Two notes on propositional primal logic

Yuri Gurevich

May 2011

Abstract

Propositional primal logic, as defined by Gurevich and Neeman, has two kinds of quotations: p `said` φ, and p `implied` φ.

Note 1. The derivation problem for propositional primal logic with one kind of quotations is solvable linear time.

Note 2. In the Hilbertian calculus for propositional primal logic, the shortest derivation of a formula φ from hypotheses H may be exponential in the length of (H, φ).

1 Introduction

These notes are prompted by the decision to retire the `implied` construct[1].

In §2, we recall some definitions and facts on propositional primal logic. In §3 we show that the derivation problem for propositional primal logic with one kind of quotations is decidable in linear time.

§4 is devoted to the propositional primal logic in the original form, with two kinds of quotations. We show that there is a sequence of instances (Γ_n, φ_n) of the derivation problem for the logic in question such that the quotation depth of (Γ_n, φ_n) is n, the length of (Γ_n, φ_n) is $O(n^2)$, and Γ_n yields φ_n but every derivation of φ_n from Γ_n contains all 2^n quotation prefixes of depth n. The result is largely due to Yury Savateev who constructed

[1]More precisely we retired the `said` construct and then renamed `implied` to `said`. This clarification is irrelevant as far as the resulting logic is concerned but it is relevant in the context of Distributed Knowledge Authorization Language (DKAL) [1] that uses primal logic. Also, the clarification helps to see that various claims of [3] remain valid for the resulting logic; see more about that in §4.

a sequence of pairs (Γ_n, φ_n) satisfying the requirements above except that "every derivation" is replaced with "every local derivation" [4]. It turns out that Savateev's example supports the stronger claim. (Yury was an intern at Microsoft Research in Redmond in the summer of 2009. His result resolved a problem that was posed to him.)

§4 refers only to §2 and, in that sense, is self-contained. §3 is not self-contained; the reader needs a copy of [3].

2 Preliminaries

We recall some definitions and facts on the original propositional primal logic of [3].

Formulas We presume an infinite vocabulary of infon variables and another infinite vocabulary of (the names of) principals. Formulas are built from infon variables by the following means:

- Conjunction. If x, y are formulas then so is $x \wedge y$.
- Implication. If x, y are formulas then so is $x \to y$.
- Two unary connectives p `said` and p `implied` for every principal p. If x is a formula then so are p `said` x and p `implied` x.

Quotation prefixes Let `told`, with or without a subscript, range over {`implied`, `said`}. A string π of the form

$$q_1 \texttt{told}_1 \; q_2 \texttt{told}_2 \; \ldots \; q_d \texttt{told}_d$$

is a *quotation prefix*; the *depth* d of π may be zero. Let `pref`, with or without a subscript, range over quotation prefixes.

We say that $\texttt{pref}_1$ is dominated by $\texttt{pref}_2$ and write $\texttt{pref}_1 \leq \texttt{pref}_2$ if $\texttt{pref}_1$ is the result of replacing some (possibly none) occurrences of `said` in $\texttt{pref}_2$ with `implied`.

A Hilbertian calculus $\mathcal{H}$ for propositional primal logic

Axioms $\quad \texttt{pref}\ \top$

Inference rules

(Deflation) $\dfrac{\mathtt{pref}_2\, x}{\mathtt{pref}_1\, x}$ where $\mathtt{pref}_1 \leq \mathtt{pref}_2$

($\wedge$ elimination) $\dfrac{\mathtt{pref}\,(x \wedge y)}{\mathtt{pref}\, x}$ $\qquad$ $\dfrac{\mathtt{pref}\,(x \wedge y)}{\mathtt{pref}\, y}$

($\wedge$ introduction) $\dfrac{\mathtt{pref}\, x \qquad \mathtt{pref}\, y}{\mathtt{pref}\,(x \wedge y)}$

($\rightarrow$ elimination) $\dfrac{\mathtt{pref}\, x \qquad \mathtt{pref}\,(x \rightarrow y)}{\mathtt{pref}\, y}$

($\rightarrow$ introduction) $\dfrac{\mathtt{pref}\, y}{\mathtt{pref}\,(x \rightarrow y)}$

Definition 2.1. A *derivation* of a formula φ from hypotheses Γ is a sequence $x_1, x_2, \ldots, x_n$ of distinct formulas, the *members* of the derivation, together with auxiliary information. The number n is the *length* of the derivation. It is required that $x_n = \varphi$ and that, for every x_k, there is a reason for x_k to be at its place in the derivation:

1. x_k is an axiom, or
2. x_k is a hypothesis, or
3. x_k is obtained by an inference rule R to one or two preceding members.

The auxiliary information specifies, for each x_k, a particular reason for x_k to be at its place in the derivation. In case 3, the rule R is specified. If R is a one-premise rule, then a particular premise x_i with $i < k$ is specified. If R is a two-premise rule, then particular premises x_i, x_j with $i, j < k$ are specified.

Definition 2.2 (Components)**.** The *components* of a formula z are defined by induction:

- z is a component of z, and
- if $\mathtt{pref}\,(x \wedge y)$ is a component of z or if $\mathtt{pref}\,(x \rightarrow y)$ is a component of z, then $\mathtt{pref}\, x$ and $\mathtt{pref}\, y$ are components of z.

Definition 2.3 (Local formulas)**.** A formula x is local to a formula z if it is dominated by a component of z. Formula x is local to a set Γ of formulas if it is local to a formula in Γ. A derivation $x_1, \ldots, x_n$ of φ from Γ in calculus $\mathcal{H}$ is local if every formula x_i is local to set $\Gamma \cup \{\varphi\}$.

3 Note 1: Primal logic with one kind of quotations

We presume that the reader has a copy of article [3]. Remove the `implied` construct from the calculus $\mathcal{H}$. Let $\mathcal{H}'$ be the resulting calculus. In $\mathcal{H}'$, every quotation prefix has the form

$$q_1 \texttt{ said } q_2 \texttt{ said } \ldots \ q_d \texttt{ said}$$

and the derivation rule (Deflation) is omitted. In $\mathcal{H}'$, the formulas local to a formula z are simply the components of z. Theorem 5.11 of [3] remains valid for $\mathcal{H}'$: if Γ yields φ then there is a local derivation of φ from Γ.

Remark. It is useful to take footnote 1 into account: we really retired the dominating construct `said` and just renamed the remaining dominated construct `implied`. Then we can view $\mathcal{H}'$ as a fragment of $\mathcal{H}$ obtained by narrowing the set of formulas but leaving the axioms and derivation rules intact; of course the deflation rule becomes useless. For example, consider our claim that, in $\mathcal{H}'$, the formulas local to a formula z are simply the components of z. By the definition, formulas local to z are dominated by the components of z, but now domination is equality. Similarly, consider Theorem 5.11. Suppose $\Gamma \vdash \varphi$ in $\mathcal{H}'$. Then $\Gamma \vdash \varphi$ in $\mathcal{H}$. By Theorem 5.11, in $\mathcal{H}$, there is a local derivation D of φ from Γ. It is easy to see that D is also a local derivation in $\mathcal{H}'$. □

Definition 3.1. The *multiple derivability problem* $\mathrm{MD}(L)$ for a logic L is to compute, given formulas $x_1, \ldots, x_m$ (the hypotheses) and $y_1, \ldots, y_n$ (the queries), which of the queries are derivable from the hypotheses.

Theorem 1. *There is a linear time algorithm for the multiple derivability problem* $\mathrm{MD}(\mathcal{H}')$ *for* $\mathcal{H}'$*.*

Proof. The proof of Theorem 1 is an adaptation of the proof of Theorem 7.2 in [3] which asserts that, for every natural number d, there is a linear time

algorithm for the multiple derivability problem for H restricted to formulas primal quotation depth $\leq d$. (The definition of primal quotation depth is not important for our purposes here.)

In [3], MD($\mathcal{H}$) reduces in linear time to the multiple derivability problem for calculus $\mathcal{R}$ obtained from $\mathcal{H}$ by removing the infon constant $\top$ and the axioms. The same procedure reduces MD($\mathcal{H}'$) to the multiple derivability problem for calculus $\mathcal{R}'$ obtained from $\mathcal{H}$ by removing the infon constant $\top$ and the axioms. It remains to prove the claim that there is a linear time algorithm for MD(R').

The proof of the claim is an adaptation of the proof of Lemma 7.7 of [3] called Main Lemma there. There is a complication in the proof of Lemma 7.7 that we do not have. While the parse tree for a given instance I of MD(R) has nodes that naturally represent every component of any formula in I, the parse tree may not have nodes representing all local formulas; hence the grafting of additional nodes. It is here that the bounded primal depth of the formulas in I plays a role. It assures that the number of grafted nodes is linear in the length of I. The rest of the proof works as is. □

4 Note 2: Savateev's example

Let p $\texttt{said}^i$ be the quotation prefix obtained by repeating p $\texttt{said}$ exactly i times. Prefix p $\texttt{implied}^i$ is defined similarly.

Lemma 1 (Savateev)**.** *Let v be a propositional variable. For every natural number n, let φ_n be the formula p $\texttt{said}^n v$, and let Γ_n consist of the formula p $\texttt{implied}^n v$ and the formulas ψ_i:*

$$p\ \texttt{said}^{n-i-1}(p\ \texttt{implied}\ p\ \texttt{said}^i v \rightarrow\ p\ \texttt{said}\ p\ \texttt{implied}^i v)$$

where i ranges from 0 to $n-1$. Then Γ_n yields φ_n but every local derivation of φ_n from Γ_n contains all 2^n formulas of the form

$$p\ \texttt{told}_1\ p\ \texttt{told}_2\ \ldots\ p\ \texttt{told}_n v.$$

Proof. Fix an arbitrary n. We prove the lemma for that particular n. Let $\Gamma = \Gamma_n$ and $\varphi = \varphi_n$.

Every binary string of length n is a binary representation (possibly padded with zeros on the left) of some natural number in $[0, 2^n - 1]$. For each $m \in [0, 2^n - 1]$, let $I(m)$ be the largest i such that m has i ones on the right.

For every $m \in [0, 2^n - 1]$, let α_m be the formula

$$p\ \mathtt{told}_1\ p\ \mathtt{told}_2\ \ldots p\ \mathtt{told}_n v$$

obtained from the binary representation of m by replacing zeros with $p\ \mathtt{implied}$ and replacing ones with $p\ \mathtt{said}$. In particular $\alpha_0 = p\ \mathtt{implied}^n v$ and $\alpha_{2^n-1} = p\ \mathtt{said}^n v$. It follows that α_m has the form $\mathtt{pref}\, p\ \mathtt{said}^{I(m)} v$.

For every i, let β_i be the implication subformula of ψ_i, so that $\psi_i = p\ \mathtt{said}^{n-i-1}\, \beta_i$. Note that φ is a component of ψ_0, and thus φ is local to Γ. It follows that all formulas α_m are local to Γ. Also, all formulas of the form $p\ \mathtt{told}^{n-i-1}\, \beta_i$ are local to Γ. In fact, there are no other formulas local to Γ. In the rest of the proof, we say that a formula is local if it is local to Γ.

All local formulas follow from Γ. Indeed, every implication-carrying local formula follows from Γ by means of the prefix deflation. By induction on m, we prove that every α_m follows from Γ. The case $m = 0$ is trivial: $\alpha_0 \in \Gamma$. Suppose that $\Gamma \vdash \alpha_m$ and $m + 1 < 2^n$, and let $i = I(m)$ so that $\alpha_m = \mathtt{pref}\, p\ \mathtt{said}^i v$. By implication elimination, α_{m+1} follows from α_m and $\mathtt{pref}\, \beta_i$.

Let Γ^* be the closure of Γ under prefix deflation. In the rest of the proof of the lemma, derivations are by default derivations from Γ^*. It suffices to prove that every local derivation D of φ contains all formulas α_m.

Since no local formula contains conjunction, D does not introduce or eliminate conjunction. Without loss of generality, D does not introduce implications. Indeed, every implication-carrying local formula belongs to Γ^*, so the use of implication introduction is unnecessary.

Let m range over $[0, 2^n - 1]$. By backward induction on m we prove that each α_m occurs in D and is not preceded by any α_k with $k > m$. The case $m = 2^n - 1$ is trivial as $\alpha_m = \varphi$ in this case, and D is a derivation of φ.

Suppose that D contains formula α_{m+1} and let $i = I(m)$ and let D' be the least initial segment of D that contains α_{m+1}. In D', the formula α_{m+1} is not preceded by any α_k with $k > m + 1$ and thus cannot be obtained by prefix deflation, so it is obtained implication elimination. The only local formula that can serve as the major premise is the formula

$$\psi_i = p\ \mathtt{said}^{n-i-1}(p\ \mathtt{implied}\ p\ \mathtt{said}^i v \rightarrow\ p\ \mathtt{said}\ p\ \mathtt{implied}^i v),$$

so that the minor premise is α_m. So α_m precedes α_{m+1} and, by the induction hypothesis, it precedes any α_k with $k > m + 1$. □

Theorem 2. *There is a sequence of pairs* (Γ_n, φ_n) *such that*

1. *each* Γ_n *is a set of propositional primal formulas and each* φ_n *is a propositional primal formula,*
2. *the quotation depth of* (Γ_n, φ_n) *is* n*, and the length of* (Γ_n, φ_n) *is* $O(n^2)$*,*
3. Γ_n *yields* φ_n *but every derivation of* φ_n *from* Γ_n *contains all* 2^n *quotation prefixes of depth* n*.*

Proof. Let pairs (Γ_n, φ_n) be as in Lemma 1. The requirements 1 and 2 of the theorem are satisfied. It remains to check that the requirement 3 is satisfied as well. We fix an arbitrary n and check the requirement 3 for that particular n. Let $\Gamma = \Gamma_n$ and $\varphi = \varphi_n$. Call a formula local if it is local to Γ.@@

Lemma 2. *Let* D *be a shortest derivation of* φ *from* Γ*. The derivation* D *is local.*

Proof of the lemma. Call a derivation E *admissible* if

- it is a derivation of φ from Γ,
- all members of E are members of D,
- if a member of E is an axiom then its justification in E is that it is an axiom, and
- if a member of E is a hypothesis but not an axiom then its justification in E is that it is a hypothesis.

Define the *weight* $W(x)$ of a formula x to be the number of the occurrences of propositional connectives in x.

Claim 1. *Let* E *be an admissible derivation with at least one non-local member. Then there is an admissible derivation that is shorter than* E*.*

Proof of the claim. Let α be the earliest non-local member of the maximal weight. First suppose that α is an axiom. Then $W(\alpha) = 0$ and all members of positive weight are local. Suppose that a member β uses α as a premise in its justification R. The rule R cannot be deflation because, in such a case, β is an axiom and is justified as such. R cannot be conjunction elimination because our axioms have no conjunctions. If R is implication elimination then α is the minor premise of R because our axioms have no implications.

The corresponding major premise of R is of positive weight and thus local. But then α is local which contradicts the choice of α. If R is an introduction rule then β is of positive weight and thus local. But then α is local which contradicts the choice of α. Thus no rule β uses α in its justification. Remove α from E and get the desired shorter admissible derivation.

Since α is non-local, it cannot be a hypothesis. Hence α is obtained by some rule S from a preceding member or preceding members of E. Since α is the earliest among the heaviest non-local members of E, S is not deflation. S cannot be an elimination rule either: one of its premises would be a non-local formula heavier than α. Thus S is an introduction rule.

We consider only the case where S is implication introduction; the case where S is conjunction introduction is similar. Thus S has the form $\dfrac{\mathtt{pref}_1\, y}{\mathtt{pref}_1\,(x \to y)}$, and $\alpha = \mathtt{pref}_1\,(x \to y)$. Let α_2 be the latest member of E dominated by α, so that $\alpha_2 = \mathtt{pref}_2\,(x \to y)$ for some $\mathtt{pref}_2 \leq \mathtt{pref}_1$. Suppose that β is any member using α_2 is a premise in its justification R'. Since α_2 is a heaviest non-local item, R' cannot be an introduction rule. Since α_2 is the latest member dominated by α, R' cannot be deflation. Thus R' is an elimination rule. Taking into account the form of α_2, the rule R' is implication elimination. Taking into account that α_2 is a heaviest member, it is the major premise of R'. Thus R' has the form

$$\frac{\mathtt{pref}_2\, x \qquad \mathtt{pref}_2\,(x \to y)}{\mathtt{pref}_2\, y}.$$

Thus β is dominated by the premise α_0 of S. Modify the justification for β to be deflation with premise α_0, so that β does not use α_2 anymore. Do that for all members that use α_2 as a premise. In the modified derivation, α_2 is not used by any subsequent member and thus can be removed. This completes the proof of the claim. □

Lemma 2 follows from the claim. □

Theorem 2 follows from Lemmas 1 and 2. □

References

[1] Andreas Blass, Yuri Gurevich, Michal Moskal and Itay Neeman, "Evidential authorization", in *The Future of Software Engineering*, Sebastian Nanz (ed.), Springer, 2011, pages 77–99.

[2] Lev Beklemishev and Yuri Gurevich, "Propositional primal logic with disjunction", Microsoft Research Technical Report MSR-TR-2011-35, March 2011.

[3] Yuri Gurevich and Itay Neeman, "Infon logic: the propositional case", *ACM Transactions on Computation Logic*, Volume 12, Issue 2, Article No. 9, January 2011.

[4] Yuri Savateev, "Investigation of primal logic", unpublished manuscript, 2009.