Applications of focusing to the proof theory of arithmetic

Matteo Manighetti

February 1st, 2021

Inria Saclay & LIX, École polytechnique, Palaiseau, France
Works in progress with Dale Miller

Introduction

Some programmatic statements:

- Structural proof theory: look into the structure of proofs
- Linear Logic as *the logic behind logic*
- Insights from linear logic...without linar logic!
- Except for: the second part on MALL (contraction, weakening free)

Sequent calculus

The sequent calculus allows for a finer analysis of proofs

It also accomodates better proof-search

But proof objects themselfes are more confusing:

Most computer scientists refer to this as the *natural* way

$$\frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

Some weaknesses in the sequent calculus

Rules are too low-level

Say I have an axiom

$\forall x \forall y \forall z\, (path(x, y) \supset path(y, z) \supset path(x, z))$

A proof could introduce the first ∀, then do something else…

Rules are too low-level

Say I have an axiom
$\forall x \forall y \forall z\,(path(x, y) \supset path(y, z) \supset path(x, z))$

A proof could introduce the first $\forall$, then do something else…

But really, what one would like are proofs that either do

$$\frac{\Gamma \vdash \Delta, path(x, y) \quad \Gamma \vdash \Delta, path(y, z)}{\Gamma \vdash \Delta, path(x, z)}$$

(use the axiom to find the required path)

Rules are too low-level

Say I have an axiom
$\forall x \forall y \forall z\, (path(x, y) \supset path(y, z) \supset path(x, z))$

A proof could introduce the first $\forall$, then do something else...

But really, what one would like are proofs that either do

$$\frac{\Gamma \vdash \Delta, path(x, y) \quad \Gamma \vdash \Delta, path(y, z)}{\Gamma \vdash \Delta, path(x, z)}$$

(use the axiom to find the required path)

or

$$\frac{\Gamma, path(x, y), path(y, z), path(x, z) \vdash \Delta}{\Gamma, path(x, y), path(y, z) \vdash \Delta}$$

(use the axiom to extend the *path* knowledge base)

Uninteresting permutations

The difference between the two proofs really seems irrelevant

$$\dfrac{\Gamma_1 \vdash B, \Delta_1 \qquad \dfrac{\Gamma_2, C \vdash [y/x]D, \Delta_2}{\Gamma_2, C \vdash \forall x.D, \Delta_2}\ \forall\text{-r}}{\Gamma_1, \Gamma_2, B \supset C \vdash \forall x.D, \Delta_1, \Delta_2}\ \supset\text{-l} \qquad \dfrac{\dfrac{\Gamma_1, \vdash B, \Delta_1 \qquad \Gamma_2, C \vdash [y/x]D, \Delta_2}{\Gamma_1, \Gamma_2, B \supset C \vdash [y/x]D, \Delta_1, \Delta_2}\ \supset\text{-l}}{\Gamma_1, \Gamma_2, B \supset C \vdash \forall x.D, \Delta_1, \Delta_2}\ \forall\text{-r}$$

Looking for both in a proof-search task is expensive

Ambiguity of cut-elimination

$$\begin{array}{c}\Xi_1\\ \vdots\\ \vdash B\end{array} \quad \leftsquigarrow \quad \dfrac{\dfrac{\dfrac{\begin{array}{c}\Xi_1\\ \vdots\\ \vdash B\end{array}}{\vdash C, B}\,\mathrm{wR} \qquad \dfrac{\begin{array}{c}\Xi_2\\ \vdots\\ \vdash B\end{array}}{C \vdash B}\,\mathrm{wL}}{\vdash B, B}\,\mathrm{cut}}{\vdash B} \quad \rightsquigarrow \quad \begin{array}{c}\Xi_2\\ \vdots\\ \vdash B\end{array}$$

Cut elimination results in…either Ξ_1 or Ξ_2, the other one is lost!

Permutations and contractions

Last observation: structural rules interfere with permutations!

$$\dfrac{\dfrac{\Gamma_1, r \vdash \Delta_1, p \quad \Gamma_2, q \vdash \Delta_2, s}{\Gamma_1, \Gamma_2, p \supset q, r \vdash \Delta_1, \Delta_2, s}\ \supset\text{L}}{\Gamma_1, \Gamma_2, p \supset q \vdash \Delta_1, \Delta_2, r \supset s}\ \supset\text{R}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma_1, r \vdash \Delta_1, p}{\Gamma_1, r \vdash \Delta_1, p, s}\ \text{wR}}{\Gamma_1, \vdash \Delta_1, r \supset s, p}\ \supset\text{R} \quad \dfrac{\dfrac{\Gamma_2, q \vdash \Delta_2, s}{\Gamma_2, q, r \vdash \Delta_2, s}\ \text{wL}}{\Gamma_2, q \vdash \Delta_2, r \supset s}\ \supset\text{R}}{\Gamma_1, \Gamma_2, p \supset q \vdash \Delta_1, \Delta_2, r \supset s, r \supset s}\ \supset\text{L}}{\Gamma_1, \Gamma_2, p \supset q \vdash \Delta_1, \Delta_2, r \supset s}\ \text{cR}$$

Building a focused sequent calculus

Summing up...

So far we hinted that:

- Invertibles can be easily permuted below non-invertibles
- The converse involves structural rules

Summing up...

So far we hinted that:

- Invertibles can be easily permuted below non-invertibles
- The converse involves structural rules

Start by: separate invertible and non-invertible rules

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} \qquad \frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta, A \supset B}$$

Call asynchronous the connectives with an invertible right rule

Can we treat all the asynchronous part before the synchronous?

One more bit

Why don't we use the rule

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$$

Then $\vee$ would become synchronous!

One more bit

Why don't we use the rule

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$$

Then $\vee$ would become synchronous!

We treat these as two different connectives: $\vee^{+}$ and $\vee^{-}$

One more bit

Why don't we use the rule

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$$

Then $\vee$ would become synchronous!

We treat these as two different connectives: $\vee^+$ and $\vee^-$

The same happens to $\wedge^-$ and $\wedge^+$. Call +/- the polarity

One more bit

Why don't we use the rule

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$$

Then $\vee$ would become synchronous!

We treat these as two different connectives: $\vee^+$ and $\vee^-$

The same happens to $\wedge^-$ and $\wedge^+$. Call +/- the polarity

$\supset, \forall$ are negative; $\exists$ positive

This is reminescent of linear logic: $\oplus, \parr\ \otimes, \&$

Atoms and polarity

It remains to fix the interaction with the initial and cut rules

Extend the notion of polarity to atoms!

Intutively:

- A positive atom justifies forward reasoning:
  use it to conclude something new
- A negative atom is a justification for backward reasoning:
  when proving something, conclude if you already know it

Designing a focused calculus

Simplification: negation normal form; single sided

Structural

$$\frac{\vdash \Gamma \Uparrow P, \Delta}{\vdash P, \Gamma \Uparrow \Delta}\ \text{store} \qquad \frac{\vdash P \Downarrow P, \Delta}{\vdash \cdot \Uparrow P, \Delta}\ \text{decide} \qquad \frac{\vdash N \Uparrow \Delta}{\vdash N \Downarrow \Delta}\ \text{release} \qquad \frac{}{\vdash p \Downarrow p^{\perp}, \Delta}\ \text{init}$$

Synchronous

$$\frac{\vdash A_1, A_2, \Gamma \Downarrow \Delta}{\vdash A_1 \wedge^+ A_2, \Gamma \Downarrow \Delta} \qquad \frac{\vdash A_i, \Gamma \Downarrow \Delta}{\vdash A_1 \vee^+ A_2, \Gamma \Downarrow \Delta} \qquad \frac{\vdash [t/x]A, \Gamma \Downarrow \Delta}{\vdash \exists x.A, \Gamma \Downarrow \Delta} \qquad \frac{}{\vdash t^+ \Downarrow \Delta}$$

Asynchronous

$$\frac{\vdash A_1, \Gamma \Uparrow \Delta \quad \vdash A_2, \Gamma \Uparrow \Delta}{\vdash A_1 \wedge^- A_2, \Gamma \Uparrow \Delta} \qquad \frac{\vdash A_1, A_2, \Gamma \Uparrow \Delta}{\vdash A_1 \vee^- A_2, \Gamma \Uparrow \Delta} \qquad \frac{\vdash [y/x]A, \Gamma \Uparrow \Delta}{\vdash \forall x.A, \Gamma \Uparrow \Delta} \qquad \frac{}{\vdash t^-, \Gamma \Uparrow \Delta}$$

P is a positive formula; p positive atom; N negative formula

- Decompose negatives, storing encountered positives
- Then, decide on a positive and focus: contraction is here!

Properties of LKF

If we remove all polarities and arrows: it's just sequents!

Theorem

The focused sequent calculus LKF is sound and complete for classical logic

Successful applications to

- Computation as deduction
- Designing formats for proof communication
- Also, computation as proof normalization

Metatheoretic applications

We can find information about the constructive content of classical proofs

Consider $\exists x \exists y \ldots A$, A quantifier-free

If we choose all connectives to be negative, an LKF proof must

- Introduce terms for x,y...in a single synchronous phase
- Either conclude immediately, or introduce another tuple of terms

This sketches of a proof of Herbrand's theorem

Treating induction

Induction in a focused calculus

We treat induction by adding connectives for least and greatest fixpoints:

- Focusing is best understood as a discipline of connective decomposition
- Emphasis on dualities: here, least/greatest

And we enrich our logic by treating equality by unification:

Let B be a predicate operator: $o \to o$ in Church-style

Then by μB we denote the least fixpoint of B

Natural numbers

For example, the usual definition of numbers

$$nat := \mu\lambda nat.\lambda x.(x = 0 \vee \exists y.x = Sy \wedge naty)$$

Said otherwise,

```
Define nat by nat 0; nat S N := nat N
```

But also Ackermann's function:

$$\mu\lambda ack\lambda m\lambda n\lambda a.$$
$$m = 0 \wedge a = sn \vee$$
$$(\exists p.m = s\,p \wedge n = 0 \wedge ack\,p(s0)a)$$
$$\vee\,(\exists p\exists q\exists b.m = s\,p \wedge n = s\,q \wedge ack\,mqb \wedge ack\,pba)$$

The induction rule:

$$\frac{\Gamma, P\bar{t} \vdash \Delta \quad BP\bar{x} \vdash P\bar{x}}{\Gamma, \mu B\bar{t} \vdash \Delta}$$

Informally: to conclude Δ from $\bar{t}$ being in the least fixpoint of B, pick a pre-fixpoint S

In the case of *nat*, we get

$$\frac{\Gamma, Pn \vdash \Delta \quad n = 0 \vee \exists y. n = Sy \wedge Py \vdash Pn}{\Gamma, nat\, n \vdash \Delta}$$

Focusing and inductive definitions

D. Baelde showed that there is a focused proof system for $\mu MALL$: no weakening, no contraction, and no exponentials!

Positive and negatives are no more provably equivalent

Focusing and inductive definitions

D. Baelde showed that there is a focused proof system for $\mu MALL$: no weakening, no contraction, and no exponentials!

Positive and negatives are no more provably equivalent

Induction is treated during asynchrony:

$$\frac{\vdash \Gamma, (P\,\bar{t})^{\perp} \Uparrow \Delta \quad \vdash (B\,P, \bar{y})^{\perp}, P, \bar{y} \Uparrow \cdot}{\vdash \Gamma, (\mu B\,\bar{t})^{\perp} \Uparrow \Delta} \qquad \frac{\vdash \Gamma \Uparrow (\mu B\,\bar{t})^{\perp}, \Delta}{\vdash \Gamma, (\mu B\,\bar{t})^{\perp} \Uparrow \Delta}$$

Either do induction immediately, or store the fixpoint forever

Positive fixpoints

Theorem

Contraction and weakening are admissible in μMALL for any purely positive formula

Many (most?) interesting inductive definitions as purely positive.

Remember the naturals:

$$nat := \mu\lambda nat.\lambda x.(x = 0 \vee^{+} \exists y.x = Sy \wedge^{+} nat y)$$

Then, within the focused calculus the rule directly becomes

$$\dfrac{\vdash \Gamma, (P\,\bar{t})^{\perp} \Uparrow \Delta \quad \dfrac{\vdash P0 \Uparrow \quad \vdash (Py)^{\perp}, P(Sy) \Uparrow}{\vdash (x = 0 \vee^{+} \exists y.x = Sy \wedge^{+} Py)^{\perp}, Px \Uparrow}}{\vdash \Gamma, (nat\, n)^{\perp} \Uparrow \Delta}$$

Some properties of focused $\mu MALL$

Remember that we are in a classical system!

The disjunctive property holds for $\vee^+$, as usual.

A strong property for $\vee^-$:

Theorem

If $A_1, \ldots A_n$ are purely positive and $\vdash A_1, \ldots A_n$ is provable in $\mu MALL$, then n is 1

Cut-elimination for the focused calculus gives us

Theorem (Witness extraction)

Let A be purely positive and Ξ a proof of $\forall \bar{x} \exists y A\, \bar{x} y$.

Then any proof of $\exists y\, A \bar{t} y$ containing a cut against Ξ contains a witness for y

Expressiveness of $\mu MALL$

There are several applications of $\mu MALL$ in CS

But what fragment of arithmetic does it capture?

An empirical limit: write Ackermann's function as a fixpoint

In order to prove $\forall x \forall y. nat\, x \multimap nat\, y \multimap \exists z\, ack\, x\, y\, z$ we need

- Either contraction on formulas with implication
- Or induction with open contexts (Alves & Mackie)

Targeting $I\Sigma_1$

Theorem

Let Θ be a set of purely positive formulas. The following rule is admissible in μMALL

$$\frac{\vdash \Gamma, (P\,\bar{t})^\perp \Uparrow \Delta \quad \vdash (B\,P\,\bar{y})^\perp, P\,\bar{y}, \Theta \Uparrow}{\vdash \Gamma, (\mu B\,\bar{t})^\perp \Uparrow \Delta, \Theta}$$

This induction rule seems enough to capture $I\Sigma_1$

Theorem

Primitive recursive functions can be expressed as purely positive formulas. Their totality is provable with the above induction rule.

Current questions:

- Formalize the correspondence between $I\Sigma_1$ and purely positive
- Posssibly extend the hierarchy?
- Prove the completeness of the focused proof system for full classical logic

Thank you