Notes about the linear complexity of cyclotomic sequences of order six and corresponding cyclic codes

Vladimir Edemskiy, Nikita Sokolovskiy, Aleksandra Tsurina
Novgorod State University, Veliky Novgorod, Russia

May 21, 2017

Using of cyclotomic classes to construct sequences, which are called cyclotomic sequences, is an important method for sequence design. The linear complexity LC of a sequence is an important parameter in its evaluation as a key stream cipher for cryptographic applications [1]. It may be defined as the length of the shortest linear feedback-shift register that can generate the sequence. The linear complexity of above-mentioned sequences over the finite field of order two was investigated in a lot of articles. Recently, series of papers have examined the linear complexity of cyclotomic sequences over the finite field $GF(q)$ where $q \geq 3$ is a prime number. In particular, the linear complexity of Legendre sequences over the finite field of any order was studied in [7]. Investigating the cyclic codes, C.Ding studied the linear complexity of the series of cyclotomic sequences of order four. Further, the linear complexity of Hall's sextic residue sequences over the finite field of odd prime order was investigated in [3, 4]. In this paper, we derive the linear complexity of a number of balanced cyclotomic sequences of order six over $GF(q)$. In conclusion we give a remark about cyclic codes which could be constructed using the cyclotomic classes of order six.

1 Preliminaries

First, we briefly repeat some of the basic definitions and general information. Let p be a prime of the form $p \equiv 1 \pmod 6$, and let g be a primitive root

Notes about the linear complexity of cyclotomic sequences of order six and corresponding cyclic codes

Vladimir Edemskiy, Nikita Sokolovskiy and Aleksandra Tsurina

Novgorod State University
Veliky Novgorod, Russia

RuFiDiM 2018,
Turku,Finland, May 16-19, 2018