Peano Arithmetic and muMALL: Work in progress

Matteo Manighetti
University of Bologna

Dale Miller
Inria Saclay & LIX, IPP

FICS 2023, Warsaw. Poland
17 February 2022

Technical Report:
http://www.lix.polytechnique.fr/Labo/Dale.Miller/papers/lfmtp22-positive-perspective.pdf

Art by Nadia Miller

Different approaches to arithmetic

The traditional approach to Peano and Heyting Arithmetic is

- formalized using (classical or intuitionistic) first-order logic with axioms (for equality) and an axiom scheme (for induction), and
- focuses on cut-elimination, consistency proofs, ordinal measures, and the arithmetic hierarchy.

We are instead interested in a structural proof theory approach to arithmetic. Our focus will be on

- the use of sequent calculus, structural inference rules, rule permutation, polarization, etc, and
- applications to proof search and automated theorem proving.

$\bar{\bar{\mu}}$MALL and $\bar{\bar{\mu}}$LK

Equality and not-equality ($=$ and $\neq$) as logical connectives

- First proposed by Schroeder-Heister and Girard in 1992. Extended by McDowell, M, Tiu, Baelde, Nadathur, Gacek.
- Builds unification into a sequent calculus.
- Provides a novel treatment of bindings and enabled the ∇-quantifier.

Least and greatest fixed points (μ and ν) as logical connectives

- $\bar{\bar{\mu}}$MALL, $\bar{\bar{\mu}}$LJ, $\bar{\bar{\mu}}$LK
- foundation of Bedwyr, a model checker [Heath & M, 2019]
- foundations of the Abella proof assistant [Baelde et al, 2014]

NB: [Baelde & M, 2007] used the name μMALL.

Unpolarized and polarized formulas

We consider two classes of formulas.

- They both contain $=$, $\neq$, $\forall$, $\exists$, μ, and ν. These reference the first-order domain.
- Unpolarized formulas contain also $\wedge$, tt, $\vee$, ff.
- Polarized formulas contain instead $\otimes$, 1, $\parr$, $\bot$, $\&$, $\top$, $\oplus$, 0.

There are no atomic formulas since there are no predicate (undefined) symbols: $x = y$ is not atomic.

There is no negation. Everything is written in negation normal form (nnf).

If we write $\overline{B}$ and $B \supset C$, we mean the corresponding nnf computed using De Morgan dualities.

Polarized version of formulas

A polarized formula $\hat{Q}$ is a polarized version of the unpolarized formula Q if the following replacement carries $\hat{Q}$ to Q:

$$\&, \otimes \ \mapsto \wedge \qquad ⅋, \oplus \ \mapsto \vee \qquad 1, \top \ \mapsto tt \qquad 0, \bot \ \mapsto ff.$$

If Q has n occurrences of propositional connectives, then there are 2^n formulas $\hat{Q}$ that are polarized versions of Q.

Proof system for $\bar{\bar{\mu}}$MALL

$$\frac{\vdash \Gamma, P \quad \vdash \Delta, Q}{\vdash \Gamma, \Delta, P \otimes Q} \qquad \frac{}{\vdash 1} \qquad \frac{\vdash \Gamma, P, Q}{\vdash \Gamma, P \parr Q} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \bot}$$

$$\frac{\vdash \Gamma, P \quad \vdash \Gamma, Q}{\vdash \Gamma, P \,\&\, Q} \qquad \frac{}{\vdash \Delta, \top} \qquad \frac{\vdash \Gamma, P_i}{\vdash \Gamma, P_0 \oplus P_1}$$

$$\frac{\{\ \vdash \Gamma\theta : \theta = mgu(t, t')\ \}}{\vdash \Gamma, t \neq t'} \qquad \frac{}{\vdash t = t} \qquad \frac{\vdash \Gamma, Pt}{\vdash \Gamma, \exists x.Px} \qquad \frac{\vdash \Gamma, Py}{\vdash \Gamma, \forall x.Px}$$

$$\frac{\vdash \Gamma, S\vec{t} \quad \vdash BS\vec{x}, \overline{(S\vec{x})}}{\vdash \Gamma, \nu B\vec{t}}\ \nu \qquad \frac{\vdash \Gamma, B(\mu B)\vec{t}}{\vdash \Gamma, \mu B\vec{t}}\ \mu \qquad \frac{}{\vdash \mu B\vec{t}, \nu\overline{B}\vec{t}}\ \mu\nu$$

Induction and coinduction are given by one rule (ν). The higher-order variable S, in that rule, is the invariant.

The $\mu\nu$ rule is a form of the initial rule.

Eigenvariables are introduced by $\forall$ rule and instantiated by $\neq$ rule.

Proof system for $\bar{\bar{\mu}}$LK

The $\bar{\bar{\mu}}$LK proof system is $\bar{\bar{\mu}}$MALL plus the two structural rules:

$$\frac{\vdash \Gamma, Q, Q}{\vdash \Gamma, Q}\ C \qquad \frac{\vdash \Gamma}{\vdash \Gamma, Q}\ W$$

We also consider the following two rules in the context of both $\bar{\bar{\mu}}$MALL and $\bar{\bar{\mu}}$LK.

$$\frac{\vdash \Gamma, B(\nu B)\vec{t}}{\vdash \Gamma, \nu B\vec{t}}\ \mathit{unfold} \qquad \frac{\vdash \Gamma, Q \quad \vdash \Delta, \overline{Q}}{\vdash \Gamma, \Delta}\ \mathit{cut}$$

The *unfold* rule is derivable in both $\bar{\bar{\mu}}$MALL and $\bar{\bar{\mu}}$LK.

Observations about $\bar{\bar{\mu}}$MALL and $\bar{\bar{\mu}}$LK

- The *unfold* and μ rules replace μB with $B(\mu B)$: thus one copy of B become two copies.
- Baelde [2012] proved that $\bar{\bar{\mu}}$MALL satisfies cut-elimination and that a natural focused proof system is complete.
- We have neither a cut-elimination theorem nor a completeness-of-focusing theorem for $\bar{\bar{\mu}}$LK.
- We have proved that $\bar{\bar{\mu}}$LK (with cut) is consistent and contains Peano arithmetic.
- Girard [1991]: the completeness of a focused form of $\bar{\bar{\mu}}$LK would allow extracting constructive content from classical Π^0_2 theorems. The usual ways the completeness of focusing and cut elimination are proved should not yield that result.

Separating $\bar{\bar{\mu}}$MALL and $\bar{\bar{\mu}}$LK

- The formula $\forall x \forall y [x = y \vee x \neq y]$ can be polarized as either

$$\forall x \forall y [x = y \parr x \neq y] \quad \text{or} \quad \forall x \forall y [x = y \oplus x \neq y].$$

  $\bar{\bar{\mu}}$MALL proves the first. $\bar{\bar{\mu}}$LK proves both.

- The totality of Ackermann's function has a simple $\bar{\bar{\mu}}$LK-proof. Here is what it looks like in Abella.

```
Define ack : nat -> nat -> nat -> prop by
  ack zero N (succ N) ;
  ack (succ M) zero R := ack M (succ zero) R ;
  ack (succ M) (succ N) R := exists R', ack (succ M) N R' /\ ack M R' R.

Theorem ack_total : forall M N, nat M -> nat N -> exists R, nat R /\ ack M N R.
induction on 1. induction on 2. intros. case H1 (keep).
  search. case H2. apply IH to H3 _ with N = (succ zero). search.
                   apply IH1 to H1 H4. apply IH to H3 H5. search.
```

  We conjecture that there is no proof in $\bar{\bar{\mu}}$MALL.

Arithmetic Hierarchy for polarized formulas

- Negative: $\parr$, $\bot$, $\&$, $\top$, $\forall$, $\neq$, ν (invertible right rules)
- Positive: $\otimes$, 1, $\oplus$, 0, $\exists$, $=$, μ
- A formula is positive or negative depending only on its top-level connective.
- A formula is purely positive (resp., purely negative) if every logical connective it contains is positive (resp., negative).
- Σ_1-formulas are exactly the purely positive formulas
- Π_1-formulas are exactly the purely negative formulas
- for $n \geqslant 1$,
  - Π_{n+1}-formulas are negative formulas for which every positive subformula occurrence is a Σ_n-formula.
  - Σ_{n+1}-formulas are positive formulas for which every negative subformula occurrence is a Π_n-formula.
- A formula in Σ_n or Π_n has at most $n-1$ polarity alternations.

Examples

- $\forall x \forall y[x = y \parr x \neq y]$ is Π_2
- $\forall x \forall y[x = y \oplus x \neq y]$ is Π_3.
- Addition and multiplication as least fixed points are in Σ_1.

$$\mu\lambda P \lambda n \lambda m \lambda p((n = z \otimes m = p) \oplus \\ \exists n' \exists p' (n = (s\ n') \otimes p = (s\ p') \otimes P\ n'\ m\ p'))$$

$$\mu\lambda M \lambda n \lambda m \lambda p\big((n = z \otimes p = z) \oplus \\ \exists n' \exists p' (n = (s\ n') \otimes \mathit{plus}\ m\ p'\ p \otimes M\ n'\ m\ p')\big)$$

- Horn clause specification naturally yield Σ_1-formulas.
- Simulation and bisimulation can be encoded as Π_2-formulas.

Basic results related to polarities:

- If B is Π_1 then $B \equiv ?\,B$ is provable in $\bar{\bar{\mu}}$LL.
- If B is Σ_1 then $B \equiv !\,B$ is provable in $\bar{\bar{\mu}}$LL.

Connections with Σ_n^0, Π_n^0 for unpolarized formulas

Let Q be an unpolarized formula of Peano arithmetic in Σ_n^0 for $n \geqslant 1$. Then there is a polarized version $\hat{Q}$ such that $\hat{Q}$ is in Σ_n.

Let Q be an unpolarized formula of Peano arithmetic in Π_n^0 for $n \geqslant 2$. Then there is a polarized version $\hat{Q}$ such that $\hat{Q}$ is in Π_n.

Conservativity results for linearized arithmetic

Theorem

$\bar{\bar{\mu}}LK$ is conservative over $\bar{\bar{\mu}}MALL$ for Σ_1-formulas: if B is Σ_1 and has a $\bar{\bar{\mu}}LK$ proof then B is provable in $\bar{\bar{\mu}}MALL$.

Definition

A sequent has a $\bar{\bar{\mu}}\mathrm{LK}(\Sigma_1)$ proof if it has a $\bar{\bar{\mu}}\mathrm{LK}$ proof in which all invariants of the proof are purely positive.

This restricted proof system is similar to the $I\Sigma_1$ restriction.

Theorem

$\bar{\bar{\mu}}LK(\Sigma_1)$ is conservative over $\bar{\bar{\mu}}MALL$ for Π_2-formulas.

These results (and many other) are straightforward if we assume that $\bar{\bar{\mu}}\mathrm{LK}$ satisfies cut-elimination and has a complete focused proof system.

Using proof search to compute functions

The binary relation ϕ computes a function if one can prove totality and determinancy, namely $\forall x \exists ! y . \phi(x, y)$:

$$\forall x \big[[\exists y . \phi(x, y)] \wedge [\forall y_1 \forall y_2 . \phi(x, y_1) \supset \phi(x, y_2) \supset y_1 = y_2] \big]. \quad (*)$$

In this case, $\lambda y . \phi(x, y)$ denotes a singleton for every x.

How can we use a proof of totality to compute the function?

- Given an intuitionistic proof of $(*)$, we exploit its constructive content.
- If ϕ is Σ_1, then $(*)$ can be polarized Π_2. If we have a $\bar{\bar{\mu}}$LK proof of $(*)$, that proof can be an oracle to guide proof search.

Proof search procedure

The search-state S is of the form $\langle \Sigma \,;\, B_1, \ldots, B_m \,;\, t \rangle$.

Theorem

Assume that P is Σ_1 and that $\exists! y. Py$ has a $\bar{\bar{\mu}}LK$ proof. Then $\langle y \,;\, P\ y \,;\, y \rangle \Rightarrow^* \langle \cdot \,;\, \cdot \,;\, t \rangle$ iff $(P\ t)$ is provable.

Nondeterministic transitions $S \Rightarrow S'$ are defined by

- If B_1 is $u = v$ and u and v are unifiable with mgu θ, then we transition to $\langle \Sigma\theta \,;\, B_2\theta, \ldots, B_m\theta \,;\, (t\theta) \rangle$.
- If B_1 is $B \otimes B'$ then we transition to $\langle \Sigma \,;\, B, B', B_2, \ldots, B_m \,;\, t \rangle$.
- If B_1 is $B \oplus B'$ then we transition to either $\langle \Sigma \,;\, B, B_2, \ldots, B_m \,;\, t \rangle$ or $\langle \Sigma \,;\, B', B_2, \ldots, B_m \,;\, t \rangle$.
- If B_1 is $\mu B \vec{t}$ then we transition to $\langle \Sigma \,;\, B(\mu B)\vec{t}, B_2, \ldots, B_m \,;\, t \rangle$.
- If B_1 is $\exists y.\ B\ y$ then we transition to $\langle \Sigma, y \,;\, B\ y, B_2, \ldots, B_m \,;\, t \rangle$ where y is not in Σ.

Conclusion

- We propose to approach the structural proof theory of arithmetic by studying both $\bar{\bar{\mu}}$MALL and $\bar{\bar{\mu}}$LK.
- Open: cut-elimination and completeness of focusing for $\bar{\bar{\mu}}$LK.
- Without the completeness of focusing result, we are incrementally attacking conservative extension results of $\bar{\bar{\mu}}$LK over $\bar{\bar{\mu}}$MALL.
- We explicitly connect the arithmetic hierarchy to polarity alternations a la Andreoli and Girard.
- Proof search in $\bar{\bar{\mu}}$MALL should be more manageable, even when faced with generating invariants.
- Proof search can be used to compute functions from their relational specifications.

Questions?