Discrete Mathematics 340 (2017) 617–629

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

A new series of optimal tight conflict-avoiding codes of weight 3

Miwako Mishima [a,*], Koji Momihara [b]

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

[b] Department of Mathematics, Faculty of Education, Kumamoto University, 2-39-1 Kurokami, Kumamoto 860-8555, Japan

ARTICLE INFO

Article history:
Received 3 February 2015
Received in revised form 21 December 2015
Accepted 7 December 2016
Available online 3 January 2017

Keywords:
Conflict-avoiding code (CAC)
Optimal code
Tight code

ABSTRACT

In this article, a construction of an optimal tight conflict-avoiding code of length $3^d p^e$ and weight 3 is shown for $d \equiv 1 \pmod 3$, $e \in \mathbb{N}$ and a prime $p \equiv 3 \pmod 8$ with $p \neq 3$, assuming that p is a non-Wieferich prime if $e \geq 2$. This is a new series of optimal conflict-avoiding code for which the number of codewords can be exactly determined.

1. Introduction

A conflict-avoiding code (CAC) is known as a protocol sequence for transmitting data packets over a multiple-access channel (collision channel) without feedback [5,8,10,15,20,22]. We save the technical description for such a channel model to other literature [1,14].

Let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ and define the notation $\overline{a}$ as an element in $\mathbb{Z}_n$ represented by an integer $a \in \{0, 1, \dots, n-1\}$, although, for simplicity, we will not distinguish between $\mathbb{Z}_n$ and $\{0, 1, \dots, n-1\}$ (thus $\overline{a}$ and a) as long as its meaning is apparent from the context. A conflict-avoiding code $\mathcal{C}$ of length n and weight w is defined mathematically as a collection of w-subsets, called *codewords*, of $\mathbb{Z}_n$ such that $\Delta(x) \cap \Delta(y) = \emptyset$ for any distinct codewords $x, y \in \mathcal{C}$, where $\Delta(x) := \{j - i \mid i, j \in x, i \neq j\}$ as an ordinary set (not a multiset). Let

$$\Delta(\mathcal{C}) := \bigcup_{x \in \mathcal{C}} \Delta(x),$$

where the union is taken as a multiset. Then, the definition of a CAC is equivalent to that $\Delta(\mathcal{C})$ covers every element of $\mathbb{Z}_n^* := \mathbb{Z}_n \backslash \{0\}$ at most once. A code $\mathcal{C}$ is said to be *tight* if $\Delta(\mathcal{C})$ covers every element of $\mathbb{Z}_n^*$ exactly once. The class of all the CACs of length n and weight w is denoted by $\mathrm{CAC}(n, w)$. If a codeword $x \in \mathcal{C}$ is of form $\{0, i, \dots, (w-1)i\}$, it is said to be *equidifference*, and i is called a *generator* of the codeword x. If a code $\mathcal{C}$ consists only of equidifference codewords, then $\mathcal{C}$ is called an *equidifference code*. The class of all CACs of length n and weight w is denoted by $\mathrm{CAC}(n, w)$, and that of all equidifference CACs of length n and weight w is denoted by $\mathrm{CAC}^e(n, w)$. Obviously $\mathrm{CAC}^e(n, w) \subseteq \mathrm{CAC}(n, w)$. The maximum sizes of a CAC and an equidifference CAC of length n and weight w are denoted as $M(n, w)$ and $M^e(n, w)$, respectively, i.e.,

$$M(n, w) = \max\{|\mathcal{C}| \mid \mathcal{C} \in \mathrm{CAC}(n, w)\} \quad \text{and} \quad M^e(n, w) = \max\{|\mathcal{C}| \mid \mathcal{C} \in \mathrm{CAC}^e(n, w)\}.$$

A code $\mathcal{C} \in \mathrm{CAC}(n, w)$ is said to be *optimal* if $|\mathcal{C}| = M(n, w)$. Especially when $w = 3$, a tight code in $\mathrm{CAC}^e(n, 3)$ is optimal.

* Corresponding author.
E-mail addresses: miwako@gifu-u.ac.jp (M. Mishima), momihara@educ.kumamoto-u.ac.jp (K. Momihara).

http://dx.doi.org/10.1016/j.disc.2016.12.003
0012-365X/

The main objective of the study on CACs has been to determine $M(n, w)$ and $M^e(n, w)$, and several results can be found in [3,4,7,10–13,16–18,23] for $w = 3, 4$. Especially, $M(n, 3)$ was settled for even n by Levenshtein and Tonchev [10], Jimbo et al. [7], Mishima et al. [16] and Fu et al. [3]. As for odd n, Momihara [17] gave a necessary and sufficient condition for the existence of a tight code in $\mathrm{CAC}^e(n, 3)$ and an algorithm for finding admissible odd n. Later, the condition given by Momihara [17] was restated by Fu et al. [4] in terms of multiplicative subgroup of modulo p for all prime factors p of n. We should note that a tight equidifference CAC of weight w is equivalent to a perfect $(w-1)$-shift code [9] and a necessary and sufficient condition for the existence of a perfect $(w-1)$-shift code in a finite abelian group has been known for $w = 2, 3$ due to Levenshtein and Vinck [9], and $w = 4, 5$ due to Munemasa [19]. However, those conditions in [4,9,17] require to examine every prime factor of n to compute the exact value of $M^e(n, 3)$. Recently, Wu and Fu [23] showed that, for two specific series $n = 2^{2k} + 1$ and $2^{2^k} - 1$ ($k \in \mathbb{N}$), there exists a tight code in $\mathrm{CAC}^e(n, 3)$, and Ma et al. [13] presented an idea for constructing an optimal code in $\mathrm{CAC}^e(p, 3)$ and an optimal tight code in $\mathrm{CAC}(p, 3)$ for prime $p \geq 5$ with the formulae for $M(p, 3)$ and $M^e(p, 3)$. In [12], the reader also can find some series of odd n for which $M^e(n, 3)$ can be explicitly determined. However, these known results are just a fraction of the full settlement of $M(n, 3)$ and $M^e(n, 3)$ for odd n.

This article will show the following theorem on $M(3^{3f+1}p^e, 3)$ for $f \geq 0$, $e \geq 1$ and a (non-Wieferich if $e \geq 2$) prime $p \equiv 3 \pmod 8$ with $p \neq 3$ by providing a construction of an optimal tight code in $\mathrm{CAC}(3^{3f+1}p^e, 3)$, which cannot be obtained by previously known results including the recursive construction due to Ma et al. [13, Construction 5.1]. In fact, the odd code length n of an optimal (tight) CAC of weight 3 resulting from Construction 5.1 in [13] cannot be divisible by 3 more than once, although they do not mention clearly this restriction in their construction.

Theorem 1.1. *Let p be a prime satisfying $p \equiv 3 \pmod 8$ with $p \neq 3$ and $v := v_3(\mathrm{ord}_p(2)) \leq 1$, where $v_3(x)$ is the highest power of 3 dividing an integer x. Moreover, let $n := 3^d p^e$ for $d, e \in \mathbb{N}$ and further assume that p is a non-Wieferich prime if $e \geq 2$. If $d \equiv 1 \pmod 3$, then there exists an optimal tight code $\mathcal{C} \in \mathrm{CAC}(n, 3)$ with*

$$|\mathcal{C}| = M(n, 3) = \frac{n+1}{4} - \frac{(2 \cdot 3^v(d-1) + 3)es + d - 1}{6},$$

where $s = (p-1)/\mathrm{ord}_p(2)$.

Note that a *Wieferich prime* is a prime satisfying $2^{p-1} \equiv 1 \pmod{p^2}$. Dorais [2] verified that, under 6.7×10^{15}, there are only two Wieferich primes $p = 1093$ and 3511 (see also [21]).

2. Preliminary

This section is devoted to the preparation for presenting a construction of a new series of optimal tight CAC of weight 3 in the next section.

For $n \geq 2$ and an integer a coprime to n, the *multiplicative order* of a modulo n, denoted by $\mathrm{ord}_n(a)$, is the smallest positive integer ℓ satisfying $a^\ell \equiv 1 \pmod n$. The smallest positive integer ℓ' satisfying $a^{\ell'} \equiv \pm 1 \pmod n$ is called the *multiplicative suborder* of a and denoted by $\mathrm{sord}_n(a)$. Thus $\mathrm{ord}_n(a) = 2\,\mathrm{sord}_n(a)$ or $\mathrm{sord}_n(a)$ depending on whether $-1 \in \langle \overline{a} \rangle$ in $\mathbb{Z}_n^\times$ or not.

If $p \equiv 3 \pmod 8$ is a prime, the second supplementary law of the quadratic reciprocity says that $2^{\frac{p-1}{2}} \equiv -1 \pmod p$, which implies that $-1 \in \langle 2 \rangle$ in $\mathbb{Z}_p^\times$ and thus $\mathrm{ord}_p(2) = 2\,\mathrm{sord}_p(2)$. We can further mention that $\mathrm{ord}_p(2) \equiv 2 \pmod 4$ holds since $\frac{p-1}{2} \equiv 1 \pmod 4$ and $\mathrm{sord}_p(2) \mid (p-1)/2$, which means that $\mathrm{ord}_{p^e}(2)$ is even for any $e \in \mathbb{N}$ since $\mathrm{ord}_p(2) \mid \mathrm{ord}_{p^e}(2)$.

Throughout this article, the highest power of a prime q dividing a nonzero integer x is denoted by $v_q(x)$ and the group of units of $\mathbb{Z}_n$ by $\mathbb{Z}_n^\times$, and, for an element $a \in \mathbb{Z}_n$ and an integer x, we may simply write xa or ax to denote $\overline{x}a \in \mathbb{Z}_n$. Furthermore, an integer g coprime to $3^\ell p^r$ such that $g\langle 2 \rangle = \{gx : x \in \langle 2 \rangle\} \subseteq \mathbb{Z}_{3^\ell p^r}^\times$ is a generator of $\mathbb{Z}_{3^\ell p^r}^\times / \langle 2 \rangle$ is simply called "*a generator of $\mathbb{Z}_{3^\ell p^r}^\times / \langle 2 \rangle$*".

2.1. Order and suborder of 2

In this subsection, we collect some basic lemmas on elementary number theory for later use.

Lemma 2.1. *For $e \in \mathbb{N}$, a prime p and an integer a coprime to p, there exists an integer $\epsilon \in [0, e)$ satisfying $\mathrm{ord}_{p^e}(a) = p^\epsilon\,\mathrm{ord}_p(a)$.*

Proof. The assertion follows from the isomorphism: $\mathbb{Z}_{p^e}^\times \simeq \mathbb{Z}_p^\times \times \mathbb{Z}_{p^{e-1}}$. □

For any odd prime p and $h \in \mathbb{N}$, it follows from Lemma 2.1 that $\mathrm{ord}_{p^h}(2) \equiv 2 \pmod 4$ as long as $\mathrm{ord}_p(2) \equiv 2 \pmod 4$, and then $\mathrm{sord}_{p^h}(2) = \mathrm{ord}_{p^h}(2)/2$ holds, which implies $-1 \in \langle 2 \rangle$ in $\mathbb{Z}_{p^h}^\times$. Then the following can be easily observed.

Corollary 2.2. *For given integers $\ell \geq 0$ and $r \geq 0$ with $(\ell, r) \neq (0, 0)$, and a prime $p \equiv 3 \pmod 8$ with $p \neq 3$, it follows that $-1 \in \langle 2 \rangle$ in $\mathbb{Z}_{3^\ell p^r}^\times$.*

Proof. Since $-1 \in \langle 2 \rangle$ both in $\mathbb{Z}_{3^\ell}^\times$ and in $\mathbb{Z}_{p^r}^\times$, the assertion is immediately proved by the Chinese Remainder Theorem. □