

Constructive Mathematics and an Interpolation Result

Peter Chapman

Overview

We intend to:

- give a brief introduction to the idea of constructivism
- introduce the system of Sequent Calculus
- use this formalism to provide a (sketch) proof of Craig's Interpolation Theorem

A Quick Proof

- **Lemma:** \exists irrational a, b . $a^b \in \mathbb{Q}$
- **Proof:** $\sqrt{2}$ is irrational
- What about $\sqrt{2}^{\sqrt{2}}$?
- Either it is rational, in which case we are done.
- Or it is irrational, in which case consider $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$.
- This is $\sqrt{2}^2 = 2$, which is rational.
- **Q.E.D**

What is the problem?

- We cannot explicitly give irrational a, b such that $a^b \in \mathbb{Q}$!
- This proof would be useless if we needed explicit values.
- This is the essence of **constructivism**.
- Every existence proof must be a procedure for constructing a witness.

Constructive versus Classical Reasoning

- We reject two principles to move from classical to constructive mathematics
- **Law of Excluded Middle:** $A \vee \neg A$ is no longer valid
- **Double Negation Elimination:** $\neg\neg A \supset A$ is no longer valid
- (Actually these amount to the same thing)

The Intuition

We have objects called **sequents**. These consist of

- a **context**, usually called Γ , which is a (multi)set of formulae. Also called an **antecedent**
- a **sequent arrow**, usually \Rightarrow
- a single formula **succedent**

For instance, $\Gamma \Rightarrow A$ is read as “from the assumptions or formulae in Γ , we can conclude A .” Or just Γ arrows A .

Putting Sequents Together

We have rules to transform sequents, or pairs of sequents, into a **single** new sequent. We write the **premisses** above a horizontal line, and the conclusion below it:

- No premiss rules, such as axioms

$$\frac{}{\Gamma, P \Rightarrow P}$$

- One premiss rules, such as right disjunction

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}$$

- Two premiss rules, such as right conjunction

$$\frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B}$$

An Example Derivation - Distributive Laws

We verify the formula $(A \wedge (B \vee C)) \supset ((A \wedge B) \vee (A \wedge C))$

$$\begin{array}{c}
 \frac{A, B \Rightarrow A \quad A, B \Rightarrow B}{A, B \Rightarrow A \wedge B} R\wedge \quad \frac{A, C \Rightarrow A \quad A, C \Rightarrow C}{A, C \Rightarrow A \wedge C} R\wedge \\
 \frac{A, B \Rightarrow (A \wedge B) \vee (A \wedge C)}{A, B \vee C \Rightarrow (A \wedge B) \vee (A \wedge C)} R\vee_1 \quad \frac{A, C \Rightarrow (A \wedge B) \vee (A \wedge C)}{A, B \vee C \Rightarrow (A \wedge B) \vee (A \wedge C)} R\vee_2 \\
 \frac{A, B \vee C \Rightarrow (A \wedge B) \vee (A \wedge C)}{A \wedge (B \vee C) \Rightarrow (A \wedge B) \vee (A \wedge C)} L\wedge \\
 \frac{A \wedge (B \vee C) \Rightarrow (A \wedge B) \vee (A \wedge C)}{\Rightarrow (A \wedge (B \vee C)) \supset ((A \wedge B) \vee (A \wedge C))} R\supset
 \end{array}$$

Implicational Interpolants

In this setting, we want interpolants for logical implication:

- Suppose $A \supset B$ is valid
- Can we find a C such that $A \supset C$ and $C \supset B$ are valid?
- Moreover, can we restrict C to be of the **language** of A and B ?

An Example

Here is a very basic example

- Suppose A is “Rick is a hamster”



- Further that B is “Rick is an animal”

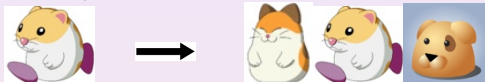


- Clearly, $A \supset B$ is valid, and the common language is “living things”

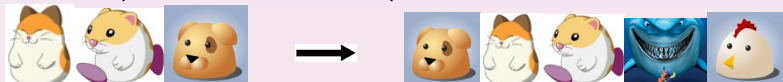


Example ctd.

- If Rick is a hamster, **then** Rick is a mammal



- Moreover**, if Rick is a mammal, **then** Rick is an animal



- Also**, being a mammal is in the common language of “living things”, hence we are done!

Interpolation for Sequent Calculi

How does this translate to sequent calculus?

What we want to prove is that if $\Gamma \Rightarrow D$ is the root of a valid derivation, then

- $\exists C \text{ dl } dr. \text{dl} \vdash \Gamma \Rightarrow C \wedge dr \vdash C \Rightarrow D$
- Any predicate occurring positively (resp. negatively) in C occurs positively (resp. negatively) in Γ and D
- The individual constants of C occur both in Γ and D

A Stronger Theorem

We actually prove a stronger result. Suppose that $\Gamma'' \Rightarrow D$.
Then, for **any** splitting of the context $\Gamma'' \equiv \Gamma \cup \Gamma'$:

- $\exists C \text{ dl } dr. \text{dl} \vdash \Gamma \Rightarrow C \wedge \text{dr} \vdash \Gamma', C \Rightarrow D$
- **POL**: Any predicate appearing positively (resp. negatively) in C occurs positively (resp. negatively) in Γ and D and negatively (resp. positively) in Γ'
- **CON**: The individual constants of C occurs in both Γ and $\Gamma' \cup D$

Individual Constants

The polarity conditions are relatively uninteresting. But what are the **individual constants**? They are the *terms* of a formula. In this case, a logic without equality, the terms are either simply variables, or zero-place function symbols. So, the individual constants are the free variables and zero-arity function symbols of a formula. A more precise definition is not needed now (and would obscure the talk)

How To Proceed

As is usual, we proceed by a structural induction proof, that is, on the *structure* of the derivation:

- Prove the result for the base cases of a derivation, the zero premiss rules **Axiom** and **L \perp**
- For each rule, we must use the induction hypothesis that a valid interpolant exists for the premisses, and construct a valid interpolant for the conclusion
- We have to analyse 19 cases for first-order intuitionistic logic!
- We're only going to look at a base subcase, a propositional subcase, and an interesting quantifier case

Base Case

Suppose that the derivation is $\Gamma, \Gamma' \Rightarrow P$, and further that $P \in \Gamma$. We need a C satisfying **POL** and **CON** such that $\Gamma \Rightarrow C$ and $C, \Gamma' \Rightarrow P$.

- Any guesses?
- Take $C \equiv P$
- Clearly, since $P \in \Gamma$, then $\Gamma \Rightarrow P$ and we also have $P, \Gamma' \Rightarrow P$ as instances of **Axiom**
- **POL** and **CON** are also trivially satisfied

Propositional Case

The problem for R_{\wedge} can be stated as

$$\frac{\Gamma; \Gamma' \xRightarrow{C} A \quad \Gamma; \Gamma' \xRightarrow{D} B}{\Gamma; \Gamma' \xRightarrow{?} A \wedge B}$$

where C and D are supplied by the induction hypothesis. Hence, we have 4 derivations with which to construct those needed by the theorem, with root sequents:

- 1 $\Gamma \Rightarrow C$
- 2 $\Gamma', C \Rightarrow A$
- 3 $\Gamma \Rightarrow D$
- 4 $\Gamma', D \Rightarrow B$

Propositional Fragment - R_{\wedge}

It makes sense to pair up the derivations according to their contexts. We see that the following derivations are both possible



$$\frac{\Gamma \Rightarrow C \quad \Gamma \Rightarrow D}{\Gamma \Rightarrow C \wedge D}$$



$$\frac{\frac{\Gamma', C \Rightarrow A}{\Gamma', C, D \Rightarrow A} \quad W \quad \frac{\Gamma', D \Rightarrow B}{\Gamma', C, D \Rightarrow B} \quad W}{\frac{\Gamma', C, D \Rightarrow A \wedge B}{\Gamma', C \wedge D \Rightarrow A \wedge B}}$$

- But do they satisfy the polarity and language conditions?

First-Order case - $R\exists$

The problem is

$$\frac{\Gamma; \Gamma' \xRightarrow{C} [t/x]A}{\Gamma; \Gamma' \xRightarrow{?} \exists xA}$$

which gives, by the IH, the derivations ending with

- $\Gamma \Rightarrow C$
- $\Gamma', C \Rightarrow [t/x]A$

A naïve approach would say that we could simply apply $R\exists$ to the second of these, leave the first one alone, and we are done.

Why will this not work?

First-Order case - language constraint bites

From the IH, we know that C is in the common language of Γ , Γ' and $[t/x]A$. Specifically, it can contain constants that appear in t and not in Γ or Γ' .

- Let us call the set of all such constants \vec{u}
- Assume there exists a constant c in C that is in \vec{u}
- None of the constants \vec{u} appear in the conclusion, except for the ones in C
- So, the constants of C **DO NOT** belong to the common language of Γ , Γ' and $\exists xA$
- C is not a valid interpolant

How to fix this?

We need to somehow remove these constants, \vec{u} , from C . We said that constants were individual constants and free variables.

- Therefore, we can quantify over these \vec{u} to bind them, and hence remove them as constants
- On the **first premiss**, we get the valid derivation

$$\frac{\Gamma \Rightarrow C}{\Gamma \Rightarrow \forall \vec{u} C}$$

- On the **second premiss**, we get the derivation

$$\frac{\frac{\Gamma', C \Rightarrow [t/x]A}{\Gamma', \forall \vec{u} C \Rightarrow [t/x]A}}{\Gamma', \forall \vec{u} C \Rightarrow \exists x A}$$

Conclusions

- We have given reasons why computers like constructive mathematics
- We've introduced a formalism for dealing with logical formulae
- We have given a constructive outline of a proof within that system

Further work

- We have formalised this result within the proof-assistant *Isabelle*
- We will turn our attention to formalising other meta-theoretical results
- The ultimate goal is to semi-automate such results, for various logics
- **Any questions?**