Journal of Scientific and Practical Computing Review
Vol. 3, No. 1 (2009) 55–55

COMPUTATIONAL GROUP THEORY AND A THEOREM BY LIPTON AND ZALCSTEIN

According to Charles C. Sims, Computational Group Theory is mainly to use computer to study groups especially to find some special groups such as the finitely-presented groups and permutation groups. In fact, another research direction dealing with the efficient algorithms for group-related computations such as orders of group elements, group decomposition, and group isomorphism is raising its importance in the recent years since quantum computing and elliptical curve cryptography.

An earlier work in 1978 by Lipton and Zalcstein is very remarkable. Here is their **Theorem**: **Let A(ε) be a probabilistic algorithm that the probability giving a wrong answer is at most ε. There is a constant time A(ε)-type-algorithm that can check a subgroup defined by the following equation:**

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} = 1, \text{ where } -2 < i_j < 2, \ j = 1, \cdots, n.$$

This theorem contains the Abelian group as an important case. Fu's paper in this issue gives a complete proof of this theorem in such the case.

References

[1] D. F. Holt, Bettina Eick, Bettina, Eamonn A. O'Brien, "Handbook of computational group theory", Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005. ISBN 1-58488-372-3

[2] C. C. Sims, "Computation with Finitely-presented Groups", Encyclopedia of Mathematics and its Applications, vol 48, Cambridge University Press, Cambridge, 1994. ISBN 0-521-43213-8.

[3]R. Lipton and Y. Zalcstein. Probabilistic algorithms for group-theoretic problems. Abstract appeared in ACM SIGSAM Bulletin, 1978.