

io-port 06070930**Jansen, Maurice; Santhanam, Rahul****Stronger lower bounds and randomness-hardness trade-offs using associated algebraic complexity classes.**

Dürr, Christoph (ed.) et al., STACS 2012. 29th international symposium on theoretical aspects of computer science, Paris, France, February 29th – March 3rd, 2012. Wadern: Schloss Dagstuhl – Leibniz Zentrum für Informatik (ISBN 978-3-939897-35-4). LIPICS – Leibniz International Proceedings in Informatics 14, 519-530, electronic only (2012).

Summary: We associate to each Boolean language complexity class \mathcal{C} the algebraic class $a \cdot \mathcal{C}$ consisting of families of polynomials $\{f_n\}$ for which the evaluation problem over \mathbb{Z} is in \mathcal{C} . We prove the following lower bound and randomness-to-hardness results: 1. If polynomial identity testing (PIT) is in NSUBEXP then $a \cdot \text{NEXP}$ does not have poly size constant-free arithmetic circuits. 2. $a \cdot \text{NEXP}^{\text{RP}}$ does not have poly size constant-free arithmetic circuits. 3. For every fixed k , $a \cdot \text{MA}$ does not have arithmetic circuits of size n^k . Items 1 and 2 strengthen two results due to *V. Kabanets* and *R. Impagliazzo* [Comput. Complexity 13, No. 1–2, 1–46 (2004; Zbl 1089.68042)]. The third item improves a lower bound due to the second author [SIAM J. Comput. 39, No. 3, 1038–1061 (2009; Zbl 1192.68302)]. We consider the special case low-PIT of identity testing for (constant-free) arithmetic circuits with low formal degree, and give improved hardness-to-randomness trade-offs that apply to this case. Combining our results for both directions of the hardness-randomness connection, we demonstrate a case where derandomization of PIT and proving lower bounds are equivalent. Namely, we show that $\text{low-PIT} \in \text{i.o-NTIME}[2^{n^{o(1)}}]/n^{o(1)}$ if and only if there exists a family of multilinear polynomials in $a \cdot \text{NE}/\text{lin}$ that requires constant-free arithmetic circuits of super-polynomial size and formal degree.

Keywords: computational complexity; circuit lower bounds; polynomial identity testing; derandomization
doi:10.4230/LIPIcs.STACS.2012.519