

Towards an Efficient and Economic Deductive System of Matching Logic

FSL group

January 11, 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.

$$\begin{aligned} P ::= & x \\ & | P_1 \rightarrow P_2 \\ & | \neg P \\ & | \forall x.P \\ & | \sigma(P_1, \dots, P_n) \\ (** \text{ extended } **) \\ & | P_1 \vee P_2 \\ & | P_1 \wedge P_2 \\ & | P_1 \leftrightarrow P_2 \\ & | \exists x.P \\ & | [P] \\ & | \lfloor P \rfloor \\ & | P_1 = P_2 \\ & | P_1 \neq P_2 \\ & | \top \\ & | \perp \\ & | P_1 \subseteq P_2 \\ & | x \in P \end{aligned}$$

with the extended grammar defined as

$$\begin{aligned}
P_1 \vee P_2 &:= \neg P_2 \rightarrow P_1 \\
P_1 \wedge P_2 &:= \neg(\neg P_1 \vee \neg P_2) \\
P_1 \leftrightarrow P_2 &:= (P_1 \rightarrow P_2) \wedge (P_2 \rightarrow P_1) \\
\exists x.P &:= \neg \forall x. \neg P \\
[P] &:= \neg[\neg P] \\
P_1 = P_2 &:= [P_1 \leftrightarrow P_2] \\
P_1 \neq P_2 &:= \neg(P_1 = P_2) \\
\perp &:= x_1 \wedge \neg x_1 \\
\top &:= \neg \perp \\
P_1 \subseteq P_2 &:= [P_1 \rightarrow P_2] \\
x \in P &:= [x \wedge P]
\end{aligned}$$

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) $P \rightarrow (Q \rightarrow P)$
- (K2) $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$
- (K3) $(\neg P \rightarrow \neg Q) \rightarrow (Q \rightarrow P)$
- (K4) $\forall x.(P \rightarrow Q) \rightarrow (P \rightarrow \forall x.Q)$ if x does not occur free in P
- (K5) $\exists y.x = y$
- (K6) $\exists y.Q = y \rightarrow (\forall x.P(x) \rightarrow P[Q/x])$ if Q is free for x in P
- (K7) $P_1 = P_2 \rightarrow (Q[P_1/x] \rightarrow Q[P_2/x])$
- (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) $x \in \sigma(\dots, P_i, \dots) = \exists y.y \in P_i \wedge x \in \sigma(\dots, y, \dots)$

Inference rules include

- (Modus Ponens) From P and $P \rightarrow Q$, 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). $\vdash \forall x.P \rightarrow P[y/x]$.

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

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 Axioms and \vee -Introduction. □

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

Proposition 11. $\vdash x \in [y]$.

Proof.

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

□

Proposition 12. $\vdash P \rightarrow [P]$.

Proof.

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

Remark Similarly we can show $\vdash [P] \rightarrow P$.

□

Proposition 13. $\vdash \forall x.(x \in P) = [P]$, where x occurs free in P .

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

$$\vdash \forall x.(x \in P) \rightarrow [P] \tag{1}$$

and

$$\vdash [P] \rightarrow \forall x.(x \in P). \tag{2}$$

To show (1),

$$\begin{aligned}
& \vdash \forall x.(x \in P) \rightarrow [P] \\
& \text{iff } \vdash \forall x.[x \wedge P] \rightarrow \neg[\neg P] \\
& \text{iff } \vdash [\neg P] \rightarrow \exists x.\neg[x \wedge P] \\
& \text{iff } \vdash \forall y.(y \in ([\neg P] \rightarrow \exists x.\neg[x \wedge P])) \\
& \text{if } \vdash y \in ([\neg P] \rightarrow \exists x.\neg[x \wedge P]) \\
& \text{iff } \vdash \exists z_1.(z_1 \notin P \wedge y \in [z_1]) \rightarrow \\
& \quad \exists x.\neg(\exists z_2.(z_2 = x \wedge z_2 \in P \wedge y \in [z_2])) \\
& \text{iff } \vdash \exists z_1.(z_1 \notin P \wedge \top) \rightarrow \quad \quad \quad (\text{Proposition 11, 8, and Corollary 10}) \\
& \quad \exists x.\neg(\exists z_2.(z_2 = x \wedge z_2 \in P \wedge \top)) \\
& \text{iff } \vdash \exists z_1.(z_1 \notin P) \rightarrow \exists x.\neg(\exists z_2.(z_2 = x \wedge z_2 \in P)) \\
& \text{iff } \vdash \forall x.(\exists z_2.(z_2 = x \wedge z_2 \in P)) \rightarrow \forall z_1.(z_1 \in P) \\
& \text{if } \vdash \forall z_1.(\forall x.(\exists z_2.(z_2 = x \wedge z_2 \in P)) \rightarrow (z_1 \in P)) \\
& \text{if } \vdash \forall x.(\exists z_2.(z_2 = x \wedge z_2 \in P)) \rightarrow (z_1 \in P).
\end{aligned}$$

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

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

And we proved (1).

Similarly, to show (2),

$$\begin{aligned}
& \vdash [P] \rightarrow \forall x.(x \in P) \\
& \text{iff } \vdash \exists x.\neg[x \wedge P] \rightarrow [\neg P] \\
& \text{iff } \vdash \forall y.(y \in \exists x.\neg[x \wedge P] \rightarrow [\neg P]) \\
& \text{if } \vdash y \in \exists x.\neg[x \wedge P] \rightarrow [\neg P] \\
& \text{iff } \vdash \exists x.\neg\exists z_2.(z_2 = x \wedge z_2 \in P) \rightarrow \exists z_1.(z_1 \notin P) \\
& \text{iff } \vdash \forall z_1.(z_1 \in P) \rightarrow \exists z_2.(z_2 = z_1 \wedge z_2 \in P) \\
& \text{iff } \vdash x \in P \rightarrow \exists z_2.(z_2 = x \wedge z_2 \in P).
\end{aligned}$$

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 $upto(n) = \{0, 1, \dots, n\}$ on \mathbb{N} . \square

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

Definition 14 (Predicate Pattern). *A pattern P is called a predicate pattern or a predicate if $\vdash (P = \top) \vee (P = \perp)$.*

Remark Predicate patterns are closed under all logic connectives.

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

Proposition 15. *For any pattern Q and any predicate pattern P , $\vdash P \vee Q$ iff $\vdash P \vee \lceil Q \rceil$.*

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

Proposition 16 (Deduction Theorem). *If $\Gamma \cup \{P\} \vdash Q$ and the derivation does not use $\forall x$ -Generalization where x is free in P , then $\Gamma \vdash \lceil P \rceil \rightarrow Q$.*

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, $\Gamma \vdash \lceil P \rceil \rightarrow Q$. If Q is P , then $\Gamma \vdash \lceil P \rceil \rightarrow Q$ 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 $\Gamma \vdash \lceil P \rceil \rightarrow P'$.

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

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 $Q_1 \rightarrow Q$, 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 $\Gamma \cup \{P\} \vdash Q_1 \rightarrow Q$, and, applying the hypothesis of induction, $\Gamma \vdash \lceil P \rceil \rightarrow Q_1$ and $\Gamma \vdash \lceil P \rceil \rightarrow (Q_1 \rightarrow Q)$. It follows immediately that $\Gamma \vdash \lceil P \rceil \rightarrow Q$.

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 $\Gamma \vdash \lceil P \rceil \rightarrow Q_1$, 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 $\Gamma \vdash \lceil P \rceil \rightarrow Q$ as follows.

$$\begin{aligned} & \Gamma \vdash \lceil P \rceil \rightarrow Q \\ \text{iff } & \Gamma \vdash \lceil P \rceil \rightarrow \forall x_i. Q_1 \\ \text{if } & \Gamma \vdash \forall x_i. (\lceil P \rceil \rightarrow Q_1) \\ \text{if } & \Gamma \vdash \lceil P \rceil \rightarrow Q_1. \end{aligned}$$

So $\Gamma \vdash \lceil P \rceil \rightarrow Q$ 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 $\Gamma \vdash [P] \rightarrow Q_1$, since there is no application of Universal Generalization involving a free variable of P . So we have a derivation of $\Gamma \vdash [P] \rightarrow Q$ as follows.

$$\begin{aligned} & \Gamma \vdash [P] \rightarrow Q \\ \text{iff } & \Gamma \vdash [P] \rightarrow \forall x_i.(x_i \in Q_1) \\ \text{iff } & \Gamma \vdash [P] \rightarrow [Q_1], \end{aligned}$$

which follows by the hypothesis of induction $\Gamma \vdash [P] \rightarrow Q_1$ and the fact that $\Gamma \vdash Q_1 \rightarrow [Q_1]$ (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, $\Gamma \vdash [P] \rightarrow \forall x_i.(x_i \in Q)$. So we have a derivation of $\Gamma \vdash [P] \rightarrow Q$ as follows.

$$\begin{aligned} & \Gamma \vdash [P] \rightarrow Q \\ \text{iff } & \Gamma \vdash \neg[P] \vee Q \\ \text{iff } & \Gamma \vdash \neg[P] \vee [Q] & \text{(Proposition 15)} \\ \text{iff } & \Gamma \vdash \neg[P] \vee \forall x_i.(x_i \in Q) \\ \text{iff } & \Gamma \vdash [P] \rightarrow \forall x_i.(x_i \in Q), \end{aligned}$$

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

Corollary 17 (Closed-form Deduction Theorem). *If P is closed, $\Gamma \cup \{P\} \vdash Q$ implies $\Gamma \vdash [P] \rightarrow Q$.*

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

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

Closed-Form Deduction Theorem

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

where P is closed.

Universal Generalization

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

Conjunction Splitting

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