Commun. Math. Res.
doi: 10.4208/cmr.2020-0520

Vol. **38**, No. 2, pp. 157-183
May 2022

Subfield Codes of Linear Codes from Perfect Nonlinear Functions and Their Duals

Dabin Zheng*, Xiaoqiang Wang, Yayao Li and Mu Yuan

Hubei Key Laboratory of Applied Mathematics, and Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China.

Received 11 December 2020; Accepted 30 March 2021

Abstract. Let $\mathbb{F}_{p^m}$ be a finite field with p^m elements, where p is an odd prime and m is a positive integer. Recently, [17] and [35] determined the weight distributions of subfield codes with the form

$$\mathcal{C}_f=\left\{\Big(\big(\mathrm{Tr}(af(x)+bx)+c\big)_{x\in\mathbb{F}_{p^m}},\mathrm{Tr}(a)\Big):a,b\in\mathbb{F}_{p^m},c\in\mathbb{F}_p\right\}$$

for $f(x)=x^2$ and $f(x)=x^{p^k+1}$, respectively, where $Tr(\cdot)$ is the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$, and k is a nonnegative integer. In this paper, we further investigate the subfield code $\mathcal{C}_f$ for $f(x)$ being a known perfect nonlinear function over $\mathbb{F}_{p^m}$ and generalize some results in [17,35]. The weight distributions of the constructed codes are determined by applying the theory of quadratic forms and the properties of perfect nonlinear functions over finite fields. In addition, the parameters of the duals of these codes are also determined. Several examples show that some of our codes and their duals have the best known parameters according to the code tables in [16]. The duals of some proposed codes are optimal according to the Sphere Packing bound if $p\geq 5$.

AMS subject classifications: 94B05, 94B25

Key words: Subfield code, perfect nonlinear function, quadratic form, weight distribution, Sphere Packing bound.

*Corresponding author. *Email addresses:* dzheng@hubu.edu.cn (D. Zheng), waxiqq@163.com (X. Wang), liyayao2020@163.com (Y. Li), yuanmu847566@outlook.com (M. Yuan)

1 Introduction

Let p be an odd prime and $\mathbb{F}_{p^m}$ be a finite field of size p^m. An $[n,k,d]$ code $\mathcal{C}$ over the finite field $\mathbb{F}_{p^m}$ is a k-dimensional linear subspace of $\mathbb{F}_{p^m}^n$ with minimum Hamming distance d. An $[n,k,d]$ code is called distance-optimal if there dose not exist $[n,k,d+1]$ code [12]. The Hamming weight of a codeword $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$ is the number of nonzero c_i for $0\leq i\leq n-1$. Let A_i denote the number of nonzero codewords with Hamming weight i in $\mathcal{C}$. The weight enumerator of $\mathcal{C}$ is defined by $1+A_1x+A_2x^2+\cdots+A_nx^n$ and the sequence $(1,A_1,\cdots,A_n)$ is called the weight distribution of $\mathcal{C}$. The weight distribution of a code is used to estimate the error correcting capability and compute the error probability of error detection and correction of the code [23]. The weight distributions of linear codes have also application in cryptography and combinatorics. Hence, the research of the weight distribution of a linear code is a hot topic in coding theory. The recent progress on weight distributions of linear codes can be seen in [10,11,21,22,25,27,30–32,34,36,38–40] and the references therein.

Let $f(x)$ be a function from $\mathbb{F}_{p^m}$ to itself. Then $f(x)$ is called a perfect nonlinear (PN) function or planar function if

$$\max_{a\in\mathbb{F}_{p^m}^*}\max_{b\in\mathbb{F}_{p^m}}\left|\{x\in\mathbb{F}_{p^m}:f(x+a)-f(x)=b\}\right|=1.$$

PN functions were first introduced to construct finite projective planes by Dembowski and Ostrom [9] in 1968. Then looking for new non-equivalent PN functions has aroused a lot of interest for many researchers in cryptography since these functions are optimally resistant to linear and differential cryptanalysis when used in DES-like cryptosystems. Up to now, all known PN functions from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ with explicit expressions are equivalent to one of the following polynomials [1,2,8,9,13,37]:

- $f_1(x)=x^{p^k+1}$, where $k\geq 0$ and $2\nmid\frac{m}{\gcd(m,k)}$ (Dembowski and Ostrom [9]).
- $f_2(x)=x^{\frac{p^k+1}{2}}$, where $p=3$, $2\nmid k$, and $\gcd(m,k)=1$ (Coulter and Matthews [8]).
- $f_3(x)=x^{10}-\beta x^6-\beta^2x^2$, where $p=3$, $2\nmid m$ and $\beta\in\mathbb{F}_{p^m}^*$ (Ding and Yuan [13]).
- $f_4(x)=\beta x^{p^k+1}-\beta^{p^s}x^{p^{ls}+p^{-ls+k}}$, where β is a primitive element in $\mathbb{F}_{p^m}$, $m=3s$, $\gcd(3,s)=1$, $2\nmid\frac{s}{\gcd(s,k)}$, $k\equiv\pm s \pmod 3$, $l=1$ if $s-k=0 \pmod 3$ and $l=-1$ if $s+k=0 \pmod 3$ (Zha *et al.* [37]).