# Formalization of Interpolation theorem in Prpositional Classical Logic With Sequent Calculus using Maehara’s method in Coq

Asha Soroushpoor

July 24, 2023

## 1 Objective

Formalizing Craig’s Interpolation theorem with constructive proof by induction on the length of the proof tree

## 2 Definitions

### 2.1 Language

**Atoms** A countable set of atomes we illustrate each memeber by $a_i$ and the whole set by $\mathbb{A}$.

**Propostions** Our props contain of atoms, $\bot$, disjunction ($\vee$), conjunction ($\wedge$) and implication ($\supset$). the inductive defenition is as below.

$$\mathbb{P} := \{\mathbb{A}|\bot|\mathbb{P} \vee \mathbb{P}|\mathbb{P} \wedge \mathbb{P}|\mathbb{P} \supset \mathbb{P}\}$$

we define $\neg P := P \supset \bot$ and we define $\top := \bot \supset \bot$ in our code also we assume that the set of propostions is countable by these axioms:

```
Axiom prop_to_nat: prop -> nat.
Axiom nat_to_prop: nat -> prop.

Axiom prop_to_prop: forall p, nat_to_prop(prop_to_nat(p)) = p.
Axiom nat_to_nat: forall n, prop_to_nat(nat_to_prop(n)) = n.
```

that is there are two functions *prop_to_nat* and *nat_to_prop* mapping propositions to natural numbers and vise versa which their combination is identity function.
Decidablity of propositions are also proved.

**Formula functionality** In *Formula.V* we defined simple functions we need for proving our theorem, first is *atoms_of* which returns whether or not an atom occured in a proposition or not.

```
Fixpoint atoms_of (p : prop) (a: atom) : bool :=
match p with
| ^x_a' => if (Nat.eqb a a') then true else false
| p1 and p2 => (atoms_of p1 a) || (atoms_of p2 a)
| p1 or p2 => (atoms_of p1 a) || (atoms_of p2 a)
| p1 imply p2 => (atoms_of p1 a) || (atoms_of p2 a)
| _ => false
end.
```

next we define proposition *atom_in* that states whether or not an atom occured in a mutiset of props it states the fact:

$$atom\_in\ (a \in \mathbb{A})\ s := \exists p \in s, atoms\_of\ p\ a = true$$

```
Definition atom_in (s: multiset) (a: atom) : Prop :=
exists (p: prop), (prop_to_nat p) In s /\ atoms_of p a.
```

and last defenition we need is the fact that atoms of a propostion is included in inclusion of two othe multiset we define it as below:

$$atoms\_incl\ (p \in \mathbb{P})\ s_1\ s_2 := \forall (a \in \mathbb{A}), atoms\_of\ p\ a- > atom\_in\ a\ s_1 \wedge atom\_in\ a\ s_2$$

```
Definition atoms_incl (p: prop) (s1 s2: multiset) : Prop :=
forall (a: atom), (atoms_of p a) ->
(atom_in s1 a) /\ (atom_in s2 a).
```

## 2.2 Multiset

We use infinite multiset for our context, although our deduction rules only generates finite context (except for bot rule). This defenition allow for easier code and more functionality in proofs. We define our own simplified version of multiset only on natural numbers and build our own library over it.
Multisets are basically any function from natural numbers to natural numbers which it's output indicates the number of occurence of the input number.

```
Definition U := nat .
Definition multiset := U -> nat.
```

We also define set theoritical relations as said propositions over multisets.

```
Definition In (x : U) (A : multiset)  : Prop := 1 <= A x.
Definition Included (A B : multiset) : Prop := forall x, A x <= B x.
Definition EmptySet : multiset := fun (x : U) => 0.
Definition Singleton (x:U) : multiset :=
    fun (x' : U) => match ( x =? x') with
```

```
        | true => 1
        |false => 0
    end.
Definition Union (A B : multiset) : multiset :=
    fun (x : U) => (A x) + (B x).
Definition Intersection (A B : multiset) : multiset :=
    fun (x : U) => min (A x) (B x).
Definition SAdd (A : multiset) (x : U) : multiset :=
    fun (x' : U) => match ( x =? x') with
        | true => S (A x')
        |false => A x'
    end.
Definition Remove (A : multiset) (x : U) : multiset :=
    fun (x' : U) => match ( x =? x') with
        | true => pred (A x')
        |false => A x'
    end.
Definition Diff (A B : multiset) : multiset :=
    fun (x : U) => (A x) - (B x).
Definition Equal (A B : multiset) : Prop :=
    forall (x : U), (A x) = (B x).
```

The definitions are simple for example in *Inculuded* we say

$$A \subset B := \forall (n \in \mathbb{N}), Ax \leq Bx$$

or in *SAdd* we define adding an element $n$ to function(multiset) $f$ is a new function $f'$ which behaves exactly the same except for $n$ which it returns $fn+1$ Other defenitions are exactly the traditional multiset defenitions except for *Union* which we define it by adding up two multisets together (Sum in traditional aspect), since we only adding up contexts together and using maximum doesn't have any point for us. And at last since syntactical equality of multisets is not enough for us we add following axiom:

```
Axiom Extensionality_multiset : forall A B, Equal A B -> A = B.
```

The main upside of using multisets as context is that we can get rid of the exchange rule this way, specially since it's interpolant is not as trivial as I thought.
There are also many set theory theorems and lemmas proven in *multiset.v* file which we use often, such as community of union and intersection, union and intersection with $\emptyset$ and so on.

## 2.3 Sequent Calculus LK

a. Axiom

$$\frac{}{A \Rightarrow A}$$

b. Weakening

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, p}$$
$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, p \Rightarrow \Delta}$$

c. Contraction

$$\frac{\Gamma \Rightarrow \Delta, p, p}{\Gamma \Rightarrow \Delta, p}$$
$$\frac{\Gamma, p, p \Rightarrow \Delta}{\Gamma, p \Rightarrow \Delta}$$

d. Bot

$$\frac{}{\bot \Rightarrow A}$$

e. Conjunction

$$\frac{\Gamma \Rightarrow \Delta, a \qquad \Gamma \Rightarrow \Delta, b}{\Gamma \Rightarrow \Delta, a \wedge b}$$
$$\frac{\Gamma, a \Rightarrow \Delta}{\Gamma, a \wedge b \Rightarrow \Delta, p}$$
$$\frac{\Gamma, b \Rightarrow \Delta}{\Gamma, a \wedge b \Rightarrow \Delta}$$

f. Disjunction

$$\frac{\Gamma, a \Rightarrow \Delta \qquad \Gamma, a \Rightarrow \Delta}{\Gamma, a \vee b \Rightarrow \Delta}$$
$$\frac{\Gamma \Rightarrow \Delta, a}{\Gamma \Rightarrow \Delta, a \vee b} \qquad \frac{\Gamma \Rightarrow \Delta, b}{\Gamma \Rightarrow \Delta, a \vee b}$$

g. Implication

$$\frac{\Gamma \Rightarrow \Delta, a \qquad \Gamma, a \Rightarrow \Delta}{\Gamma, a \to b \Rightarrow \Delta}$$

$$\frac{\Gamma, a \Rightarrow \Delta, b}{\Gamma \Rightarrow \Delta, a \to b}$$

One little addition to the calculus we made in code as addition of nodes, nodes are a very simplified binary tree illustration. We stick the to each step of proof so we save the data of the proof tree construction.

```
Inductive Node : Type :=
|leaf : Node
|onen: Node -> Node
|twon: Node -> Node -> Node.
```

# 3 Interpolation Theorem

Since the code is so lengthy and complex we only state the full constructive proof by hand here, the proof formalized in code is exactly the same with lots and lots of mind grinding little details.

**Lemma 3.1.** *For all multisets* $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ *that we have*

$$\Gamma_1 \cup \Gamma_2 \Rightarrow \Delta_1 \cup \Delta_2$$

*there exists an interpolant c such that*

$$\Gamma_1 \Rightarrow \Delta_1, c \tag{1}$$

$$\Gamma_2, c \Rightarrow \Delta_2 \tag{2}$$

$$atoms\_incl\ c\ (\Gamma_1 \cup \Delta_1)\ (\Gamma_2 \cup \Delta_2) \tag{3}$$

*Proof.* We find the interpolant for each rule:

I. Axiom Rule: if our proof tree is ended with axiom rule we have different following cases, assume that our end premise is $p \Rightarrow p$ p can be in either $\Delta_1$ or $\Delta_2$ same is true for $\Gamma_1$ and $\Gamma_2$ so overall we have 4 cases.

i. if $p \in \Delta_1$, $\Delta_2 = \emptyset$, $p \in \Gamma_1$, $\Gamma_2 = \emptyset$ our interpolant is $\bot$

1. first condition is trivial

$$\cfrac{\cfrac{}{p \Rightarrow p}\ \text{Axiom}}{p \Rightarrow p, \bot}\ \text{Wr}$$

2. second condtion is just a bot rule

$$\cfrac{}{\bot \Rightarrow}\ \text{Bot}$$

3. since bot doesn't have any atom third condition is trivial.
from now on we only prove 3 conditions.

ii. if $p \in \Delta_2$, $\Delta_1 = \emptyset$, $p \in \Gamma_1$, $\Gamma_2 = \emptyset$ our interpolant is $p$

1.

$$\cfrac{}{p \Rightarrow p}\ \text{Axiom}$$

2. same as previous.
3. $p \in \{p\} \cap \{p\}$

iii. if $p \in \Delta_1$, $\Delta_2 = \emptyset$, $p \in \Gamma_2$, $\Gamma_1 = \emptyset$ our interpolant is $\neg p$

1.

$$\cfrac{\cfrac{\cfrac{}{p \Rightarrow p}\ \text{Axiom}}{p \Rightarrow p, \bot}\ \text{Wr}}{\Rightarrow p, p \supset \bot}\ \supset r$$

2.

$$\dfrac{\dfrac{}{p \Rightarrow p}\,\text{Axiom} \qquad \dfrac{\dfrac{}{\bot \Rightarrow}\,\text{Bot}}{p, \bot \Rightarrow}\,\text{Wl}}{p, p \supset \bot \Rightarrow}\,\supset l$$

3. $\neg p \in \{p\} \cap \{p\}$

iv. if $p \in \Delta_2$, $\Delta_1 = \emptyset$, $p \in \Gamma_2$, $\Gamma_1 = \emptyset$ our interpolant is $\top$

1.

$$\dfrac{\dfrac{}{\bot \Rightarrow \bot}\,\text{Bot}}{\Rightarrow \bot \supset \bot}\,\supset$$

2.

$$\dfrac{\dfrac{}{p \Rightarrow p}\,\text{Axiom}}{p \Rightarrow p, \bot}\,\text{Wr}$$

3. since $\top$ doesn't have and atom this condition is trivial.

II. Bot Rule: we have 2 cases

i. $\bot \in \Gamma_1$ and $\Gamma_2 = \emptyset$ here our interpolant is $\bot$

ii. $\bot \in \Gamma_2$ and $\Gamma_1 = \emptyset$ here our interpolant is $\top$

III. Weak left: here the additional $p$ is either in $\Delta_1$ or $\Delta_2$ in both cases our interpolant from induction hypothesis works just fine (detailed proof is written in the code).

IV. Weak Right: same as previous case

V. Contraction Right: again the contracted $p$ is either in $\Delta_1$ or $\Delta_2$ in both cases our interpolant from induction hypothesis works just fine

VI. Contraction Left: same as previous case

VII. Left Conjunction 1: similarly we have 2 cases $p \wedge q$ is either in $\Gamma_1$ or $\Gamma_2$ again if we assume the interpolant from induction hypothesis and use the rule on needed conditions (condition 1 for first case and condition 2 for second) we have our interpolant, 3rd condition is always trivial since we added more propositions and we didn't remove any.

VIII. Left Conjunction 2: same as previous case

IX. Right Disjunction 1: same as previous case

X. Right Disjunction 2: same as previous case

XI. Right Implication : this one is also similar but since it's the trickiest we go throught full detail for it. so assume our proof tree ended like this.

$$\dfrac{\Gamma_1' \cup \Gamma_2', a \Rightarrow \Delta_1' \cup \Delta_2', b}{\Gamma_1' \cup \Gamma_2', \Rightarrow \Delta_1' \cup \Delta_2', a \supset b}$$

and all Γs and Δs are arbitrary, we have to find the interpolant for any given partition of sucecedents $(\Delta_1, \Delta_2)$ and antecedents $(\Gamma_1, \Gamma_2)$. we have two cases as below:

i. $a \supset b \in \Delta_1$ so there as $\Delta'$ which $\Delta_1 = \Delta', a \supset b$ we take desired partitions in the induction hypothesis antecedents as $(\Gamma_1, a)$,$(\Gamma_2)$ and in succedents as $(\Delta', b)$, $(\Delta_2)$ and take our interpolant c from hypothesis.

   1.

$$\dfrac{\dfrac{\Gamma_1, a \Rightarrow \Delta', b, c}{\Gamma_1 \Rightarrow \Delta', a \supset b, c}\supset r}{\Gamma_1 \Rightarrow \Delta_1, c}$$

   2. in induction hypothesis we have desired sequence.

$$\Gamma_2, c \Rightarrow \Delta_2$$

   3. since in our induction hypotheses a and b are at one side of the intersection this part is obvious too.

ii. $a \supset b \in \Delta_2$ so there as $\Delta'$ which $\Delta_2 = \Delta', a \supset b$ we take desired partitions in the induction hypothesis antecedents as $(\Gamma_1)$,$(\Gamma_2, a)$ and in succedents as $(\Delta_1)$, $(\Delta', b)$ and take our interpolant c from hypothesis, the rest is similar to previous case.

XII. Right Conjunction: these ones are a little tricky, so our proof tree ended as follows.

$$\dfrac{\Gamma \Rightarrow \Delta, a \qquad \Gamma \Rightarrow \Delta, b}{\Gamma \Rightarrow \Delta, a \wedge b}\wedge r$$

for our partitions in succedents we have 2 cases:

i. $a \wedge b \in \Delta_1$ so there is so there as $\Delta'$ which $\Delta_1 = \Delta', a \wedge b$ here we have 2 induction hypothesis, for left one we take $\Gamma_1$ and $\Gamma_2$ for antecedent partitions $\Delta', a$ and $\Delta_2$ for succedent partition and name the interpolant c, for right is also similar we take $\Gamma_1$ and $\Gamma_2$ for antecedent partitions $\Delta', b$ and $\Delta_2$ for succedent partition and name the interpolant c' we argue that $c \vee c'$ is our desired interpolant.

   1.

$$\dfrac{\dfrac{\dfrac{\Gamma_1 \Rightarrow \Delta', a, c}{\Gamma_1 \Rightarrow \Delta', a, c \vee c'}\vee r1 \qquad \dfrac{\Gamma_1 \Rightarrow \Delta', a, c'}{\Gamma_1 \Rightarrow \Delta', a, c \vee c'}\vee r2}{\Gamma_1 \Rightarrow \Delta', a \wedge b, c \vee c'}\wedge r}{\Gamma_1 \Rightarrow \Delta_1, a \wedge b}$$

   2. we can use any of the induction hypotheses second conditions

$$\dfrac{\Gamma_2, c \Rightarrow \Delta_2 \qquad \Gamma_2, c' \Rightarrow \Delta_2}{\Gamma_2, c \vee c' \Rightarrow \Delta_2}\vee 2$$

   3. trivial

ii. $a \wedge b \in \Delta_2$ so there is so there as $\Delta'$ which $\Delta_2 = \Delta', a \wedge b$ here we have 2 induction hypothesis, for left one we take $\Gamma_1$ and $\Gamma_2$ for antecedent partitions $\Delta_1$ and $\Delta', a$ for succedent partition and name the interpolant c, for right is also similar we take $\Gamma_1$ and $\Gamma_2$ for antecedent partitions $\Delta_1$ and $\Delta', b$ for succedent partition and name the interpolant c' we argue that $c \wedge c'$ is our desired interpolant.

1.

$$\frac{\Gamma_1 \Rightarrow \Delta_1, c \qquad \Gamma_1 \Rightarrow \Delta_1, c'}{\Gamma_1 \Rightarrow \Delta_1, c \wedge c'} \wedge r$$

2.

$$\frac{\dfrac{\dfrac{\Gamma_2, c \Rightarrow \Delta', a}{\Gamma_2, c \wedge c' \Rightarrow \Delta', a} \wedge l1 \qquad \dfrac{\Gamma_2, c' \Rightarrow \Delta', a}{\Gamma_2, c \wedge c' \Rightarrow \Delta', a} \wedge l2}{\Gamma_2, c \wedge c' \Rightarrow \Delta', a \wedge b} \wedge r}{\Gamma_2, c \wedge c' \Rightarrow \Delta_2}$$

3. trivial

XIII. Left Disjunction: exactly same as previous one

XIV. LeftImplication : this one is also similar

i. $a \supset b \in \Gamma_1$ so there is so there as $\Gamma'$ which $\Gamma_1 = \Gamma', a \supset b$ here we have 2 induction hypothesis, for left one we take $\Gamma', b$ and $\Gamma_2$ for antecedent partitions $\Delta_1$ and $\Delta_2$ for succedent partition and name the interpolant c, for right is also similar we take $\Gamma'$ and $\Gamma_2$ for antecedent partitions $\Delta_1, a$ and $\Delta_2$ for succedent partition and name the interpolant c' we argue that $c \vee c'$ is our desired interpolant.

1.

$$\frac{\dfrac{\dfrac{\Gamma', b \Rightarrow \Delta_1, c}{\Gamma', b \Rightarrow \Delta_1, c \vee c'} \vee r \qquad \dfrac{\Gamma' \Rightarrow \Delta_1, a, c}{\Gamma' \Rightarrow \Delta_1, a, c \vee c'} \vee r}{\Gamma', a \supset b \Rightarrow \Delta_1, c \vee c'} \supset l}{\Gamma_1 \Rightarrow \Delta_1, c \vee c'}$$

2.

$$\frac{\Gamma_2, c \Rightarrow \Delta_2 \qquad \Gamma_2, c' \Rightarrow \Delta_2}{\Gamma_2, c \vee c' \Rightarrow \Delta_2} \vee l$$

3. trivial

ii. $a \supset b \in \Gamma_2$ so there is so there as $\Gamma'$ which $\Gamma_2 = \Gamma', a \supset b$ here we have 2 induction hypothesis, for left one we take $\Gamma_1$ and $\Gamma', b$ for antecedent partitions $\Delta_1$ and $\Delta_2$ for succedent partition and name the interpolant c, for right is also similar we take $\Gamma_1$ and $\Gamma'$ for antecedent partitions $\Delta_1$ and $\Delta_2, b$ for succedent partition and name the interpolant c' we argue that $c \wedge c'$ is our desired interpolant.

1. $$\dfrac{\Gamma_1 \Rightarrow \Delta_1, c \qquad \Gamma_1 \Rightarrow \Delta_1, c'}{\Gamma_1 \Rightarrow \Delta_1, c \wedge c'} \wedge r$$

2. $$\dfrac{\dfrac{\dfrac{\Gamma', b, c \Rightarrow \Delta_2}{\Gamma', b, c \wedge c' \Rightarrow \Delta_2} \wedge l \qquad \dfrac{\Gamma', c \Rightarrow \Delta_2, a}{\Gamma', c \wedge c' \Rightarrow \Delta_2, a} \wedge l}{\Gamma', c \wedge c', a \supset b \Rightarrow \Delta_2} \supset l}{\Gamma_2, c \wedge c' \Rightarrow \Delta_2}$$

3. trivial

□

**Theorem 3.2** (Craig's Interpolation Theorem)**.** *forall* $\Gamma$ *and* $\Delta$ *that we have* $\Gamma \Rightarrow \Delta$ *there exists an intepolant c which*

$$\Gamma \Rightarrow c$$

$$c \Rightarrow \Delta$$

$$atoms\_incl\ c\ (\Gamma)\ (\Delta)$$

*Proof.* we use Lemma 3.1 with $\Gamma_1 = \Gamma$, $\Delta_2 = \Delta$ and $\Gamma_2 = \emptyset$ $\Delta_1 = \emptyset$ □

# References

Barras, Bruno (Jan. 2010). "Sets in Coq, Coq in Sets". In: *Journal of Formalized Reasoning* 3.1, pp. 29–48. DOI: 10.6092/issn.1972-5787/1695. URL: https://jfr.unibo.it/article/view/1695.

Blot, Arthur, Pierre-Évariste Dagand, and Julia Lawall (2016). "From Sets to Bits in Coq". In: *Functional and Logic Programming - 13th International Symposium, FLOPS 2016, Kochi, Japan, March 4-6, 2016, Proceedings*. Ed. by Oleg Kiselyov and Andy King. Vol. 9613. Lecture Notes in Computer Science. Springer, pp. 12–28. DOI: 10.1007/978-3-319-29604-3_2. URL: https://doi.org/10.1007/978-3-319-29604-3%5C_2.

Pfeiffer, Helmut (1989). "Jean-Yves Girard. Proof theory and logical complexity. Volume I. Studies in proof theory, no. 1. Bibliopolis, Naples 1987, also distributed by Humanities Press, Atlantic Highlands, N.J., 503 pp." In: *The Journal of Symbolic Logic* 54.4, pp. 1493–1494. DOI: 10.2307/2274839.

Simpson, Carlos (2004). *Set-theoretical mathematics in Coq*. arXiv: math/0402336 [math.LO].

Takeuti, G. (1975). *Proof Theory. Number 81 in Studies in Logic and the Foundations of Mathematics*. North-Holland.