Trace representation of the binary $pq^2$-periodic sequences derived from Euler quotients.

Zhang, Jingwei; Hu, Chuangqiang; Fan, Xiang; Zhao, Chang-An

Summary: Given a binary sequence, its trace representation allows us to reconstruct itself efficiently and to analyze its properties, such as the linear complexity. In this paper, we study a family of the binary sequences derived from Euler quotients modulo $pq$, where $p$ and $q$ are two distinct odd primes and $p$ divides $q - 1$. Our main contribution is to give a trace representation of this family within these assumptions by determining the defining pairs of the corresponding subsequences. As a byproduct, we rediscover some known results of linear complexities by using trace representations of the proposed sequences.

MSC:
94A55 Shift register sequences and sequences over finite alphabets in information and communication theory
94A60 Cryptography
11B50 Sequences (mod $m$)

Keywords:
cryptography; Euler quotients; finite fields; binary sequences; trace representation

Full Text: DOI

References:


No, JS; Lee, HK; Chung, H.; Song, HY; Yang, K., Trace representation of Legendre sequences of Mersenne prime period, IEEE Trans. Inf. Theory, 42, 6, 2254-2255 (1996) · Zbl 0872.94023 · doi:10.1109/18.556617


Zhao, XX; Tian, T.; Qi, WF, A ring-like cascade connection and a class of NFSRs with the same cycle structures, Des. Codes Crypt., 86, 12, 2775-2790 (2018) · Zbl 1448.94185 · doi:10.1007/s10623-018-0473-6

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.