Towards an Efficient and Economic Deductive System of Matching Logic

FSL group

January 14, 2017

We aim for a Hilbert style deductive system which has a relatively large number of axioms but only a few inference rules.

1 Grammar and extended grammar

The formal language $\mathcal{L}$ we use to write matching logic patterns is defined as follows.

$$
\begin{aligned}
P ::= {} & x \\
& \mid P_1 \to P_2 \\
& \mid \neg P \\
& \mid \forall x.P \\
& \mid \sigma(P_1, \ldots, P_n) \\
(*** \ & \texttt{extended} ***) \\
& \mid P_1 \vee P_2 \\
& \mid P_1 \wedge P_2 \\
& \mid P_1 \leftrightarrow P_2 \\
& \mid \exists x.P \\
& \mid \lceil P \rceil \\
& \mid \lfloor P \rfloor \\
& \mid P_1 = P_2 \\
& \mid P_1 \neq P_2 \\
& \mid \top \\
& \mid \bot \\
& \mid P_1 \subseteq P_2 \\
& \mid x \in P
\end{aligned}
$$

with the extended grammar defined as

$$
\begin{aligned}
&P_1 \vee P_2 \coloneqq \neg P_2 \to P_1\\
&P_1 \wedge P_2 \coloneqq \neg(\neg P_1 \vee \neg P_2)\\
&P_1 \leftrightarrow P_2 \coloneqq (P_1 \to P_2) \wedge (P_2 \to P_1)\\
&\exists x.P \coloneqq \neg\forall x.\neg P\\
&\lfloor P \rfloor \coloneqq \neg\lceil \neg P \rceil\\
&P_1 = P_2 \coloneqq \lfloor P_1 \leftrightarrow P_2 \rfloor\\
&P_1 \neq P_2 \coloneqq \neg(P_1 = P_2)\\
&\bot \coloneqq x_1 \wedge \neg x_1\\
&\top \coloneqq \neg\bot\\
&P_1 \subseteq P_2 \coloneqq \lfloor P_1 \to P_2 \rfloor\\
&x \in P \coloneqq \lceil x \wedge P \rceil
\end{aligned}
$$

We will extend the grammar to a many-sorted one in the future.

2 Hilbert proof system

Axioms in $\mathcal{L}$ are given by the following nine axiom schemata where P, Q, R are arbitrary patterns and x, y are variables.

- (K1) $P \to (Q \to P)$
- (K2) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
- (K3) $(\neg P \to \neg Q) \to (Q \to P)$
- (K4) $\forall x.(P \to Q) \to (P \to \forall x.Q)$ if x does not occur free in P
- (K5) $\exists y.x = y$
- (K6) $\exists y.Q = y \to (\forall x.P(x) \to P[Q/x])$ if Q is free for x in P
- (K7) $P_1 = P_2 \to (Q[P_1/x] \to Q[P_2/x])$
- (M1) $x \in y = (x = y)$
- (M2) $x \in \neg P = \neg(x \in P)$
- (M3) $x \in P \wedge Q = (x \in P) \wedge (x \in Q)$
- (M4) $x \in \exists y.P = \exists y.x \in P$ where x is distinct from y
- (M5) $x \in \sigma(\ldots, P_i, \ldots) = \exists y.y \in P_i \wedge x \in \sigma(\ldots, y, \ldots)$

Inference rules include

- (Modus Ponens) From P and $P \to Q$, deduce Q.

- (Universal Generalization) From P, deduce $\forall x.P$.
- (Membership Introduction) From P, deduce $\forall x.x \in P$, where x occurs free in P.
- (Membership Elimination) From $\forall x.x \in P$, deduce P, where x occurs free in P.

Theorem 1 (Soundness of $K_{\mathcal{L}}$). *Theorems of $K_{\mathcal{L}}$ are valid.*

Proof. Trivial. □

We provide some metatheorems of $K_{\mathcal{L}}$.

Proposition 2 (Tautology). *For any propositional tautology $\mathcal{A}(p_1, \dots, p_n)$ where $p_1, \dots, p_n$ are propositional variables,*

$$\vdash \mathcal{A}(P_1, \dots, P_n).$$

Proof. Omit proof here. □

Remark Proposition 2 makes any metatheorem of propositional logic a metatheorem of $K_{\mathcal{L}}$.

Proposition 3 (Variable Substitution). $\vdash \forall x.P \to P[y/x]$.

Proposition 4 (Functional Substitution). $\vdash \exists y.(Q = y) \to (P[Q/x] \to \exists x.P(x))$.

Proposition 5 ($\vee$-Introduction). $\vdash P$ *implies* $\vdash P \vee Q$.

Proof. Use Proposition 2 and Modus Ponens. Note that in general, $\vdash P \vee Q$ does not imply $\vdash P$ or $\vdash Q$. □

Proposition 6 ($\wedge$-Introduction and Elimination). $\vdash P$ *and* $\vdash Q$ *iff* $\vdash P \wedge Q$.

Proof. Use Proposition 2 and Modus Ponens. □

Proposition 7 (Equality Introduction). $\vdash P = P$.

Proof. Use Membership Introduction and Proposition 2. □

Proposition 8 (Equality Replacement). $\vdash P_1 = P_2$ *and* $\vdash Q[P_1/x]$ *implies* $\vdash Q[P_2/x]$.

Proof. Use Axiom (K7) and Modus Ponens. □

Proposition 9 (Equality Establishment). $\vdash P \leftrightarrow Q$ *implies* $\vdash P = Q$.

Proof. Use Membership Axoims and $\vee$-Introduction. □

Corollary 10. $\vdash P$ *implies* $\vdash P = \top$.

Proposition 11. $\vdash x \in \lceil y \rceil$.

Proof.

$$\begin{aligned} & \vdash x \in \lceil y \rceil \\ \text{if } & \vdash \forall x.(x \in \lceil y \rceil) && (K5,\ K6, \text{ and Modus Ponens}) \\ \text{iff } & \vdash \lceil y \rceil. \end{aligned}$$

□

Proposition 12. $\vdash P \to \lceil P \rceil$.

Proof.

$$\begin{aligned} & \vdash P \to \lceil P \rceil \\ \text{iff } & \vdash \forall x.(x \in P \to \lceil P \rceil) \\ \text{if } & \vdash x \in P \to \lceil P \rceil \\ \text{iff } & \vdash x \in P \to x \in \lceil P \rceil \\ \text{iff } & \vdash x \in P \to \exists y.(y \in P \wedge x \in \lceil y \rceil) \\ \text{iff } & \vdash x \in P \to \neg\forall y.(y \notin P \vee x \notin \lceil y \rceil) \\ \text{iff } & \vdash \forall y.(y \notin P \vee x \notin \lceil y \rceil) \to x \notin P \\ \text{if } & \vdash x \notin P \vee x \notin \lceil x \rceil \to x \notin P \\ \text{iff } & \vdash x \in P \to x \in P \wedge x \in \lceil x \rceil \\ \text{iff } & \vdash x \in P \to x \in \lceil x \rceil \\ \text{if } & \vdash x \in \lceil x \rceil \end{aligned}$$

Remark Similarly we can show $\vdash \lfloor P \rfloor \to P$. □

Proposition 13. $\vdash \forall x.(x \in P) = \lfloor P \rfloor$, *where x occurs free in P.*

Proof. By Proposition 9 and 6, it suffices to show

$$\vdash \forall x.(x \in P) \to \lfloor P \rfloor \tag{1}$$

and

$$\vdash \lfloor P \rfloor \to \forall x.(x \in P). \tag{2}$$

To show (1),

$$
\begin{aligned}
&\vdash \forall x.(x \in P) \to \lfloor P \rfloor \\
\text{iff } &\vdash \forall x.\lceil x \wedge P \rceil \to \neg\lceil \neg P \rceil \\
\text{iff } &\vdash \lceil \neg P \rceil \to \exists x.\neg\lceil x \wedge P \rceil \\
\text{iff } &\vdash \forall y.(y \in (\lceil \neg P \rceil \to \exists x.\neg\lceil x \wedge P \rceil)) \\
\text{if } &\vdash y \in (\lceil \neg P \rceil \to \exists x.\neg\lceil x \wedge P \rceil \\
\text{iff } &\vdash \exists z_1.(z_1 \notin P \wedge y \in \lceil z_1 \rceil) \to \\
&\qquad \exists x.\neg(\exists z_2.(z_2 = x \wedge z_2 \in P \wedge y \in \lceil z_2 \rceil)) \\
\text{iff } &\vdash \exists z_1.(z_1 \notin P \wedge \top) \to \qquad\qquad \text{(Proposition 11, 8, and Corollary 10)} \\
&\qquad \exists x.\neg(\exists z_2.(z_2 = x \wedge z_2 \in P \wedge \top)) \\
\text{iff } &\vdash \exists z_1.(z_1 \notin P) \to \exists x.\neg(\exists z_2.(z_2 = x \wedge z_2 \in P)) \\
\text{iff } &\vdash \forall x.(\exists z_2.(z_2 = x \wedge z_2 \in P)) \to \forall z_1.(z_1 \in P) \\
\text{if } &\vdash \forall z_1.(\forall x.(\exists z_2.(z_2 = x \wedge z_2 \in P)) \to (z_1 \in P)) \\
\text{if } &\vdash \forall x.(\exists z_2.(z_2 = x \wedge z_2 \in P)) \to (z_1 \in P).
\end{aligned}
$$

Since $\vdash \forall x.(\exists z_2.(z_2 = x \wedge z_2 \in P)) \to \exists z_2.(z_2 = z_1 \wedge z_2 \in P)$, it suffices to show

$$
\begin{aligned}
&\vdash \exists z_2.(z_2 = z_1 \wedge z_2 \in P) \to (z_1 \in P) \\
\text{iff } &\vdash z_1 \notin P \to \forall z_2.(z_2 \neq z_1 \vee z_2 \notin P) \\
\text{if } &\vdash \forall z_2.(z_1 \notin P \to z_2 \neq z_1 \vee z_2 \notin P) \\
\text{if } &\vdash z_1 \notin P \to z_2 \neq z_1 \vee z_2 \notin P \\
\text{if } &\vdash z_2 = z_1 \wedge z_2 \in P \to z_1 \in P.
\end{aligned}
$$

And we proved (1).

Similarly, to show (2),

$$
\begin{aligned}
&\vdash \lfloor P \rfloor \to \forall x.(x \in P) \\
\text{iff } &\vdash \exists x.\neg\lceil x \wedge P \rceil \to \lceil \neg P \rceil \\
\text{iff } &\vdash \forall y.(y \in \exists x.\neg\lceil x \wedge P \rceil \to \lceil \neg P \rceil) \\
\text{if } &\vdash y \in \exists x.\neg\lceil x \wedge P \rceil \to \lceil \neg P \rceil \\
\text{iff } &\vdash \exists x.\neg\exists z_2.(z_2 = x \wedge z_2 \in P) \to \exists z_1.(z_1 \notin P) \\
\text{iff } &\vdash \forall z_1.(z_1 \in P) \to \exists z_2.(z_2 = x \wedge z_2 \in P) \\
\text{iff } &\vdash x \in P \to \exists z_2.(z_2 = x \wedge z_2 \in P).
\end{aligned}
$$

We proved (2).

Remark If x occurs free in P, the result does not hold. For example, let P be $upto(x)$ where $upto(\cdot)$ is interpreted to $upto(n) = \{0, 1, \ldots, n\}$ on $\mathbb{N}$. □

Remark From Membership Introduction and Elimination inference rules and Proposition 13, $\vdash P$ iff $\vdash \lfloor P \rfloor$.

Proposition 14 (Classification Reasoning)**.** *For any P and Q, from $\vdash P \to Q$ and $\vdash \neg P \to Q$ deduce $\vdash Q$.*

Proof. From $\vdash \neg P \to Q$ deduce $\vdash \neg Q \to P$. Notice that $\vdash P \to Q$, so we have $\vdash \neg Q \to Q$, i.e., $\vdash \neg\neg Q \vee Q$ which concludes the proof. □

Corollary 15. *For any P_1, P_2, and Q are patterns with $\vdash P_1 \vee P_2$, from $\vdash P_1 \to Q$ and $\vdash P_2 \to Q$, deduce $\vdash Q$.*

Definition 16 (Predicate Pattern)**.** *A pattern P is called a predicate pattern or a predicate if $\vdash (P = \top) \vee (P = \bot)$.*

Remark Predicate patterns are closed under all logic connectives.

Remark For any P, $\lceil P \rceil$ is a predicate pattern.

Proposition 17. *For any predicate P, $\vdash (P \neq \top) = (P = \bot)$ and $\vdash (P \neq \bot) = (P = \top)$.*

Proposition 18. *For any pattern Q and any predicate pattern P, $\vdash P \vee Q$ iff $\vdash P \vee \lfloor Q \rfloor$.*

Proof. ($\Rightarrow$) is obtained immediately by the remark of Proposition 12. We now prove ($\Leftarrow$).

Because $\vdash Q = \top \vee Q \neq \top$, it suffices to show

$$\vdash Q = \top \to (P \vee \lfloor Q \rfloor = \top) \tag{3}$$

and

$$\vdash Q \neq \top \to (P \vee \lfloor Q \rfloor = \top) \tag{4}$$

by Corollary 15, and the fact that $\vdash P \vee \lfloor Q \rfloor = \top$ and $\vdash \top$ imply $\vdash P \vee \lfloor Q \rfloor$.

The proof of (3) is straightforward as follows.

$$\begin{array}{ll} & \vdash Q = \top \to (P \vee \lfloor Q \rfloor = \top) \\ \text{if} & \vdash Q = \top \to (P \vee \lfloor \top \rfloor = \top) \\ \text{if} & \vdash Q = \top \to (\top = \top) \\ \text{if} & \vdash \top. \end{array}$$

The proof of (4) needs more effort. We first show that $\vdash (Q \neq \top) = (\lfloor Q \rfloor = \bot)$. Since $\lfloor Q \rfloor$ is a predicate pattern, it suffices to show $\vdash (Q = \top) = (\lfloor Q \rfloor = \top)$.

It is trivial to show $\vdash (Q = \top) \to (\lfloor Q \rfloor = \top)$. We show the other direction $\vdash (\lfloor Q \rfloor = \top) \to (Q = \top)$ through the following backward reasoning.

have the backward reasoning as follows.

$$\begin{array}{ll} & \vdash Q \neq \top \to (P \vee \lfloor Q \rfloor = \top) \\ \text{if} & \vdash \end{array}$$

□

Proposition 19 (Deduction Theorem)**.** *If* $\Gamma \cup \{P\} \vdash Q$ *and the derivation does not use* $\forall x$*-Generalization where* x *is free in* P*, then* $\Gamma \vdash \lfloor P \rfloor \to Q$*.*

Proof. The proof is by induction on n, the length of the derivation of Q from $\Gamma \cup \{P\}$.

Base step: $n = 1$, and Q is an axiom, or P, or a member of Γ. If Q is an axiom or a member of Γ, then $\Gamma \vdash Q$ and as a result, $\Gamma \vdash \lfloor P \rfloor \to Q$. If Q is P, then $\Gamma \vdash \lfloor P \rfloor \to Q$ by Proposition 12.

Induction step: Let $n > 1$. Suppose that if P' can be deduced from $\Gamma \cup \{P\}$ without using $\forall x$-Generalization where x is free in P, in a derivation containing fewer than n steps, then $\Gamma \vdash \lfloor P \rfloor \to P'$.

Case 1: Q is an axiom, or P, or a member of Γ. Precisely as in the Base step, we show that $\vdash \lfloor P \rfloor \to Q$.

Case 2: Q follows from two previous patterns in the derivation by an application of Modus Ponens. These two patterns must have the forms Q_1 and $Q_1 \to Q$, and each one can certainly be deduced from $\Gamma \cup \{P\}$ by a derivation with fewer than n steps, by just omitting the subsequent members from the original derivation from $\Gamma \cup \{P\} \vdash Q$. So we have $\Gamma \cup \{P\} \vdash Q_1$ and $\Gamma \cup \{P\} \vdash Q_1 \to Q$, and, applying the hypothesis of induction, $\Gamma \vdash \lfloor P \rfloor \to Q_1$ and $\Gamma \vdash \lfloor P \rfloor \to (Q_1 \to Q)$. It follows immediately that $\Gamma \vdash \lfloor P \rfloor \to Q$.

Case 3: Q follows from a previous pattern in the derivation by an application of $\forall x_i$-Generalization where x_i does not occur free in P. So Q is $\forall x_i.Q_1$, say, and Q_1 appears previously in the derivation. Thus $\Gamma \cup \{P\} \vdash Q_1$, and the derivation has fewer than n steps, so $\Gamma \vdash \lfloor P \rfloor \to Q_1$, since there is no application of Universal Generalization involving a free variable of P. Also x_i cannot occur free in P, as it is involved in an application of Universal Generalization in the deduction of Q from $\Gamma \cup \{P\}$. So we have a derivation of $\Gamma \vdash \lfloor P \rfloor \to Q$ as follows.

$$\begin{array}{ll} & \Gamma \vdash \lfloor P \rfloor \to Q \\ \text{iff} & \Gamma \vdash \lfloor P \rfloor \to \forall x_i.Q_1 \\ \text{if} & \Gamma \vdash \forall x_i.(\lfloor P \rfloor \to Q_1) \\ \text{if} & \Gamma \vdash \lfloor P \rfloor \to Q_1. \end{array}$$

So $\Gamma \vdash \lfloor P \rfloor \to Q$ as required.

Case 4: Q follows from a previous pattern in the derivation by an application of Membership Introduction. So Q is $\forall x_i.(x_i \in Q_1)$ with x_i is free in Q_1, say, and Q_1 appears previously in the derivation. Thus $\Gamma \cup \{P\} \vdash Q_1$, and the derivation has fewer than n steps, so $\Gamma \vdash \lfloor P \rfloor \to Q_1$, since there is no application of Universal Generalization involving a free variable of P. So we have a derivation of $\Gamma \vdash \lfloor P \rfloor \to Q$ as follows.

$$\begin{array}{ll} & \Gamma \vdash \lfloor P \rfloor \to Q \\ \text{iff} & \Gamma \vdash \lfloor P \rfloor \to \forall x_i.(x_i \in Q_1) \\ \text{iff} & \Gamma \vdash \lfloor P \rfloor \to \lfloor Q_1 \rfloor, \end{array}$$

which follows by the hypothesis of induction $\Gamma \vdash \lfloor P \rfloor \to Q_1$ and the fact that $\Gamma \vdash Q_1 \to \lfloor Q_1 \rfloor$ (by the Remark in Proposition 12).

Case 5: Q follows from a previous pattern in the derivation by an application of Membership Elimination. The previous pattern must have the form $\forall x_i.(x_i \in Q)$, and can be deduced from $\Gamma \cup \{P\}$ by a derivation with fewer than n steps, by just omitting the subsequent members from the original derivation from $\Gamma \cup \{P\} \vdash Q$. So we have $\Gamma \cup \{P\} \vdash \forall x_i.(x_i \in Q)$, and, applying the hypothesis of induction, $\Gamma \vdash \lfloor P \rfloor \to \forall x_i.(x_i \in Q)$. So we have a derivation of $\Gamma \vdash \lfloor P \rfloor \to Q$ as follows.

$$
\begin{array}{lll}
 & \Gamma \vdash \lfloor P \rfloor \to Q & \\
\text{iff} & \Gamma \vdash \neg\lfloor P \rfloor \vee Q & \\
\text{iff} & \Gamma \vdash \neg\lfloor P \rfloor \vee \lfloor Q \rfloor & \text{(Proposition 18)} \\
\text{iff} & \Gamma \vdash \neg\lfloor P \rfloor \vee \forall x_i.(x_i \in Q) & \\
\text{iff} & \Gamma \vdash \lfloor P \rfloor \to \forall x_i.(x_i \in Q), &
\end{array}
$$

which is the hypothesis of induction. And this concludes our inductive proof. □

Corollary 20 (Closed-form Deduction Theorem)**.** *If P is closed,* $\Gamma \cup \{P\} \vdash Q$ *implies* $\Gamma \vdash \lfloor P \rfloor \to Q$.

3 Inference rules

Axioms

$$\frac{\cdot}{\Gamma \vdash A}$$

where A is an axiom.

Inclusion

$$\frac{\cdot}{\Gamma \vdash P}$$

where $P \in \Gamma$.

Modus Ponens

$$\frac{\Gamma \vdash Q \to P \quad \Gamma \vdash Q}{\Gamma \vdash P}$$

Closed-Form Deduction Theorem

$$\frac{\Gamma \cup \{P\} \vdash Q}{\Gamma \vdash P \to Q}$$

where P is closed.

Universal Generalization

$$\frac{\Gamma \vdash P}{\Gamma \vdash \forall x.P}\ (\forall x)$$

Conjunction Splitting

$$\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q}$$