

Generating Matrix Identities and Hard Instances for Strong Proof Systems

Fu Li* Iddo Tzameret†

June 8, 2014

Abstract. We study the complexity of generating identities of matrix rings. We establish an unconditional lower bound on the minimal number of generators needed to generate a matrix identity, where the generators are substitution instances of elements from any given finite basis of the matrix identities. Based on our findings, we propose to consider matrix identities (and their encoding) as hard instances for strong proof systems, and we initiate this study under different settings and assumptions. We show that this direction, under certain conditions, can potentially lead up to exponential-size lower bounds on arithmetic proofs, which are proofs of polynomial identities operating with arithmetic circuits and whose axioms are the polynomial-ring axioms (these proofs serve as an algebraic analogue of the Extended Frege propositional proof system). We also discuss shortly the applicability of our approach to strong propositional proof systems.

Formally, the algebraic problem we study is this: for a field $\mathbb{F}$ let A be a non-commutative (associative) $\mathbb{F}$ -algebra (e.g., the algebra $\text{Mat}_d(\mathbb{F})$ of $d \times d$ matrices over $\mathbb{F}$). We say that a non-commutative polynomial $f(x_1, \dots, x_n)$ over $\mathbb{F}$ is an *identity* of A , if for all $\bar{c} \in A^n$, $f(\bar{c}) = 0$. Let $\mathcal{B}$ be a set of non-commutative polynomials that forms a *basis* for the identities of A , in the following sense: for every identity f of A there exist non-commutative polynomials $g_1, \dots, g_k$, for some k , that are *substitution instances* of polynomials from $\mathcal{B}$, such that f is in the (two-sided) ideal $\langle g_1, \dots, g_k \rangle$. We ask the following question: *Given $A, \mathcal{B}$ and f as above, what is the minimal number k of such generators $g_1, \dots, g_k$ for which $f \in \langle g_1, \dots, g_k \rangle$?* In particular, we focus on the case where the algebra A is $\text{Mat}_d(\mathbb{F})$, and $\mathbb{F}$ has characteristic 0. Our main technical contribution is a generalization of the lower bound presented in Hrubeš [1] (for the case $d = 1$) to *any* $d > 2$:

- For every natural number $d > 2$ and *every* finite basis $\mathcal{B}$ for the identities of

*Institute for Theoretical Computer Science, The Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, Beijing. Supported in part by NSFC grant 61373002

†Institute for Theoretical Computer Science, The Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, Beijing tzameret@tsinghua.edu.cn Supported in part by the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, the National Natural Science Foundation of P. R. China; Grants 61033001, 61061130540, 61073174, 61373002.

$\text{Mat}_d(\mathbb{F})$, where $\mathbb{F}$ is of characteristic 0, there exists an identity f_n with n variables, that requires $\Omega(n^{2d})$ generators (i.e., substitution instances from $\mathcal{B}$) to generate.

The proof uses fundamental results from the theory of algebras with polynomial identities (PI-algebras) together with a generalization of the arguments in [1].

The full paper is available at [2].

Acknowledgements

We wish to thank V. Arvind, Michael Forbes, Kristoffer Arnsfelt Hansen, Jan Krajíček, Satya Lokam, Periklis Papakonstantinou, Youming Qiao, Ran Raz and Amir Shpilka for useful discussions related to this work. We are also greatly indebted to Vesselin Drensky for his help with the bibliography and providing us with his monograph.

References

- [1] Pavel Hrubeš. How much commutativity is needed to prove polynomial identities? *Electronic Colloquium on Computational Complexity, ECCC*, (Report no.: TR11-088), June 2011. [\(document\)](#)
- [2] Fu Li and Iddo Tzameret. Generating matrix identities and hard instances for strong proof systems. *Electronic Colloquium on Computational Complexity, TR13-185*, 2013. arXiv:1312.6242 [cs.CC] <http://arxiv.org/abs/1312.6242>. [\(document\)](#)