Finite Fields and Their Applications 16 (2010) 4–13

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Cyclotomy and its application to duadic codes

Hideki Tada, Shigeto Nishimura, Toyokazu Hiramatsu *

Department of Systems and Control Engineering, College of Engineering, Hosei University, Kajino 3-7-2, Koganei, Tokyo 184-8584, Japan

ARTICLE INFO

Article history:
Received 10 October 2006
Revised 17 November 2009
Available online 23 December 2009
Communicated by Gary L. Mullen

Keywords:
Duadic codes
Cyclotomy
Higher reciprocity laws
Tschebotareff's density theorem

ABSTRACT

In this paper we treat cyclotomic binary duadic codes. The conjecture of Ding and Pless is that there are infinitely many cyclotomic duadic codes of prime lengths that are not quadratic residue codes. We shall prove this conjecture by using the special case of Tschebotareff's density theorem.

1. Introduction

Duadic codes were defined by J.S. Leon, J.M. Masley and V. Pless in [5] related to the study of idempotent generators of quadratic residue codes. This family of binary duadic codes includes the binary quadratic codes of prime length. One of the open problems on duadic codes stated by C. Ding and V. Pless in [1] and [2] is the following: For which primes p are there duadic codes of length p that are not quadratic residue codes? They answered there exist infinitely many cyclotomic duadic codes of order 4, 6. In this paper we shall show that infinitely many cyclotomic duadic codes of order $2e$ exist in general. Indeed, cyclotomic duadic codes of order $2e$ can be found by the orbit decomposition of $\mathbb{F}_p^\times$ via multiplicative action by 2, when 2 is a $2e$-th power modulo p. The idempotent generator of a cyclotomic duadic code is obtained as a union of those orbits and clearly some generators yield codes that are not quadratic residue codes. The infinitely many cyclotomic duadic codes of order $2e$ thereby exist if $\mathrm{Spl}\{x^{2e}-2\}$ is an infinite set, where $\mathrm{Spl}\{x^{2e}-2\}$ denotes the set of all primes such that $x^{2e}-2$ factors into distinct linear polynomials modulo p. It follows from the special case of Tschebotareff's density theorem.

* Corresponding author.
E-mail addresses: r_doll@watv.ne.jp (H. Tada), hiramatu@k.hosei.ac.jp (T. Hiramatsu).

1071-5797/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2009.11.003

In Section 2 we define generalized cyclotomic numbers and describe some elementary properties about these numbers. In Section 3 we will define duadic codes and cyclotomic duadic codes, and we study for some orbit decomposition of $\mathbb{F}_p^\times$. In Section 4, first we recall the higher reciprocity law for polynomial, and we prove the conjecture of Ding and Pless using the Tschebotareff's density theorem.

2. Cyclotomy and its generalization

2.1. Generalized cyclotomic numbers

Let $n \geqslant 2$ be a positive integer, and let $\mathbb{F}_n^\times$ be the multiplicative group of $\mathbb{F}_n$ where $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$. A partition $\{D_0, D_1, \dots, D_{d-1}\}$ of $\mathbb{F}_n^\times$ is a family of sets with

$$D_i \cap D_j = \phi \quad \text{for all } i \neq j$$

and

$$\mathbb{F}_n^\times = \bigcup_{i=0}^{d-1} D_i.$$

If D_0 is a subgroup of $\mathbb{F}_n^\times$, and there are $g_1, \dots, g_{d-1}$ of $\mathbb{F}_n^\times$ such that $D_i = g_i D_0$ for all i, these D_i are called generalized cyclotomic classes of order d. The generalized cyclotomic numbers of order d are defined by

$$(i, j)_d = \left|(D_i + 1) \cap D_j\right|, \quad i, j = 0, 1, \dots, d-1.$$

When n is prime, it is referred to as classical cyclotomic number considered in detail by C.F. Gauss in his book ‘Disquisitiones Arithmeticae’.

2.2. Elementary properties of the number $(i, j)_d$

Let $df + 1$ be an odd prime and let θ be a fixed primitive element of $\mathbb{F}_n$. Denote the subgroup $\langle \theta^d \rangle$ as D_0, then the coset decomposition of $\mathbb{F}_n^\times$ is

$$\mathbb{F}_n^\times = \bigcup_{i=0}^{d-1} D_i,$$

where $D_i = \theta^i D_0$ for $i \geqslant 0$. Clearly, there are at most d^2 distinct (classical) cyclotomic numbers of order d and these numbers depend not only on n, d, i, j but also on which of the $\varphi(n-1)$ primitive elements of $\mathbb{F}_n$ is chosen. We have the following elementary properties about cyclotomic numbers which are not hard to prove:

$$1^\circ \quad \sum_{j=0}^{d-1} (i, j)_d = f - n_i, \quad \text{where } n_i = \begin{cases} 1, & \text{if } i \equiv 0 \bmod d,\ f\text{: even}, \\ 1, & \text{if } i \equiv \frac{d}{2} \bmod d,\ f\text{: odd}, \\ 0, & \text{otherwise.} \end{cases}$$

$$2^\circ \quad \sum_{i=0}^{d-1} (i, j)_d = f - k_j, \quad \text{where } k_j = \begin{cases} 1, & \text{if } j \equiv 0 \bmod d, \\ 0, & \text{otherwise.} \end{cases}$$

$$3^\circ \quad \text{Diagonal sums: } \sum_{i=0}^{d-1} (i, i+j)_d = \begin{cases} f - 1, & \text{if } j = 0, \\ f, & \text{if } j \neq 0. \end{cases}$$