Linear Algebra Appl. 488 (2016) 302–319

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

On cyclotomic cosets and code constructions

Giuliano G. La Guardia [a,*], Marcelo M.S. Alves [b]

[a] *Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil*

[b] *Department of Mathematics, Federal University of Parana (UFPR), Av. Cel. Francisco H. dos Santos, 210, Jardim das Americas, 81531-970, Curitiba, PR, Brazil*

ARTICLE INFO

Article history:
Received 24 March 2015
Accepted 18 September 2015
Submitted by V. Mehrmann

MSC:
11T71

Keywords:
Cyclotomic cosets
BCH codes
CSS construction

ABSTRACT

New properties of q-ary cyclotomic cosets modulo $n = q^m - 1$, where $q \geq 3$ is a prime power, are investigated in this paper. Based on these properties, the dimension as well as bounds for the designed distance of some families of classical cyclic codes can be computed. As an application, new families of nonbinary Calderbank–Shor–Steane (CSS) quantum codes as well as new families of convolutional codes are constructed in this work. These new CSS codes have parameters better than the ones available in the literature. The convolutional codes constructed here have free distance greater than the ones available in the literature.

1. Introduction

Properties of cyclotomic cosets are extensively investigated in the literature in order to obtain the dimension as well as lower bounds for the minimum distance of cyclic codes

* Corresponding author.
E-mail address: gguardia@uepg.br (G.G. La Guardia).

http://dx.doi.org/10.1016/j.laa.2015.09.034
0024-3795/

[23,22,24,30,33,34]. Such properties were useful to derive efficient quantum codes [6,31,5, 32,12,2,3,13–15,20]. In [24], the authors explored properties of binary cyclotomic cosets to compute the ones containing two consecutive integers. In [30,33,34], properties of q-ary cyclotomic cosets (q-cosets for short) modulo $q^m - 1$ were investigated. In [2,3], the authors established properties on q-cosets modulo n, where $\gcd(n, q) = 1$, to compute the exact dimension of BCH codes of small designed distance, providing new families of quantum codes. Additionally, they employed such properties to show necessary and sufficient conditions for dual containing (Euclidean and Hermitian) BCH codes. Recently, in [13,15,20], the author has investigated properties of q-cosets as well as properties of q^2-cosets in order to construct several new families of good quantum BCH codes.

Motivated by all these works, we show new properties of q-cosets modulo $n = q^m - 1$, where $q \geq 3$ is a prime power. Since the nonbinary case has received less attention in the literature, in this paper we deal with nonbinary alphabets. As was said previously, these properties allow us to compute the dimension and bounds for the designed distance of some families of cyclic codes. Since the true dimension and minimum distance of BCH codes are not known in general, this paper contributes to this research. As an application of these results, we construct families of new Calderbank–Shor–Steane (CSS) quantum codes (i.e., CSS codes with new parameters; codes with parameters not known in the literature) as well as new families of convolutional codes. These new CSS codes have parameters given by

- $[[q^2 - 1, q^2 - 4c + 5, d \geq c]]_q$, where $2 \leq c \leq q$ and $q \geq 3$ is a prime power;
- $[[n, n - 2m(c - 2) - m/2 - 1, d \geq c]]_q$, where $n = q^m - 1$, $q \geq 3$ is a prime power, $2 \leq c \leq q$ and $m \geq 2$ is even;
- $[[n, n - m(2c - 3) - 1, d \geq c]]_q$, where $n = q^m - 1$, $q \geq 3$ is a prime power, $m \geq 2$ and $2 \leq c \leq q$.

The new convolutional codes constructed here have parameters

- $(n, n - 2q + 1, 2q - 3; 1, d_{free} \geq 2q + 1)_q$, where $q \geq 4$ is a prime power and $n = q^2 - 1$;
- $(n, n - 2q, 2q - 4; 1, d_{free} \geq 2q + 1)_q$, where $q \geq 4$ is a prime power and $n = q^2 - 1$;
- $(n, n - 2[q + i], 2[q - 2 - i]; 1, d_{free} \geq 2q + 1)_q$, where $1 \leq i \leq q - 3$, $q \geq 4$ is a prime power and $n = q^2 - 1$;
- $(n, n - 2q + 1, 1; 1, d_{free} \geq q + 2)_q$, $q \geq 4$ is a prime power and $n = q^2 - 1$;
- $(n, n - 2q + 1, 2i + 1; 1, d_{free} \geq q + i + 3)_q$, $1 \leq i \leq q - 3$, $q \geq 4$ is a prime power and $n = q^2 - 1$.

The paper is organized as follows. In Section 2, we review some basic concepts on q-cosets and cyclic codes. In Section 3, we present new results and properties of q-cosets. In Section 4, by applying some properties of q-cosets developed in the previous section, we compute the dimension and lower bounds for the minimum distance of some families of classical cyclic codes. Further, we utilize these cyclic codes to construct new good