Towards feasibility in arithmetic via linear logic

Patrick Baillot & Anupam Das

March 7, 2016

In this work-in-progress we intend to extend the scope of linear logic to first-order theories, i.e. with nonlogical axioms and inference rules, in particular for fragments of arithmetic. The aim is to use the restrictions on contraction in substructural logics to model resource usage in an interpretation of first-order proofs, e.g. via realisability/Dialectica interpretations or via proof-theoretic means, such as the witness function method. At the same time, we would like to draw parallels between substructural approaches to implicit computational complexity and bounded arithmetic, by linking structural restrictions in the former to quantifier restrictions in the latter.

A motivating example

A classic distinction in weak theories of arithmetic is between usual induction,

$$IND\ \frac{\Gamma, A(a) \vdash A(a+1)}{\Gamma, A(0) \vdash A(t)} \tag{1}$$

and a 'divide-and-conquer' variant, known as *polynomial induction*:

$$PIND\ \frac{\Gamma, A(a) \vdash A(2a) \quad \Gamma, A(a) \vdash A(2a+1)}{\Gamma, A(0) \vdash A(t)} \tag{2}$$

The formula $A(a)$ is called the *induction formula*. A proof of their equivalence proceeds by proving IND from $PIND$ using a metalogical argument as follows. Suppose we have,

$$A(a) \to A(a+1) \tag{3}$$

We proceed by $PIND$ on the following formula:

$$\forall x \leq (t-a).(A(x) \to A(x+a)) \tag{4}$$

The base case, when $a = 0$, is trivial. For the inductive step, suppose $b \leq t - 2a$. Then, by the inductive hypothesis (4) we have $A(b) \to A(b+a)$. However, since also $b + a \leq t - a$, we have from (4) again that $A(b+a) \to A(b+2a)$, yielding $A(b) \to A(b+2a)$ as required. For the $2a+1$ step we simply apply (3) at this point. Consequently, by $PIND$, we obtain:

$$\forall x \leq (t-s).(A(x) \to A(x+t))$$

for any term s, whence we obtain $A(0) \to A(t)$ by setting $s := t$, as required.

Therefore, in order to distinguish IND from $PIND$, we must control some aspect of the reasoning in this argument. There are (at least) three possibilities:

1. The *quantifier complexity* of the induction formula has increased, by an extra $\forall$.

2. The *type level* of the induction formula has increased, by an extra $\rightarrow$ symbol.

3. The number of calls to the inductive hypothesis has increased: we must apply (4) at $x = b$ and $x = b + a$.

The first approach, arguably the most well studied, is that taken in *bounded arithmetic*, e.g. in Buss' S^i_2-T^i_2 hierarchy [Bus86]. Quantifier alternation in such settings is closely related to hierarchies of complexity classes, and questions of logical strength are associated with separation hypotheses.

The second approach cannot be realised in classical logic, due to the De Morgan laws, and so is naturally set in intuitionistic logic. This corresponds to recursion at higher type levels and, again, induces hierarchies of associated complexity classes, depending on the setting, e.g. [Lei02].

The third approach is only realisable in a resource conscious logic, such as linear logic: we may reject the argument by restricting the use of *contraction* on induction formulae. This is the least developed approach of the three, and this is what we are concerned with in this work.

1 Previous work: first-order theories in linear logic

The study of first-order theories such as arithmetic in linear logic is still somewhat undeveloped, in contrast to certain related substructural logics, e.g. relevant logic. Existing works such as [Gri81] and [Ter04] explore fragments of set theory in linear logic, but we seek to build upon [BH02] due to its thematic relationship to bounded arithmetic. In that work a fragment $\mathcal{A}^1_2$ of Peano Arithmetic is presented, based on a substructural modal logic, with the restriction that induction formulae must be free of the modality $\Box$. Using a *realisability* interpretation, via an intuitionistic variant of the theory, Bellantoni and Hofmann are able to show the following witnessing theorem:

Theorem 1 ([BH02])**.** *The provably total functions of $\mathcal{A}^1_2$ are precisely the functions computable in polynomial time.*

This realisability proof is complementary to that for the analogous result for Buss' S^1_2, a textbook theory in bounded arithmetic, which relies on the *witness function method* [Bus86]. To this end, researchers in bounded arithmetic rely crucially on a 'free-cut free' form of proofs in theories of arithmetic.

Theorem 2 ([Tak75])**.** *An arithmetic proof can be transformed into one whose formulae are all subformulae of the conclusion or an induction formula.*

While both methods have their advantages, one drawback of the former is that it does not easily admit finer analysis of logical fragments due to the double-negation translation into intuitionistic logic. For example, this proof method does not allow us to obtain the tight association between the S^i_2 hierarchy and the polynomial hierarchy presented in [Bus86], via the witness function method.

The notion of free-cut elimination for linear logic is only partially developed, e.g. in [LMSS92] and more recently [BM07], with a general result lacking.[1]

[1] While it is not be very surprising that some analogous results holds, the question is rather how general such a result can be.

2 Work in progress

Free-cut elimination for FO theories in linear logic

We consider arbitrary nonlogical rules, which we can assume are written as follows:

$$\frac{\{!\Gamma, \Sigma_i \vdash \Pi_i, ?\Delta\}_i}{!\Gamma, \Sigma \vdash \Pi, ?\Delta} \tag{5}$$

We call $!\Gamma$ and $?\Delta$ the side formulae, Σ and Π the principal formulae.

Theorem 3. *Every linear logic proof can be transformed to one where each cut formula is principal for an instance of a nonlogical rule.*

Proof sketch. Mostly adapting known methods, we proceed via a *local* rewriting procedure. Termination arguments remain correct even in presence of nonlogical steps, due to locality, only the normal forms change. The ultimate normal forms obtained are precisely the free-cut free proofs. □

Corollary 4 (Arithmetic)**.** *The subformula property of Thm. 2 holds for arithmetic in linear logic when induction side formulae are appropriately modalised:*

$$_{IND}\frac{!\Gamma, A(a) \vdash A(a+1), ?\Delta}{!\Gamma, A(0) \vdash A(t), ?\Delta}$$

This result holds for $PIND$ as well, and this normal form opens the door to 'direct' interpretations of proofs, as we will now discuss.

The witness function method for arithmetic in linear logic

At the heart of the witness function method is the simple definability of a predicate in a given theory which decides if a given word (or functional) witnesses the truth of a given formula. The method then proceeds by showing one can build up witnesses by structural induction on a free-cut free proof.

Proposition 5. *There is a notion of witness predicate that is 'correct' for arbitrary arithmetic formulae in linear logic.*

The idea behind this is that we resort to functions of type level 1 to express witnesses of arbitrary formulae, rather than words (functions of type level 0), morally using Skolemisation to deal with universal quantifiers. Therefore, to adapt the method to theories in linear logic without quantifier restrictions, we must work at one level higher for the entire argument, i.e. of level 2, equivalently polynomial-time functions over streams [KC96].

Conjecture 6. *For induction formulae free of exponentials $!, ?$, we can show that the provably total functions are polynomial-time computable by the witness function method, equipped with an appropriate characterisation of polytime functions over streams.*

The current problem with proving this is, as usual, the $\forall$-right rule in the classical setting.[2] However we believe that this can be avoided, thus preserving the structure of proofs, by employing an induction on the quantifier complexity of induction formulae, thus remaining at bounded type level.

[2] This is one of the reasons why Dialectica and realisability interpretations first employ the double negation translation.

Extending $\mathcal{A}_2^1$

Finally, we would like to apply the previous research directions to extend the work done of [BH02]. One result crucial to this work is the observation that their logic can be embedded into linear logic.

Theorem 7. *The underlying logic of $\mathcal{A}_2^1$ is equivalent to multiplicative exponential affine logic.*[3]

The proof is fairly simple, induced at the level of the connectives and scaled to proofs by usual Hilbert-Gentzen-Frege style metalogical reasoning.

There are two main directions in which we are currently extending the result of [BH02]. First, we are exploring extensions of the logic by second-order quantification (which admits an encoding of the additives), or the *light* and *soft* exponentials from [Gir98] and [Laf04] respectively. For this direction we believe it is simplest to adapt the existing proof via realisability, but appealing to a light or soft logic to type the functionals obtained by the interpretation.

Secondly, we would like to use a proof of Thm. 1 via a direct interpretation, cf. Conj. 6, to obtain finer characterisations of complexity classes, due to the better preservation of formula and proof structure. In particular we would like to match the structure of formulae with hierarchies in computational complexity, and in this way examine their relationships with associated hierarchies of theories in bounded arithmetic.

References

[BH02] Stephen Bellantoni and Martin Hofmann. A new "feasible" arithmetic. *J. Symb. Log.*, 67(1):104–116, 2002.

[BM07] David Baelde and Dale Miller. Least and greatest fixed points in linear logic. In *Logic for Programming, Artificial Intelligence, and Reasoning, 14th International Conference, LPAR 2007, Yerevan, Armenia, October 15-19, 2007, Proceedings*, pages 92–106, 2007.

[Bus86] Samuel R Buss. *Bounded arithmetic*, volume 86. Bibliopolis, 1986.

[Gir98] Jean-Yves Girard. Light linear logic. *Inf. Comput.*, 143(2):175–204, 1998.

[Gri81] Vyacheslav Nikolaevich Grishin. Predicate and set-theoretic calculi based on logic without contractions. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 45(1):47–68, 1981.

[KC96] Bruce M. Kapron and Stephen A. Cook. A new characterization of type-2 feasibility. *SIAM J. Comput.*, 25(1):117–132, 1996.

[Laf04] Yves Lafont. Soft linear logic and polynomial time. *Theor. Comput. Sci.*, 318(1-2):163–180, 2004.

[Lei02] Daniel Leivant. Calibrating computational feasibility by abstraction rank. In *17th IEEE Symposium on Logic in Computer Science (LICS 2002), 22-25 July 2002, Copenhagen, Denmark, Proceedings*, page 345, 2002.

[3] This is linear logic extended by the weakening rule: $A \oplus B \to A$.

[LMSS92] P. Lincoln, J. Mitchell, A. Scedrov, and N. Shankar. Decision problems for propositional linear logic. *Annals of Pure and Applied Logic*, 56(1–3):239–311, 1992.

[Tak75] Gaisi Takeuti. *Proof Theory*, volume 81 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, 1975.

[Ter04] Kazushige Terui. Light affine set theory: A naive set theory of polynomial time. *Studia Logica*, 77(1):9–40, 2004.