ATLANTIS PRESS
Advances in Computer Science Research (ACSR), volume 73
7th International Conference on Education, Management, Information and Computer Science (ICEMC 2017)

Generating Idempotents of Residue Codes over the Binary Field

Xuedong Dong [1,*] and Yan Zhang [2]

[1] College of Information Engineering, Dalian University, Dalian 116622, P.R.China

[2] School of Mathematics, Liaoning Normal University, Dalian 116029, P.R.China

Corresponding author: dongxuedong@sina.com

Keywords: Generating idempotent; Residue code; Cyclic code

Abstract. This paper gives explicit expressions of generating idempotents of higher power residues codes of length p over the binary field, where p is a prime. By computing the greatest common divisors of these generating idempotents and the polynomial x^p-1 with computer software such as Matlab and Maple, one can get the generating polynomials of residue codes over the binary field .

Introduction

Quadratic residue codes are nice family of cyclic codes that has approximately 1/2 code rates, tends to have high minimum distance and includes some Hamming codes and Golay codes [1]. Idempotents of quadratic residue codes were discussed in Chapter 16 of [2]. Decoding algorithms for quadratic residue codes were still interesting [3]. There are various generalizations of quadratic residue codes. Charters [4] provided a generalization of binary quadratic residue codes to the cases of higher power prime residues over the finite field of the same order. Higher power residue codes and forms of generating polynomials of these codes were proposed in [5-9].Generating polynomials of higher power residue codes are factors of x^n-1. Generally speaking, it is difficult to factor the polynomial x^n-1 over finite fields. In [7-10], generating idempotents of cubic, quartic, quintic, and sixth residue codes over the binary field F_2 were given. This paper gives explicit expressions of generating idempotents of higher power residues codes of length p over the binary field, where p is a prime. Thus, the generating polynomials of higher power residues codes over the binary field can be obtained by computing the greatest common divisors of these generating idempotents and the polynomial x^n-1 with computer software such as Matlab. The rest of this paper is organized as follows. In Section 2 we give some preliminaries. Generating idempotents of residue codes over the binary field are given in Section 3. Finally, summary is given in Section 4.

Preliminaries

Definition 1.If there exists an integer x such that $x^t \equiv a(\bmod p)$, where $a \in Z$ and $(a,p)=1$,then a is called a t-th residue modulo p.

In the following we assume that p is an odd prime and ρ is a primitive element of the finite field F_p. Let $R_0=\{\rho^{tk} \in F_P \mid k \in Z\}$, $R_1=\{\rho^{tk+1} \in F_P \mid k \in Z\}$, $\cdots, R_{t-1}=\{\rho^{tk+(t-1)} \in F_P \mid k \in Z\}$. Let m be the smallest positive integer such that $2^m \equiv 1(\bmod p)$, α a primitive p-th root of unity in F_{2^m}, and $g_0(x)=\prod_{r_0 \in R_0}(x-\alpha^{r_0}), g_1(x)=\prod_{r_1 \in R_1}(x-\alpha^{r_1}), \cdots, g_{t-1}(x)=\prod_{r_{t-1} \in R_{t-1}}(x-\alpha^{r_{t-1}})$.

Lemma 1. $x^p-1=(x-1)g_0(x)\cdots g_{t-1}(x)$ and $g_j(x)=\prod_{r_j\in R_j}\left(x-\alpha^{r_j}\right)\in F_2[x]$ for $j=0,1,2,\cdots,t-1$.

Definition 2.[7] The t-th residue codes $C_0,\cdots,C_{t-1},\overline{C}_0,\cdots,\overline{C}_{t-1}$ are cyclic codes of $F_2[x]/(x^p-1)$ with generator polynomials $g_0(x),\cdots,g_{t-1}(x),(x-1)g_0(x),\cdots,(x-1)g_{t-1}(x)$ respectively.

Definition 3.[10,p.132] An element $e(x)\in F_2[x]/(x^p-1)$ satisfying $e(x)^2\equiv e(x)(\mathrm{mod}(x^p-1))$ is called an idempotent. Each cyclic code contains a unique idempotent which generates the ideal. This idempotent is called the generating idempotent of the cyclic code.

Definition 4.[10, p.138] Let a be an integer such that $(a,n)=1$. The function μ_a defined on $\{0,1,\cdots,n-1\}$ by $i\mu_a\equiv ia(\mathrm{mod}\,n)$ is a permutation of the coordinate positions $\{0,1,\cdots,n-1\}$ of a cyclic code of length n and is called a multiplier. μ_a acts on $F_p[x]/(x^n-1)$ by $f(x)\mu_a\equiv f(xa)\ (\mathrm{mod}\,x^n-1)$, where $f(x)\in F_p[x]/(x^n-1)$.

Lemma 2.[10, p.139] Let C be a cyclic code of length n over the finite field F_q with generating idempotent $e(x)$. Let a be an integer such that $(a,n)=1$. Then $e(x)\ \mu_a$ is the generating idempotent of the cyclic code $C\mu_a$.

Lemma 3.[7] $C_0,\cdots,C_{t-1}$ are pairwise equivalent and $\overline{C}_0,\cdots,\overline{C}_{t-1}$ are pairwise equivalent.

In the following assume that $e_0(x)=\sum_{r_0\in R_0}x^{r_0}\ e_1(x)=\sum_{r_1\in R_1}x^{r_1}\ \cdots,e_{t-1}(x)=\sum_{r_{t-1}\in R_{t-1}}x^{r_{t-1}}$,

Lemma 4. [7] $e_0(x)+e_1(x)+\cdots+e_{t-1}(x)+\sum_{i=0}^{p-1}x^i=1$

Lemma 5.[7] Let $E(x)$ be the generating idempotent of a t-th residue code C. Then $E(x)=a+\sum_{i=0}^{t-1}a_ie_i(x)$, where $a,a_0,a_1,\cdots,a_{t-1}\in F_2$.

Lemma 6. If $\overline{E}_0(x)$ is the generating idempotent of the residue code $\overline{C}_0$, then $E_0(x)=\overline{E}_0(x)+\sum_{i=0}^{p-1}x^i$ is the generating idempotent of C_0.

Proof. The proof is similar to that of Lemma 9 in [7].

Lemma 7.If $E_0(x)$ and $\overline{E}_0(x)$ are respectively the generating idempotents of the t-th residue codes C_0 and $\overline{C}_0$, and $d=\rho^{tk+t-1}\in R_{t-1}$, then

1. $E_0(x)\mu_d=E_1(x),E_1(x)\mu_d=E_2(x),\cdots,E_{t-2}(x)\mu_d=E_{t-1}(x)$ are respectively the generating idempotents of the t-th residue codes $C_1,\cdots,C_{t-1}$.
2. $\overline{E}_0(x)\mu_d=\overline{E}_1(x),\overline{E}_1(x)\mu_d=\overline{E}_2(x),\cdots,\overline{E}_{t-2}(x)\mu_d=\overline{E}_{t-1}(x)$ are respectively the generating idempotents of the t-th residue codes $\overline{C}_1,\cdots,\overline{C}_{t-1}$.

Proof. The proof is similar to that of Lemma 10 in [7].

Generating Idempotents of the Residue Codes

Theorem 1.Let p be an odd prime, t a positive integer, $t \mid (p-1)$, and $2^{\frac{p-1}{t}} \equiv 1 (\bmod p)$. Let α be a primitive p -th root of unity in an extensiton of the binary field F_2.Then

（1）If $t = 2k+1, k \geq 0$ and $e_i(\alpha) = 1, e_{i+1(\bmod t)}(\alpha) = e_{i+2(\bmod t)}(\alpha) = \cdots = e_{i+(t-1)(\bmod t)}(\alpha) = 0$, where the subscript is the smallest nonnegative residue modulo t,then the set of the generating idempotents of $C_0, \cdots, C_{t-1}$ is $\{1+e_0(x), 1+e_1(x), \cdots 1+e_{t-1}(x)\}$, the set of the generating idempotents of $\overline{C}_0, \cdots, \overline{C}_{t-1}$ is $\{e_1(x)+e_2(x)+\cdots+e_{t-1}(x), e_0(x)+e_2(x)+\cdots+e_{t-1}(x), \cdots, e_0(x)+e_2(x)+\cdots+e_{t-2}(x)\}$.

（2）Suppose that $t = 4k$ or $t = 4k+2, k \geq 0$ and $p \equiv 1 (\bmod 8)$.

1) If $e_i(\alpha) = 1, e_{i+1(\bmod t)}(\alpha) = e_{i+2(\bmod t)}(\alpha) = \cdots = e_{i+(t-1)(\bmod t)}(\alpha) = 0$, then the set of the generating idempotents of $C_0, \cdots, C_{t-1}$ is $\{1+e_0(x), 1+e_1(x), \cdots, 1+e_{t-1}(x)\}$,the set of the generating idempotents of $\overline{C}_0, \cdots, \overline{C}_{t-1}$ is $\{e_1(x)+e_2(x)+\cdots+e_{t-1}(x), e_0(x)+e_2(x)+\cdots+e_{t-1}(x), \cdots, e_0(x)+e_2(x)+\cdots+e_{t-2}(x)\}$.

2) If $e_i(\alpha) = 0, e_{i+1(\bmod t)}(\alpha) = e_{i+2(\bmod t)}(\alpha) = \cdots = e_{i+(t-1)(\bmod t)}(\alpha) = 1$,then the set of the generating idempotents of $C_0, \cdots, C_{t-1}$ is $\{1+e_1(x)+e_2(x)+\cdots+e_{t-2}(x)+e_{t-1}(x)$, $1+e_0(x)+e_2(x)+\cdots+e_{t-2}(x)$ $+e_{t-1}(x), \cdots, 1+e_0(x)+e_1(x)+\cdots+e_{t-2}(x)\}$,the set of the generating idempotents of $\overline{C}_0, \cdots, \overline{C}_{t-1}$ is $\{e_0(x), e_1(x), \cdots, e_{t-1}(x)\}$.

（3） Suppose that $t = 4k+2, k \geq 0$ and $p \equiv -1 (\bmod 8)$.

1) If $e_i(\alpha) = 0, e_{i+1(\bmod t)}(\alpha) = e_{i+2(\bmod t)}(\alpha) = \cdots = e_{i+(t-1)(\bmod t)}(\alpha) = 1$,then the set of the generating idempotents of $C_0, \cdots, C_{t-1}$ is $\{e_0(x), e_1(x), \cdots, e_{t-1}(x)\}$,the set of the generating idempotents of $\overline{C}_0, \cdots, \overline{C}_{t-1}$ is $\{1+e_1(x)+e_2(x)+\cdots+e_{t-2}(x)+e_{t-1}(x)$, $1+e_0(x)+e_2(x)+\cdots+e_{t-2}(x)+e_{t-1}(x), \cdots, 1+e_0(x)+e_1(x)+\cdots+e_{t-2}(x)\}$.

2) If $e_i(\alpha) = 1, e_{i+1(\bmod t)}(\alpha) = e_{i+2(\bmod t)}(\alpha) = \cdots = e_{i+(t-1)(\bmod t)}(\alpha) = 0$, then the set of the generating idempotents of $C_0, \cdots, C_{t-1}$ is $\{e_1(x)+e_2(x)+\cdots+e_{t-1}(x), e_0(x)+e_2(x)+\cdots+e_{t-1}(x), \cdots, e_0(x)+e_2(x)+\cdots+e_{t-2}(x)\}$, the set of the generating idempotents of $\overline{C}_0, \cdots, \overline{C}_{t-1}$ is $\{1+e_0(x), 1+e_1(x), \cdots 1+e_{t-1}(x)\}$.

Proof：（1）Suppose that $t = 2k+1, k \geq 0$ and $e_{i+1(\bmod t)}(\alpha) = e_{i+2(\bmod t)}(\alpha) = \cdots = e_{i+(t-1)(\bmod t)}(\alpha) = 0,\ e_i(\alpha) = 1.$ Since $(p-1)/t$ is an even,we have $(p-1)/t = 0$ over the binary field F_2.From $e_0(\alpha)+e_1(\alpha)+\cdots+e_{t-1}(\alpha) = 1$ it follows that the number of 1 among $e_0(\alpha), e_1(\alpha), \cdots, e_{t-1}(\alpha)$ is odd. Let $E(x) = 1+e_i(x)$ .Then $E(x) = 1+e_i(x)$ is an idempotent. If $e_i(\alpha) = 1, e_{i+1(\bmod t)}(\alpha) = e_{i+2(\bmod t)}(\alpha) = \cdots = e_{i+(t-1)(\bmod t)}(\alpha) = 0$,then

$\forall s \in R_0, E(\alpha^s)=1+e_i(\alpha^s)=1+e_i(\alpha)=1+1=0$, $\forall s \in R_1$, $E(\alpha^s)=1+e_i(\alpha^s)=1+e_{i+1(\bmod t)}(\alpha)=1+0=1,\cdots$, $\forall s \in R_{t-1}$, $E(\alpha^s)=1+e_i(\alpha^s)=1+e_{i+t-1(\bmod t)}(\alpha)$ $=1+0=1$, $E(1)=1+e_i(1)=1+\frac{p-1}{t}=1+0=1$. This shows that $E(x)=1+e_i(x)$ is the generating idempotent of C_0. By lemma 7,the set of generating idempotents of the residue codes $C_0,\cdots,C_{t-1}$ is $\{1+e_0(x),1+e_1(x),\cdots,1+e_{t-1}(x)\}$,the set of generating idempotents of $\overline{C}_0,\cdots,\overline{C}_{t-1}$ is $\{e_1(x)+e_2(x)+\cdots+e_{t-1}(x), e_0(x)+e_2(x)+\cdots+e_{t-1}(x), \cdots, e_0(x)+e_2(x)+\cdots+e_{t-2}(x)\}$.

（2） Suppose that $t=4k$ or $t=4k+2, k\ge 0$ and $p\equiv 1(\bmod 8)$. Since $(p-1)/t$ is an even,we have $(p-1)/t=0$ over the binary field F_2.

1) When $e_i(\alpha)=1, e_{i+1(\bmod t)}(\alpha)=e_{i+2(\bmod t)}(\alpha)=\cdots=e_{i+(t-1)(\bmod t)}(\alpha)=0$,we use the same method as in （1）to prove that the set of generating idempotents of $C_0,\cdots,C_{t-1}$ is $\{1+e_0(x),1+e_1(x),\cdots,1+e_{t-1}(x)\}$, the set of generating idempotents of $\overline{C}_0,\cdots,\overline{C}_{t-1}$ is $\{e_1(x)+e_2(x)+\cdots+e_{t-1}(x), e_0(x)+e_2(x)+\cdots+e_{t-1}(x), \cdots, e_0(x)+e_2(x)+\cdots+e_{t-2}(x)\}$.

2) When $e_i(\alpha)=0, e_{i+1(\bmod t)}(\alpha)=e_{i+2(\bmod t)}(\alpha)=\cdots=e_{i+(t-1)(\bmod t)}(\alpha)=1$,let $E(x)=1+e_{i+1(\bmod t)}(x)$ $+e_{i+2(\bmod t)}(x)+\cdots+e_{i+t-1(\bmod t)}(x)$.Then $E(x)$ is an idempotent and

$$\forall s \in R_0, E(\alpha^s)=1+e_{i+1(\bmod t)}(\alpha^s)+e_{i+2(\bmod t)}(\alpha^s)+\cdots+e_{i+t-2(\bmod t)}(\alpha^s)+e_{i+t-1(\bmod t)}(\alpha^s)$$
$$=1+e_{i+1(\bmod t)}(\alpha)+e_{i+2(\bmod t)}(\alpha)+\cdots+e_{i+t-2(\bmod t)}(\alpha)+e_{i+t-1(\bmod t)}(\alpha)=\underbrace{1+1+\cdots+1+1}_{t个}=0,$$

$$\forall s \in R_1, E(\alpha^s)=1+e_{i+1(\bmod t)}(\alpha^s)+e_{i+2(\bmod t)}(\alpha^s)+\cdots+e_{i+t-2(\bmod t)}(\alpha^s)+e_{i+t-1(\bmod t)}(\alpha^s)$$
$$=1+e_{i+2(\bmod t)}(\alpha)+e_{i+3(\bmod t)}(\alpha)+\cdots+e_{i+t-1(\bmod t)}(\alpha)+e_i(\alpha)=1+\underbrace{1+1+\cdots+1}_{(t-2)}+0=1,$$

$\cdots$

$$\forall s \in R_{t-1}, E(\alpha^s)=1+e_{i+1(\bmod t)}(\alpha^s)+e_{i+2(\bmod t)}(\alpha^s)+\cdots+e_{i+t-2(\bmod t)}(\alpha^s)+e_{i+t-1(\bmod t)}(\alpha^s)$$
$$=1+e_i(\alpha)+e_{i+1(\bmod t)}(\alpha)+\cdots+e_{i+t-2(\bmod t)}(\alpha)=1+0+\underbrace{1+1+\cdots+1}_{(t-2)}=1,$$

$E(1)=1+e_{i+1(\bmod t)}(1)+e_{i+2(\bmod t)}(1)+\cdots+e_{i+t-1(\bmod t)}(1)=1+(t-1)(p-1)/t=1$. This shows that $E(x)=1+e_{i+1(\bmod t)}(x)+e_{i+2(\bmod t)}(x)+\cdots+e_{i+t-1(\bmod t)}(x)$ is the generating idempotent of C_0. By lemma 7, the set of generating idempotents of the residue codes $C_0,\cdots,C_{t-1}$ is $\{1+e_1(x)+e_2(x)+\cdots+e_{t-2}(x)+e_{t-1}(x)$, $1+e_0(x)+e_2(x)+\cdots+e_{t-2}(x)+e_{t-1}(x)$, $\cdots,1+e_0(x)+e_1(x)+\cdots+e_{t-2}(x)\}$,the set of generating idempotents of $\overline{C}_0,\cdots,\overline{C}_{t-1}$ is $\{e_0(x),e_1(x),\cdots,e_{t-1}(x)\}$.

（3）The proof is similar to that of (2).

Summary

Using coding theory, we have given explicit expressions of generating idempotents of higher power residue codes of length p over the binary field. By computing the greatest common divisors of these generating idempotents and the polynomial $x^p - 1$ with computer software such as Matlab and Maple, one can get the generating polynomials of residue codes over the binary field .

Acknowledgements

This research was financially supported by the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

[1] E.Prange, I.S.Reed and T.K.Truong, Air Force Cambridge Research Center, Cambridge, 2(1958)58-156.
[2] F.J.Macwilliams,N.J.A.Sloane, The Theory of Error-Correcting Codes (Amsterdam, the Netherlands: North-Holland,1977).
[3] T.C.Lin, H.P.Lee, H.C.Chang, T.K.Truong, Information Sciences, 197(2012)215-222.
[4] P. Charters, Finite Fields and Their Applications, 15(2009)404-413.
[5] S.Zhu and A.Chen, Acta Electronic Sinica, 36(2008)2312-2314.
[6] X.Dong, W.Li and Y.Zhang, Computer Engineering and Applications, 49(2013)41-44.
[7] X.Dong, Yao Zhang and Yan Zhang, Computer Engineering and applications, 50(2014)113-117.
[8] X.Dong, Advances in Intelligent Systems Research, 135(2016)357-362.
[9] X.Dong, Y. Zhang, Advances in Computer Science Research (ACSR), 61 (2017)612-617.
[10] W.C.Huffman and V. Pless, Fundamentals of Error Correcting Codes(Cambridge University Press 2003).