Finite Fields and Their Applications 54 (2018) 230–252

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Improved linear programming bound on sizes of doubly constant-weight codes

Phan Thanh Toan [a,*], Hyun Kwang Kim [b], Jaeseon Kim [b]

[a] *Fractional Calculus, Optimization and Algebra Research Group, Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam*

[b] *Department of Mathematics, Pohang University of Science and Technology, Pohang 37673, Republic of Korea*

ARTICLE INFO

Article history:
Received 16 June 2018
Accepted 16 August 2018
Available online xxxx
Communicated by Gary L. Mullen

MSC:
94B65
90C05

Keywords:
Binary code
Doubly constant-weight code
Linear programming
Upper bound

ABSTRACT

In this paper we give new constraints on the distance distribution of doubly constant-weight (binary) codes. These constraints improve the linear programming bound on sizes of doubly constant-weight codes. Computations are done for all codes of length $n \leq 28$ and all improved upper bounds are shown. We moreover show that the improved upper bounds give rise to further new upper bounds.

1. Introduction

Let $\mathcal{F} = \{0, 1\}$ and let n be a positive integer. The *(Hamming) distance* between two vectors u, v in $\mathcal{F}^n$, denoted by $d(u, v)$, is the number of coordinates where they differ.

* Corresponding author.
E-mail addresses: phanthanhtoan@tdt.edu.vn (P.T. Toan), hkkim@postech.ac.kr (H.K. Kim), arkenjs@postech.ac.kr (J. Kim).

https://doi.org/10.1016/j.ffa.2018.08.009
1071-5797/

The *weight* of a vector u in $\mathcal{F}^n$, denoted by $wt(u)$, is the distance between it and the zero vector. Let d be a positive integer. An (n, d) *(binary) code* is a subset $\mathcal{C}$ of $\mathcal{F}^n$ such that the distance between any two different vectors in $\mathcal{C}$ is at least d. An element of $\mathcal{C}$ is called a *codeword* and the number of codewords in $\mathcal{C}$ is called the *size* of $\mathcal{C}$, denoted by $|\mathcal{C}|$. An (n, d, w) *constant-weight code* is an (n, d) code such that each of its codewords has weight w. Is spite of being restricted on the weight of codewords, constant-weight codes do have many applications and form a very important class of codes (see for example [1–4]). If $n_1+n_2 = n$ and $w_1+w_2 = w$, then a (w_1, n_1, w_2, n_2, d) *doubly constant-weight code* is an (n, d) code such that each of its codewords has weight w_1 in the first n_1 coordinates and weight w_2 in the last n_2 coordinates. By definition, a (w_1, n_1, w_2, n_2, d) doubly constant-weight code is an (n, d, w) constant-weight code. Doubly constant-weight codes were first introduced in [5,6], where they were used to sharpen upper bounds for constant-weight codes (see also [7,8]). The authors of [9] showed that doubly constant-weight codes can be even used to sharpen upper bounds for codes. In [10], a more special kind of doubly constant-weight codes, called multiply constant-weight codes, was introduced. If $n_1+n_2+\cdots+n_m = n$ and $w_1+w_2+\cdots+w_m = w$, then a $(w_1, n_1, w_2, n_2, \ldots, w_m, n_m, d)$ *multiply constant-weight code* is an (n, d) code such that each of its codeword has weight w_1 in the first n_1 coordinates, weight w_2 in the next n_2 coordinates, and so on and so forth. These codes were shown to have applications in improving the reliability of certain physically unclonable function response [10] (see also [11]). Bounds and constructions for multiply constant-weight codes (in the case $w_1 = w_2 = \cdots = w_m$) were studied in [12].

Let $A(n, d)$, $A(n, d, w)$, and $T(w_1, n_1, w_2, n_2, d)$ be the largest possible size of an (n, d) code, an (n, d, w) constant-weight code, and a (w_1, n_1, w_2, n_2, d) doubly constant-weight code, respectively. $A(n, d)$, $A(n, d, w)$, and $T(w_1, n_1, w_2, n_2, d)$ are basic functions in coding theory. Upper bounds for these functions can be obtained from linear programming, which is based on linear constraints on the distance distribution of pairs of codewords (see [13–15]). For $A(n, d)$ and $A(n, d, w)$, the linear programming bound has been generalized to semidefinite programming bound, which is based on constraints on triples of codewords [16] or even on quadruples of codewords [17,18]. However, all of these generalizations have not yet been done for $T(w_1, n_1, w_2, n_2, d)$. In this paper, we first give two types of linear constraints on the distance distribution of doubly constant-weight codes. We then show that these new constraints improve the linear programming bound for $T(w_1, n_1, w_2, n_2, d)$. Computations are done for all doubly constant-weight codes of length $n \leq 28$.

The paper is organized as follows. In Section 2, we show elementary properties of $T(w_1, n_1, w_2, n_2, d)$ and the linear programming bound for this function. In Section 3, we give the first type of linear constraints on the distance distribution of doubly constant-weight codes. To obtain this type of constraints, we consider a code as a matrix (where each codeword is a row) and count in two ways the number of $2 \times k$ submatrices satisfying some given conditions. Our method is a variant of known counting methods for obtaining upper bounds on sizes of (constant-weight) codes such as counting the number of 2×1 submatrices containing an odd number of ones (the Plotkin type bound), counting the