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 $\varphi$, and $p$ implied $\varphi$.

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 $\varphi$ from hypotheses $H$ may be exponential in the length of $(H, \varphi)$.

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 $(\Gamma_n, \varphi_n)$ of the derivation problem for the logic in question such that the quotation depth of $(\Gamma_n, \varphi_n)$ is $n$, the length of $(\Gamma_n, \varphi_n)$ is $O(n^2)$, and $\Gamma_n$ yields $\varphi_n$ but every derivation of $\varphi_n$ from $\Gamma_n$ 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) \(^2\) 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 \((\Gamma_n, \varphi_n)\) 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 \(x \land y\).
- Implication. If \(x, y\) are formulas then so is \(x \rightarrow y\).
- Two unary connectives \(p \text{ said}\) and \(p \text{ implied}\) for every principal \(p\). If \(x\) is a formula then so are \(p \text{ said } x\) and \(p \text{ implied } x\).

### Quotation prefixes

Let \(\text{told}\), with or without a subscript, range over \{\text{implied, said}\}. A string \(\pi\) of the form

\[ q_1 \text{ told}_1 q_2 \text{ told}_2 \ldots q_d \text{ told}_d \]

is a quotation prefix; the depth \(d\) of \(\pi\) may be zero. Let \(\text{pref}\), with or without a subscript, range over quotation prefixes.

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

### A Hilbertian calculus \(\mathcal{H}\) for propositional primal logic

**Axioms**

\[ \text{pref } \top \]
Inference rules

(Deflation) \[
\frac{\text{pref}_2 x}{\text{pref}_1 x} \quad \text{where} \quad \text{pref}_1 \leq \text{pref}_2
\]

(∧ elimination) \[
\frac{\text{pref} (x \land y) \quad \text{pref} (x \land y)}{\text{pref} x}
\]

(∧ introduction) \[
\frac{\text{pref} x \quad \text{pref} y}{\text{pref} (x \land y)}
\]

(→ elimination) \[
\frac{\text{pref} x \quad \text{pref} (x \rightarrow y)}{\text{pref} y}
\]

(→ introduction) \[
\frac{\text{pref} y}{\text{pref} (x \rightarrow y)}
\]

Definition 2.1. A derivation of a formula \( \varphi \) from hypotheses \( \Gamma \) is a sequence \( x_1, x_2, \ldots, x_n \) of distinct formulas, the members of the derivation, together with auxiliary information. 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 \( \text{pref} (x \land y) \) is a component of \( z \) or if \( \text{pref} (x \rightarrow y) \) is a component of \( z \), then \( \text{pref} x \) and \( \text{pref} y \) 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 \( \Gamma \) of formulas if it is local to a formula in \( \Gamma \). A derivation \( x_1, \ldots, x_n \) of \( \varphi \) from \( \Gamma \) 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

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

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 $\Gamma$ yields $\varphi$ then there is a local derivation of $\varphi$ from $\Gamma$.

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 $\varphi$ from $\Gamma$. It is easy to see that $D$ is also a local derivation in $\mathcal{H}'$.

Definition 3.1. The multiple derivability problem $\text{MD}(L)$ 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 $\text{MD}(\mathcal{H}')$ 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 $\mathcal{H}$ restricted to formulas primal quotation depth $\leq d$. (The definition of primal quotation depth is not important for our purposes here.)

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

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($\mathcal{R}$) 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.

\[ \square \]

4 Note 2: Savateev’s example

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

**Lemma 2 (Savateev).** Let $v$ be a propositional variable. For every natural number $n$, let $\varphi_n$ be the formula $p \text{ said}^n v$, and let $\Gamma_n$ consist of the formula $p \text{ implied}^n v$ and the formulas $\psi_i$: $p \text{ said}^{n-i-1}(p \text{ implied} p \text{ said}^i v \rightarrow p \text{ said} p \text{ implied}^i v)$ where $i$ ranges from $0$ to $n-1$. Then $\Gamma_n$ yields $\varphi_n$ but every local derivation of $\varphi_n$ from $\Gamma_n$ contains all $2^n$ formulas of the form $p \text{ told}_1 p \text{ told}_2 \ldots p \text{ told}_n v$.

**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 $\alpha_m$ be the formula $p \text{ told}_1 p \text{ told}_2 \ldots p \text{ told}_n v$ obtained from the binary representation of $m$ by replacing zeros with $p \text{ implied}$ and replacing ones with $p \text{ said}$. In particular $\alpha_0 = p \text{ implied}^n v$ and $\alpha_{2^n-1} = p \text{ said}^n v$. It follows that $\alpha_m$ has the form $\text{pref} p \text{ said}^{I(m)} v$. 

\[ 5 \]
For every $i$, let $\beta_i$ be the implication subformula of $\psi_i$, so that $\psi_i = p \text{ said}^{n-i-1} \beta_i$. Note that $\varphi$ is a component of $\psi_0$, and thus $\varphi$ is local to $\Gamma$. It follows that all formulas $\alpha_m$ are local to $\Gamma$. Also, all formulas of the form $p \text{ told}^{n-i-1} \beta_i$ are local to $\Gamma$. In fact, there are no other formulas local to $\Gamma$. In the rest of the proof, we say that a formula is local if it is local to $\Gamma$.

All local formulas follow from $\Gamma$. Indeed, every implication-carrying local formula follows from $\Gamma$ by means of the prefix deflation. By induction on $m$, we prove that every $\alpha_m$ follows from $\Gamma$. 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 $\alpha_m = \text{pref } p \text{ said}^i v$. By implication elimination, $\alpha_{m+1}$ follows from $\alpha_m$ and $\text{pref } \beta_i$.

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

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 $\Gamma^*$, 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 $\alpha_m$ occurs in $D$ and is not preceded by any $\alpha_k$ with $k > m$. The case $m = 2^n - 1$ is trivial as $\alpha_m = \varphi$ in this case, and $D$ is a derivation of $\varphi$.

Suppose that $D$ contains formula $\alpha_{m+1}$ and let $i = I(m)$ and let $D'$ be the least initial segment of $D$ that contains $\alpha_{m+1}$. In $D'$, the formula $\alpha_{m+1}$ is not preceded by any $\alpha_k$ 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

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

so that the minor premise is $\alpha_m$. So $\alpha_m$ precedes $\alpha_{m+1}$ and, by the induction hypothesis, it precedes any $\alpha_k$ with $k > m + 1$.

**Theorem 3.** There is a sequence of pairs $(\Gamma_n, \varphi_n)$ such that

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


Proof. Let pairs \((\Gamma_n, \varphi_n)\) be as in Lemma 2. 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 \(\varphi = \varphi_n\).

Lemma 4. For every derivation \(D\) of \(\varphi\) from \(\Gamma\), there is a local derivation whose members are also members of \(D\).

To prove Lemma 4, we adapt the proof of Lemma 5.10 in [3]. Call a formula local if it is local to \(\Gamma\). We prove Lemma 4 by induction on the length of \(D\), that is, the number of members of \(D\). If all members of \(D\) are local, \(D\) is the desired local proof. Suppose that some members of \(D\) are non-local. Define the weight \(W(x)\) of a formula \(x\) to be the number of the occurrences of propositional connectives in \(x\). Let \(W^*\) be the weight of the heaviest non-local member of \(D\). Pick the earliest non-local member \(\alpha\) of weight \(W^*\).

Without loss of generality, we assume that if a member \(x\) of \(D\) is an axiom then the justification for \(x\) is that it is an axiom (rather than it is a hypothesis or that it is derived from preceding members). It follows that \(\alpha\) cannot be an axiom. Indeed suppose by contradiction that \(\alpha\) is an axiom so that \(W^* = W(\alpha) = 0\), and thus all members of positive weight are local. If no member uses \(\alpha\) as a premise item then remove \(\alpha\) from \(D\), and we are done. Otherwise let \(\beta\) be any member of \(D\) that uses \(\alpha\) as a premise of a rule \(R\). Note that \(R\) cannot be deflation because, in such a case, \(\beta\) is an axiom and thus does not need any derivation rule to justify its position. So \(R\) is either an elimination or an introduction rule. Since our axioms do not contain conjunction, \(R\) cannot be conjunction elimination. If \(R\) is implication elimination then \(\alpha\) is the minor premise because our axioms do not contain implications. The corresponding major premise of \(\beta\) is of positive weight and thus local. But then \(\alpha\) is local which is impossible. If \(R\) is an introduction rule then \(\beta\) is of positive weight and thus local. But then \(\alpha\) is local which is impossible.

Since \(\alpha\) is non-local, it cannot be a hypothesis. Hence \(\alpha\) is obtained by a rule \(R\) from a preceding member or preceding members of \(D\). Since \(\alpha\) is the earliest among the heaviest non-local members of \(D\), \(R\) is not deflation rule. \(R\) cannot be an elimination rule; otherwise one of its premises would be a non-local formula heavier than \(\alpha\). Thus \(R\) is an introduction rule.

We consider only the case where \(R\) is implication introduction; the case where \(R\) is conjunction introduction is similar. Thus \(R\) has the form
\[ \text{pref}_1(y) \]

\[ \text{pref}_1(x \rightarrow y) \]

, and \( \alpha = \text{pref}_1(x \rightarrow y) \). Let \( \alpha_2 \) be the latest member of \( D \) dominated by \( \alpha \), so that \( \alpha_2 = \text{pref}_2(x \rightarrow y) \) for some \( \text{pref}_2 \leq \text{pref}_1 \).

If \( \alpha_2 \) is not used by any subsequent member of \( D \) then \( \alpha_2 \) can be removed, and we are done. Otherwise let \( \beta \) be any later member that uses \( \alpha_2 \) is a premise of some rule \( R' \). Since \( \alpha_2 \) is a heaviest non-local item, \( R' \) cannot be an introduction rule. Since \( \alpha_2 \) is the latest member dominated by \( \alpha \), \( R' \) cannot be deflation. Thus \( R' \) is an elimination rule. Taking into account the form of \( \alpha_2 \), the rule \( R' \) is implication elimination. Taking into account that \( \alpha_2 \) is a heaviest member, it is the major premise of \( R' \). Thus \( R' \) has the form

\[ \text{pref}_2(x \quad \text{pref}_2(x \rightarrow y) \quad \text{pref}_2 y) \]

Thus \( \beta \) is dominated by the premise \( \alpha_0 \) of \( R \). Modify the justification for \( \beta \) to be the result of deflation of \( \alpha_0 \), so that \( \beta \) does not use \( \alpha_2 \) anymore. Do that for all members that use \( \alpha_2 \) as a premise. In the modified derivation, \( \alpha_2 \) is not used by any subsequent member and thus can be removed. This completes the proof of Lemma 4.

Theorem 3 follows from Lemmas 2 and 4.

References


