Idempotent Polynomials: An Easy Supplant to Generator Polynomials

LUTFUL KARIM, MOHAMMAD SHORFUZZAMAN, and JOBAIDA BEGUM
Department of Computer Science
University of Manitoba
Winnipeg, MB
CANADA

Abstract: Cyclic codes are very useful in error correcting codes. Hence, the construction of good cyclic codes is of utmost importance. A generic class of polynomials called generator polynomials is used to construct the cyclic codes. Finding a generator polynomial necessitates factoring a base polynomial called monic polynomial. Unfortunately, factoring a polynomial is not always an easy task. Idempotent polynomials provide an alternative to get rid of this difficulty where factoring of a polynomial is not necessary. This paper presents different properties and classification of idempotent polynomials such as primitive idempotents and how idempotent polynomials outperform the generator polynomials in constructing good cyclic codes.

Keywords: - Coding theory, Idempotent, Polynomial, Primitive Idempotent, Coset, and Cyclotomic.

1. Introduction
Coding theory, sometimes called algebraic coding theory deals with the design of error correcting codes for the reliable transmission of information across noisy channels. It makes use of classical and modern algebraic techniques involving finite fields, group theory, polynomial algebra, and idempotents. This paper deals with idempotent generators for constructing binary cyclic codes. Before going into the detail, it is necessary to understand the structure of the codes. A $q$-ary code $S$ is a subset of $T = \{0,1,\ldots, q-1\}^n$, $n \geq 1$. The elements of $S$ are called codewords and $n$ is the codeword length. Codes are divided into two main categories: linear codes, nonlinear codes. An $[n, k]$ linear binary code is the set of all linear combinations of $k$ independent codewords. The word linear means that if two (or more) codewords are in a code, so is their sum. On the other hand, a nonlinear code is just a set of codewords. We will consider only the binary linear codes in this paper.

The generator polynomial $[1, 2, 4]$ gives us much information about a code. Cyclic codes are constructed using generator polynomials. A monic polynomial (i.e., $a_n = 1$) $g(x)$ of smallest degree in $C$ is called the generator polynomial of $C$. From the property of generator polynomial, it is obvious that $g(x)$ must divide $1 + x^n$. So, if we can factor $1 + x^n$ over $GF(2)$, then we can construct all cyclic codes of length $n$ over $GF(2)$. However, once we have the generator polynomial we can form a generator matrix for the corresponding code. The idea is to take the generator polynomial as the top row, and filling the other rows with cyclic (right) shifts of $g(x)$. We then convert $G$ into standard form.

Unfortunately, finding codes this way is not always easy, as it is often quite difficult to factor $1 + x^n$. Idempotents are the generators which can be found without factoring $1 + x^n$. A cyclic code can contain many idempotents, one of which only generates the code.

The remainder of the paper is organized as follows. Section 2 briefly describes the idempotent polynomials and their properties. Section 3 then presents a special idempotent called primitive idempotent with its properties. Next, section 4 provides the technique to generate idempotent polynomials without having the necessity of factoring the monic polynomial. Finally, the paper ends with conclusions in section 5.
2. Idempotent Polynomial

There is a polynomial except the generator polynomial which is used to generate cyclic code, called idempotent polynomial [1]. A polynomial \( e(x) \) of a ring \( R_n \) is called idempotent if

\[
e(x) = e(x)^2 = e(x)
\]

Example 1:

\[
(x^3 + x^6 + x^5) \text{ is an idempotent in the ring } R_7.
\]

As, \((x^3 + x^6 + x^5)^2 = (x^3 + x^6 + x^5) = (x^3 + x^6 + x^5)\)

In this way, \( 1, (x^3 + x^6 + x^5) \), \((1 + x + x^2 + x^4), (1 + x^3 + x^6 + x^5) \) are idempotent in \( R_7 \).

Therefore, each cyclic code \( C \) contains a unique idempotent which generates the ideal and it is known as generating idempotent of the cyclic code. For example, \( 0 \) is the generating idempotent of \( \{0\} \) cyclic code and \( 1 \) is the generating idempotent of \( R_n \).

If \( e(x) \) is an idempotent then \( 1 + e(x) \) is also idempotent. For example, when \( (x^3 + x^6 + x^5) \) is idempotent, then \( (1 + x^3 + x^6 + x^5) \) is also an idempotent.

2.1 Properties of Idempotent

Idempotent polynomials hold the following properties [1, 2, 4].

For every ideal \( I \) in \( R_n \), there is a unique polynomial \( e(x) \in I \) called idempotent which have the following properties:

(a) \( e(x) = e(x)^2 = e(x^2) \)

Example 2:

\[
(x + x^2 + x^4) = (x^2 + x^4)^2 = (x + x^2 + x^4)
\]

(b) \( e(x) \) generates \( I \)

Example 3:

For \( n = 7 \),

\[
g(x) = 1 + x + x^3
\]

\[
e(x) = x + x^2 + x^4 = x(1 + x^2 + x^3)
\]

Now,

\[
(x + x^2 + x^3)(x + x^2 + x^4) = 1 + x + x^3
\]

(c) \( e(x) \) is a unit of \( I \)

By (ii) we know that every polynomial \( a(x) \in I \) generated by \( e(x) \) (i.e. multiple of \( e(x) \))

\[
a(x) = a_1(x)e(x)
\]

\[
\Rightarrow a(x)e(x) = a_1(x)e^2(x)
\]

\[
\Rightarrow a(x)e(x) = e(x)a_1(x) \quad [\Theta e(x) = e^2(x)]
\]

\[
\Rightarrow a(x)e(x) = a(x)
\]

Therefore, \( e(x) \) is a unit in \( I \).

Example 4:

Let \( a(x) = x^2 + x^3 + x^5 \) and \( e(x) = x + x^2 + x^4 \)

\[
\therefore a(x)e(x) = (x^2 + x^3 + x^5)(x + x^2 + x^4) = x^2 + x^3 + x^5 = a(x)
\]

(d) Let \( C_1 \) and \( C_2 \) be cyclic codes with idempotent generators \( e_1(x) \) and \( e_2(x) \). Then \( C_1 \cap C_2 \) has as idempotent generator \( e_1(x)e_2(x) \), and \( C_1 + C_2 \) has as idempotent generator \( e_1(x) + e_2(x) - e_1(x)e_2(x) \)

Example 5:

Let \( C_1 = \langle g_1 \rangle \) where, \( g_1 = (1 + x)(1 + x + x^3) \)

\[
c_1 \in C_1, \text{ and let } c_1 = (x + x^2 + x^4)
\]

\[
C_2 = \langle g_2 \rangle \text{ where, } g_2 = (1 + x)(1 + x^2 + x^3)
\]

\[
c_2 \in C_2, \text{ and let } c_2 = (x + x^3 + x^4)
\]

\[
C_1 + C_2 = \langle g \rangle \text{ where } g = (1 + x)
\]

\[
c_1 + c_2 = (x^2 + x^3) = x^2(1 + x) \in (C_1 + C_2)
\]

Again

\[
e_1 = 1 + x^3 + x^5 + x^6, \quad e_2 = 1 + x + x^2 + x^4
\]

Therefore,

\[
e_1 + e_2 - e_1e_2 = x(1 + x)(1 + x^2 + x^4)
\]

It is seen that

\[
(x(1 + x)(1 + x^2 + x^4))^2 = x(1 + x)(1 + x^2 + x^4)
\]

Therefore, \( e_1 + e_2 - e_1e_2 \) is an idempotent of \( C_1 + C_2 \).
On the other hand,
\[(c_1 + c_2)(e_1 + e_2 - e_1e_2) = ((x^2 + x^3))\]
\[x(1+x)(1+x^2 + x^4) = x^2 + x^3 = (c_1 + c_2)\]
In this way, we can also show the idempotent of the intersection of two idempotents.

(e)
Let \(C\) be a cyclic code over \(F[q]\) with generating idempotent \(e(x)\). The generating polynomial of \(C\) is \(g(x) = \gcd(e(x), x^n - 1)\) computed in \(F[q]\).

Example 6:
We know that \((x^4 + x^2 + x)\) is an idempotent of \(C_7\)
\[\gcd((x^4 + x^2 + x),(x^7 - 1)) = x^3 + x + 1\]
and \(x^3 + x + 1\) is a generator polynomial of \(C_7\)

3 Primitive Idempotent
The idempotent of a minimal ideal that does not contain any smaller nonzero ideal is called primitive idempotent. Any idempotent is a sum of primitive idempotents and any vector in \(R_n\) can be written as a sum of vectors from minimal ideals.
The nonzeros of a minimal ideal must be \(\{\alpha^j : i \in C_s\}\) for cyclotomic coset \(C_s\),
\[\theta_s(\alpha^j) = \begin{cases} 1 & \text{if } j \in C_s \\ 0 & \text{otherwise} \end{cases}\]
Where,
\(\alpha^j\) = a minimal nonzero ideal
\(\theta_s\) = a primitive idempotent of \(\alpha^j\)
\(C_s\) = some cyclotomic coset

3.1 Properties of primitive idempotent
Primitive idempotents hold the following properties [1].
(a) \(\theta_s(x) = \sum_{i=0}^{n-1} e_i x^i\)
Where, \(e_i = \sum_{j=0}^{j \in C_s} \alpha^{-ji}\) for \(i \geq 0\)

Example 7:
\[e_i = \sum_{j=0}^{n-1} \theta_s(\alpha^j) \alpha^{-ji} = \sum_{j=0}^{n-1} \alpha^{-ji}\]
If \(n = 7\), the coefficients of \(\theta_1, \theta_3\) are
\[\theta_1 : e_i = \alpha^{-i} + \alpha^{-2i} + \alpha^{-4i}\]
\[\theta_3 : e_i = \alpha^{-3i} + \alpha^{-6i} + \alpha^{-5i}\]
Now we can show that \(\theta_1 = 1 + x + x^2 + x^4\)
\[\theta_1 = \sum_{i=0}^{6} (\alpha^{-i} + \alpha^{-2i} + \alpha^{-4i})x^i\]
= \(1 + (\alpha^{-1} + \alpha^{-2} + \alpha^{-4})(x + x^3 + x^4) + (\alpha^{-4} + \alpha^{-3} + \alpha^{-5})(x^3 + x^6 + x^4)\)
= \(1 + (\alpha^6 + \alpha^5 + \alpha^2)(x + x^3 + x^4) + (\alpha + \alpha^2 + \alpha^4)(x^3 + x^6 + x^4)\)
= \(1 + \{x^3 + x^4\} + 0 \{x^3 + x^6 + x^5\}\)
= \(1 + x + x^2 + x^4\)
In this way we can also show that \(\theta_3 = 1 + x^3 + x^5 + x^6\)

(b) The primitive idempotents satisfy:
(i) \(\sum \theta_s = 1\)
We know that the idempotent of the addition of two ideals \(I_i, I_j\) is the unit of \(I_i + I_j\) and
\(\sum \theta_s\) will be the sum of all idempotents of the cyclotomic cosets \(C_s\). Thus, it will also be a unit. \(\therefore \sum \theta_s = 1\)
(ii) \(\theta_i \theta_j = 0\) if \(i \neq 0\)
In the example 7, we have found,
\[\theta_1 = 1 + x + x^2 + x^4\]
\[\theta_3 = 1 + x^3 + x^5 + x^6\]
Here
\[\theta_1 \theta_3 = (1 + x + x^2 + x^4)(1 + x^3 + x^5 + x^6) = 0\]

4. Generation of Idempotent
Idempotent generators are found from the union of cyclotomic cosets of \(n\). A cyclotomic coset \(C_i\) is found by
\[C_i = ip^m \pmod{n}\]
for all \(m\) (for binary codes, \(p\) is 2). The idempotent generators \(f(x)\) are formed by letting unions of the cyclotomic cosets \(C_i\), for all \(i\) such that \(0 \leq i \leq n\), be powers of \(x\) that occur in \(f(x)\) with nonzero coefficients.
For example, we find the idempotent generators for n=7. Letting p = 2, the cyclotomic cosets of n are C₀ = {0}, C₁ = {1, 2, 4}, and C₃ = {3, 6, 5}. So the idempotents for 1 + x⁷ are 0, 1, x + x² + x⁴ x³ + x⁵ + x⁶, 1 + x + x² + x⁴ x³ + x⁵ + x⁶, 1 + x⁵ + x⁶, x + x² + x³ + x⁴ + x⁵ + x⁶, and 1 + x + x² + x³ + x⁴ + x⁵ + x⁶. All but 0 and 1 are idempotent generators of x⁷ – 1, since 1 generates the whole space and 0 generates the zero vector.

We have already seen in the class that the cyclotomic cosets for n = 7 are C₀ = {0}, C₁ = {1,2,4} and C₃ = {3,6,5}.

From this we can find all eight idempotent listed given bellow with generator polynomials [4, 5].

<table>
<thead>
<tr>
<th>Generator polynomial</th>
<th>Idempotent generators</th>
</tr>
</thead>
<tbody>
<tr>
<td>g₁(x) = (1 + x + x³)(1 + x² + x³)</td>
<td>e₁(x) = g₁(x) = (1 + x + x² + x³ + x⁴ + x⁵ + x⁶)</td>
</tr>
<tr>
<td>g₂(x) = (1 + x)(1 + x + x³)</td>
<td>e₂(x) = x³ g₂(x) = 1 + x³ + x⁵ + x⁶</td>
</tr>
<tr>
<td>g₃(x) = (1 + x)(1 + x² + x³)</td>
<td>e₃(x) = g₃(x) = 1 + x + x² + x⁴</td>
</tr>
<tr>
<td>g₄(x) = (1 + x)</td>
<td>e₄(x) = e₂ + e₃ = x + x² + x³ + x⁴ + x⁵ + x⁶</td>
</tr>
<tr>
<td>g₅(x) = (1 + x + x³)</td>
<td>e₅(x) = x g₅ = x + x² + x³ + x⁵ + x⁶</td>
</tr>
<tr>
<td>g₆(x) = (1 + x² + x³)</td>
<td>e₆(x) = x³ g₆ = x³ + x⁵ + x⁶</td>
</tr>
</tbody>
</table>

*Table 1: Idempotent generators for x⁷ – 1

5. Conclusion

We have shown that idempotent polynomials can be generated directly from the cyclotomic cosets without having the necessity of factoring the monic polynomial. On the contrary, generator polynomials are generated by factoring 1 + xⁿ, which is not always easy to be performed. Hence, generating idempotent polynomials provides a much easier replace for the generator polynomials. Properties of idempotent polynomials have also been described in this paper.

References: