Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2018 vol.10936 LNCS, pages 20-29

Polynomial-time presentations of algebraic number fields

Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2018, Springer International Publishing AG, part of Springer Nature. Using an extension of the notion of polynomial time presentable structure we show that some natural presentations of the ordered field $\mathbb{R}$algof algebraic reals and of the field $\mathbb{C}$algof algebraic complex numbers are polynomial-time equivalent to each other and are polynomial time. We also establish upper complexity bounds for the problem of rational polynomial evaluation in $\mathbb{C}$algand for the problem of root-finding for polynomials in $\mathbb{C}$alg[x] which improve the previously known bound.

http://dx.doi.org/10.1007/978-3-319-94418-0_2

Keywords

Algebraic number, Complexity bound, Ordered field, Polynomial, Polynomial-time presentable structure

References

[1] Ershov, Y.L., Goncharov, S.S.: Constructive Models. Plenum, New York (1999)

[2] Stoltenberg-Hansen, V., Tucker, J.V.: Effective algebras. In: Handbook of Logic in Computer Science: Semantic Modelling, vol. 4, pp. 357–526. Oxford University Press, Oxford (1995)

[3] Rabin, M.O.: Computable algebra, general theory and theory of computable fields. Trans. Am. Math. Soc. 95, 341–360 (1960)

[4] Ershov, Y.L.: Theorie der Nummerierungen III. Ziets. Math. Logik Grundl. Math. 23, 289–371 (1977)

[5] Nerode, A., Remmel, J.B.: Complexity theoretic algebra I, vector spaces over finite fields. In: Proceedings of Structure in Complexity, 2nd Annual Conference, pp. 218–239. Computer Sci. Press, New York (1987)

[6] Cenzer, D., Remmel, J.B.: Complexity theoretic model theory and algebra. In: Handbook of Recursive Mathematics, vol. 1. Elsevier, New York City (1998)

[7] Cenzer, D., Remmel, J.: Polynomial time versus recursive models. Ann. Pure Appl. Log. 54, 17–58 (1991)

[8] Basu, S., Pollack, R., Roy, M.: Algorithms in Real Algebraic Geometry. Springer, Heidelberg (2006). https://doi.org/10.1007/3-540-33099-2

[9] Aho, A.V., Hopcroft, J.E., Ullman, J.D.: The Design and Analysis of Computer Algorithms. Addison-Wesley Pub. Co., Boston (1974)

[10] Alaev, P.E.: Structures computable in polynomial time I. Algebra Log. 55(6), 421– 435 (2016). https://doi.org/10.1007/s10469-017-9416-y

[11] Van der Waerden, B.L.: Algebra. Springer, Berlin (1967)

[12] Balcázar, J.L., Díaz, J., Gabarró, J., Structural, C.I.: Structural Complexity I. EATCS, vol. 11. Springer, Heidelberg (1988). https://doi.org/10.1007/978-3-642-97062-7

[13] Akritas, A.G.: Elements of Computer Algebra with Applications. Wiley, New York (1989)

[14] Collins, G.E., Loos, R.: Real zeros of polynomials. In: Buchberger, B., Collins, G.E., Loos, R., Albrecht, R. (eds.) Computer Algebra: Symbolic and Algebraic Computations. COMPUTING, vol. 4, pp. 83–94. Springer, Vienna (1982). https://doi.org/10.1007/978-3-7091-7551-4 7

[15] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. 261, 515–534 (1982)

[16] Loos, R.: Computing in algebraic extensions. In: Buchberger, B., Collins, G.E., Loos, R. (eds.) Computer Algebra: Symbolic and Algebraic Computations. COMPUTING, vol. 4, pp. 173–187. Springer, Vienna (1982). https://doi.org/10.1007/978-3-7091-3406-1 12

[17] Coste, M., Roy, M.F.: Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. J. Symb. Comput. 5, 121–129 (1988)

[18] Schrijver, A.: Theory of Linear and Integer Programming. Wiley, New York (1986)

[19] Jian-Ping, Z.: On the degree of extensions generated by finitely many algebraic numbers. J. Number Theory 34, 133–141 (1990)

[20] Collins, G.E.: The Calculation of multivariate polynomial resultants. J. Assoc. Comput. Mach. 18(4), 515–532 (1971)

[21] Winkler, F.: Polynomial Algorithms in Computer Algebra. Springer, Wien (1996). https://doi.org/10.1007/978---7091-6571-3

[22] Cohen, H.: A Course in Computational Algebraic Number Theory. Springer, Heidelberg (1996). https://doi.org/10.1007/978-3-662-02945-9

[23] Yap, C.K.: Fundamental Problems in Algorithmic Algebra. Oxford University Press, Oxford (2000)

[24] Collins, G.E.: Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In: Brakhage, H. (ed.) GI-Fachtagung 1975. LNCS, vol. 33, pp. 134–183. Springer, Heidelberg (1975). https://doi.org/10.1007/3-540-07407-4 17