

Canonicity¹

Nachum Dershowitz²

School of Computer Science, Tel Aviv University, Tel-Aviv 69978, Israel

Abstract

We explore how different proof orderings induce different notions of saturation. We relate completion, paramodulation, saturation, redundancy elimination, and rewrite system reduction to proof orderings.

They are not capable to ground a canonicity of universal consistency.

—Alexandra Deligiorgi (ΠΑΙΔΕΙΑ, 1998)

1 Introduction

We show how to define the *canonical* basis of an abstract deductive system in three distinct ways: (1) Formulæ appearing in minimal proofs; (2) non-redundant lemmata; (3) minimal trivial theorems. Well-founded orderings of proofs [1] are used to distinguish between cheap “direct” proofs, those that are of a computational flavor (e.g. rewrite proofs), and expensive “indirect” proofs, those that require search to find. This approach suggests generalizations of the concepts of “redundancy” and “saturation”, as elaborated by Nieuwenhuis and Rubio in [6]. Saturated, for us, means that all *cheap* proofs are supported. By considering different orderings on proofs, one gets different kinds of saturated sets.

This work continues our development of an abstract theory of “canonical inference”, initiated in [5]. Although we will use ground equations as an illustrative example, the framework applies equally well in the first-order setting, whether equational or clausal. Though our motivation is primarily æsthetic; our expectation is that practical applications will follow.

2 Proof Systems

Let \mathbb{A} be the set of all formulæ (ground equations and disequations, in our examples) over some fixed vocabulary. Let \mathbb{P} be the set of all (ground equational) proofs.

¹ This research was supported in part by the Israel Science Foundation (grant no. 254/01).

² Email: Nachumd@tau.ac.il

These sets are linked by two functions: $\Gamma : \mathbb{P} \rightarrow 2^{\mathbb{A}}$ gives the assumptions in a proof, and $\Delta : \mathbb{P} \rightarrow \mathbb{A}$ gives its conclusion. Both are extended to sets of proofs in the usual fashion. (We assume for simplicity that proofs use only a finite number of assumptions.)

The framework proposed here is predicated on two *well-founded* partial orderings over \mathbb{P} : a *proof ordering* \geq and a *subproof relation* \triangleright . They are related by a monotonicity requirement given below (7). We will assume for convenience that the proof ordering only compares proofs with the same conclusion ($p \geq q \Rightarrow \Delta p = \Delta q$), rather than mention this condition each time we will have cause to compare proofs.

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 deductively closed presentations. Let A^* denote the *theory* of presentation A , that is, the set of conclusions of all proofs with assumptions A :

$$(1) \quad A^* := \Delta \Gamma^{-1} A = \{\Delta p : p \in \mathbb{P}, \Gamma p = A\}$$

We assume the following three standard properties of Tarskian consequence relations:

$$(2) \quad A^* \subseteq (A \cup B)^*$$

$$(3) \quad A \subseteq A^*$$

$$(4) \quad A^{**} = A^*$$

Thus, $-^*$ is a closure operation. We say that presentation A is a *basis* for theory C if $A^* = C$. Presentations A and B are *equivalent* if their theories are identical: $A^* = B^*$.

As a very simple running example, let the vocabulary consist of the constant 0 and unary symbol s . Abbreviate tally terms $s^i 0$ as numeral i . The set \mathbb{A} consists of all *unordered* equations $i = j$ (so symmetry is built into the structure of proofs). We postpone dealing with disequations for the time being. An equational inference system for this vocabulary might consist of the following inference rules:

$$\frac{\square}{0 = 0} \mathbf{Z} \qquad \frac{\boxed{i = j}}{i = j} \mathbf{I}_{i=j}$$

$$\frac{i = j \quad j = k}{i = k} \mathbf{T} \qquad \frac{i = j}{si = sj} \mathbf{S}$$

where \mathbf{Z} is an (assumptionless) axiom, \mathbf{I} introduces assumptions, \mathbf{S} infers that $i + 1 = j + 1$ from a proof of $i = j$, and proof tree branches of the transitivity rule \mathbf{T} are *unordered*. To accommodate (2), and ignore unneeded assumptions, we also need projection:

$$\frac{a \quad c}{c} \mathbf{P}$$

For example, if $A = \{4 = 2, 4 = 0\}$, then $A^* = \{i = j : i \equiv j \pmod{2}\}$.

Consider the proof schemata:

$$\begin{array}{c}
 \vdots \\
 \hline
 \boxed{4=0} \quad \boxed{4=2} \quad \frac{i-j-2=0}{i-j-1=1} \\
 \hline
 \frac{\boxed{4=0}}{4=0} \quad \frac{\boxed{4=2}}{4=2} \quad \frac{2=0}{i-j=2} \\
 \hline
 \frac{0=0}{1=1} \quad \frac{2=0}{i-j=0} \\
 \hline
 \frac{\vdots}{i=i} \quad \frac{\vdots}{i+2=i} \quad \frac{\vdots}{i=j}
 \end{array}$$

Let's use proof terms for proofs, denoting the above three trees by $S^i Z$, $S^i T(I(4, 0), I(4, 2))$, and $S^j T(T(I(4, 0), I(4, 2)), SS(\nabla_{i-j-2=0}))$, respectively. With a recursive path ordering [4] to order proofs, precedence $Z < S < T < I < P < 0 < 1 < 2 < \dots$, and multiset “status” for I , minimal proofs of the theorems in A^* must take one of these two forms, or the form of one of their subproofs.

We call a proof *trivial* when it proves only itself and has no subproofs other than itself, that is, if $\Gamma p = \{\Delta p\}$ and $p \triangleright q \Rightarrow p = q$. 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 $a \in A$. For example, $I(4, 0) = \widehat{4=0}$.

We assume that proofs use their assumptions, that subproofs don't use non-existent assumptions, and that proof orderings are monotonic with respect to subproofs. Specifically, for all proofs p, q, r and formulæ a :

- (5) $a \in \Gamma p \Rightarrow p \triangleright \hat{a}$
- (6) $p \triangleright q \Rightarrow \Gamma p \supseteq \Gamma q$
- (7) $p \triangleright q > r \Rightarrow \exists v \in \mathbb{P}. p > v \triangleright r$

We make no other assumptions regarding proofs or their structure.

Postulate (7) is the most significant for the development that follows. It states that $>$ (restricted to proofs with the same conclusion) and \triangleright commute (i.e. $\triangleright \circ > \subseteq > \circ \triangleright$). In other words, “replacing” a subproof q of a proof p with a smaller proof r “results” in a proof v that is smaller than the original p . All proof orderings in the literature obey this monotonicity requirement. On account of (5), this also means that proofs are monotonic with respect to any inessential assumptions they refer to, should the latter admit smaller proofs.

Every formula a admits a trivial proof \hat{a} by (3,5). Let $\Sigma p = \{q : p \triangleright q\}$ denote the subproofs of p , and likewise $\Sigma P = \cup_{p \in P} \Sigma p$. This way, (5) can be abbreviated $\widehat{\Gamma p} \subseteq \Sigma p$.

It may be convenient to think of a proof-tree “leaf” as a subproof with only itself as a subproof; other subproofs are the “internal nodes”. There are two kinds of leaves: trivial proofs \hat{a} (such as inferences **I**), and vacuous proofs \bar{a} with $\Gamma \bar{a} = \emptyset$ and $\Delta \bar{a} = a$ (such as **Z**). By well-foundedness of \triangleright , there are no infinite “paths” in proof trees. It follows from (7) that the transitive closure of $> \cup \triangleright$ is also well-founded.

3 Canonical Systems

Denote the set of all proofs using assumptions of A by:

$$\Pi A := \{p \in \mathbb{P} : \Gamma p \subseteq A\}$$

and define the *minimal* proofs in a set of proofs as:

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

On account of well-foundedness, minimal proofs always exist.

Note that Γ , Δ , $*$, and Π are all monotonic with respect to set inclusion, but $\mu\Pi$ is not.

Proposition 3.1 *For all justifications P :*

$$(8) \quad P \subseteq \Pi \Gamma P$$

And for all presentations A, B :

$$(9) \quad \Gamma \Pi A = A$$

$$(10) \quad \Sigma \mu \Pi A = \mu \Pi A$$

$$(11) \quad \Pi A = \Pi B \Leftrightarrow A = B$$

Proof. (8) follows from the definitions, as does one direction of (9). $A \subseteq \Gamma \Pi A$ is a consequence of reflexivity (3). (10) is a consequence of (7). The interesting direction of (11) follows immediately from (9) and monotonicity of Γ . \square

We say that presentation A is *reduced* when $A = \Gamma \mu \Pi A$. Our main definition is:

Definition 3.2 [Canonical Presentation] The *canonical presentation* contains those formulæ that appear as assumptions of minimal proofs, allowing as assumptions any lemma of the theory:

$$A^\sharp := \Gamma \mu \Pi A^*$$

So, we say that A is *canonical* if $A = A^\sharp$.

Proof orderings are lifted to sets of proofs, as follows:

Definition 3.3 Justification Q is *better* than justification P if:

$$P \sqsupseteq Q \quad :\equiv \quad \forall p \in P. \exists q \in Q. p \geq q$$

It is *much better* if:

$$P \sqsupset Q \quad :\equiv \quad \forall p \in P. \exists q \in Q. p > q$$

Justifications are *similar* if:

$$P \simeq Q \quad :\equiv \quad P \sqsupseteq Q \sqsupseteq P$$

Transitivity of these three relations follows from the definitions. They are compatible: $\sqsupseteq \circ \sqsupseteq \subseteq \sqsupseteq$, $\sqsupseteq \circ \simeq \subseteq \sqsupseteq$, etc. Since it is also reflexive, \sqsupseteq is a quasi-ordering.

Proposition 3.4 *For all justifications P, Q :*

- (12) $P \sqsupseteq \mu P$
- (13) $P \sqsupseteq Q \Leftrightarrow \mu P \sqsupseteq \mu Q$
- (14) $P \sqsupset Q \Leftrightarrow \mu P \sqsupset \mu Q$
- (15) $P \simeq Q \Leftrightarrow \mu P = \mu Q$

Proof. Well-foundedness ensures that minimal proofs exist (12). Suppose $P \sqsupseteq Q$. Trivially, $\mu P \sqsupseteq P$; by (12), $Q \sqsupseteq \mu Q$; so $\mu P \sqsupseteq \mu Q$. For the other direction of (13): $P \sqsupseteq \mu P \sqsupseteq \mu Q \sqsupseteq Q$. (14) is similar. For (15), Suppose $p \in \mu P \simeq \mu Q$. There must be $q \in \mu Q$ and $p' \in \mu P$ such that $p \geq q \geq p'$. Since p is minimal, $p = p' = q \in \mu Q$. By symmetry, $\mu P = \mu Q$. \square

Proposition 3.5 *The relation \sqsupseteq is a partial ordering of minimal proofs.*

Proof. By (15). \square

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

Definition 3.6 Presentation B is said to be *simpler* than an equivalent presentation A when B provides better proofs than does A :

$$A \succsim B \quad :\equiv \quad A^* = B^* \wedge \Pi A \sqsupseteq \Pi B$$

Presentations are *similar* if their proofs are:

$$A \approx B \quad :\equiv \quad \Pi A \simeq \Pi B$$

These relations are also compatible.

Proposition 3.7 *For all presentations A, B :*

- (16) $\Pi A \sqsupseteq \Pi(A \cup B)$
- (17) $\mu \Pi A = \mu \Pi B \Leftrightarrow A \approx B$
- (18) $A \subseteq B \wedge A^* = B^* \Rightarrow A \succsim B$
- (19) $A \subseteq B \wedge \Pi B \sqsupseteq \Pi A \Rightarrow A \approx B$

Proof. (16) is a consequence of the monotonicity of Π ; (17) is a direct consequence of (15); and (18) is a consequence of (16) and the definitions. If $A \subseteq B$ and $\Pi A \sqsupseteq \Pi B$, as on the left of (19), then $\Pi A \simeq \Pi B$, again by (16). Hence, their theories are the same, and, by definition, $A \approx B$. \square

Proposition 3.8 *The relation \succsim is a quasi-ordering and \approx is its associated equivalence relation.*

The function $_^\sharp$ is “canonical” with respect to equivalence of presentations. That is: $A^{\sharp*} = A^*$; $A^* = B^* \Leftrightarrow A^\sharp = B^\sharp$; and $A^{\sharp\sharp} = A^\sharp$. This justifies the terminology of Definition 3.2.

We conclude this section by showing that the canonical presentation is indeed the simplest:

Lemma 3.9 $A \succsim A^\sharp$.

Proof. By (3) and (16), we have $A \succsim A^*$. It can be shown [5, Lemma 2] that $\mu\Pi A^\sharp = \mu\Pi A^*$, so $\Pi A^* \supseteq \mu\Pi A^* = \mu\Pi A^\sharp \supseteq \Pi A^\sharp$. In other words, $A^* \succsim A^\sharp$. \square

4 Saturated Systems

By a ‘‘normal-form proof’’, we will mean a proof in $\mu\Pi A^*$, the minimal proofs allowing any theorem as a lemma. Recall (7) that all subproofs of normal-form proofs are also in normal form. We propose the following definitions:

Definition 4.1 [Saturation] A presentation A is *saturated* if it supports all possible normal form proofs: $\Pi A \supseteq \mu\Pi A^*$. A presentation A is *complete* if every theorem has a normal form proof: $A^* = \Delta(\Pi A \cap \mu\Pi A^*)$.

In fact, a presentation is saturated iff $\mu\Pi A = \mu\Pi A^*$.

A presentation is complete if it is saturated, but for the converse, we need a further hypothesis: *minimal proofs are unique* if for all theorems $c \in \Pi A$ there is exactly one minimal proof in $\mu\Pi A^*$ with conclusion c .

Proposition 4.2 *If minimal proofs are unique, then a presentation is saturated iff it is complete.*

For example, suppose all rewrite (valley) proofs are minimal but incomparable. Then any Church-Rosser system is complete, since every identity has a rewrite proof, but only the full deductive closure is saturated.

Theorem 4.3 ([5]) *A presentation A is saturated iff it contains its own canonical presentation: $A \supseteq A^\sharp$. In particular, A^\sharp is saturated. Moreover, the canonical presentation A^\sharp is the smallest saturated set: No equivalent proper subset of A^\sharp is saturated; if A is saturated, then every equivalent superset also is.*

Corollary 4.4 *Presentation A is saturated iff $A^* \approx A$.*

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

Lemma 4.5 *Similar presentations are either both saturated or neither is; similar presentations are either both complete or neither is.*

Proof. The first claim follows directly from the previous result. For the second, one can verify that $A \approx B$ implies:

$$\begin{aligned} B^* &= A^* = \Delta(\Pi A \cap \mu\Pi A^*) = \Delta(\mu\Pi A \cap \mu\Pi A^*) \\ &= \Delta(\mu\Pi B \cap \mu\Pi B^*) = \Delta(\Pi B \cap \mu\Pi B^*) \end{aligned}$$

\square

Formulae that can be removed from a presentation—without making proofs worse—are “redundant”:

Definition 4.6 [Redundancy] A set R of formulae is (*globally*) *redundant* with respect to a presentation A when: $A \cup R \simeq A \setminus R$. The set of all (*locally*) *redundant* formulae of a given presentation A will be denoted ρA :

$$\rho A := \{r \in A : A \simeq A \setminus \{r\}\}$$

A presentation A is *irredundant* if $\rho A = \emptyset$.

Proposition 4.7 ([5]) *The following facts hold for all presentations A :*

- (20) $\rho A^\# = \emptyset$
- (21) $A \approx A \setminus \rho A$
- (22) $A^\# = A^* \setminus \rho A^*$
- (23) $A^\# = \Delta(\mu \Pi A^* \cap \widehat{A^*})$
- (24) $\widehat{A^\#} = \mu \Pi A^* \cap \widehat{A^*}$

It is thanks to well-foundedness of $>$ that the set of all *locally* redundant formulae in ρA is *globally* redundant (Eq. 21). Thus, it can be shown that A is reduced iff it is irredundant. The alternate definition of the canonical set (23) is made possible by the properties of subproofs. For details, see [5].

Theorem 4.8 *A presentation is canonical iff it is saturated and reduced.*

Proof. One direction follows immediately from Theorem 4.3 and (20). For the other direction, let A be saturated and reduced. We aim to show that $A = A^\#$. By Lemma 3.9, $A \simeq A^\#$ and the two presentations are equivalent. If A is saturated, then by Theorem 4.3, $A \supseteq A^\#$. By (18), for any $r \in A \setminus A^\#$, $A \simeq A^\# \simeq A \setminus \{r\}$. But $\rho A = \emptyset$, since A is reduced, so it cannot be that $r \in A$. In other words, $A \setminus A^\# = \emptyset$, and A is canonical. \square

Returning to our simple example, we can add three inference rules for disequalities:

$$\frac{i = j \quad j \neq k}{i \neq k} \mathbf{T} \quad \frac{i \neq i}{j = k} \mathbf{F}_{j=k} \quad \frac{\boxed{i \neq j}}{i \neq j} \mathbf{I}_{i \neq j}$$

With them, one can infer, for example, $0 \neq 0$ from $1 \neq 1$. If F is smaller than other proof combinators, and I nodes are incomparable, then the canonical basis of any inconsistent set is $\{i \neq j : i, j \in \mathbf{N}\}$. All positive equations are redundant.

5 Variations

Consider the above inference rules for ground equality and disequality: S, T, F, I, Z , with S extended to apply to all function symbols of any arity. Suppose we are using something like the recursive path ordering for proof terms.

Refutation.

If the inference rule F is the cheapest in the proof ordering, $T < I$, and $I(i, j)$ nodes are measured by the values of i and j , then the canonical basis of any inconsistent presentation is a (smallest) trivial disequation $\{t \neq t\}$.

Deduction.

If the proof ordering prefers direct application I of axioms over all other inferences (including Z), then trivial proofs are best. In that case, $\rho A^* = \emptyset$ and the canonical basis includes the whole theory $A^\# = A^*$.

Paramodulation.

If the proof ordering makes functional reflexivity S smaller than I , but the only ordering on leaves is $I(u, t) \leq I(c[u], c[t])$ for any context c , then the canonical basis will be the congruence closure, as generated by paramodulation: $\rho A = \{f(u_1, \dots, u_n) = f(t_1, \dots, t_n) : u_1 = t_1, \dots, u_n = t_n \in A^*\}$. The theory A^* is the closure under functional reflexivity of the basis $A^\#$. If A is as in our first example, then $A^\# = \{2j = 0 : j > 0\}$.

Completion.

On the other hand, if the ordering on leaves compares terms in some simplification ordering \gg , then the canonical basis will be the fully reduced set, as generated by (ground) completion: $\rho A = \{u = u\} \cup \{u = t : t = v \in A^*, t \gg v, v \text{ is not } u\}$. For our first example, $A^\# = \{2 = 0\}$. For another example, if $A = \{a = c, sa = b\}$ and $sa \gg sb \gg sc \gg a \gg b \gg c$, then $I(sa, b) > T(S(I(a, c)), I(sc, b))$, and hence $A^\# = \{a = c, sc = b\}$.

Superposition.

If one distinguishes between T steps based on the weight of the shared term j , making $T > I$ when j is the smallest, and $T < I$ otherwise, then the canonical basis is also closed under paramodulation into the larger side of equations.

6 Derivations

Theorem proving with simplification (cf. [3, Chap. 2]) entails two processes: **Expansion**, whereby any sound deductions (anything in E^*) may be added to the set of derived theorems; and **Contraction**, whereby any redundancies (anything in ρE) may be removed.

A sequence of presentations $E_0 \rightsquigarrow E_1 \rightsquigarrow \dots$ is called a *derivation*. Let $E_* = \cup_i E_i$. The *result* of the derivation is, as usual [1], its *persisting* formulæ:

$$E_\infty := \liminf_{j \rightarrow \infty} E_j$$

We will say that a proof p *persists* when $\Gamma p \subseteq E_\infty$. Thus, if a proof persists, so do its subproofs (by 6). By (16), we have $\Pi E_i \sqsupseteq \Pi E_*$.

Definition 6.1 A derivation $E_0 \rightsquigarrow E_1 \rightsquigarrow \dots$ is *good* if $E_i \succsim E_{i+1}$ for all i .

We are only interested in good derivations. From here on in, only good derivations will be considered. It is easy to see that:

Lemma 6.2 *Derivations, the steps of which are expansions and contractions, are good.*

Proposition 6.3 *If a derivation is good, then the limit supports the best proofs: $E_* \approx E_\infty$.*

Proof. One direction, namely $\Pi E_\infty \sqsupseteq \Pi E_*$, follows by (16) from the fact that $E_\infty \subseteq E_*$. To establish that $\Pi E_* \sqsupseteq \Pi E_\infty$, we show that $\mu \Pi E_* \sqsupseteq \Pi E_\infty$ and rely on (12). Suppose $p \in \mu \Pi E_*$. It follows from (5,10) that $\widehat{\Gamma} p \subseteq \Sigma p \subseteq \mu \Pi E_* \subseteq \mu \Pi E_*$. By goodness, each $a \in \Gamma p$ persists from some E_i on. Hence, $\Gamma p \subseteq E_\infty$, and $p \in \Pi E_\infty$. \square

Definition 6.4 A good derivation is *fair* if $C(E_\infty) \sqsupseteq \Pi E_*$ where $C(E)$ is the set of *critical proof obligations*:

$$(25) \quad C(E) \quad := \quad \{p \in \Pi E : p \notin \mu \Pi E^*, \forall q \triangleleft p. q \in \mu \Pi E^*\}$$

It is *clean* if $\rho E_* \cap E_\infty = \emptyset$.

Critical obligations are proofs that are not in normal form but all of whose proper subproofs are already in normal form. Fairness means that all persistent obligations are eventually ‘‘subsumed’’ by a strictly smaller proof.

Lemma 6.5 *If a derivation is clean, then its limit is reduced.*

Proof. Suppose, on the contrary, that some $r \in \rho E_\infty \subseteq E_\infty \subseteq E_*$. Consider \widehat{r} , and compare it to a smaller proof $p \in \Pi E_\infty$. Let $A = \Gamma p \subseteq E_\infty \subseteq E_*$. Let $q \in \mu \Pi E_*$. Were $r \in \Gamma q$, then replacing \widehat{r} as a subproof of q with p , would by (7) result in a smaller proof than q . It follows that $r \in \rho E_*$, which contradicts cleanliness. \square

Lemma 6.6 *If a derivation is fair, then its limit is complete.*

Proof. Any presentation A is complete if $\Pi A \sqsupseteq \Pi A \cap \mu \Pi A^*$. since $a \in A^*$ implies $a \in \Delta (\Pi A \cap \mu \Pi A^*)$, whence completeness. Let $A = E_*$ be all formulæ proved at any stage in the derivation. We show that A is complete in the above manner. Completeness of E_∞ follows from Lemma 4.5. Consider any proof in $p \in \Pi A$ of a . Let $p_\infty \in \Pi E_\infty \subseteq \Pi A$ be the persisting proof of a , for which $p_\infty \leq p$ by the previous proposition. If $p_\infty \in \mu \Pi A^*$, we’re done. Otherwise, p_∞ has a minimal (with respect to \trianglelefteq) non-normal-form (possibly trivial) subproof q , all subproofs of which (persist and) are in normal form. By fairness, there is a proof $r \in \Pi A$ of the same theorem as q such that $p_\infty \triangleright q > r$. By (7), there is therefore a better proof $p' < p_\infty \leq p$. By induction, there is a $p'' \leq p'$ in both ΠA and $\mu \Pi A^*$, also proving a . \square

For example, suppose a proof ordering makes $\widehat{c} > \frac{\widehat{a}}{c}$ and $\frac{\widehat{c}}{a} > \widehat{a}$. Start with $E_0 = \{c\}$, and consider \widehat{c} . Were \widehat{c} to persist, then by fairness a better proof would

evolve, the better proof being $\frac{\hat{a}}{c}$. If \hat{a} is in normal form, then $a \in E_\infty$ and both minimal proofs persist. Another example: $\mu\mathbb{P} = \{\hat{a}, \hat{c}, \frac{\hat{a}}{c}\}$ and $E = \{a\}$, then $E \rightsquigarrow E \rightsquigarrow \dots$ is fair, since $E_\infty = E$ and $C(E_\infty) = \emptyset$. The result is complete but unsaturated (c is missing).

Together, these lemmata and Proposition 4.2 yield:

Theorem 6.7 *If minimal proofs are unique and a derivation is fair and clean, then its limit is canonical.*

By (23), this also means that each $e \in E_\infty$ is its own ultimate proof \hat{e} , so is not susceptible to contraction.

Returning to our main example, if projection P is the most expensive type of inference, then no minimal proof includes it. And if proofs are compared in a simplification ordering (subproofs are always smaller than their superproofs), then minimal proofs will never have superfluous transitivity inferences of the form

$$\frac{u = t \quad t = t}{u = t} \mathbf{T}$$

Let \gg be a total simplification-ordering of terms, let $P > I > T > S > Z$ in the precedence, let proofs be greater than terms, and compare proof trees in the corresponding total recursive path simplification-ordering. *Ground completion* is an inference mechanism consisting of the following inference rules:

$$\mathbf{Deduce:} \quad E \cup \{w = t[u]\} \rightsquigarrow E \cup \{w = t[v]\} \quad \text{if } u = v \in E \text{ and } u \gg v$$

$$\mathbf{Delete:} \quad E \cup \{t = t\} \rightsquigarrow E$$

Furthermore, operationally, completion implements these inferences “fairly”: No persistently enabled inference rule is ignored forever.

Corollary 6.8 (Completeness of Completion) *Ground completion results—at the limit—in the canonical, Church-Rosser basis: $E_\infty = E_0^\#$.*

Proof. Ground completion is good, since **Deduce** and **Delete** don’t increase proofs ($\rightsquigarrow \subseteq \rightsquigarrow$). In particular, $I(w, t[u]) > T(I(w, t[v]), S^n(I(u, v)))$ if $u \gg v$, since $t[u] \gg t[v]$ and $t[u] \gg u \gg v$. Ground completion is fair and clean. For example, the critical obligation

$$\frac{w = t \quad t = v}{w = v} \mathbf{T}$$

when $t \gg w, v$, is resolved by **Deduce**. Also, since $T > S$, non-critical cases resolve naturally:

$$\frac{\frac{w = t}{fw = ft} \quad \frac{t = v}{ft = fv}}{fw = fv} > \frac{w = t \quad t = v}{w = v} \quad \frac{w = t \quad t = v}{fw = fv}$$

7 Discussion

We have suggested here 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”) proof. Then an inference system is complete if it has the ability to generate all formulæ needed for such ideal proofs. Given a formula ordering, one can, of course, choose to compare proofs by simply comparing the multiset of their assumptions.

The notion of “saturation” in theorem proving, in which superfluous deductions are not necessary for completeness, was suggested by Rusinowitch [7, 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. This concept was refined by Bachmair and Ganzinger (see, most recently, [2]) and by Nieuwenhuis and Rubio [6, pp. 29–42]. They define saturation in terms of a more general kind of redundancy: An inference is redundant if its conclusion can be inferred from smaller formulæ; a presentation is saturated if every inference is redundant.

We propose alternate definitions of saturation and redundancy, defining both in terms of the proof ordering. This appears to be more flexible, since it allows small proofs to use large assumptions. The definition of redundancy in [6] coincides with ours when proofs are measured first by their maximal assumption. The one given in [3, Def. 2.4.4]—a sentence is redundant if adding it to the set of assumptions does not decrease any minimal proof—is equivalent.

In [1], a completion sequence is deemed fair if all persistent critical inferences are generated. In [6, fn. 8], an inference sequence is held to be fair if all persistent inferences are either generated or become redundant. The definition of fairness propounded here combines the two ideas. But fairness only earns completeness, not saturation. (A stronger version of fairness is needed for saturation when the proof ordering is partial.) Our definition of critical obligations also allows one to incorporate “critical pair criteria”.

References

- [1] Leo Bachmair and Nachum Dershowitz. Equational inference, canonical proofs, and proof orderings. *J. of the Association for Computing Machinery*, 41(2):236–276, 1994.
- [2] Leo Bachmair and Harald Ganzinger. Resolution theorem proving. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 2, pages 19–99. Elsevier Science, 2001.

- [3] Maria Paola Bonacina. *Distributed automated deduction*. PhD thesis, Department of Computer Science, State University of New York at Stony Brook, December 1992.
- [4] Nachum Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17(3):279–301, March 1982.
- [5] Nachum Dershowitz and Claude Kirchner. Abstract saturation-based inference. In *Proceedings of the 18th Annual Symposium on Logic in Computer Science*, Ottawa, June 2003. IEEE Computer Society Press.
- [6] Robert Nieuwenhuis and Albert Rubio. Paramodulation-based theorem proving. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, chapter 7, pages 371–443. Elsevier Science, 2001.
- [7] Michaël Rusinowitch. *Démonstration Automatique: Techniques de Réécriture*. Science Informatique. InterEditions, Paris, 1989.