Existence of Minimal Logarithmic Signature for Finite Simple Groups

A. R. Ashrafi[1] and A. R. Rahimipour[2]

[1]Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317-51116, I. R. Iran

[2]Department of Mathematics, Faculty of Science, University of Qom, P.O. Box 37161−46611, Qom, I. R. Iran

March 31, 2015

Abstract

A logarithmic signature (LS for short) of a finite group G is a sequence $\alpha = [A_1, \cdots, A_s]$ of subsets of G such that every element $g \in G$ can be uniquely written in the form $g = g_1 \cdots g_s$, where $g_i \in A_i$, $1 \leq i \leq s$. The number $\sum_{i=1}^{s} |A_i|$ is called the length of α and denoted by $l(\alpha)$. An observation by González Vasco and Steinwandt shows that $l(\alpha) \geq \sum_{i=1}^{s} m_i p_i$. A logarithmic signature α is said to be minimal (MLS) if $l(\alpha) = \sum_{i=1}^{s} m_i p_i$.

In this talk, recent progress on this conjecture is reported. We also present an efficient algorithm for providing MLS for sporadic groups.

Keywords: Minimal logarithmic signature, sporadic group.

AMS Subject Classification Number: $05C25$, $05C50$.

References

[1] M. I. González Vasco, M. Rötteler and R. Steinwandt, On minimal length factorizations of finite groups, *Exp. Math.* **12** (1) (2003) 1–12.

[2] M. I. González Vasco and R. Steinwandt, Obstacles in two public key cryptosystems based on group factorizations, *Tatra Mt. Math. Publ.* **25** (2002) 23–37.

[3] S. S. Magliveras and N. D. Memon, Algebraic properties of cryptosystem PGM, *J. Cryptol.* **5** (1992) 167–183.

[4] S. S. Magliveras and N. D. Memon, Properties of cryptosystem PGM, in *Advances in Cryptology – Crypto '89*, Lecture Notes in Computer Science **435**, Springer-Verlag, Berlin (1990), pp. 447–460.