

Automated Deduction in Matching Logic

FSL group

January 30, 2017

Recent success in building very fast automated theorem provers (especially for first-order theories) makes us look forward to an highly efficient automated deductive system for matching logic. This project aims at that.

1 Grammar

As in most logic, formulas of matching logic, called *patterns*, are written in a formal language, denoted as \mathcal{L} , who has a very similar grammar as first order logic.

The language \mathcal{L} in general is a many-sorted language. A signature of \mathcal{L} contains not only a finite set Σ of symbols, but also a finite nonempty set S of sorts. Each symbol $\sigma \in \Sigma$ is, of course, sorted, with a fixed nonempty arity. We write $\sigma \in \Sigma_{s_1, \dots, s_n, s}$ when we want to emphasize that σ takes n arguments (with suggested sorts) and returns a pattern in sort s , but we hope in most cases sorting is clear from context.

The basic grammar for \mathcal{L} , as defined below, is almost identical to first-order logic, except that in \mathcal{L} there is no difference between relational (predicate) and functional symbols, and we accept first-order terms as patterns in matching logic.

$$\begin{aligned} P ::= & x \\ & | P_1 \rightarrow P_2 \\ & | \neg P \\ & | \forall x. P \\ & | \sigma(P_1, \dots, P_n). \end{aligned}$$

For simplicity, we did not mention sorting in the grammar definition, and assume it should be clear to all readers. For example, in $P_1 \rightarrow P_2$, both patterns P_1 and P_2 should have the same sort, and that sort is the sort of $P_1 \rightarrow P_2$. The sort of $\forall x. P$ is the sort of P , where the sort of variable x does not matter. To see why it is the case, consider the pattern $\exists x. \text{list}(x, 1 \cdot 3 \cdot 5)$, which is the set of all memory configurations that has a list (1, 3, 5) in it.

Propositional connectives are always assumed, including conjunction (\wedge), disjunction (\vee), and equivalence (\leftrightarrow). Existential quantifier ($\exists x$) is defined by universal quantifier ($\forall x$) in the normal way. Bottom (\perp_s) and top (\top_s) in sort s are given by $x \wedge \neg x$ and $\neg \perp_s$, respectively, where x is a variable in sort s . It does not matter which variable we pick.

1.1 Extension

The formal language is often extended with definedness symbols. A definedness symbol $\llbracket _ \rrbracket_{s_1}^{s_2} \in \Sigma_{s_1, s_2}$ is a *predicate* symbol, i.e., $\llbracket P \rrbracket_{s_1}^{s_2}$ is either \top or \perp for any pattern P . We often write $\llbracket P \rrbracket$ when sorting information can be derived from the context.

Definedness extends the formal language:

$$\begin{aligned}\llbracket P \rrbracket &:= \neg \llbracket \neg P \rrbracket \\ P_1 = P_2 &:= \llbracket P_1 \leftrightarrow P_2 \rrbracket \\ P_1 \neq P_2 &:= \neg(P_1 = P_2) \\ P_1 \subseteq P_2 &:= \llbracket P_1 \rightarrow P_2 \rrbracket \\ x \in P &:= x \subseteq P\end{aligned}$$

and provides convenient ways to write *predicate patterns*, patterns that is either \top or \perp . The sort of a predicate patterns is often of no importance. It is its “truth value” that is important. For example, $\llbracket P \rrbracket$ is “true” if P is not empty, and this fact can be used in any context. This leads us to polymorphic sorting in matching logic.

1.2 Polymorphism

Predicate symbols are often polymorphic sorting. As a result, many predicate connectives are of polymorphic types, too. Predicate pattern $P_1 = P_2$ only requires P_1 and P_2 have the same sort, and its result can be of any sort. If P_1 and P_2 have different sorts, $P_1 = P_2$ is *ill-sorted*.

Polymorphism means in mathematics a mapping from $\mathcal{P} \dashv \sqcup \sqcup \nabla \setminus f$

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 does not occur free in P .
- (Membership Elimination) From $\forall x.(x \in P)$, deduce P , where x does not occur 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 \forall -Introduction. □

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

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

Proof.

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

□

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

Proof.

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

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 $\vdash [P]$.

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

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

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

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

Remark Predicate patterns are closed under all logic connectives.

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

Proposition 17. $\vdash (\lceil P \rceil = \perp) = (P = \perp)$ and $\vdash (\lfloor P \rfloor = \top) = (P = \top)$.

Proof. It is easy to prove one derivation from the other, so we only prove the first one. By Proposition 9, it suffices to prove

$$\vdash (\lceil P \rceil = \perp) \rightarrow (P = \perp) \quad (3)$$

and

$$\vdash (P = \perp) \rightarrow (\lceil P \rceil = \perp) \quad (4)$$

The proof of (4) is trivial and we left it as an exercise. We now prove (3) through the following backward reasoning.

$$\begin{aligned} & \vdash (\lceil P \rceil = \perp) \rightarrow (P = \perp) \\ \text{iff} \quad & \vdash \forall y. (y \in ((\lceil P \rceil = \perp) \rightarrow (P = \perp))) \\ \text{if} \quad & \vdash y \in ((\lceil P \rceil = \perp) \rightarrow (P = \perp)) \\ \text{iff} \quad & \vdash (y \in (\lceil P \rceil = \perp) \rightarrow (y \in (P = \perp))). \end{aligned} \quad (5)$$

While for any pattern Q ,

$$\begin{aligned} & \vdash y \in (Q = \perp) \\ \text{iff} \quad & \vdash y \in \neg[\neg(Q \leftrightarrow \perp)] \\ \text{iff} \quad & \vdash y \in \neg[Q] \\ \text{iff} \quad & \vdash \neg\exists z. (z \in Q \wedge y \in \lceil z \rceil) \\ \text{iff} \quad & \vdash \neg\exists z. (z \in Q) \end{aligned}$$

So we continue to prove (5) by showing

$$\begin{aligned}
& \vdash (y \in ([P] = \perp)) \rightarrow (y \in (P = \perp)) \\
\text{iff } & \vdash \neg \exists z. (z \in [P]) \rightarrow \neg \exists z. (z \in P) \\
\text{iff } & \vdash \exists z. (z \in P) \rightarrow \exists z. (z \in [P]) \\
\text{iff } & \vdash \exists z. (z \in P) \rightarrow \exists z. (\exists z_1. (z_1 \in P \wedge z \in [z_1])) \\
\text{iff } & \vdash \exists z. (z \in P) \rightarrow \exists z. \exists z_1. (z_1 \in P) \\
\text{iff } & \vdash \exists z_1. (z_1 \in P) \rightarrow \exists z. \exists z_1. (z_1 \in P).
\end{aligned}$$

And we finish the proof by noticing the fact that for any pattern Q and variable x ,

$$\vdash Q \rightarrow \exists x. Q.$$

□

Proposition 18. *For any predicate P , $\vdash (P \neq \top) = (P = \perp)$ and $\vdash (P \neq \perp) = (P = \top)$.*

Proof. We only prove the first derivation, by showing both

$$\vdash (P \neq \top) \rightarrow (P = \perp) \tag{6}$$

and

$$\vdash (P = \perp) \rightarrow (P \neq \top). \tag{7}$$

Proving (7) is trivial. We now prove (6), which is also trivial by transforming disjunction to implication. □

Proposition 19. *For any pattern Q and any predicate pattern P , $\vdash P \vee Q$ iff $\vdash P \vee [Q]$.*

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

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

$$\vdash Q = \top \rightarrow (P \vee [Q] = \top) \tag{8}$$

and

$$\vdash Q \neq \top \rightarrow (P \vee [Q] = \top) \tag{9}$$

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

The proof of (8) is straightforward as follows.

$$\begin{aligned}
& \vdash Q = \top \rightarrow (P \vee [Q] = \top) \\
\text{if } & \vdash Q = \top \rightarrow (P \vee [\top] = \top) \\
\text{if } & \vdash Q = \top \rightarrow (\top = \top) \\
\text{if } & \vdash \top.
\end{aligned}$$

The proof of (9) needs more effort:

$$\begin{aligned}
& \vdash Q \neq \top \rightarrow (P \vee \lfloor Q \rfloor = \top) \\
\text{iff } & \vdash (Q = \top) \vee (P \vee \lfloor Q \rfloor = \top) \\
\text{iff } & \vdash (\lfloor Q \rfloor = \top) \vee (P \vee \lfloor Q \rfloor = \top) \\
\text{iff } & \vdash \lfloor Q \rfloor \neq \top \rightarrow (P \vee \lfloor Q \rfloor = \top) \\
\text{iff } & \vdash \lfloor Q \rfloor = \perp \rightarrow (P \vee \lfloor Q \rfloor = \top) \\
\text{if } & \vdash \lfloor Q \rfloor = \perp \rightarrow (P \vee \perp = \top) \\
\text{iff } & \vdash \lfloor Q \rfloor = \perp \rightarrow (P = \top) \\
\text{if } & \vdash Q = \top \vee P = \top.
\end{aligned}$$

Notice that P is a predicate pattern, so it suffices to show

$$\vdash P = \top \rightarrow (Q = \top \vee P = \top),$$

whose validity is obvious, and

$$\vdash P = \perp \rightarrow (Q = \top \vee P = \top),$$

which is proved by showing

$$\vdash P = \perp \rightarrow Q = \top. \quad (10)$$

Because $\vdash P \vee Q$, it suffices to show

$$\begin{aligned}
& \vdash P = \perp \rightarrow (P \vee Q) \rightarrow (Q = \top) \\
\text{if } & \vdash P = \perp \rightarrow (\perp \vee Q) \rightarrow (Q = \top) \\
\text{iff } & \vdash P = \perp \rightarrow Q \rightarrow (Q = \top) \\
\text{if } & \vdash Q \rightarrow (Q = \top) \\
\text{iff } & \vdash (Q \neq \top) \rightarrow \neg Q \\
\text{iff } & \vdash (\lfloor Q \rfloor = \perp) \rightarrow \neg Q.
\end{aligned}$$

Notice we have $\vdash Q \rightarrow \lfloor Q \rfloor$, which means $\vdash \neg \lfloor Q \rfloor \rightarrow \neg Q$, so it suffices to show

$$\begin{aligned}
& \vdash (\lfloor Q \rfloor = \perp) \rightarrow \neg \lfloor Q \rfloor \\
\text{iff } & \vdash (\lfloor Q \rfloor = \perp) \rightarrow \neg \perp \\
\text{iff } & \vdash (\lfloor Q \rfloor = \perp) \rightarrow \top \\
\text{iff } & \vdash \top.
\end{aligned}$$

And this concludes the proof. \square

Proposition 20 (Deduction Theorem). *If $\Gamma \cup \{P\} \vdash Q$ and the derivation does not use $\forall x$ -Generalization where x is free in P , then $\Gamma \vdash \lfloor P \rfloor \rightarrow Q$.*

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, $\Gamma \vdash [P] \rightarrow Q$. If Q is P , then $\Gamma \vdash [P] \rightarrow Q$ 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 $\Gamma \vdash [P] \rightarrow P'$.

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

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, $\Gamma \vdash [P] \rightarrow Q_1$ and $\Gamma \vdash [P] \rightarrow (Q_1 \rightarrow Q)$. It follows immediately that $\Gamma \vdash [P] \rightarrow Q$.

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 $\Gamma \vdash [P] \rightarrow Q_1$, 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 $\Gamma \vdash [P] \rightarrow Q$ as follows.

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

So $\Gamma \vdash [P] \rightarrow Q$ 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.

$$\begin{aligned}
& \Gamma \vdash [P] \rightarrow Q \\
\text{iff } & \Gamma \vdash \neg[P] \vee Q \\
\text{iff } & \Gamma \vdash \neg[P] \vee [Q] & \text{(Proposition 19)} \\
\text{iff } & \Gamma \vdash \neg[P] \vee \forall x_i.(x_i \in Q) \\
\text{iff } & \Gamma \vdash [P] \rightarrow \forall x_i.(x_i \in Q),
\end{aligned}$$

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

Corollary 21 (Closed-form Deduction Theorem). *If P is closed, $\Gamma \cup \{P\} \vdash Q$ implies $\Gamma \vdash [P] \rightarrow Q$.*

Theorem 22 (Frame Rule). *Let $\sigma \in \Sigma$ be a symbol in the signature. From $P_1 \rightarrow P_2$, deduce $\sigma(P_1) \rightarrow \sigma(P_2)$. In its most general form, $P_1 \rightarrow P_2$ deduces $\sigma(Q_1, \dots, P_1, \dots, Q_n) \rightarrow \sigma(Q_1, \dots, P_2, \dots, Q_n)$.*

Proof. we write $\sigma(Q_1, \dots, P_i, \dots, Q_n)$ as $\sigma(P_i, \vec{Q})$ for short, for any $i \in \{1, 2\}$.

$$\begin{aligned}
& \vdash \sigma(P_1, \vec{Q}) \rightarrow \sigma(P_2, \vec{Q}) \\
\text{iff } & \vdash y \in (\sigma(P_1, \vec{Q}) \rightarrow \sigma(P_2, \vec{Q})) \\
\text{iff } & \vdash (y \in \sigma(P_1, \vec{Q})) \rightarrow (y \in \sigma(P_2, \vec{Q})) \\
\text{iff } & \vdash \exists z_1. \exists \vec{z}. (z_1 \in P_1 \wedge \vec{z} \in \vec{Q} \wedge y \in \sigma(z_1, \vec{z})) \\
& \rightarrow \exists z_2. \exists \vec{z}. (z_2 \in P_2 \wedge \vec{z} \in \vec{Q} \wedge y \in \sigma(z_2, \vec{z})) \\
\text{iff } & \vdash \exists z_1. \exists \vec{z}. (z_1 \in P_1 \wedge \vec{z} \in \vec{Q} \wedge y \in \sigma(z_1, \vec{z})) \\
& \rightarrow z_1 \in P_2 \wedge \vec{z} \in \vec{Q} \wedge y \in \sigma(z_1, \vec{z})) \\
\text{iff } & \vdash \exists z_1. \exists \vec{z}. (z_1 \in P_1 \rightarrow z_1 \in P_2) \\
\text{if } & \vdash \exists z_1. (z_1 \in P_1 \rightarrow z_1 \in P_2) \\
\text{if } & \vdash P_1 \rightarrow P_2.
\end{aligned}$$

\square

Corollary 23 (Frame Rule as Implication). $\vdash [P \rightarrow Q] \rightarrow (\sigma(P) \rightarrow \sigma(Q))$

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

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