Feasible combinatorial matrix theory

Polytime proofs for König's Min-Max and related theorems

Ariel Fernández
McMaster University
Hamilton, Canada
fernanag@mcmaster.ca

Michael Soltys
McMaster University
Hamilton, Canada
soltys@mcmaster.ca

***Abstract*—We show that the well-known König's Min-Max Theorem (KMM), a fundamental result in combinatorial matrix theory, can be proven in the first order theory $\mathbf{LA}$ with induction restricted to Σ_1^B formulas. This is an improvement over the standard textbook proof of KMM which requires Π_2^B induction, and hence does not yield feasible proofs — while our new approach does. $\mathbf{LA}$ is a weak theory that essentially captures the ring properties of matrices; however, equipped with Σ_1^B induction $\mathbf{LA}$ is capable of proving KMM, and a host of other combinatorial properties such as Menger's, Hall's and Dilworth's Theorems. Therefore, our result formalizes Min-Max type of reasoning within a feasible framework.**

I. Introduction

In this paper we are concerned with the complexity of formalizing reasoning about combinatorial matrix theory. We are interested in the strength of the bounded arithmetic theories necessary in order to prove the fundamental results of this field. We show, by introducing new proof techniques, that the logical theory $\mathbf{LA}$ with induction restricted to bounded existential matrix quantification is sufficient to formalize a large portion of combinatorial matrix theory.

Perhaps the most famous theorem in combinatorial matrix theory is the König's Mini-Max Theorem (KMM) which arises naturally in all areas of combinatorial algorithms — for example "network flows" with "min-cut max-flow" type of reasoning. See [1] for recent work related to formalizing proof of correctness of the Hungarian algorithm, which is an algorithm based on KMM. As far as we know, we give the first feasible proof of KMM.

As KMM is a cornerstone result, it has several counterparts in related areas of mathematics: Menger's Theorem, counting disjoint paths; Hall's Theorem, giving necessary and sufficient conditions for the existence of a "system of distinct representatives" of a collection of sets; Dilworth's Theorem, counting the number of disjoint chains in a poset, etc. We note that we actually show the equivalence of KMM with a *restricted* version of Menger's Theorem.

We show that KMM can be proven feasibly, and we do so with a new proof of KMM that relies on introducing a new notion ("diagonal property"). Furthermore, we show that the theorems related to KMM, and listed in the above paragraph, can also be proven feasibly; in fact, all these theorems are equivalent to KMM, and the equivalence can be shown in $\mathbf{LA}$. We believe that this captures the proof complexity of Min-Max reasoning.

Our results show that Min-Max reasoning can be formalized with uniform Extended Frege. It would be very interesting to know whether the techniques recently introduced by [2] could bring the complexity further down to quasi-polynomial Frege.

References

[1] D. T. M. Lê and S. A. Cook, "Formalizing randomized matching algorithms," *Logical Methods in Computer Science*, vol. 8, pp. 1–25, 2012.
[2] P. Hrubes and I. Tzameret, "Short proofs for the determinant identities," *CoRR*, vol. abs/1112.6265, December 2011.
[3] R. A. Brualdi and H. J. Ryser, *Combinatorial Matrix Theory*. Cambridge University Press, 1991.
[4] M. Soltys and S. Cook, "The complexity of derivations of matrix identities," *Annals of Pure and Applied Logic*, vol. 130, no. 1–3, pp. 207–275, December 2004.
[5] E. Jeřábek, "Weak pigeonhole principle, and randomized computation," Ph.D. dissertation, Faculty of Mathematics and Physics, Charles University, Prague, 2005.
[6] M. Soltys, "LA, permutations, and the Hajós calculus," *Theoretical Computer Science*, vol. 348, no. 2–3, pp. 321–333, December 2005.
[7] J. E. Hopcroft and R. M. Karp, "An $n^{5/2}$ algorithm for maximum matchings in bipartite graphs," *SIAM Journal on Computing*, vol. 2, no. 4, December 1973.
[8] M. Soltys and A. Fernandez, "A linear-time algorithm for computing minimum vertex covers from maximum matchings," October 2012, available from www.cas.mcmaster.ca/~soltys.
[9] K. Menger, "Zur allgemeinen kurventheorie," *Fund. Math*, vol. 10, no. 95-115, 1927.
[10] F. Göring, "Short proof of Menger's theorem," *Discrete Mathematics*, vol. 219, pp. 295–296, 2000. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0012365X00000881
[11] J. S. Pym, "A proof of Menger's theorem," *Monatshefte für Mathematik*, vol. 73, no. 1, pp. 81–83, 1969.
[12] P. Hall, "On representatives of subsets," in *Classic Papers in Combinatorics*, ser. Modern Birkhäuser Classics, I. Gessel and G.-C. Rota, Eds. Birkhäuser Boston, 1987, pp. 58–62.
[13] C. J. Everett and G. Whaples, "Representations of sequences of sets," *American Journal of Mathematics*, vol. 71, no. 2, pp. pp. 287–293, April 1949. [Online]. Available: http://www.jstor.org/stable/2372244
[14] P. R. Halmos and H. E. Vaughan, "The marriage problem," *American Journal of Mathematics*, vol. 72, no. 1, pp. pp. 214–215, Januar 1950. [Online]. Available: http://www.jstor.org/stable/2372148
[15] R. P. Dilworth, "A decomposition theorem for partially ordered sets," *Annals of Mathematics*, vol. 51, no. 1, pp. pp. 161–166, January 1950. [Online]. Available: http://www.jstor.org/stable/1969503
[16] M. A. Perles, "A proof of dilworth's decomposition theorem for partially ordered sets," *Israel Journal of Mathematics*, vol. 1, pp. 105–107, 1963.
[17] M. Soltys, "Feasible proofs of Szpilrajn's theorem: a proof-complexity framework for concurrent automata," *Journal of Automata, Languages and Combinatorics (JALC)*, vol. 16, no. 1, pp. 27–38, 2011.