CERTAIN DIAGONAL EQUATIONS AND CONFLICT-AVOIDING CODES OF PRIME LENGTHS

LIANG-CHUNG HSIA, HUA-CHIEH LI, AND WEI-LIANG SUN

ABSTRACT. We study the construction of optimal conflict-avoiding codes (CAC) from a number theoretical point of view. The determination of the size of optimal CAC of prime length p and weight 3 is formulated in terms of the solvability of certain twisted Fermat equations of the form $g^2X^\ell + gY^\ell + 1 = 0$ over the finite field $\mathbb{F}_p$ for some primitive root g modulo p. We treat the problem of solving the twisted Fermat equations in a more general situation by allowing the base field to be any finite extension field $\mathbb{F}_q$ of $\mathbb{F}_p$. We show that for q greater than a lower bound of the order of magnitude $O(\ell^2)$ there exists a generator g of $\mathbb{F}_q^\times$ such that the equation in question is solvable over $\mathbb{F}_q$. Using our results we are able to contribute new results to the construction of optimal CAC of prime lengths and weight 3.

Keywords: binary protocol sequence, conflict-avoiding code, diagonal equation, Hasse-Weil bound, Ramanujan's sum, Fibonacci primitive root.

1. INTRODUCTION

A binary protocol sequence set for transmitting data packets over a multiple-access collision channel without feedback is called a *conflict-avoiding code* (CAC) in information theory. It has been studied a few decades ago by [Mat90, NGM92, GV93, TR02, LT05, Lev07]. A mathematical model for CACs of *length n* and (*Hamming*) *weight w* is as follows. Let $\mathbb{Z}/n\mathbb{Z}$ be the additive group of the integer ring $\mathbb{Z}$ modulo n. For a w-subset $\mathbf{x} = \{x_1, \ldots, x_w\}$ of $\mathbb{Z}/n\mathbb{Z}$, let $\Delta(\mathbf{x}) = \{x_i - x_j \mid i \neq j\}$. A CAC of length n and weight w is a collection $\mathscr{C}$ of w-subsets of $\mathbb{Z}/n\mathbb{Z}$ such that $\Delta(\mathbf{x}) \cap \Delta(\mathbf{y}) = \varnothing$ for every distinct $\mathbf{x}, \mathbf{y} \in \mathscr{C}$. Each w-subset $\mathbf{x}$ of $\mathscr{C}$ is called a *codeword*. A CAC $\mathscr{C}$ is said to be *optimal* if its size is maximal among all CACs of the same length and weight. In the case where the weight is one or two, there is no difficulty to find the optimal size. However, for weights more than 2, finding an optimal CAC and determining its size is still an open problem. The first challenge is the case of weight 3. One of the purpose of this note is to treat the problem of finding optimal CAC's from a number theoretical point of view and contribute new results to the construction of optimal CAC of weight 3. Thus, all CACs which we are concerned with will be of weight 3.

In the case of even lengths and weight 3, the problem of constructing optimal CACs has a complete answer by the work [LT05, JMJ$^+$07, MFU09, FLM10]. In contrast, it is incomplete for odd lengths. Let $o_m(2)$ denote the multiplicative order of 2 modulo a positive odd integer m. For a CAC of odd length n, we write $n = n_1 n_2$ such that $o_p(2)$ is a multiple of 4 for all the prime divisors p of n_1 while $o_p(2)$ is not divisible by 4 for all