and $p \in \Pi\, A_\infty$.

If $p \in \Pi\, A_\infty$, then each $a_j \in \Gamma\, p \subseteq A_\infty$ persists in A_i from some point on. Postulating $|\Gamma\, p| < \infty$ implies that all of $\Gamma\, p$ persists in A_i from some point on. Hence, p persists in $\Pi\, A_i$ from that point on. $\Box$

Lemma 50 *If proofs are continuous then*

$$\Theta A_0 \quad = \quad \Theta A_\infty$$

for any simplifying derivation $\{A_i\}_i$.

Proof: By continuity

$$\Theta A_\infty = \Delta\, \Pi\, A_\infty = \Delta \textstyle\bigcup_j \bigcap_{i>j} \Pi\, A_i$$

So, if $c \in \Theta A_\infty$, then $c \in \Delta\, \Pi\, A_i = \Theta A_i$ for some i. But $\Theta A_i = \Theta A_0$ is guaranteed for simplifying deductions. Proposition 44 gives the other direction. $\Box$

Definition 51 (Reducing) *A derivation is* reducing *if its persistent equations are all reduced:*

$$A_\infty \quad = \quad A_\infty^\flat$$

In other words, the limit does not contain any redundancy: $\rho A_\infty = \emptyset$.

Lemma 52 *A sufficient condition for a derivation $\{A_i\}_i$ to be reducing is that no formula remain persistently redundant:*

$$\limsup_{i\to\infty} \rho A_i = \emptyset \quad (or \quad \rho A_i \cap A_\infty = \emptyset)$$

Definition 53 (Canonical Derivation) *A derivation is* canonical *if it is both complete and reducing.*

Lemma 54 *For continuous proofs: A derivation is canonical iff*

$$A_\infty \quad = \quad A_0^\sharp$$

Proof:

$$\Delta\,(\Pi\, A_0^\sharp \cap \amalg\, \Theta A_0^\sharp) = \Delta\,(\Pi\, A_0^\sharp \cap \amalg\, \Theta A_0^\sharp)$$

$$= \Delta\ \amalg\ A_0^\sharp = \Delta\, \Pi\, A_0^\sharp = \Theta A_0^\sharp = \Theta A_\infty = \Theta A_0$$

□

Definition 55 (Expansion and Contraction) *A deduction step $A \rightsquigarrow A \cup B$ is an* expansion *provided*

$$B \subseteq \Theta A$$

A deduction step $A \cup B \rightsquigarrow A$ is a contraction *provided*

$$A \cup B \succsim A$$

Proposition 56 *Expansions and contractions are sound.*

Definition 57 (Progressive) *A deduction mechanism δ is* progressive *if it makes every non-minimal proof better:*

$$\delta(A) \quad \subseteq \quad \Theta A \tag{15}$$

$$\Pi\, A \setminus \amalg\, \Theta A \quad \sqsupset \quad \Pi\,(A \cup \delta(A)) \tag{16}$$

Definition 58 (Fairness) *A derivation $\{A_i\}_i$ is* fair for *a progressive mechanism δ if all persistently progressive formulæ are derived:*

$$\delta(A_\infty) \ \subseteq \ \textstyle\bigcup_i A_i$$

Lemma 59 *For finitely-based proof systems, simplifying fair derivations are complete.*

Proof: Suppose $c \in \Theta A_0 = \Theta A_\infty$ with proof $p \in \Pi\, A_\infty$. If $p \in \amalg\, \Theta A_0$, we are done. If $p \notin \amalg\, \Theta A_0 = \amalg\, \Theta A_\infty$, then by progressiveness c has a proof

$$q \in \Pi\,(A_\infty \cup \delta(A_\infty)) \subseteq \Pi\,(A_\infty \cup \textstyle\bigcup_i A_i) = \Pi\,(\bigcup_i A_i)$$

such that $q < p$. But by finiteness, $q \in \Pi\, A_j$ for some j, and since the derivation is simplifying, there is an $r \in \Pi\, A_\infty$ such that $r \leq q$. By well-foundedness, eventually we get a normal-form proof. □

6 Subproofs

We now impose an additional structure on proofs: We assume the existence of a well-founded *subproof* (partial) order on proofs, for which we employ the notation $p[q] \rhd q$. We extend this notation to sets:

$$P \rhd Q \quad \Leftrightarrow \quad \forall q \in Q.\ \exists p \in P.\ p \rhd q$$

and use $\trianglerighteq$ for its reflexive closure. ¿From now on, we assume three things about subproofs:

Postulate E (Trivia) *Assumptions are subproofs:*

$$P \quad \trianglerighteq \quad \widehat{\Gamma\, P}$$

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

$$P \trianglerighteq Q \quad \Rightarrow \quad \Gamma\, P \supseteq \Gamma\, Q$$

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

$$p \rhd q \succ q' \quad \Rightarrow \quad \exists p' \in \mathbb{P}.\ p \succ p' \rhd q' \tag{17}$$

Proposition 60

$$\widehat{A^\flat} \quad \subseteq \quad \amalg\, A$$

Proof: Suppose $a \in A^\flat$. Then there is some proof $p \in \amalg\, A^\flat$ such that $p \trianglerighteq \widehat{a}$. Were $\widehat{a}$ not minimal, then by the replacement postulate, neither would p be minimal. □

Theorem 61

$$A^\flat \quad = \quad \Delta\,(\amalg\, A \cap \widehat{A})$$

Proof: Clearly $\widehat{A^\flat} \subseteq \widehat{A}$. By the preceding proposition, $\widehat{A^\flat} \subseteq \amalg\, A$. Hence, $A^\flat = \Delta\, \widehat{A^\flat} \subseteq \Delta\,(\widehat{A} \cap \amalg\, A)$.

For the other direction, suppose $c \in \Delta\,(\amalg\, A \cap \widehat{A})$. Then $c \in \Gamma\,(\amalg\, A \cap \widehat{A}) \subseteq \Gamma\ \amalg\ A =^\flat$.

□

Corollary 62 *The canonical basis is the set of conclusions of all trivial minimal proofs:*

$$\boxed{A^\sharp \quad = \quad \Delta\,(\amalg\,\Theta A \cap \widehat{\Theta A})}$$

Lemma 63 *A derivation is complete if its limit is saturated.*

Proof: Suppose A_∞ is saturated. If $c \in \Theta A_0$ then by Lemma 15 there is a proof

$$q \in \amalg\,\Theta A_0$$

of c. So by continuity (Corollary 50) and saturation

$$\Gamma\, q \subseteq \Gamma\ \amalg\ \Theta A_0 = [\Theta A_0]^\flat = [\Theta A_\infty]^\flat \subseteq A_\infty$$

and, hence

$$q \in (\Pi\, A_\infty \cap \amalg\,\Theta A_0)$$

$\square$

Lemma 64 *If minimal proofs are unique, then the limit of a derivation is saturated if the derivation is complete.*

Proof: If $a \in \Gamma\ \amalg\ \Theta A_\infty$, then, by the replacement property, $\widehat{a}$ must be minimal. By totality,

$$\{\widehat{a}\} = \mu\Pi(\Theta A_\infty \vdash a) = \mu\Pi(\Theta A_0 \vdash a)$$

By completeness

$$a \in [\Theta A_\infty]^\flat \subseteq \Theta A_\infty \subseteq \Theta A_0 \subseteq \Delta\,(\Pi\, A_\infty \cap \amalg\,\Theta A_0)$$

But then

$$a \in \Delta\,(\Pi(A_\infty \vdash a) \cup \{p\})$$

Thus

$$\widehat{a} \in \Pi(A_\infty \vdash a)$$

and $a \in \mathbb{A}_\infty$. $\square$

Lemma 65 *Fair simplifying derivations are complete.*

Proof: By Lemma 56, $\Theta A_0 = \Theta A_\infty$. Suppose $c \in \Theta A_0$. Then it has a proof $p \in \Pi\, A_\infty$. If $p \in \Pi\, \Theta A_\infty$, we are done. So assume $p \in \Pi\, A_\infty \setminus \Pi\, \Theta A_\infty$. The progressive mechanism δ guarantees the existence of a smaller proof $q \in \Pi\,(A_\infty \cup \delta A_\infty)$. Since proofs are finite all of $\Gamma\, q$ appear in $\bigcup_{i \le n} A_i$ for some n. Since the derivation is simplifying, if $a \in A_i$, then for all $j \ge i$, $\widehat{a} \ge q_j$ for some proof $q_j \in \Pi\, A_j$. By the replacement property, there is a proof $r \in \Pi\, A_n$ such that $p > q \ge r$. By induction, we eventually get a minimal proof of c.

□

7 Completion

Completion processes have been studied intensively since their independent discovery and application to automated theorem proving by [6] and [16]. The fundamental role of orderings to enhance the proof search have been in particular discovered by [5]. The completion principle can be applied to numerous situations [8] including equational rewriting [18, 14, 3] induction [15] or unification [12]. A fundamental concept behind completion is the existence of critical proofs. An attempt to get an abstraction of critical pairs in category theory is presented in [19]. Because we have been generic in our approach, the results below can be applied to any completion based framework.

Definition 66 (Critical Proof) *A minimal proof* $p \in \Pi\, A$ *is* critical *if it is not in normal form, but all its subproofs are:*

$$\begin{array}{rcl} p & \in & \Pi\, A \setminus \Pi\, \Theta A \\ p \rhd q & \Rightarrow & q \in \Pi\, \Theta A \end{array}$$

Definition 67 (Critical Formulæ)

$$\nabla A \quad = \quad \{\Delta\, p \,|\, p \textit{ critical for } A\}$$

Lemma 68 *If* $\nabla A \subseteq \delta A \subseteq \Theta A$*, then* δ *is progressive.*

Definition 69 (Bulk Completion) Bulk completion *is a sequence of steps:*

$$A \quad \rightsquigarrow \quad [A \cup \nabla A]^\flat \tag{18}$$

Each step $A \rightsquigarrow A'$ is the composition of an expansion, $A \rightsquigarrow A \cup \nabla A = B$, and a contraction, $B \rightsquigarrow B^\flat = A'$.

Lemma 70 *Bulk completion is simplifying.*

Proof:

$$A \rightsquigarrow A' \Rightarrow A \gtrsim A \cup \nabla A \gtrsim [A \cup \nabla A]^{\flat} = A'$$

□

Lemma 71

$$\nabla(A^{\sharp}) \quad = \quad \emptyset$$

Corollary 72

$$A^{\sharp} \rightsquigarrow A' \quad \Rightarrow \quad A' = A^{\sharp}$$

Theorem 73 *Bulk completion is canonical.*

Definition 74 (Fair Completion) Fair completion *is a derivation that is fair for* ∇*, and which eventually deletes every redundancy.*

Theorem 75 *Fair completion is canonical.*

Theorem 76 *For fair completion:*

$$\boxed{A_0^{\sharp} \quad = \quad A_{\infty}}$$

8 Conclusion

The focus of this paper is the definition of *the* canonical basis for any deductive theory supplied with a proof ordering. The canonical basis is exactly what is needed for all theorems to enjoy normal-form proofs. The structure of normal-form (or "direct") proofs is fixed by the ordering which makes them minimal. We have given alternate characterizations of the canonical set, derived many of its properties, and shown how it can be generated.

Readers who are familiar with the Knuth-Bendix completion procedure [16], as developed in [13] and [5, 4], will see the analogy between the abstract concepts developed here and that concrete instance for equational proofs. Space limitations preclude expanding on this and first-order instances of our framework.

Acknowledgment

We thank Arnon Avron for asking what corresponds to completion in other deductive settings.

References

[1] Marc Aiguier, Diane Bahrami, and Catherine Dubois. Axioms for rewriting theory. Presented at the RULE'2000 workshop, September 2000.

[2] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[3] Leo Bachmair and Nachum Dershowitz. Completion for rewriting modulo a congruence. *Theoretical Computer Science*, 67(2-3):173–202, October 1989.

[4] Leo Bachmair and Nachum Dershowitz. Equational inference, canonical proofs, and proof orderings. *Journal of Association for Computing Machinery*, 41(2):236–276, 1994.

[5] Leo Bachmair, Nachum Dershowitz, and Jieh Hsiang. Orderings for equational proofs. In *Proceedings 1st IEEE Symposium on Logic in Computer Science, Cambridge (Mass., USA)*, pages 346–357, June 1986.

[6] Bruno Buchberger. *Multidimensional Systems Theory*, chapter Gröbner bases: an algorithmic method in polynomial ideal theory, pages 184–232. Reidel, Bose, N.K. Ed., 1985.

[7] Hubert Comon and Claude Kirchner. Constraint solving on terms. *Lecture Notes in Computer Science*, 2002, 2001.

[8] Nachum Dershowitz. Completion and its applications. In H. Aït-Kaci and M. Nivat, editors, *Resolution of Equations in Algebraic Structures, Volume 2: Rewriting Techniques*, pages 31–86. Academic Press inc., 1989.

[9] Nachum Dershowitz, Leo Marcus, and Andrzej Tarlecki. Existence, uniqueness and construction of rewrite systems. *SIAM Journal of Computing*, 17(4):629–639, August 1988.

[10] Nachum Dershowitz and Mitsuhiro Okada. Proof-theoretic techniques and the theory of rewriting. In *Proceedings 3rd IEEE Symposium on Logic in Computer Science, Edinburgh (UK)*, pages 104–111. IEEE, 1988.

[11] Nachum Dershowitz and David A. Plaisted. Rewriting. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 9, pages 535–610. Elsevier Science, 2001.

[12] N. Doggaz and Claude Kirchner. Completion for unification. *Theoretical Computer Science*, 85(1):231–251, 1991.

[13] Gérard Huet. A complete proof of correctness of the Knuth–Bendix completion algorithm. *Journal of Computer and System Sciences*, 23(1):11–21, August 1981. Also as: Rapport 25, INRIA, 1980.

[14] Jean-Pierre Jouannaud and Hélène Kirchner. Completion of a set of rules modulo a set of equations. *SIAM Journal of Computing*, 15(4):1155–1194, 1986. Preliminary version in Proceedings 11th ACM Symposium on Principles of Programming Languages, Salt Lake City (USA), 1984.

[15] Deepak Kapur and David R. Musser. Proof by consistency. *Artificial Intelligence*, 13(2):125–157, 1987.

[16] Donald E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, Oxford, 1970.

[17] Yves Metivier. About the rewriting systems produced by the Knuth-Bendix completion algorithm. *Information Processing Letters*, 16(1):31–34, January 1983.

[18] Gerald Peterson and Mark E. Stickel. Complete sets of reductions for some equational theories. *Journal of the ACM*, 28:233–264, 1981.

[19] Jean-Claude Raoult. On graph rewritings. *Theoretical Computer Science*, 32(1,2):1–24, July 1984.