최소거리가 5인 이진 순회부호의 최소거리에 관한 새로운 증명

정회원 정 하 봉*, 노 종 선**

New Proof of Minimum Distance for Binary Cyclic Codes with $d_{\min}=5$

Habong Chung*, Jong-Seon No** *Regular Members*

요 약

부호길이가 2^n-1이고 생성다항식이 $g(x)=m_1(x)m_d(x)$인 이진 순회부호에서 최소거리가 5가 되기 위한 조건은 x^d가 APN 함수라는 것으로 이는 이미 알려진 내용인데 이에 관한 새로운 증명을 제시하였다.

ABSTRACT

We investigated into the minimum distance of a primitive binary cyclic code C with a generator polynomial $g(x)=m_1(x)m_d(x)$. It is known that the necessary and sufficient condition for C to have minimum distance five is the fact that x^d is an APN power function. In this paper, we derive the new proof of minimum distance for the primitive binary cyclic codes with minimum distance five.

Ⅰ. INTRODUCTION

Finding the true minimum distance of a binary cyclic code with a given generator polynomial has long been studied since the notion of cyclic codes were brooded. Several lower bounds on the minimum distance of a cyclic code are known. The oldest one is BCH bound [1] and this BCH bound has been improved by Hartmann and Tzeng [2], Roos [3], and van Lint and Wilson [4].

Binary cyclic codes with small minimum distance has also been studied. Charpin, et. al. [5] studied the case of minimum distance 3 and Charpin, et. al. [6] and van Lint and Wilson [8] studied the case of minimum. It is known that the necessary and sufficient condition for C to have minimum distance five is the fact that x^d is an APN power function [7].

In this paper, we derive the another proof of minimum distance for a primitive binary cyclic code to have minimum distance 5. In section II, the notion of almost perfect nonlinear(APN) power function is reviewed. The proof of minimum distance for the cyclic code is derived in section III.

Ⅱ. PRELIMINARIES

Let $GF(2^m)$ be a finite field with 2^m elements and α be a primitive element. Let $m_i(x)$ be the minimal polynomial of the element α^i over $GF(2)$. A primitive binary cyclic code is the one

* 홍익대학교 전기전자공학부 ** 서울대학교 전기공학부

논문번호 : 00319-0804, 접수일자 : 2000년 8월 4일

※ 본연구는 한국과학재단의 특정기초연구사업(97-0100-0501-3)의 지원에 의해 수행되었습니다.

whose length is 2^m-1 and the generator polynomial $g(x)$ is given by $g(x)=\prod_{i\in I} m_i(x)$, where each element in I belongs to distinct cyclotomic cosets.

In this paper, we are concentrating on the minimum distance property of the primitive cyclic code of the case when $g(x)= m_1(x)m_d(x)$. In the forthcoming discussions, the notion of APN property of a function plays an important role so that we will review the APN property.

Definition 1 : A mapping F from $GF(p^m)$ to $GF(p^m)$ is called APN if each equation

$$F(t+a)-F(t)=b$$

has at most two solutions t in $GF(p^m)$ for any a in $GF(p^m)^*$ and b in $GF(p^m)$. □

APN power functions on $GF(2^m)$ were originally studied for applications in cryptology. See Beth and Ding [9], Helleseth, Rong and Sandberg [10], Nyberg [11], and Dobbertin [12]. All the known APN power functions x^d on $GF(2^m)$ are listed in [12].

When m is odd, all the APN power functions are one-to-one mappings and when m is even, they are all three-to-one. Following lemma shows that the APN power functions are either one-to-one or three-to- one.

Lemma 2 : If x^d is an APN power function on $GF(2^m)$, then $(2^m-1,d)=1$ or 3.

Proof : Manifest by considering the equation $x^d+(x+1)^d=0$. □

Let C be a binary cyclic code with length 2^m-1 whose generator polynomial $g(x)$ is given by $g(x)=m_1(x)m_d(x)$. From the following lemma, we can easily see that the code C has no codewords of weight 3 or 4, if x^d is an APN power function on $GF(2^m)$.

Lemma 3 : Let C be a binary cyclic code of length 2^m-1 with a generator polynomial $g(x)=m_1(x)m_d(x)$. If x^d is an APN power function over $GF(2^m)$, then the minimum distance of C is at least 5.

Proof : Since the code C is a subset of a Hamming code whose generator polynomial is $m_1(x)$, it is enough to show the nonexistence of codewords of weight 3 and 4. The nonexistence of codewords of weight 3 and 4 can be directly shown from the APN property of x^d. The existence of a codeword of weight 3 implies that the following equation

$$x^d+(x+1)^d=1 \tag{1}$$

has a solution other than $x=0$ or 1. But this is impossible since (1) has exactly 2 solutions, $x=0$ and 1 from the APN property of x^d. The nonexistence of a codeword of weight 4 is also straightforward. If C has a codeword of weight 4, then two equations $x+y+z=1$ and $x^d+y^d+z^d=1$ has a common solution (x,y,z) such that $x\neq y\neq z\neq x$ and $x,y,z\notin\{0,1\}$. Thus, the solution must satisfy

$$x^d+(x+x+1)^d=y^d+(y+x+1)^{d.} \tag{2}$$

But, since x^d is an APN function, (2) implies either $x=y$ or $y=1$, which violate the condition above. □

Naturally, the next question is whether the minimum distance of the above code is 5. The answer is yes and it is stated as the main theorem.

Ⅲ. NEW PROOF OF THE MINIMUM DISTANCE

It is known that the necessary and sufficient condition for C to have minimum distance five is the fact that x^d is an APN power function as given in the following theorem [7].

Theorem 4 : Let C be a binary cyclic code of length 2^m-1, with a generator polynomial $g(x)=m_1(x)m_d(x)$. If and only if x^d is an APN power function, then the minimum distance of C is 5. □

In this paper, we derive the new proof of the above theorem. Due to Lemma 3, it is enough to show the existence of a codeword of weight 5. From Lemma 2, there are two cases on d, the case when $(d, 2^m-1)=1$ and $(d, 2^m-1)=3$. Now consider the case when $(d, 2^m-1)=1$ first. Let us define a set A_u for $u\in GF(2^m)^*$ as

$$A_u=\{x^d+(x+u)^d+(1+u)^d \mid x\in GF(2^m)\}. \quad (3)$$

Since $x^d+(x+u)^d+(1+u)^d = u^d\left\{\left(\frac{x}{u}\right)^d + \left(\frac{x}{u+1}\right)^d\right\}+(1+u)^d$, the set A_u can also be written as

$$A_u=u^dA_1+(1+u)^d. \quad (4)$$

The existence of a codeword of weight 5 implies that two equations

$$x+y+z+w=1 \quad (5)$$

and

$$x^d+y^d+z^d+w^d=1 \quad (6)$$

has a common solution (x,y,z,w) such that x,y,z,w are all distinct and $x,y,z,w\notin\{0,1\}$. Thus the solution must satisfy

$$x^d+y^d+z^d+(x+y+z+1)^d=1. \quad (7)$$

In (7), set $y=x+v$ and divide (7) by v^d, then we have

$$\left(\frac{x}{v}\right)^d+\left(\frac{x}{v}+1\right)^d = \left(\frac{z}{v}\right)^d+\left(\frac{z}{v}+1+\frac{1}{v}\right)^d+\left(\frac{1}{v}\right)^d. \quad (8)$$

By setting $u=1+\frac{1}{v}$, we can say that (8) implies that two sets A_1 and A_u have some common elements under the condition that $x,y,z,w\notin\{0,1\}$, are all distinct. The following lemma summarizes this discussion.

Lemma 5 : If C has no codewords of weight 5, then for any $u(\neq 1)$ in $GF(2^m)^*$,

$$A_1\cap A_u=\{1, u^d+(1+u)^d\}. \quad (9)$$

Proof : The two sets A_1 and A_u can be written as follows:

$$A_1=\{x^d+(x+1)^d \mid x\in GF(2^m)\} \quad (10)$$

$$A_u=\{y^d+(y+u)^d+(1+u)^d \mid y\in GF(2^m)\}. \quad (11)$$

Certainly, $x=1$ in (10) and $y=1$ in (11) yield the element 1, and $x=u$ in (10) and $y=0$ in (11) yield the element $u^d+(1+u)^d$ in $A_1\cap A_u$. If there is some other element s in $A_1\cap A_u$, then we can write

$$s=x^d+(x+1)^d=y^d+(y+u)^d+(1+u)^d. \quad (12)$$

The equation (12) implies the existence of a codeword of weight 5 if x^d, $(x+1)^d$, y^d, $(y+u)^d$, and $(1+u)^d$ are all distinct and none of them are zero. But, it is easy to show that if any two of the above 5 elements are the same, then the resulting s is either 1 or $u^d+(1+u)^d$. □

Since the cardinality of A_u is $2^{m}-1$ for any u, Lemma 5 tells us that only two elements in $GF(2^m)$ are missing in $A_1\cap A_u$. Now let us call these two elements as $m_1(u)$ and $m_2(u)$. Then we have the following lemma.

Lemma 6 : Let C have no codewords of weight 5. If $(1+u)^d\notin A_1$, then $\{m_1(u), m_2(u)\}=\{(1+u)^d, 1+u^d\}$ and if $\left(1+\frac{1}{u}\right)^d\notin A_1$, then $\{m_1(u), m_2(u)\} = \{0, 1+u^d+(1+u)^d\}$.

Proof : Since $\sum_{z\in A_u} z=0$, it is easy to see that $m_1(u)+m_2(u)=1+u^d+(1+u)^d$. From (10),

$0 \notin A_1$.

Thus from (4), $(1+u)^d \notin A_u$. Therefore, if $(1+u)^d \notin A_1$, then $(1+u)^d \notin A_1 \cap A_u$, which implies that one of $m_1(u)$ and $m_2(u)$ is $(1+u)^d$, in turn, the other is $1+u^d$. Similarly, if $\left(1+\frac{1}{u}\right)^d \notin A_1$, then $u^d\left(1+\frac{1}{u}\right)^d + (1+u)^d = 0 \notin A_u$. Thus, $0 \notin A_1 \cap A_u$, which tells us that one of $m_1(u)$ and $m_2(u)$ is 0, and consequently, the other is $1+u^d+(1+u)^d$. □

Since the sets $\{(1+u)^d, 1+u^d\}$ and $\{0, 1+u^d+(1+u)^d\}$ are disjoint, Lemma 6 tells us that $(1+u)^d \in A_1$ implies $\left(1+\frac{1}{u}\right)^d \notin A_1$, and vice versa. It also tells that $(1+u)^d \notin A_1$ implies $1+u^d \notin A_1$, and $(1+u)^d \in A_1$implies $1+u^d \in A_1$. These can be summarized as follows:

Corollary 7 : If C has no codewords of weight 5, then for any $u(\neq 1) \in GF(2^m)^*$, $(1+u)^d \in A_1$ implies that $1+u^d \in A_1$ and $\left(1+\frac{1}{u}\right)^d \notin A_1$. □

Lemma 8 : If C has no codewords of weight 5, then for any $u(\neq 1) \in GF(2^m)^*$, $(1+u)^d \in A_1$ implies $u^d \notin A_1$.

Proof : If not, there must exist some u such that $u^d \notin A_1$ and $(1+u)^d \notin A_1$. Now, $(1+u)^d \notin A_1 \Rightarrow \left(1+\frac{1}{u}\right)^d \in A_1$. Thus, from (4), we have

$$\left(\frac{u}{u+1}\right)^d\left(1+\frac{1}{u}\right)^d + \left(1+\frac{u}{u+1}\right)^d$$
$$= 1+\left(\frac{1}{u+1}\right)^d \in A_{\frac{u}{u+1}}.$$

Since the only two elements belonging to both A_1 and $A_{\frac{u}{u+1}}$ are 1 and $\left(\frac{u}{u+1}\right)^d + \left(\frac{1}{u+1}\right)^d$, we have

$$1+\left(\frac{1}{u+1}\right)^d \notin A_1. \tag{13}$$

But, $u^d = \{1+(1+u)\}^d \notin A_1 \Rightarrow 1+(1+u)^d \notin A_1 \Rightarrow \left(1+\frac{1}{u+1}\right)^d \in A_1$. Thus, we have

$$1+\left(\frac{1}{u+1}\right)^d \in A_1, \tag{14}$$

□

From the Corollary 7 and Lemma 8, we can have following corollaries.

Corollary 9 : If C has no codewords of weight 5, then $\overline{A_1} = 1 + A_1$. □

Corollary 10 : If C has no codewords of weight 5, then for any $u(\neq 1) \in GF(2^m)^*$, $u^d \in A_1$ implies $\frac{1}{u^d} \notin A_1$. □

Proof of the Theorem 4 :

i) The case when $(d, 2^m-1)=1$:

Let $u(\neq 1)$ be some nonzero element such that $u^d \in A_1$. From Lemma 8, $u^d \in A_1 \Rightarrow (1+u)^d \notin A_1$. Thus, from Lemma 6, we have

$$A_1 \cap A_u = \{1, u^d + (1+u)^d\},$$

and

$$\overline{A_1} \cap \overline{A_u} = \{1+u^d, (1+u)^d\}.$$

Consider the element $s_1 = \frac{(1+u)^d}{1+u^d}$. Since $s_1 = u^d s_1 + (1+u)^d$, s_1 is either in $A_1 \cap A_u$ or in $\overline{A_1} \cap \overline{A_u}$. In other words, s_1 must be one of the four elements, 1, $1+u^d$, $(1+u)^d$, and $u^d+(1+u)^d$. But we can easily check that $s_1 \neq 1$, $s_1 \neq (1+u)^d$, and $s_1 \neq u^d + (1+u)^d$. Therefore, s_1 must be $1+u^d$, so we have $(1+u)^d = 1+u^{2d}$. This tells that whenever $u^d \in A_1$, $(1+u)^d = 1+u^{2d}$, and alternately if $(1+u)^d \in A_1$, then $u^d = (1+u)^{2d}+1$. Since only one of x^d and $(1+x)^d$ is in A_1 for any x, we have

$$x^d + (1+x)^d = \begin{cases} x^{2d} + x^d + 1, & \text{if } x^d \in A_1 \\ (1+x)^{2d} + (1+x)^d + 1, & \text{if } x^d \notin A_1 \end{cases} \tag{15}$$

From (15) we have $tr_1^m\{x^d+(1+x)^d\}=tr_1^m(1)$. Since the set A_1 is the collection of all the elements of the form $x^d+(1+x)^d$ and the size of A_1 is 2^m-1, we have

$$A_1=\{x\in GF(2^m)\mid tr_1^m(x)=tr_1^m(1)\}, \qquad (16)$$

which in turn implies that

$$\overline{A_1}=\{x\in GF(2^m)\mid tr_1^m(x)=tr_1^m(1)+1\}. \qquad (17)$$

Now, if m is even, then (16) and (17) become $A_1=\{x\in GF(2^m)\mid tr_1^m(x)=0\}$ and $\overline{A_1}=\{x\in GF(2^m)\mid tr_1^m(x)=1\}$, respectively, which contradicts the Corollary 9, since $tr_1^m(x)=tr_1^m(x+1)$.

If m is odd, then (16) and (17) become $A_1=\{x\in GF(2^m)\mid tr_1^m(x)=1\}$ and $\overline{A_1}=\{x\in GF(2^m)\mid tr_1^m(x)=0\}$, respectively, which contradicts the Corollary 10 since there always exists some nonzero element $v(\neq 1)$ such that $tr_1^m(v)=tr_1^m(v^{-1})$ in the field $GF(2^m)$ if $m>3$. The last statement can be proven as follows : If every nonzero element $v(\neq 1)$ in $GF(2^m)$ satisfies that $tr_1^m(v)=tr_1^m(v^{-1})+1$, then two polynomials

$$f(x)=\frac{x^{2^{m-1}}+x^{2^{m-2}}+\cdots+x^4+x^2+x}{x} \qquad (18)$$

and

$$g(x)=\frac{x^{2^{m-1}}+x^{2^{m-2}}+\cdots+x^4+x^2+x+1}{x+1} \qquad (19)$$

are reciprocal to each other, i.e., $f(x)=x^{2^{m-1}-1}\cdot g\left(\frac{1}{x}\right)$, since $x^{2^m}+x=x(x+1)f(x)g(x)$ and the roots of $f(x)$ are all the elements whose trace is 0 except 0 and the roots of $g(x)$ cover all but 1 whose trace is 1. The polynomial $g(x)$ can be rewritten as

$$\begin{aligned} g(x) &= \frac{x^{2^{m-1}}+1}{x+1}+\frac{x^{2^{m-2}}+1}{x+1}+\cdots+\frac{x^2+1}{x+1}+\frac{x+1}{x+1} \\ &= \sum_{j=0}^{2^{m-1}-1}x^j+\sum_{j=0}^{2^{m-2}-1}x^j+\cdots+\sum_{j=0}^{1}x^j+1. \end{aligned} \qquad (20)$$

For example, compare the coefficient of x^2 in $f(x)$ and the coefficient of $x^{2^{m-1}-3}$ in $g(x)$. From (18), the coefficient of x^2 in $f(x)$ is 0, but from (20), the coefficient of $x^{2^{m-1}-3}$ in $g(x)$ is 1 unless $m=3$. Therefore, $f(x)$ can not be reciprocal to $g(x)$ if $m>3$, which leads us to a contradiction.

ii) The case when $(d, 2^m-1)=3$:

In this case, m must be even, thus $GF(4)$ is a subfield of $GF(2^m)$. Let β be a primitive element of $GF(4)$. Now, pick some $u(\notin GF(4))$ such that

$$z^d+(z+u)^d=1 \qquad (21)$$

has a nonzero solution. Set $z=v$ to be the solution of (21). Then, $x=\beta(u+1)$, $y=\beta^2(u+1)$, $z=v$, and $w=v+u$ are the common solutions of the equations (5) and (6), which implies the existence of a codeword of weight 5. □

REFERENCES

[1] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inform. and Control 3*, pp. 68-79, 1960.

[2] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH bound," *Inform. and Control 20*, pp. 489-498, 1972.

[3] C. Roos, "A new lower bound on the minimum distance of a cyclic code," *IEEE Trans. Inform. Theory*, IT-29, pp. 330-332, 1983.

[4] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, IT-32, pp. 23-40, 1986.

[5] P. Charpin, A. Tietavainen and V. A. Zinoviev, "On binary cyclic codes with minimum distance three," *Proc. Fifth Intern. Workshop on Algebraic and Combinatorial Coding Theory*, pp. 93-97, Sozopol, Bulgaria, 1966.

[6] P. Charpin, A. Tietavainen and V. A. Zinoviev, "On the minimum distance of

certain cyclic codes," *Proc. 1997 Intern. Symp. on Inform. Theory*, p. 505, Ulm, Germany, 1997.

[7] C. Carlet, P. Charpin, and V. Zinoviev, "'Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125-156, 1998.

[8] J. H. van Lint and R. M. Wilson, "Binary cyclic codes generated by m_1m_7," {\em IEEE Trans. Inform. Theory}, IT-32, p. 283, 1986.

[9] T. Beth and C. Ding, "On almost perfect nonlinear permutations," *Advances in Cryptology - EUROCRYPT '93}, T. Helleseth (ed.), Lecture Notes in Computer Science*, vol. 765, pp. 65-76, Springer-Verlag, 1994.

[10] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Trans. Inform. Theory*, to be published.

[11] K. Nyberg, "Differentially uniform mappings for cryptography," *Advances in Cryptology - EUROCRYPT '93}, T. Helleseth (ed.), Lecture Notes in Computer Science*, vol. 765, pp. 55-64, Springer-Verlag, 1994.

[12] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case," *IEEE Trans. Inform. Theory*, IT-45, pp. 1271-1275, 1999.

정 하 봉(Habong Chung) 정회원
한국통신학회논문지 제23권 5호 참조

노 종 선(Jong-Seon No) 종신회원
한국통신학회논문지 제25권 4A호 참조