MR2796057 (2012c:68097) 68Q25 20M05
Kambites, Mark (4-MANC-SM)

Generic complexity of finitely presented monoids and semigroups. (English summary)

Comput. Complexity **20** (2011), *no. 1,* 21–50.

From the introduction: "The main aim of this paper is to study generic properties of finitely presented monoids and semigroups and hence to understand the generic-case complexity of uniform decision problems for monoids and semigroups. Our main results show that, with respect to a number of very natural stratifications, the generic finite monoid presentation (over a given alphabet and with a given number of generators) satisfies small overlap conditions. Small overlap conditions are natural semigroup-theoretic analogues of the small cancellation conditions extensively used by combinatorial group theorists, and so, our main result can be viewed as loosely analogous (although our objectives and hence our formalism are rather different) to the well-known fact, first asserted by M. Gromov [in *Essays in group theory*, 75–263, Math. Sci. Res. Inst. Publ., 8, Springer, New York, 1987; MR0919829 (89e:20070)] and proved in detail by A. Yu. Ol′shanskii [Internat. J. Algebra Comput. **2** (1992), no. 1, 1–17; MR1167524 (93j:20068)], that the generic finitely presented group is word hyperbolic.

"These results immediately tell us a great deal about the algebraic structure of the generic finitely presented monoid. For example, we learn that it is $\mathcal{J}$-trivial (that is, every element generates a distinct principal ideal) and hence torsion-free with no nontrivial subgroups. Even more important, by recent results of the author, the uniform word problem for such presentations is solvable in (worst-case RAM) time linear in the word lengths and quadratic in the presentation size. Since it can be checked in (worst-case RAM) polynomial time whether a presentation satisfies a small overlap condition, it follows that the uniform word problem for finitely presented monoids is generically solvable in polynomial time (in the RAM model, linear in the word lengths and quadratic in the presentation size). All of these results apply equally to semigroups without identity elements.

"An additional objective of this article is to provide a relatively gentle exposition of generic sets, generic properties and generic-case complexity, in a form fully intelligible to the reader without a specialist algebraic background. Monoid presentations are combinatorially simpler objects than group presentations; the relatively straightforward combinatorial nature of many of our proofs should allow them to double as detailed worked examples to give the reader a feel for generic-case complexity." *Saeed Salehi*

References

1. M. Bóna (2002). *A walk through combinatorics*. World Scientific Publishing Co. Inc., River Edge, NJ. ISBN 981-02-4900-4, xviii+406. MR1936456
2. G. B. Dantzig (1951). Maximization of a linear function of variables subject to linear inequalities. In *Activity Analysis of Production and Allocation*, Cowles Commission Monograph No. 13, 339–347. John Wiley & Sons Inc., New York, N.Y. MR0056260 (15,47k)
3. A. Duncan & R. H. Gilman (2004). Word hyperbolic semigroups. *Math. Proc. Cambridge Philos. Soc.* **136**(3), 513–524. ISSN 0305-0041. MR2055042 (2004m:20106)
4. R. Gilman, A. G. Miasnikov, A. D. Myasnikov & A. Ushakov (2007). Report

on Generic Case Complexity. *Herald of Omsk University* 103–110. Available online at http://www.acc.stevens.edu/Files/GC/gc_survey.pdf.

5. M. Gromov (1987). Hyperbolic groups. In *Essays in Group Theory*, volume 8 of *Math. Sci. Res. Inst. Publ.*, 75–263. Springer, New York. MR0919829 (89e:20070)
6. Y. Gurevich (1991). Average case complexity. In *Automata, languages and programming (Madrid, 1991)*, volume 510 of *Lecture Notes in Comput. Sci.*, 615–628. Springer, Berlin. MR1129940
7. P. M. Higgins (1992). *Techniques of semigroup theory*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York. ISBN 0-19-853577-5, x+258. With a foreword by G. B. Preston. MR1167445 (93d:20101)
8. M. Kambites (2009a). Small overlap monoids I: the word problem. *J. Algebra* **321**, 2187–2205. MR2501517 (2011a:20141)
9. M. Kambites (2009b). Small overlap monoids II: automatic structures and normal forms. *J. Algebra* **321**, 2302–2316. MR2501522 (2011a:20142)
10. I. Kapovich, A. Myasnikov, P. Schupp &V. Shpilrain (2003). Generic-case complexity, decision problems in group theory, and random walks. *J. Algebra* **264**(2), 665–694. ISSN 0021-8693. MR1981427 (2005m:20080)
11. V. Klee & G. J. Minty (1972). How good is the simplex algorithm? In *Inequalities, III (Proc. Third Sympos., Univ. California, Los Angeles, Calif., 1969*; *dedicated to the memory of Theodore S. Motzkin),* 159–175. Academic Press, New York. MR0332165 (48 #10492)
12. R. C. Lyndon & P. E. Schupp (1977). *Combinatorial Group Theory*. Springer-Verlag. MR0577064 (58 #28182)
13. A. Markov (1947). On the impossibility of certain algorithms in the theory of associative systems. *C.R. (Doklady) Acad. Sci. URSS (N.S.)* **55** 583–586. MR0020528 (8,558c)
14. A. Yu. Ol'shanskiĭ (1992). Almost every group is hyperbolic. *Internat. J. Algebra Comput.* **2**(1), 1–17. ISSN 0218-1967. MR1167524 (93j:20068)
15. E. L. Post (1947). Recursive unsolvability of a problem of Thue. *J. Suybolic Loagc* **12**, 1–11. ISSN 0022-4812. MR0020527 (8,558b)
16. J. H. Remmers (1971). *Some algorithmic problems for semigroups: a geometric approach*. Ph.D. thesis, University of Michigan. MR2620684
17. J. H. Remmers (1980). On the geometry of semigroup presentations. *Adv. in Math.* **36**(3), 283–296. ISSN 0001-8708. MR0577306 (81m:20074)
18. D. Ruinskiy, A. Shamir & B. Tsaban (2007). Length-based cryptanalysis: the case of Thompson's group. *J. Math. Cryptol.* **1**, 359–372. MR2441065 (2010m:94121)
19. J. Sakarovitch (1987). Easy Multiplications I. The Realm of Kleene's Theorem. *Inform. and Comput.* **74**, 173–197. MR0906959 (88m:68024)
20. V. Shpilrain & A. Ushakov (2005). Thompson's group and public key cryptography. *Lecture Notes in Computer Science* **3531**.
21. V. Shpilrain & G. Zapata (2006). Combinatorial group theory and public key cryptography. *Appl. Algebra Engrg. Comm. Comput.* **17**(3–4), 291–302. ISSN 0938-1279. MR2233788 (2007b:94254)

Note: This list reflects references listed in the original paper as accurately as possible with no attempt to correct errors.