

# Superpolynomial Lower Bounds for Monotone Span Programs \*

László Babai <sup>†</sup>      Anna Gál<sup>‡</sup>      Avi Wigderson<sup>§</sup>

## Abstract

In this paper we obtain the first superpolynomial lower bounds for *monotone span programs* computing explicit functions. The best previous lower bound was  $\Omega(n^{5/2})$  by Beimel, Gál, Paterson [BGP]; our proof exploits a general combinatorial lower bound criterion from that paper. Our lower bounds are based on an analysis of Paley-type bipartite graphs via Weil's character sum estimates. We prove an  $n^{\Omega(\log n / \log \log n)}$  lower bound for the size of monotone span programs for the clique problem. Our results give the first superpolynomial lower bounds for linear secret sharing schemes.

We demonstrate the surprising power of monotone span programs by exhibiting a function computable in this model in linear size while requiring superpolynomial size monotone circuits and exponential size monotone formulae. We also show that the perfect matching function can be computed by polynomial size (non-monotone) span programs over arbitrary fields.

---

\*Part of this work has been presented at the 28th ACM STOC'96. The second two authors wish to thank DIMACS for its hospitality and acknowledge its supporting agencies, the National Science Foundation under contract STC-91-19999 and the New Jersey Commission on Science and Technology.

<sup>†</sup>Department of Computer Science, University of Chicago, Chicago IL 60637-1504. E-mail: [laci@cs.uchicago.edu](mailto:laci@cs.uchicago.edu). Supported in part by NSA grant MSPR-96G-184.

<sup>‡</sup>Dept. of Computer Sciences, The University of Texas at Austin, Austin, TX 78712. Email: [panni@cs.utexas.edu](mailto:panni@cs.utexas.edu). Most of this work was done while at the Institute for Advanced Study, Princeton supported by NSF Grant DMS-9304580, and DIMACS at Princeton University.

<sup>§</sup>Institute of Computer Science, Hebrew University, Jerusalem, Israel. Most of this work was done while visiting the Institute for Advanced Study, Princeton, and DIMACS at Princeton University. Research supported by the Sloan Foundation, American-Israeli BSF grant 92-00106, and a grant from the Israel Research Foundation, founded by the Israel Academy of Sciences and Humanities. Email: [avi@cs.huji.ac.il](mailto:avi@cs.huji.ac.il).