Discrete Mathematics 339 (2016) 2288–2303

Contents lists available at ScienceDirect

Discrete Mathematics

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

Perspective

A construction of binary linear codes from Boolean functions☆

Cunsheng Ding

Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Received 29 October 2015
Accepted 31 March 2016
Available online 6 May 2016

Keywords:
Almost bent functions
Bent functions
Difference sets
Linear codes
Semibent functions
O-polynomials

ABSTRACT

Boolean functions have important applications in cryptography and coding theory. Two famous classes of binary codes derived from Boolean functions are the Reed–Muller codes and Kerdock codes. In the past two decades, a lot of progress on the study of applications of Boolean functions in coding theory has been made. Two generic constructions of binary linear codes with Boolean functions have been well investigated in the literature. The objective of this paper is twofold. The first is to provide a survey on recent results, and the other is to propose open problems on one of the two generic constructions of binary linear codes with Boolean functions. These open problems are expected to stimulate further research on binary linear codes from Boolean functions.

1. Introduction

Let p be a prime and let $q = p^m$ for some positive integer m. An $[n, k, d]$ code $\mathcal{C}$ over GF(p) is a k-dimensional subspace of $\mathrm{GF}(p)^n$ with minimum (Hamming) distance d. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The *weight enumerator* of $\mathcal{C}$ is defined by $1 + A_1z + A_2z^2 + \cdots + A_nz^n$. The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the *weight distribution* of the code $\mathcal{C}$. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \ldots, A_n)$ is equal to t.

Boolean functions are functions from $\mathrm{GF}(2^m)$ or $\mathrm{GF}(2)^m$ to GF(2). They are important building blocks for certain types of stream ciphers, and can also be employed to construct binary codes. Two famous families of binary codes are the Reed–Muller codes [61,57] and Kerdock codes [9,10,47]. In the literature two generic constructions of binary linear codes from Boolean functions have been well investigated. A lot of progress on the study of one of the two constructions has been made in the past decade. The objective of this paper is twofold. The first one is to provide a survey on recent development on this construction, and the other is to propose open problems on this generic constructions of binary linear codes with Boolean functions. These open problems are expected to stimulate further research on binary linear codes from Boolean functions.

2. Mathematical foundations

2.1. Difference sets

For convenience later, we define the *difference function* of a subset D of an abelian group $(A, +)$ as

$$\mathrm{diff}_D(x) = |D \cap (D + x)|, \tag{1}$$

where $D + x = \{y + x : y \in D\}$.

☆ C. Ding's research was supported by The Hong Kong Research Grants Council, under Proj. No. 16300415.
E-mail address: cding@ust.hk.

http://dx.doi.org/10.1016/j.disc.2016.03.029
0012-365X/

A subset D of size k in an abelian group $(A, +)$ with order v is called a (v, k, λ) *difference set* in $(A, +)$ if the difference function $\mathrm{diff}_D(x) = \lambda$ for every nonzero $x \in A$. A difference set D in $(A, +)$ is called *cyclic* if the abelian group A is cyclic.

Difference sets could be employed to construct linear codes in different ways. The reader is referred to [26,27] for detailed information. Some of the codes presented in this survey paper are also defined by difference sets.

2.2. Group characters in GF(q)

An *additive character* of $\mathrm{GF}(q)$ is a nonzero function χ from $\mathrm{GF}(q)$ to the set of nonzero complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \mathrm{GF}(q)^2$. For each $b \in \mathrm{GF}(q)$, the function

$$\chi_b(c) = \epsilon_p^{\mathrm{Tr}(bc)} \quad \text{for all } c \in \mathrm{GF}(q) \tag{2}$$

defines an additive character of $\mathrm{GF}(q)$, where and whereafter $\epsilon_p = e^{2\pi\sqrt{-1}/p}$ is a primitive complex pth root of unity and Tr is the absolute trace function. When $b = 0$, $\chi_0(c) = 1$ for all $c \in \mathrm{GF}(q)$, and is called the *trivial additive character* of $\mathrm{GF}(q)$. The character χ_1 in (2) is called the *canonical additive character* of $\mathrm{GF}(q)$. It is known that every additive character of $\mathrm{GF}(q)$ can be written as $\chi_b(x) = \chi_1(bx)$ [48, Theorem 5.7].

2.3. Special types of polynomials over GF(q)

It is well known that every function from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ can be expressed as a polynomial over $\mathrm{GF}(q)$. A polynomial $f \in \mathrm{GF}(q)[x]$ is called a *permutation polynomial* if the associated polynomial function $f : a \mapsto f(a)$ from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ is a permutation of $\mathrm{GF}(q)$.

Dickson polynomials of the first kind over $\mathrm{GF}(q)$ are defined by

$$D_h(x, a) = \sum_{i=0}^{\lfloor \frac{h}{2} \rfloor} \frac{h}{h-i} \binom{h-i}{i} (-a)^i x^{h-2i}, \tag{3}$$

where $a \in \mathrm{GF}(q)$ and h is called the *order* of the polynomial. Some of the linear codes that will be presented in this paper are defined by Dickson permutation polynomials of order 5 over $\mathrm{GF}(2^m)$.

A polynomial $f \in \mathrm{GF}(q)[x]$ is said to be *e-to-1* if the equation $f(x) = b$ over $\mathrm{GF}(q)$ has either e solutions $x \in \mathrm{GF}(q)$ or no solution for every $b \in \mathrm{GF}(q)$, where $e \ge 1$ is an integer, and e divides q. By definition, permutation polynomials are 1-to-1. In this survey paper, we need e-to-1 polynomials over $\mathrm{GF}(2^m)$ for the construction of binary linear codes.

2.4. Boolean functions and their expressions

A function f from $\mathrm{GF}(2^m)$ or $\mathrm{GF}(2)^m$ to $\mathrm{GF}(2)$ is called a *Boolean function*. A function f from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ is called *linear* if $f(x+y) = f(x) + f(y)$ for all $(x, y) \in \mathrm{GF}(2^m)^2$. A function f from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ is called *affine* if f or $f - 1$ is linear.

The *Walsh transform* of $f : \mathrm{GF}(2^m) \to \mathrm{GF}(2)$ is defined by

$$\hat{f}(w) = \sum_{x \in \mathrm{GF}(2^m)} (-1)^{f(x)+\mathrm{Tr}(wx)} \tag{4}$$

where $w \in \mathrm{GF}(2^m)$. The *Walsh spectrum* of f is the following multiset

$$\left\{\left\{\hat{f}(w) : w \in \mathrm{GF}(2^m)\right\}\right\}.$$

Let f be a Boolean function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$. The *support* of f is defined to be

$$D_f = \{x \in \mathrm{GF}(2^m) : f(x) = 1\} \subseteq \mathrm{GF}(2^m). \tag{5}$$

Clearly, $f \mapsto D_f$ is a one-to-one correspondence between the set of Boolean functions from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ and the power set of $\mathrm{GF}(2^m)$.

3. The first generic construction of linear codes from functions

Let f be any polynomial from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$, where $q = p^m$. A code over $\mathrm{GF}(p)$ is defined by

$$\mathcal{C}(f) = \{\mathbf{c} = (\mathrm{Tr}(af(x) + bx))_{x \in \mathrm{GF}(q)} : a \in \mathrm{GF}(q),\ b \in \mathrm{GF}(q)\},$$

where Tr is the absolute trace function. Its length is q, and its dimension is at most $2m$ and is equal to $2m$ in many cases. The dual of $\mathcal{C}(f)$ has dimension at least $q - 2m$.

Let f be any polynomial from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ such that $f(0) = 0$. A code over $\mathrm{GF}(p)$ is defined by

$$\mathcal{C}^*(f) = \{\mathbf{c} = (\mathrm{Tr}(af(x) + bx))_{x \in \mathrm{GF}(q)^*} : a \in \mathrm{GF}(q),\ b \in \mathrm{GF}(q)\}.$$