Abstract

Logarithmic signatures are a special type of group factorizations, introduced as basic components of certain cryptographic keys. Thus, *short* logarithmic signatures are of special interest. We deal with the question of finding logarithmic signatures of *minimal length* in finite groups. In particular, such factorizations exist for solvable, symmetric, and alternating groups.

We show how to use the known examples to derive minimal length logarithmic signatures for other groups. Namely, we prove the existence of such factorizations for several classical groups and — in parts by direct computation — for all groups of order $< 175560 (= ord(J_1)$, where J_1 is Janko's first sporadic simple group). Whether there exists a minimal length logarithmic signature for each finite group still remains an open question.