Finite Fields and Their Applications 26 (2014) 49–68

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Optimal equi-difference conflict-avoiding codes of odd length and weight three

Yiling Lin [a,*], Miwako Mishima [b], Junya Satoh [a], Masakazu Jimbo [a]

[a] *Graduate School of Information Science, Nagoya University, Furo-cho, Chikusa-ku, 464-8601, Japan*

[b] *Department of Electrical, Electronic and Computer Engineering, Faculty of Engineering, Gifu University, 1-1 Yanagido, Gifu, 501-1193, Japan*

A R T I C L E   I N F O

Article history:
Received 29 June 2013
Received in revised form 3 October 2013
Accepted 8 November 2013
Available online 28 November 2013
Communicated by L. Storme

MSC:
05B30
05B99
94B25
94B65

Keywords:
CAC
Equi-difference conflict-avoiding code
Optimal code
Tight code
Multiplicative order
Cyclotomic polynomial

A B S T R A C T

A conflict-avoiding code (CAC) is known as a protocol sequence for transmitting data packets over a collision channel without feedback. The study of CACs has been focused on determining the size of an optimal code, i.e., the maximum size of a code, and in the past few years it has been settled by several researchers for even length and weight 3 together with constructions. As for odd length, a necessary and sufficient condition for the existence of a 'tight equi-difference' CAC of weight 3 can be found in Momihara (2007), but the condition is fairly complex and thus only a few explicit series of code lengths are known. Recently, Fu et al. (2013) restated the condition given by Momihara (2007) in a different way, which requires to examine the multiplicative suborder of 2 modulo p for each prime factor p of m. Meanwhile, Ma et al. (2013) presented constructions of an optimal equi-difference CAC and an optimal tight CAC of odd prime length p and weight 3, and formulated the sizes of such optimal codes. However, for their formulae to have practical meaning, the number of cosets of $-(2)_p \cup (2)_p$ still needs to be determined, where $(2)_p$ is the multiplicative subgroup of $\mathbb{Z}_p^*$ with generator 2. Moreover, their construction of an optimal tight CAC imposes a certain condition. This implies that even restricting ourselves to odd prime length, to provide a series of odd code length for which the maximum size of a CAC of weight 3 can be determined is a demanding problem.

In this article, we will give some explicit series of tight/optimal equi-difference CACs of odd length and weight 3 by revisiting some

* Corresponding author.
E-mail addresses: lin@math.cm.is.nagoya-u.ac.jp (Y. Lin), miwako@gifu-u.ac.jp (M. Mishima), jsatoh@is.nagoya-u.ac.jp (J. Satoh), jimbo@is.nagoya-u.ac.jp (M. Jimbo).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.11.001

properties of multiplicative order of a unit in the ring of residues modulo m and cyclotomic polynomials.

1. Introduction

A conflict-avoiding code has been studied as a protocol sequence for a multiple-access channel (collision channel) without feedback [6,9,10,13,17,20]. For the technical description of such a multiple-access channel model, see [1,12].

In mathematical terms, a conflict-avoiding code (CAC) of length m and weight w is defined as a set $C \subseteq \{0,1\}^m$ of binary vectors, called *codewords*, of Hamming weight w such that arbitrary cyclic shifts x', y' of distinct codewords $x, y \in C$ intersect at most at one coordinate, i.e., $\mathrm{dist}(x', y') \geqslant 2w-2$ holds, where $\mathrm{dist}(x', y')$ is the Hamming distance between x' and y'. We denote the class of all the CACs of length m and weight w by $\mathrm{CAC}(m, w)$.

The *support* of a codeword $x = (x_0, x_1, \ldots, x_{m-1})$ is the set of indices of its nonzero coordinates. In this article, a codeword is expressed by its support, not as a binary vector. Then any code $C \in \mathrm{CAC}(m, w)$ can be regarded as a collection of w-subsets of $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, the ring of residues modulo m, such that

$$\Delta(x) \cap \Delta(y) = \emptyset \quad \text{for any } x, y \in C,$$

where $\Delta(x) = \{j - i \pmod{m}\colon\ i, j \in x,\ i \neq j\}$ is the set of differences arising from x. Since for any codeword x in a code $C \in \mathrm{CAC}(m, w)$, the elements of $\Delta(x)$ are symmetric with respect to $m/2$, we henceforth consider the halved difference set

$$\Delta_2(x) = \left\{ i \in \Delta(x)\colon\ i \leqslant \left\lfloor \frac{m}{2} \right\rfloor \right\}$$

instead of $\Delta(x)$. We also use the notation $\Delta_2(C)$ to denote $\bigcup_{x \in C} \Delta_2(x)$.

If x is of form $\{0, i, \ldots, (w-1)i\}$, then it is said to be *equi-difference* (or *centered* when $w = 3$), and if every codeword in a code $C \in \mathrm{CAC}(m, w)$ is equi-difference, then C is called an *equi-difference* code (or *centered* code when $w = 3$). The class of all the equi-difference CACs of length m and weight w is denoted by $\mathrm{CAC}^e(m, w)$. Obviously $\mathrm{CAC}^e(m, w) \subseteq \mathrm{CAC}(m, w)$.

Let $M(m, w)$ be the maximum size of a code in $\mathrm{CAC}(m, w)$, i.e.,

$$M(m, w) = \max\bigl\{|C|\colon\ C \in \mathrm{CAC}(m, w)\bigr\}.$$

A code $C \in \mathrm{CAC}(m, w)$ is said to be *optimal* if $|C| = M(m, w)$. Furthermore, an optimal code $C \in \mathrm{CAC}(m, w)$ is said to be *tight* if $\Delta_2(C) = \{1, 2, \ldots, \lfloor \frac{m}{2} \rfloor\}$. The maximum size of a code in $\mathrm{CAC}^e(m, w)$ is defined as

$$M^e(m, w) = \max\bigl\{|C|\colon\ C \in \mathrm{CAC}^e(m, w)\bigr\}$$

similarly to $M(m, w)$. Several constructions for optimal equi-difference CACs of weight $w \geqslant 4$ can be found in [16].

As for $w = 3$, the functions $M(m, 3)$ and $M^e(m, 3)$ were studied in [8–10,15]. Levenshtein and Tonchev [10] proved that

$$M(m, 3) = M^e(m, 3) = \frac{m-2}{4} \quad \text{if } m \equiv 2 \pmod{4}$$