Avrupa Bilim ve Teknoloji Dergisi
Sayı 38, S. 514-519, Ağustos 2022
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 38, pp. 514-519, August 2022
Copyright © 2022 EJOSAT
Research Article

Some Binary Quasi-perfect Linear Codes Defined by APN Functions

Seher Tutdere [*]

[*]Balıkesir University, Faculty of Science and Letters, Departmant of Mathematics, Balıkesir, Turkey, (ORCID: 0000-0001-5645-8174), stutdere@gmail.com

(First received 13 January 2022 and in final form 28 August 2022)

(**DOI:**10.31590/ejosat.1057393)

ATIF/REFERENCE: Tutdere, S. (2022). The Covering Radii of Some Linear Codes Defined by APN Functions. *European Journal of Science and Technology*, (38), 514-519.

Abstract

In 2022, Tutdere proved that the covering radii R of a class of primitive binary cyclic codes with minimum distance strictly greater than an odd integer ℓ satisfy $r \leq R \leq \ell$, where ℓ, r are some integers depending on the given code. We here first discuss some equivalences of linear codes defined by Gold functions, which are quadratic APN (almost perfect nonlinear) functions. We then show that by applying the result of Tutdere one can find the covering radii of these quasi-perfect codes. In 2016, Li and Helleseth proved that the linear codes defined by the quadratic APN functions are quasi-perfect and they asked whether the linear codes defined by the non-quadratic APN functions are quasi-perfect or not. We here prove that the linear codes defined by some non-quadratic APN functions over the finite field $\mathbb{F}_{2^m}$, for $1 \leq m \leq 8$, are quasi-perfect, by computing the covering radii of these codes.

Keywords: APN functions, Finite field, Covering radius, Cyclic code.

APN Fonksiyonlar ile Tanımlanan Bazı İkili Yarı-mükemmel Lineer Kodlar

Öz

2022 yılında, Tutdere, minimum uzaklığı bir tek ℓ sayısından büyük olan bir primitif ikili devirli kodlar sınıfının örtme yarıçapı R nin $r \leq R \leq \ell$ eşitsizliğini sağladığını göstermiştir, burada ℓ, r verilen koda bağlı olan tam sayılardır. Burada, ilk olarak kuadratik APN (hemen hemen mükemmel lineer olmayan) fonksiyon olan Gold fonksiyonlar ile tanımlanan lineer kodların bazı denklikleri incelenmiştir. Daha sonra Tutdere'nin elde ettiği sonucun uygulanarak bu yarı-mükemmel kodların örtme yarıçaplarının hesaplanabileceği gösterilmiştir. 2016 yılında Li ve Helleseth, kuadratik APN fonksiyonlar ile tanımlanan lineer kodların yarı-mükemmel olduklarını göstermişlerdir ve kuadratik olmayan APN fonksiyonlar ile tanımlanan kodların yarı-mükemmel olup olmadığı problemini sunmuşlardır. Burada, sonlu cisim $\mathbb{F}_{2^m}$, $1 \leq m \leq 8$ için, üzerinde tanımlanan kuadratik olmayan bazı APN fonksiyonlar ile tanımlanan lineer kodların örtme yarıçapları hesaplanarak bu kodların yarı-mükemmel olduğu gösterilmiştir.

Anahtar Kelimeler: APN fonksiyonlar, Sonlu Cisim, Örtme Yarıçapı, Devirli Kodlar.

[*]Corresponding Author: stutdere@gmail.com

1. Introduction

In coding theory, cyclic codes are an important class of error-correcting codes which have favorable algebraic properties for efficient error detection and correction. In literature, there are many examples and studies on these codes, for instance see (Çalışkan, 2021), (Moreno et al., 2003), (Kavut et al., 2019). We here consider binary primitive cyclic codes defined by the APN functions over finite fields, which are linear codes. Let $\mathbb{F}_q$ be a finite field, with $q = 2^m$ where $m \geq 1$ is an integer, and let C be a binary cyclic $[n, k, d]$ code having length n, dimension k, minimum distance $d \coloneqq d(C)$, and covering radius $R \coloneqq R(C)$. By definition, R is the smallest integer r such that every element of $\mathbb{F}_q^{n-k}$ can be written as a linear combination of at most r columns of the parity-check matrix of C. In other words, the covering radius of C is the maximal distance of any vector from the code, i.e.,

$$R \coloneqq \max\{\min\{d(x,c) : c \in C\} : x \in \mathbb{F}_q\}$$

where $d(.,.)$ is the Hamming distance. It has many applications in the information theory, such as data compression, testing, and write-once memories, for instance see (Cohen et al., 1997).

The covering radii of cyclic codes has been comprehensively studied by many researchers since the paper (Delsarte, 1973), for instance see (Carlet, 2010), (Cohen et al., 1985). Let α be a primitive element of $\mathbb{F}_{2^m}$ and let C be a primitive binary cyclic code. In (Moreno et al., 2003, Theorem 6), Moreno and Castro proved that if the zeros of C are α, α^{2^i+1} with $(i, m) = 1$, then $R(C) = 3$, where $d(C) = 5$ (Van Lint et al.,1986). They also showed that if the zeros of C are α, α^{2^i+1}, α^{2^j+1} with distinct positive integers i, j and $d(C) = 7$, then $R(C) = 5$ for $m > 8$ (Moreno et al., 2003, Theorem 9). In (Kavut et al., 2019) Kavut and Tutdere gave a generalization of the aforementioned results of Moreno and Castro as follows: if the zeros of C are α, $\alpha^{2^{i_1}+1}$, …,$\alpha^{2^{i_t}+1}$, where $t = (r-1)/2$, r is any odd integer such that $d(C) \geq r + 2$, then $R(C) = r$, under some restrictions on m and r. In (Tutdere, 2022), Tutdere proved the following: if the zeros of C are α^{d_0}, α^{d_1}, …,α^{d_t}, where d_i's are distinct positive integers, and the sum of 2-weights of d_i's, which we call ℓ, is odd such that $d(C) > l$, then $r \leq R(C) \leq \ell$, under some assumptions on m and r.

APN functions have a great importance in cryptography for the attacks on block ciphers. In (Li et al., 2016), Li and Helleseth proved that the codes defined by the binary quadratic APN functions are quasi-perfect by computing the covering radii of these codes, and they asked whether the codes defined by the non-quadratic functions are quasi-perfect or not. Note that quasi-perfect codes are the codes having covering radius one more than their packing radius. To find a classification of the parameters for which quasi-perfect codes exist is a hard task. In particular, binary quasi-perfect codes play a fundemental role in information theory when using a binary symmetric channel.

We here first discuss some linear equivalent quasi-perfect cyclic codes defined by the Gold functions, which are quadratic APN functions. We then show that one can obtain the covering radii of these codes by applying the result of (Tutdere, 2022).

We next prove that the codes defined by some non-quadratic APN functions over the finite field $\mathbb{F}_{2^m}$, for $1 \leq m \leq 8$, are quasi-perfect, by computing the covering radii of these codes. Further, we find in the process that the covering radii of the codes defined by the inverse function for odd values of m, which are not APN, is the same as those of the APN functions.

The organization of the paper is as follows: We give, in Section 2, some basic background and known results which will be used in the subsequent sections. In Section 3, we give the main results and discussion. Section 4 is devoted to the conclusion and some recommendations.

2. Material and Method

For any prime number p, let $f\colon \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be a function with $f(0) = 0$ and let α be a primitive element of the field $\mathbb{F}_{p^m}$. Set $n := p^m - 1$. Consider the matrix

$$H_f = \begin{bmatrix} 1 & \alpha & \alpha^2 \ldots & \alpha^{n-1} \\ f(1) & f(\alpha) & f(\alpha^2)\ldots & f(\alpha^{n-1}) \end{bmatrix}$$

where each entry stands for the column of its coordinate with respect to a basis of the vector space $\mathbb{F}_{p^m}$ over the field $\mathbb{F}_p$. We denote the code having H_f as a parity-check matrix by C_f. It is clear that when $f(x) = x^d$ is a power function, C_f is a cyclic code with the generator polynomial $g(x) = m_1(x)m_d(x)$, where $m_i(x)$ is the minimal polynomial of α^i over $\mathbb{F}_p$ for $i = 1$, d. We here consider only power functions. Throughout this paper, f is a power function and the related code C_f is a binary primitive cyclic $[n, k, d]$ code having length $n = 2^m - 1$, dimension k, minimum distance $d = d(C)$, and covering radius $R = R(C_f)$.

Definition 2.1. The linear codes satisfying the conditon that $R = \left\lfloor \frac{d+1}{2} \right\rfloor$ are called quasi-perfect codes.

Definition 2.2. A function$f\colon \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ of the form

$$f(x) = \sum_{i,j=0}^{m-1} a_{ij} x^{2^i+2^j},$$

where $a_{ij} \in \mathbb{F}_{p^m}$ is called a quadratic function.

Definition 2.3. A function $f\colon \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is called almost perfect nonlinear (APN) if

$$\max_{a,b \in \mathbb{F}_{p^m}, a\neq 0} \left|\{x \in \mathbb{F}_{p^m} : f(x+a) - f(x) = b\}\right| = 2.$$

In other words, if f is differentially 2-uniform, then it is called an APN function. In particular, when $p = 2$, f is called APN if and only if the function $x \to f(x+a) - f(x)$ is two-to-one for all $0 \neq a \in \mathbb{F}_{2^m}$.

Lemma 2.1.(Carlet et al., 1998, Theorem 5(ii)) Let $f\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a function with $f(0) = 0$. Then f is APN if and only if the code C_f defined by f has minimum distance 5.

In (Carlet et al., 1998), it is shown that if f is a quadratic APN function in odd number of variables, i.e., m is odd, then the related code C_f has covering radius 3. In (Li et al., 2016), the followig result is obtained.

Theorem 2.1.(Li et al., 2016, Theorem 1) Let $m \geq 3$ and

$$f(x) = \sum_{i,j=0}^{m-1} a_{ij} x^{2^i+2^j},$$

where $a_{ij} \in \mathbb{F}_{2^m}$, be a quadratic function. Then the code C_f defined by f is quasi-perfect if and only if f is APN.

In (Li et al., 2016), the following open problem is proposed:

Open problem: For all APN functions f over $\mathbb{F}_{2^m}$, are the codes C_f defined by f quasi-perfect or not?

Theorem 2.2. (Tutdere, 2022) Let C be a primitive binary cyclic code with the zero set $Z(C) = \{\alpha^{d_0}, \alpha^{d_1}, \dots, \alpha^{d_t}\}$ for some distinct positive integers $d_0, d_1, \dots, d_t$. Suppose that there is a code C' such that $C \subset C'$ and $d(C') = r$ for any integer r. Assume that the sum $\ell := \sum_{i=0}^{t} \sigma_2(d_i)$ is an odd integer. If $d(C) > l$, then $r \leq R(C) \leq \ell$ for

$$f > (\ell - s)\max \sigma_2(d_i),$$

where s is the largest integer such that $2^s | (\ell + 1)$.

In Section 3.1. we propose an application of Theorem 2.2. We now give the following notion which will be used frequently throughout the paper.

Definition 2.4. Let p be a prime number and n be an integer with p-expansion

$$n = a_0 + a_1 p + \cdots + a_s p^s$$

where $0 \leq a_i < p$.The sum $\sigma_p(n) := \sum_{i=0}^{s} a_i$ is called the p-weight of n and the p-weight degree of a monomial $x^d := x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$is defined as

$$\omega_p(x^d) := \sigma_p(d_1) + \sigma_p(d_2) + \cdots + \sigma_p(d_n).$$

The p-weight degree of a polynomial $F(x_1, x_2, \dots, x_n) = \sum_d a_d x^d$ is

$$\omega_p(F) := \max_{x^d, a_d \neq 0} \omega_p(x^d)$$

Definition 2.5. Two codes C_1 and C_2 of the same length over the field $\mathbb{F}_q$ are called equivalent if C_2 is obtained from C_1 by applying a combination of the following operations:
(i) multiplication of the symbols appearing in a fixed position in all codewords of C_1 by a nonzero scaler,
(ii) a permutation of the digits in all codewords of C_1.

Note that a function f from $\mathbb{F}_{2^m}$ has a unique representation as follows:

$$f(x) = \sum_{i=0}^{2^m-1} a_i x^i \ , \quad \text{where each } a_i \in \mathbb{F}_{2^m}.$$

3. Results and Discussion

3.1. Some Equivalences of Linear Codes Defined by Gold Functions

The functions $f_i(x) = x^{2^i+1}$, with $(i, m) = 1$ are called Gold functions (Gold, 1968) for all $m \geq 3$, which are quadratic APN power functions. In this section we first discuss some equivalences of codes defined by Gold functions. We then more generally mention from some equivalences of codes defined by power functions.

Proposition 3.1. Let C be a primitive cyclic code with the zero set $\{\alpha^{d_1}, \alpha^{d_2}\}$ for some distinct d_1 and d_2 over the field $\mathbb{F}_{2^m}$ such that $(d_1, 2^m - 1) = 1$. Then C is equivalent to the code defined by Gold function $f(x) = x^{2^i+1}$, for some i such that $(i, m) = 1$ if $d_2 \equiv d_1(2^i + 1) \bmod (2^m - 1)$, and hence these codes are quasi-perfect.

Proof. Set $n = 2^m - 1$. It is well-known that if $(d_1, 2^m - 1) = 1$, then $\beta = \alpha^{d_1}$ is also a primitive element of $\mathbb{F}_{2^m}$. Therefore, there is a positive integer k such that $\alpha^{d_2} = \beta^k$ for some k. Then by assumption we have $\beta^k = \alpha^{d_2} = \alpha^{d_1(2^i+1) \bmod (2^m-1)}$, and so $k = 2^i + 1$. That means, C is equivalent to the code with the zero set $\{\beta, \beta^{2^i+1}\}$, which corresponds to the code defined by the Gold function $f(x) = x^{2^i+1}$.

It is known from (Moreno et al., 2003) that the code with the zero set $\{\beta, \beta^{2^i+1}\}$ is quasi-perfect. We here give a detailed proof by using the result of (Tutdere, 2022) which covers that result of (Moreno et al., 2003). The parity-check matrix of the code corresponding to the function f is as follows:

$$H_f = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ f(1) & f(\beta) & f(\beta^2) & \dots & f(\beta^{n-1}) \end{bmatrix}$$
$$= \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^{2^i+1} & \beta^{2(2^i+1)} & \dots & \beta^{(n-1)(2^i+1)} \end{bmatrix}.$$

By Lemma 2.1, the code C_f has minimum distance $d(C) = 5$. It is well-known that the code C' with the zero set $\{\beta\}$ is the Hamming code and $d(C') = 3$. Since $C \subset C'$, we can apply Theorem 2.2 with $\beta, C = C_f, C'$, and the parameters $r = 3$, $d_0 = 1$, $d_1 = 2^i + 1$. Then the parameter $\ell = 1 + 2 = 3$. Clearly, the codition $d(C) > l$ is satisfied. Thus, it follows from Theorem 2.2 that $R(C) = 3$ for all $m > (l - s)\max_i \sigma_2(d_i) = (3 - 2) \cdot 2 = 2$, i.e., $m \geq 3$. Then, it follows from Definition 2.1 that the related code is quasi-perfect.

Example 3.1. Let us consider the code C over $\mathbb{F}_{2^4}$ having the zero set $\{\alpha^3, \alpha^7\}$, where α is a primitive element of $\mathbb{F}_{2^4}$.The parity-check matrix H of the code C is then obtained as follows:

$$H = \begin{bmatrix} 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^{14} \\ 1 & \alpha^7 & (\alpha^7)^2 & \dots & (\alpha^7)^{14} \end{bmatrix}.$$

As $(7,15) = 1$, $\beta = \alpha^7$ is also a primitive element of $\mathbb{F}_{2^4}$ and then we have $\beta^k = \alpha^3 = (\alpha^7)^k$, from which it is found that $k = 2^3 + 1 = 9$. Therefore, the zero set $\{\alpha^3, \alpha^7\}$ can be equivalently considered as $\{\beta, \beta^9\}$, which gives the code equivalent to the one defined by the Gold function $f_3(x) = x^{2^3+1}$ (notice that $(3,4) = 1$, satisfying the condition imposed by the definition). Hence, the parity-check matrix H can be expressed in the following form:

$$H = \begin{bmatrix} 1 & \beta^9 & (\beta^9)^2 & \dots & (\beta^9)^{14} \\ 1 & \beta & \beta^2 & \dots & \beta^{14} \end{bmatrix}$$
$$= \begin{bmatrix} 1 & \beta^9 & (\beta^2)^9 & \dots & (\beta^{14})^9 \\ 1 & \beta & \beta^2 & \dots & \beta^{14} \end{bmatrix}.$$

Since permuting the positions of a code generates an equivalent code, the code C is equivalent to the code C' having the parity check matrix H' given below:

$$H' = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{14} \\ 1 & \beta^9 & (\beta^2)^9 & \dots & (\beta^{14})^9 \end{bmatrix}.$$

In (Tutdere, 2022) the covering radii and the minimum distances of the primitive cyclic codes having distinct zero sets are given for $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^5}$ in Tables 1 and 2, respectively. It can be seen from Table 1 in (Tutdere, 2022) that there are only three quasi-perfect codes having distinct zero sets which are $\{\alpha^5\}$, $\{\alpha, \alpha^3\}$

and $\{\alpha^3, \alpha^7\}$. We have already shown that the code with zero set $\{\alpha, \alpha^3\}$ is equivalent to the one with zero set $\{\alpha, \alpha^9\}$; however as α^3 and α^9 are in the cyclotomic coset, i.e., $\alpha^9 = \alpha^{3\cdot 2^i \bmod 15}$ for $i = 3$, these two codes are also equivalent. As a consequence, there is only one quasi-perfect code defined by the power functions different up to the equivalence which corresponds to the code defined by the Gold function for the field $\mathbb{F}_{2^4}$.

Let us now relax the condition of being equivalent to the Gold function in Proposition 3.1, by permitting that the exponent k can be any positive integer. In this case, assuming as in Proposition 3.1 that the primitive cyclic code C has the zero set $\{\alpha^{d_1}, \alpha^{d_2}\}$ for some distinct d_1 and d_2 over the field $\mathbb{F}_{2^4}$ such that $(d_1, 2^m - 1) = 1$, the code C is equivalent to the code defined by the power function $f(x) = x^d$ for some d if $d_2 \equiv d_1 d \mod (2^m - 1)$, which can be considered as a more general form of Proposition 3.1. Next, we give an example for this situation.

Example 3.2. We here consider the code C over $\mathbb{F}_{2^5}$ with the zero set $\{\alpha^3, \alpha^{11}\}$, where α is a primitive element of $\mathbb{F}_{2^5}$. The parity-check matrix H of the code C is then obtained as follows:

$$H = \begin{bmatrix} 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^{30} \\ 1 & \alpha^{11} & (\alpha^{11})^2 & \dots & (\alpha^{11})^{30} \end{bmatrix}.$$

One can choose $\beta = \alpha^3$, which is another primitive element of $\mathbb{F}_{2^5}$ and then it is found that $(\alpha^3)^{14} = \beta^{14} = \alpha^{11}$. Thus, the zero set can be equivalently represented by $\{\beta, \beta^{14}\}$, for which the parity-check matrix H can be written as follows:

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \dots & \beta^{30} \\ 1 & \beta^{14} & (\beta^{14})^2 & \dots & (\beta^{14})^{30} \end{bmatrix}.$$

Consequently, the code with the zero set $\{\alpha^3, \alpha^{11}\}$ is equivalent to that with the zero set $\{\alpha, \alpha^k\}$ for any $k \in \{7, 14, 19, 25, 28\}$, as α^7, α^{14}, α^{19}, α^{25}, α^{28} are in the same cyclotomic coset. In (Tutdere, 2022), it can be seen from Table 2 that every code over the field $\mathbb{F}_{2^5}$ with the zero set $\{\alpha^{d_1}, \alpha^{d_2}\}$ such that $\{d_1, d_2\} \in \{1, 3, 5, 7, 11, 15\}$ has the covering radius 3 and the minimum distance 5, satisfying the condition of being quasi-perfect. Hence, the code C that we consider in this example is quasi-perfect.

As the mentioned quasi-perfect codes given in (Tutdere, 2022) is complete for the field $\mathbb{F}_{2^5}$, we have checked the codes which are different up to the equivalence, following our argument used in the above examples. Then we have found that there are five such codes having the zero sets $\{\alpha, \alpha^3\}$, $\{\alpha, \alpha^5\}$, $\{\alpha, \alpha^7\}$, $\{\alpha, \alpha^{11}\}$, and $\{\alpha, \alpha^{15}\}$. On the other hand, it is well-known that the inverse of an APN function is also an APN (Carlet, 2010). Recalling from (Nyberg, 1994) that the inverse of x^{2^i+1} is x^d, where

$$d = \sum_{k=0}^{\frac{m-1}{2}} 2^{2ik} \mod (2^m - 1),$$

with m being odd. It can be easily found that the exponents x^7 and x^{11} are obtained from the inverses of the Gold functions.

3.2. Covering Radius for Non-quadratic APNs

In (Li et al., 2016), Li and Helleseth computationally find for small values of m that the covering radius of the codes defined by the known non-quadratic APN functions on $\mathbb{F}_{2^m}$ is 3 and mainly based on this observation, whether the codes for all APN functions are quasi-perfect is posed as an open question (see Section 2), which is still unsettled. However, the details of their computation and the values of m is not given in (Li et al., 2016). We here compute the covering radii for $m \leq 8$ for all the known non-quadratic APN functions, which are listed in Table 1, and find that the codes defined by those APN functions have covering radius 3, which confirms the result of (Li et al., 2016) independently. As a result we obtain the following.

Theorem 3.2. The codes defined by the non-quadratic APN functions given in Table 1 are quasi-perfect for all $m \leq 8$.

Proof. Let C_f be a code defined by a non-quadratic APN function f over the finite field $\mathbb{F}_{2^m}$ given in Table 1. By Lemma 2.1. the minimum distance of C_f is 5. By using the Sage code given in Figure 1, we obtain that the covering radius of C_f is 3. Therefore, by Definition 2.1, C_f is a quasi-perfect code.

Tablo 1. $\mathbb{F}_{2^m}$ üzerinde kuadratik olmayan ve bilinen tüm x^d biçimindeki APN fonksiyonları.

Table 1. All the known non-quadratic APN functions in the form of x^don $\mathbb{F}_{2^m}$.

Family	Exponent (d)	Condition
(Dobbertin,2001)	$16^i + 8^i + 4^i + 2^i - 1$	$i = m/5$
Inverse (Nyberg, 1994)	$4^i - 1$	$i = \frac{m-1}{2}$
(Kasami,1971)	$4^i - 2^i + 1$	$(i, m) = 1$
Niho (Dobbertin,1999), (Hollmann et al., 2001)	$2^i + 2^{i/2} - 1$, for even i $2^i + 2^{\frac{3i+1}{2}} - 1$, for odd i	$i = \frac{m-1}{2}$
Welch (Canteaut et al., 2000), (Dobbertin, 1999)	$2^i + 3$	$i = \frac{m-1}{2}$

We use Sage (Developers et al., 2020) with GAP package Guava, which is limited to computing with finite fields of size at most 256, to find the covering radius of codes corresponding to the APN functions in Table 1. The Sage code that we use is given in Figure 1.

```
1:   m=eval(input('Enter m:'))
2:   d=eval(input('Enter d:'))
3:   R.<x> = PolynomialRing(GF(2))
4:   F.<t> = GF(2^m)
5:   p = t.minpoly()
6:   q = (t^d).minpoly()
7:   g = p*q
8:   C = codes.CyclicCode(generator_pol = g, length = 2^m-1)
9:   print('Covering radius =',C.covering_radius())
```

Figure 1. Sage code used to compute the covering radius.

Şekil 1. Örtme yarıçapını hesaplamak için kullanılan Sage kodu.

In Figure 1, lines 1 and 2 request from user to enter the degree of the extension field (m) and the exponent (d), respectively. Line 3 creates a univariate polynomial ring R in x over $\mathbb{F}_2$ and line 4 builds a finite field F in t of size 2^m. Lines 5 and 6 obtain the minimal polynomials of t and t^d as p and q, respectively. Then, multiplying the minimal polynomials p and q, the generator polynomial g of the cyclic code C is found in line 7. After that, the cyclic code C of length $2^m - 1$ is constructed in line 8 by using the generator polynomial g. Finally, line 9 computes and displays the covering radius of the code C. Notice that the command *covering_radius* in line 9 requires the GAP package Guava.

Remark 3.3. It is well-known that the inverse function $x \to x^{-1}$ on $\mathbb{F}_{2^m}$ is differentially 4-uniform for even values of m, that is, it is not an APN function. For this case, we have checked the covering radius of the inverse function for even $m \leq 8$ and found that it is also 3. However, it is necessary to find the minimum distance to show that whether they are quasi-perfect or not (see Definition 2.1), which may require a huge computation power. Hence, with a personel computer we could only compute (by using Sage) for a small value of $m = 4$ that the inverse function is not quasi-perfect as the minimum distance is found as 3.

We now give an example to illustrate the computation of the covering radius of a code corresponding to an APN function.

Example 3.3. For simplicity, let us consider the inverse function $f(x) = x^3$ on $\mathbb{F}_{2^3}$, i.e., $m = 3$ and $d = 3$ (see Table 1) . It should be noted that in this case all the APN functions (except the Dobbertin family for which the corresponding condition is not satisfied for $m = 3$) in Table 1 are quadratic and equivalent to the Gold function. The parity-check matrix of the corresponding code C_f of length $2^3 - 1 = 7$ is then obtained as follows:

$$H_f = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ f(1) & f(\alpha) & f(\alpha^2) & f(\alpha^3) & f(\alpha^4) & f(\alpha^5) & f(\alpha^6) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \end{bmatrix},$$

where α is a primitive element of the field $\mathbb{F}_{2^3}$ and each element of the parity-check matrix H_f can be represented by a binary vector of length 3. The binary representation of the elements of $\mathbb{F}_{2^3}$ is given by Table 2, in which α is the primitive element of the irreducible polynomial $\alpha^3 + \alpha + 1$.

Tablo 2. $\mathbb{F}_{2^3}$ sonlu cisim elemanlarının ikili gösterimleri.

Tablo 2. The binary representations of the elements of the finite field $\mathbb{F}_{2^3}$.

Field elements	Polynomial representation	Binary representation
0	0	$(0,0,0)$
1	1	$(0,0,1)$
α	α	$(0,1,0)$
α^2	α^2	$(1,0,0)$
α^3	$\alpha+1$	$(0,1,1)$
α^4	$\alpha^2+\alpha$	$(1,1,0)$
α^5	$\alpha^2+\alpha+1$	$(1,1,1)$
α^6	α^2+1	$(1,0,1)$

Substituting the binary representations for the respective field elements of the parity-check matrix, we get the following form of H_f:

$$H_f = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix},$$

from which we should find the smallest number such that every element of $\mathbb{F}_2^6$, i.e., every binary vector of length 6 corresponding to the 8-ary 2-tuples, can be represented by a linear combination of at most that number of columns to determine the covering radius of the code C. Clearly, there are 7 columns of H_f and the numbers $1 + \binom{7}{1} = 8$ and $1 + \binom{7}{1} + \binom{7}{2} = 29$ of the linear combinations of at most one and two columns, respectively, are less than the number $2^6 = 64$ of the elements of $\mathbb{F}_2^6$. Thus, the covering radius should be greater than 2. One can computationally check that when we take into account the linear combinations of 3 columns, all the binary vectors of length 6 are produced, and consequently the covering radius of the code C_f obtained from the inverse function $f(x) = x^3$ on $\mathbb{F}_{2^3}$ is 3. Notice that the code C_f has minimum distance 5 due to Lemma 2.1, and hence the condition of being quasi-perfect given by Definition 2.1 is satisfied.

4. Conclusions and Recommendations

In this paper, we studied on the covering radii of some cyclic codes defined by the quadratic and non-quadratic APN functions over the finite fields $\mathbb{F}_{2^m}$.We first gave a discussion on some equivalences of quasi-perfect codes defined by Gold functions, and showed that by applying the result of (Tutdere, 2022), one can obtain the covering radii of these codes. Next, by computing the covering radii of the codes defined by some non-quadratic APN functions over the finite field $\mathbb{F}_{2^m}$, for $1 \leq m \leq 8$, we showed that these codes are quasi-perfect. Moreover, we found out in the process that the covering radii of the codes defined by the inverse function for odd values of m, which are not APN, is the same as those of the APN functions. By studying on the method of (Tutdere, 2022), one may obtain the covering radii of the codes defined by the non-quadratic APN functions for large values of m ($m \geq 9$) as a future work. If it is true that all these codes have covering radius 3, then as the minimum distance of these codes is 5, one obtains a large class of binary quasi-perfect codes.

References

Canteaut, A., P. Charpin, P., & Dobbertin, H. (2000). Binary m-sequences with three-valued crosscorrelation: a proof of Welch’s conjecture. *IEEE Trans. Inf. Theory,* 46(1), 4-8.

Carlet, C. (2010). Vectorial Boolean functions for cryptography. In Boolean Models and Methods in Mathematics. Computer Science, and Engineering. Eds. Y. Crama and P. L. *Hammer, Cambridge Univ. Press*, 398-469.

Carlet, C., Charpin, P., & Zinoviev, V. (1998). Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes. Crypt.*, 15(2), 125-156.

Cohen, G. D., Honkala, I., Litsyn, S., & Lobstein, A. (1997). Covering Codes. *Elsevier*.

Cohen, G. D., Karpovsky, M. G., Jr. Mattson, H. F., and Schatz, J. R. (1985). Covering radius-survey and recent results. *IEEE Trans. Inform. Theory*, 31(3), 328-343.

Cohen, G. D., Litsyn, S. N., Lobstein, A. C., & Jr. Mattson, H. F. (1997). Covering radius 1985-1994. *Appl. Algebra Engrg. Comm. Comput.*, 8(3), 173-239.

Çalışkan, B. (2021). $\mathbb{Z}_8$+$u\mathbb{Z}_8$+$v\mathbb{Z}_8$ Üzerinde Aykırı Devirli Kodlar İçin Bazı Sonuçlar. *Avrupa Bilim ve Teknoloji Dergisi*, (28), 660-664.

Delsarte, P. (1973). Four fundamental parameters of a code and their combinatorial significance. *Inf. Control*, 23, 407-438.

Dobbertin, H. (1999). Almost perfect nonlinear power functions on GF(2^n): the Welch case. *IEEE Trans. Inf. Theory*, 45(4), 1271-1275.

Dobbertin, H. (1999). Almost perfect nonlinear power functions on GF(2^n): the Niho case. *Inf. Comput.*, 151(1), 57-72.

Dobbertin, H. (2001). Almost perfect nonlinear power functions on GF(2^n): a new case for *n* divisible by 5. *Finite Fields and Applications, Springer, Berlin, Heidelberg.* 113-121. *https://doi.org/10.1007/978-3-642-56755-1_11*

Gold, R. (1968). Maximal recursive sequences with three-valued recursive cross-correlation functions. *IEEE Trans. Inf. Theory*, 14(1), 154-156.

Hollmann, H. & Xiang, Q. (2001). A proof of the Welch and Niho conjectures on cross-correlations of binary *m*-sequences. *Finite Fields and Their Applications*, 7(2), 253-286.

Kavut, S. & S. Tutdere, S. (2019). The covering radii of a class of binary cyclic codes and some BCH codes. *Des. Codes Cryptogr.*, 87, 317-325.

Kasami, T. (1971).The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Inf. Control*, 18(4), 369-394.

Nyberg, K. (1994). Differentially uniform mappings for cryptography. *Advances in Cryptology- Eurocrypt'93, LNCS 765. Springer, Berlin Heidelberg*, 55-64.

Li, C. & Helleseth, T. (2016). Quasi-perfect linear codes from planar and APN functions. *Cryptography and Communications*, 8(2), 215-227.

Moreno, O. & Castro, N. F. (2003). Divisibility properties for covering radius of certain cyclic codes. *IEEE Trans. Inform. Theory*, 49(12), 3299-3303.

Tutdere, S. (2022). On the covering radii of a class of binary primitive cyclic codes. *Hacettepe Journal of Mathematics and Statistics*, 51(1), 20-26.

Van Lint, J. H. & R. Wilson, R. (1986). On the minimum distance of cyclic codes. *IEEE Trans. Inform. Theory*, 32(1), 23-40.

Developers, T. S., Stein, W., Joyner, D., Kohel, D., Cremona, J., & Eröcal, B. (2020). *SageMath, version 9.0*. Retrieved from http://www.sagemath.org