MR2900636 (Review) 03F20 03D15 68Q15
Cook, Stephen [Cook, Stephen A.] (3-TRNT-C); **Fontes, Lila** (3-TRNT-C)
Formal theories for linear algebra. (English summary)
Log. Methods Comput. Sci. **8** (2012), *no. 1,* 1:25, 31 *pp.*

From the introduction: "This paper is a contribution to bounded reverse mathematics, that part of proof complexity concerned with determining the computational complexity of concepts needed to prove theorems of interest in computer science. We are specifically interested in theorems of linear algebra over finite fields and the integers. The relevant complexity classes for each case have been well-studied in the computational complexity literature. The classes are $\oplus L$ and DET, associated with linear algebra over $\mathbb{Z}_2$ and $\mathbb{Z}$, respectively. We introduce formal theories $V\oplus L$ and $V\#L$ for $\oplus L$ and DET, each intended to capture reasoning in the corresponding class. Each theory allows induction over any relation in the associated complexity class, and the functions definable in each theory are exactly the functions in the class. In particular determinants and coefficients of the characteristic polynomial of a matrix can be defined.

"To study the question of which results from linear algebra can be proved in the theories we take advantage of Soltys's theory $\mathrm{LA_P}$ for formalizing linear algebra over an arbitrary field or integral domain. We present two interpretations of $\mathrm{LA_P}$: one into $V\oplus L$ and one into $V\#L$. Both interpretations translate theorems of $\mathrm{LA_P}$ to theorems in the corresponding theory, but the meaning of the theorems differs in the two translations since the ring elements range over $\mathbb{Z}_2$ in one and over $\mathbb{Z}$ in the other. We show that the theories prove some interesting properties of determinants, but leave open the question of whether the proofs of some basic theorems such as the Ca[y]ley-Hamilton Theorem can be formalized in the theories. We also leave open the question of whether the theories prove simple matrix identities such as $AB = I \to BA = I$. An affirmative answer would shed light on interesting questions in propositional proof complexity concerning the lengths of proofs required in various proof systems to prove tautology families corresponding to the identities."

Saeed Salehi

References

1. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES in P. *Annals of Mathematics*, 160:781–793, 2004. MR2123939 (2006a:11170)
2. Eric Allender. Arithmetic Circuits and Counting Complexity Classes. In Jan Krajicek, editor, *Complexity of computations and proofs*, pages 33–72. Quaderni di Matematica, 2004. MR2131405 (2005m:68071)
3. Eric Allender and Mitsunori Ogihara. Relationships Among *PL*, *#L*, and the Determinant. *RAIRO - Theoretical Informatics and Applications*, 30:1–21, 1996.
4. Maria Luisa Bonet, Samuel R. Buss, and Toniann Pitassi. Are there Hard Examples for Frege Systems? In P. Clote and J. B. Remmel, editors, *Feasible Mathematics II*, pages 30–56. Birkhauser, 1994. MR1322273 (96a:03066a)
5. Gerhard Buntrock, Carsten Damm, Ulrich Hertrampf, and Christoph Meinel. Structure and Importance of Logspace-MOD Class. *Mathematical Systems Theory*, 25:223–237, 1992. MR1151340 (93d:68029)
6. S. J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18:147–150, 1984. MR0760366 (85k:65111)

7. Mark Braverman, Raghav Kulkarni, and Sambuddha Roy. Space-Efficient Counting in Graphs on Surfaces. *Computational Complexity*, 18:601–649, 2009. MR2570452 (2011e:05234)
8. Stephen Cook and Lila Fontes. Formal Theories for Linear Algebra. In *Computer Science Logic*, volume LNCS 6247, pages 245–259. Springer, 2010. MR2755306 (2012d:68060)
9. Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity*. Cambridge University Press, 2010. Draft available from URL http://www.cs.toronto.edu/∼sacook. MR2589550 (2011g:03001)
10. S. A. Cook. A Taxonomy of Problems with Fast Parallel Algorithms. *Information and Control*, 64:2–22, 1985. MR0837088 (87k:68043)
11. Lila Fontes. Interpreting LAP into $V \oplus L$ and $V//L$. Draft available at www.cs.toronto.edu/∼fontes.
12. Lila Fontes. Formal Theories for Logspace Counting. Master's thesis, University of Toronto, 2009. Available at http://arxiv.org/abs/1001.1960.
13. Neil Immerman. *Descriptive Complexity*. Springer, 1999. MR1732784 (2001f:68044)
14. Emil Jeřábek. *Weak pigeonhole principle, and randomized computation*. PhD thesis, Faculty of Mathematics and Physics, Charles University, Prague, 2005.
15. Meena Mahajan and V. Vinay. Determinant: Combinatorics, Algorithms, and Complexity. *Chicago Journal of Theoretical Computer Science*, 5, 1997. MR1484546 (98m:15016)
16. Phuong Nguyen. *Bounded Reverse Mathematics*. PhD thesis, Department of Computer Science, University of Toronto, 2008.
17. Michael Soltys and S. A. Cook. The Proof Complexity of Linear Algebra. *Annals of Pure and Applied Logic*, 130:277–323, 2004. MR2092854 (2005g:03099)
18. Stephen Simpson. *Subsystems of Second Order Arithmetic*. Springer, 1999. MR1723993 (2001i:03126)
19. Michael Soltys-Kulinicz. *The Complexity of Derivations of Matrix Identities*. PhD thesis, University of Toronto, 2001. MR2702681

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.