On the logical complexity of cyclic arithmetic

Anupam Das[1]*

University of Copenhagen, Denmark
anupam.das@di.ku.dk

Abstract

We study the logical complexity of proofs in cyclic arithmetic (CA), as introduced by Simpson in [33], in terms of quantifier alternations of formulae occurring. Writing $\mathrm{C}\Sigma_n$ for (the logical consequences of) cyclic proofs containing only Σ_n formulae, our main result is that $\mathrm{I}\Sigma_{n+1}$ and $\mathrm{C}\Sigma_n$ prove the same Π_{n+1} theorems, for $n \geq 0$. Furthermore, due to the 'uniformity' of our method, we also show that CA and Peano Arithmetic (PA) proofs of the same theorem differ only elementarily in size. These results improve upon the bounds on proof complexity and logical complexity implicit in [33] and [4].

This abstract is based on a preprint of the same name, [14].

Introduction and motivation

Cyclic and *non-wellfounded* proofs have been studied by a number of authors as an alternative to proofs by induction. This includes cyclic systems for fragments of the modal μ-calculus, e.g. [26, 34, 16, 18, 17, 1], structural proof theory for logics with fixed-points, e.g. [31, 20, 19, 2], (automated) proofs of program termination in separation logic, e.g. [7, 8, 30] and, in particular, cyclic systems for first-order logic with inductive definitions, e.g. [5, 6, 10, 11]. Due to the somewhat implicit nature of invariants they define, cyclic proof systems can be advantageous for metalogical analysis, for instance offering better algorithms for proof search, e.g. [9, 15].

Cyclic proofs may be seen as more intuitively analogous to proofs by 'infinite descent' rather than proofs by induction (see, e.g., [33]); this subtle difference is enough to make inductive invariants rather hard to generate from cyclic proofs. Indeed it was recently shown that simulating cyclic proofs using induction is not possible for some sub-arithmetic languages [3], although becomes possible once arithmetic reasoning is available [33, 4].

Cyclic arithmetic was proposed as a general subject of study by Simpson in [33]. Working in the language of arithmetic, it replaces induction by non-wellfounded proofs with a certain 'fairness' condition on the infinite branches. The advantage of this approach to infinite proof theory as opposed to, say, infinite well-founded proofs via an ω-rule (see, e.g., [32]), is that it admits a notion of *finite proof*: those that have only finitely many distinct subproofs, and so may be represented by a finite (possibly cyclic) graph.

Cyclic arithmetic itself is to cyclic proofs what Peano arithmetic is to traditional proofs. It provides a general framework in which many arguments can be interpreted and/or proved in a uniform manner, and thus constitutes a pertinent subject of study. This is already clear from, say, the results of [4], where the study of cyclic proofs for pure first-order logic with inductive definitions relied on an underlying arithmetic framework.

Contribution

In [33], Simpson shows that Peano Arithmetic (PA) (i.e. with induction) is able to simulate cyclic reasoning by proving the soundness of the former in the latter. (The converse result

*The author is supported by a Marie Skłodowska-Curie fellowship, ERC project 753431.

is obtained much more easily.) Nonetheless, several open questions remain from [33], concerning constructivity, normalisation, logical complexity and proof complexity for cyclic and non-wellfounded proofs.

In this work we address the *logical complexity* and *proof complexity* of proofs in Cyclic Arithmetic (CA), as compared to PA. Namely, we study how quantifier alternation of proofs in one system compares to that in the other, and furthermore how the size of proofs compare. Writing $\mathrm{C}\Sigma_n$ for (the logical consequences of) cyclic proofs containing only Σ_n formulae, we show, for $n \geq 0$:

(1) $\mathrm{I}\Sigma_{n+1} \subseteq \mathrm{C}\Sigma_n$ over Π_{n+1} theorems.

(2) CA and PA proofs of the same theorem differ only elementarily in size.

(3) $\mathrm{C}\Sigma_n \subseteq \mathrm{I}\Sigma_{n+1}$ over all theorems.

(1) is obtained by proof theoretic techniques, relying on normal forms and structural manipulations of Peano Arithmetic proofs. It improves upon the natural result that $\mathrm{I}\Sigma_n \subseteq \mathrm{C}\Sigma_n$, although induces a non-elementary blowup in the size of proofs. (2) is obtained via a certain 'uniformisation' of the approach of [33], formalising a proof of the soundness of CA within PA. In particular, by specialising the key intermediate results to the case of cyclic proofs, we are able to extract small PA proofs of some required properties of infinite word automata from analogous ones in 'second-order' (SO) arithmetic. Finally, (3) is obtained by 'un-uniformising' the argument of (2) and calibrating it with recent results on the reverse mathematics of Büchi's theorem [22], allowing us to bound the logical complexity of proofs in the simulation. Together, these results completely characterise the logical and proof complexity theoretic strength of cyclic proofs in arithmetic, resolving questions (ii) and (iii), Sect. 7 of [33].

Further observations

Failure of cut-admissibility Stefano Berardi pointed out to me that, as a corollary of these results, we may formally conclude that the cut rule is not admissible in CA, or indeed any of its fragments $\mathrm{C}\Sigma_n$. The argument is as follows. Since $\mathrm{I}\Sigma_{n+1}$ proves the consistency of $\mathrm{I}\Sigma_n$, which is a Π_1 sentence, so does $\mathrm{C}\Sigma_n$ by (1). But then, by degeneralising, we arrive at an open Δ_0 formula which is not provable using only Σ_{n-1} formulae in CA, for otherwise it would be provable in $\mathrm{I}\Sigma_n$, by (3), which is impossible by Gödel's second incompleteness result. So indeed, not only is the cut not admissible in CA, but we may not even bound the logical complexity of proofs of even open bounded formulae. See, e.g., [12, 21] for further discussions on the provability of consistency principles for fragments of arithmetic.

Provably total functions of $\mathrm{C}\Delta_0$ As a corollary of the results (1) and (3), we have that, for $n \geq 1$, the provably total functions of $\mathrm{C}\Sigma_n$ (i.e. its Π_2-theorems) are precisely those of $\mathrm{I}\Sigma_{n+1}$. This apparently leaves open a gap for the case of $\mathrm{C}\Delta_0$ (equivalently, $\mathrm{C}\Sigma_0$). However, notice that, since $\mathrm{C}\Delta_0$ is Π_1-axiomatised (namely by the universal closures of conclusions of cyclic proofs containing only Δ_0 formulae), we have that it is a 'bounded' theory; therefore, by Parikh's theorem (cf. [27]), $\mathrm{C}\Delta_0$ proves the totality of just the functions in the *linear-time hierarchy*, and hence actually coincides with the provably total functions of $\mathrm{I}\Delta_0$. See, e.g., [12, 13] for further discussions on the provably total functions of fragments of (bounded) arithmetic.

Interpreting ordinary inductive definitions in arithmetic In earlier work by Brotherston and Simpson, cyclic proofs were rather considered over a system of FO logic extended by 'ordinary' *Martin-Löf* inductive definitions [25], known as FOL_{ID} [6, 10, 11]. Berardi and Tatsuta showed in [4] that the cyclic system CLKID^ω for FOL_{ID} is equivalent to the inductive system LKID, when at least arithmetic is present, somewhat generalising Simpson's result [33]. We point out that the two results are arguably equipotent since ordinary Martin-Löf inductive definitions can be *interpreted* in arithmetic, with the necessary properties provable. This is because the closure ordinals for ordinary Martin-Löf inductive definitions are $\leq \omega$, and so a Σ_1 inductive construction of 'approximants' can always determine whether an individual belongs to an inductive predicate or not. Notice that this was crucial for our use of ArAcc over the SO acceptance formula. This is also precisely the role of the 'stage numbers' in [4]; there the fresh inductive predicates P' can be expressed as Δ_0-formulae. In particular, this means that $\mathsf{CLKID}^\omega(+\mathsf{PA})$ is *conservative* over CA. We stress that the interest behind the results of [4] is rather the structural nature of the transformations, but this observation also exemplifies why CA is a natural and canonical object of study, cf. [33].

Towards propositional proof complexity One perspective gained from this work comes in the setting of *propositional proof complexity* (see, e.g., [13, 24]). From the results and methods herein, we may formalise in $\mathrm{C}\Delta_0(X)$, say, a proof of the relativised version of the (finitary) pigeonhole principle, which is known to be unprovable in $\mathrm{I}\Delta_0(X)$ due to lower bounds on propositional proofs of bounded depth [23, 29].

At the same time the 'Paris-Wilkie' translation [28], which fundamentally links $\mathrm{I}\Delta_0$ to bounded-depth proofs, works locally on a proof, at the level of formulae. Consequently one may still apply the translation to the lines of a $\mathrm{C}\Delta_0$ proof to obtain small 'proof-like' objects containing only formulae of bounded depth, and a cyclic proof structure. One would expect that this corresponds to some strong form of 'extension', since it is known that adding usual extension to bounded systems already yields full 'extended Frege' proofs. However at the same time, some of this power has been devolved to the proof structure rather than simply at the level of the formula, and so could yield insights into how to prove simulations between fragments of Hilbert-Frege systems with extension.

Acknowledgements

I would like to thank Stefano Berardi, James Brotherston and Alex Simpson for many fruitful discussions on this subject, and for encouraging me to undertake this research. I would also like to thank the anonymous reviewers for a previous version of this work for their useful comments.

References

[1] Bahareh Afshari and Graham E. Leigh. Cut-free completeness for modal mu-calculus. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12, 2017.

[2] David Baelde, Amina Doumane, and Alexis Saurin. Infinitary proof theory: the multiplicative additive case. In *25th EACSL Annual Conference on Computer Science Logic, CSL 2016, August 29 - September 1, 2016, Marseille, France*, pages 42:1–42:17, 2016.

[3] Stefano Berardi and Makoto Tatsuta. Classical system of martin-löf's inductive definitions is not equivalent to cyclic proof system. In *Foundations of Software Science and Computation Structures -*

20th International Conference, FOSSACS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings, pages 301–317, 2017.

[4] Stefano Berardi and Makoto Tatsuta. Equivalence of inductive definitions and cyclic proofs under arithmetic. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12, 2017.

[5] James Brotherston. Cyclic proofs for first-order logic with inductive definitions. In *Automated Reasoning with Analytic Tableaux and Related Methods, International Conference, TABLEAUX 2005, Koblenz, Germany, September 14-17, 2005, Proceedings*, pages 78–92, 2005.

[6] James Brotherston. *Sequent calculus proof systems for inductive definitions*. PhD thesis, University of Edinburgh, 2006.

[7] James Brotherston, Richard Bornat, and Cristiano Calcagno. Cyclic proofs of program termination in separation logic. In *Proceedings of the 35th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2008, San Francisco, California, USA, January 7-12, 2008*, pages 101–112, 2008.

[8] James Brotherston, Dino Distefano, and Rasmus Lerchedahl Petersen. Automated cyclic entailment proofs in separation logic. In *CADE-23 - 23rd International Conference on Automated Deduction, Wroclaw, Poland, July 31 - August 5, 2011. Proceedings*, pages 131–146, 2011.

[9] James Brotherston, Nikos Gorogiannis, and Rasmus Lerchedahl Petersen. A generic cyclic theorem prover. In *Programming Languages and Systems - 10th Asian Symposium, APLAS 2012, Kyoto, Japan, December 11-13, 2012. Proceedings*, pages 350–367, 2012.

[10] James Brotherston and Alex Simpson. Complete sequent calculi for induction and infinite descent. In *22nd IEEE Symposium on Logic in Computer Science (LICS 2007), 10-12 July 2007, Wroclaw, Poland, Proceedings*, pages 51–62, 2007.

[11] James Brotherston and Alex Simpson. Sequent calculi for induction and infinite descent. *J. Log. Comput.*, 21(6):1177–1216, 2011.

[12] Samuel R Buss. *Handbook of proof theory*, volume 137. Elsevier, 1998.

[13] Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. Cambridge University Press, New York, NY, USA, 1st edition, 2010.

[14] Anupam Das. On the logical complexity of cyclic arithmetic, 2017. Preprint. http://www.anupamdas.com/wp/log-comp-cyc-arith/.

[15] Anupam Das and Damien Pous. A cut-free cyclic proof system for kleene algebra. In *Automated Reasoning with Analytic Tableaux and Related Methods - 26th International Conference, TABLEAUX 2017, Brasília, Brazil, September 25-28, 2017, Proceedings*, pages 261–277, 2017.

[16] Christian Dax, Martin Hofmann, and Martin Lange. A proof system for the linear time μ-calculus. In *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science, 26th International Conference, Kolkata, India, December 13-15, 2006, Proceedings*, pages 273–284, 2006.

[17] Amina Doumane. Constructive completeness for the linear-time μ-calculus. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12, 2017.

[18] Amina Doumane, David Baelde, Lucca Hirschi, and Alexis Saurin. Towards completeness via proof search in the linear time μ-calculus: The case of büchi inclusions. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016*, pages 377–386, 2016.

[19] Jérôme Fortier. *Puissance expressive des preuves circulaires. (Expressive Power of Circular Proofs)*. PhD thesis, Aix-Marseille University, Aix-en-Provence, France, 2014.

[20] Jérôme Fortier and Luigi Santocanale. Cuts for circular proofs: semantics and cut-elimination. In *Computer Science Logic 2013 (CSL 2013), September 2-5, 2013, Torino, Italy*, pages 248–262, 2013.

[21] Richard Kaye. Models of peano arithmetic. 1991.

[22] Leszek Aleksander Kolodziejczyk, Henryk Michalewski, Pierre Pradic, and Michał Skrzypczak. The logical strength of büchi's decidability theorem. In *25th EACSL Annual Conference on Computer Science Logic, CSL 2016, August 29 - September 1, 2016, Marseille, France*, pages 36:1–36:16, 2016.

[23] Jan Krajíček, Pavel Pudlák, and Alan Woods. An exponential lower bound to the size of bounded depth frege proofs of the pigeonhole principle. *Random Structures & Algorithms*, 7(1):15–39, 1995.

[24] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory.* Cambridge University Press, New York, NY, USA, 1995.

[25] Per Martin-Lf. Hauptsatz for the intuitionistic theory of iterated inductive definitions. In J.E. Fenstad, editor, *Proceedings of the Second Scandinavian Logic Symposium*, volume 63 of *Studies in Logic and the Foundations of Mathematics*, pages 179 – 216. Elsevier, 1971.

[26] Damian Niwinski and Igor Walukiewicz. Games for the mu-calculus. *Theor. Comput. Sci.*, 163(1&2):99–116, 1996.

[27] Rohit Parikh. Existence and feasibility in arithmetic. *J. Symb. Log.*, 36(3):494–508, 1971.

[28] J.B. Paris and A.J. Wilkie. Δ_0 sets and induction. *Open Days in Model Theory and Set Theory, W. Guzicki, W. Marek, A. Pelc, and C. Rauszer, eds*, pages 237–248, 1981.

[29] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993. 10.1007/BF01200117.

[30] Reuben N. S. Rowe and James Brotherston. Automatic cyclic termination proofs for recursive procedures in separation logic. In *Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs, CPP 2017, Paris, France, January 16-17, 2017*, pages 53–65, 2017.

[31] Luigi Santocanale. A calculus of circular proofs and its categorical semantics. In *Foundations of Software Science and Computation Structures, 5th International Conference, FOSSACS 2002, Grenoble, France, April 8-12, 2002, Proceedings*, pages 357–371, 2002.

[32] Kurt Schtte. *Proof Theory.* Grundlehren der mathematischen Wissenschaften 225. Springer Berlin Heidelberg, 1977. Translation of Beweistheorie, 1968.

[33] Alex Simpson. Cyclic arithmetic is equivalent to peano arithmetic. In *Foundations of Software Science and Computation Structures - 20th International Conference, FOSSACS 2017, Proceedings*, pages 283–300, 2017.

[34] Christoph Sprenger and Mads Dam. On the structure of inductive reasoning: Circular and tree-shaped proofs in the μ-calculus. In *Foundations of Software Science and Computational Structures, 6th International Conference, FOSSACS 2003, Warsaw, Poland, April 7-11, 2003, Proceedings*, pages 425–440, 2003.