The Internal and External Algebraic Structure of Complexity Classes

Lance Fortnow*
Department of Computer Science
The University of Chicago
1100 East 58th Street
Chicago, Illinois 60637

Abstract

The report forms a bibliographic companion to a talk given at the Workshop on Algebraic Methods in Complexity Theory in Madras, India in December, 1994. In this report we will give many references that the reader may find useful in studying the internal and external algebraic structure of complexity classes.

1 Introduction

The external algebraic structure of a complexity class refers to algebraic closure properties that a class may possess such as the fact that #P functions are closed under addition and multiplication. The internal algebraic structure refers to how we can give alternate definitions of complexity classes based on building these classes from algebraic operations on top of very simple functions. For example #P functions in some sense look like low-degree polynomials over their inputs.

This report will give a list of many references related to the internal and external algebraic structure of complexity classes. Please note that this report is in no sense complete and only meant as a place for interested researchers to find some references in this area.

2 Study of Structure

This section lists some papers that have studied algebraic structures of complexity classes in their own right.

*Email: fortnow@cs.uchicago.edu. Partially supported by NSF grant CCR 92-53582.

Papers on Study of Structure

[1] S. Arora, R. Impagliazzo, and U. Vazirani. Relativizing versus nonrelativizing techniques: The role of local checkability. Manuscript, University of California, Berkeley, 1992.

[2] L. Babai and L. Fortnow. Arithmetization: A new method in structural complexity theory. *Computational Complexity*, 1(1):41–66, 1991.

[3] S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994.

[4] A. Razborov and S. Rudich. Natural proofs. In *Proceedings of the 26th ACM Symposium on the Theory of Computing*, pages 204–213. ACM, New York, 1994.

3 External Structure

In this section we list papers that prove theorems using the external structure of complexity theory. These theorems generally show that classes have certain closure properties based on their external algebraic structure. We feel that this study may prove more important as it may lead us to understand how to separate complexity classes. If two complexity classes do not have the same external algebraic structure then they cannot coincide.

Papers Using External Structure

[1] L. Babai and S. Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.

[2] R. Beigel and J. Gill. Counting classes: Thresholds, parity, mods, and fewness. *Theoretical Computer Science*, 103:3–23, 1992.

[3] J. Cai, A. Condon, and R. Lipton. On bounded round multi-prover interactive proof systems. In *Proceedings of the 5th IEEE Structure in Complexity Theory Conference*, pages 45–54. IEEE, New York, 1990.

[4] J. Cai, A. Condon, and R. Lipton. On games of incomplete information. *Theoretical Computer Science*, 103(1):25–38, 1992.

[5] A. Condon and R. J. Lipton. On the complexity of space bounded interactive proofs. In *Proceedings of the 30th IEEE Symposium on Foundations of Computer Science*, pages 462–467. IEEE, New York, 1989.

[6] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 73–90. JAI Press, Greenwich, 1989.

[7] U. Hertrampf. Relations among MOD classes (note). *Theoretical Computer Science*, 74:325–328, 1990.

[8] R. Impagliazzo and D. Zuckerman. How to recycle random bits. In *Proceedings of the 30th IEEE Symposium on Foundations of Computer Science*, pages 248–253. IEEE, New York, 1989.

[9] J. Köbler and U. Schöning and J. Toran. On counting and approximation. *Acta Informatica*, 26:363–379, 1989.

[10] J. Köbler, U. Schöning, S. Toda, and J. Torán. Turing machines with few accepting computations and low sets for PP. *Journal of Computer and System Sciences*, 44(2):272–286, 1992.

[11] J. Köbler, U. Schöning, and J. Torán. Graph isomorphism is low for PP. *Computational Complexity*, 2(4):301–330, 1992.

[12] R. Mathon. A note on the graph isomorphism counting problem. *Information Processing Letters*, 8:131–132, 1979.

[13] L. Valiant and V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.

4 Internal Structure

In this section, we list papers that use the internal algebraic structure of complexity classes to prove theorems about these classes. By expressing a complexity class in terms of simple algebraic operations, we can often "simulate" that class using other means. Many important circuit complexity and interactive proof system results use this method.

Papers Using Internal Structure

[1] M. Abadi, J. Feigenbaum, and J. Kilian. On hiding information from an oracle. *Journal of Computer and System Sciences*, 39:21–50, 1989.

[2] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and hardness of approximation problems. In *Proceedings of the 33rd IEEE Symposium on Foundations of Computer Science*, pages 14–23. IEEE, New York, 1992.

[3] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. In *Proceedings of the 33rd IEEE Symposium on Foundations of Computer Science*, pages 2–13. IEEE, New York, 1992.

[4] L. Babai, L. Fortnow, L. Levin, and M. Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the 23rd ACM Symposium on the Theory of Computing*, pages 21–31. ACM, New York, 1991.

[5] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[6] L. Babai, L. Fortnow, N. Nisan, and A. Wigderson. BPP has subexponential simulations unless EXPTIME has publishable proofs. In *Proceedings of the 6th IEEE Structure in Complexity Theory Conference*, pages 213–219. IEEE, New York, 1991.

[7] D. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *Journal of Computer and System Sciences*, 38(1):150–164, 1989.

[8] D. Beaver and J. Feigenbaum. Hiding instances in multioracle queries. In *Proceedings of the 7th Symposium on Theoretical Aspects of Computer Science*, volume 415 of *Lecture Notes in Computer Science*, pages 37–48. Springer, Berlin, 1990.

[9] D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway. Security with low communication overhead. In *Advances in Cryptology – Crypto '90*, volume 537 of *Lecture Notes in Computer Science*, pages 62–76. Springer, Berlin, 1991.

[10] R. Beigel and J. Tarui. On ACC. In *Proceedings of the 32nd IEEE Symposium on Foundations of Computer Science*, pages 783–792. IEEE, 1991.

[11] M. Blum, M. Luby, and R. Rubinfeld. Self-testing and self-correcting programs, with applications to numerical programs. *Journal of Computer and System Sciences*, 47:549–595, 1993.

[12] D. Bovet, P. Crescenzi, and R. Silvestri. A uniform approach to define complexity classes. *Theoretical Computer Science*, 104:263–283, 1992.

[13] J. Cai and M. Furst. PSPACE survives constant-width bottlenecks. *International Journal of Foundations of Computer Science*, 2:67–76, 1991.

[14] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy. Approximating clique is almost NP-complete. In *Proceedings of the 32nd IEEE*

Symposium on Foundations of Computer Science, pages 2–12. IEEE, New York, 1991.

[15] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proceedings of the 24th ACM Symposium on the Theory of Computing*, pages 733–744. ACM, New York, 1992.

[16] L. Fortnow and C. Lund. Interactive proof systems and alternating time-space complexity. *Theoretical Computer Science A*, 113:55–73, 1993.

[17] N. Linial, Y. Mansour, and N. Nisan. Constant depth circuits, fourier transform, and learnability. *Journal of the ACM*, 40(3):607–620, 1993.

[18] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.

[19] K. Mulmuley, U. Vazirani, and V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987.

[20] N. Nisan and M. Szegedy. On the degree of boolean functions as real polynomial. In *Proceedings of the 24th ACM Symposium on the Theory of Computing*, pages 462–467. ACM, New York, 1992.

[21] N. Nisan and A. Wigderson. Hardness vs. randomness. In *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, pages 2–11. IEEE, New York, 1988.

[22] A. Razborov. Lower bounds of monotone complexity of the logical permanent function. *Mathematical Notes of the Academy of Sciences of the USSR*, 37:485–493, 1985.

[23] A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

[24] A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Combinatorica*, 10(1):81–93, 1990.

[25] A. Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.

[26] A. Shen. IP = PSPACE: A simplified proof. *Journal of the ACM*, 39(4):878–880, 1992.

5 Internal and External Structure

The papers that we find most interesting use both the internal and external structure of complexity classes. These papers use the internal structure to "simulate" the classes and the external structure to keep these operations within the class. This section includes some of the most important results in complexity theory.

Papers Using Both Internal and External Structure

[1] E. Allender. A note on the power of threshold circuits. In *Proceedings of the 30th IEEE Symposium on Foundations of Computer Science*, pages 580–584. IEEE, New York, 1989.

[2] R. Beigel. Perceptrons, PP and the polynomial hierarchy. In *Proceedings of the 7th IEEE Structure in Complexity Theory Conference*, pages 14–19. IEEE, New York, 1992.

[3] R. Beigel, N. Reingold, and D. Spielman. The perceptron strikes back. In *Proceedings of the 6th IEEE Structure in Complexity Theory Conference*, pages 286–291. IEEE, New York, 1991.

[4] R. Beigel, N. Reingold, and D. Spielman. PP is closed under intersection. *Journal of Computer and System Sciences*, 1994. To appear. Paper also appeared in Proceedings of 23rd STOC conference, 1991, pages 1-9.

[5] D. Lapidot and A. Shamir. Fully parallelized multi prover protocols for NEXP-time. In *Proceedings of the 32nd IEEE Symposium on Foundations of Computer Science*, pages 13–18. IEEE, New York, 1991.

[6] A. Razborov. Bounded Arithmetic and lower bounds in Boolean complexity. *Feasible Mathematics II*, 1994. To appear.

[7] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on the Theory of Computing*, pages 77–82. ACM, New York, 1987.

[8] J. Tarui. Probabilistic polynomials, AC^0 functions and the polynomial-time hierarchy. *Theoretical Computer Science A*, 113:167–183, 1993.

[9] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[10] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 21(2):316–328, 1992.

[11] S. Toda and O. Watanabe. Polynomial time 1-turing reductions from $\#PH$ to $\#P$. *Theoretical Computer Science*, page to appear, 1991.

[12] L. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.

[13] A. Yao. On ACC and threshold circuits. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 619–631. IEEE, New York, 1990.