CHAPTER-6

CODES OBTAINED BY COMPOSITION OF EXISTING CODES

The content of this Chapter is based on my following published paper:

CHAPTER-6

CODES OBTAINED BY COMPOSITION OF EXISTING CODES

6.1 INTRODUCTION

The construction of good codes has almost as long a history as coding theory itself. Coding is now required not only for communication but in all electronic items, automatic devices remote control systems, etc. In various applications, we need longer or larger codes, which can be easily implemented. Search for longer length code with desired error correction capability is a difficult exercise and such codes independently developed tend to be inefficient. It has therefore been synthesized to generate such codes by composition of smaller codes. There are various ways in which two codes can be combined to give a new code. From the beginning of coding theory many rules to develop a code with larger size or longer length from codes of smaller size or shorter length have been proposed, some of them have become standard construction in coding theory. A method of combination, called Kronecker product codes, was suggested by Peter Elias in 1954 [26]. A rather powerful generalization with elegant properties of product-codes has later been studied by Sharma by considering partitioned Kronecker product of matrices of the code [90].

There is thus interest in developing new mathematical composition laws on vectors, matrices and polynomials. Elias [26] used Kronecker product of matrices to develop higher efficiency codes by combination of lower order codes. The method was powerful, but it could develop only a sparse class of product codes and the all important duality property was lost. Sharma [90], introduced a new matrix-multiplication called the ‘partitioned product of matrices’, and obtained a rather large class of ‘rank-partitioned product codes’ in which the duality property was preserved.

Cyclic codes, as is known, are ideally suited for implementation through shift registers. It was first noticed by Prange [81] that the class of cyclic codes have a rich algebraic structure. Most important codes like BCH, Goppa codes etc. are cyclic codes.
Another important class of cyclic codes are quasi cyclic (QC) codes having some good algebraic structure. Quasi-Cyclic codes were introduced by Townsend and Weldon [101]. This was followed shortly thereafter by the works of Karlin [57, 58] and Chen [16]. Since then extensive research has been done by Bhargava [8, 9, 100], which are best characterized through their generator polynomials.

Composing higher order cyclic codes from lower order codes in terms of their generator polynomials has not been explored at any length. The reason for not been able to do that is that there does not exist a suitable method of multiplying two polynomials leading to what may be used to consider ‘product of two cyclic codes’.

In this Chapter, we start by introducing a new product of two polynomials defined over a field. It is a generalization of the ordinary product. For convenience we call the two polynomials as outer and inner polynomials. The new defined product then results in non-overlapping segments obtained by multiplying it with coefficients of outer polynomials and expanding powers of the variable. We called it ‘Ordered Power Product’. It has elegant algebraic properties leading to new algebraic structures. Chapter carries a section on applications of the above concepts in developing product of two cyclic and quasi cyclic codes, in terms of the new product defined by us for two polynomials.

Paper is organized as follows:

Section 6.2 gives basic definitions required for later study. In Section 6.3, the ‘Ordered Power Product’ of two polynomials in introduced and its algebraic properties are reported. Section 6.4 carries ‘Applications of Ordered Power Product’ OPP of polynomials in Coding Theory and examples are given to illustrate cyclic and quasi cyclic codes arising from the OPP of two cyclic and quasi cyclic codes.

6.2 BASIC DEFINITIONS

For our purpose, we begin with following simple well known algebraic ideas of polynomials over a field $F$ and recall some definitions and results given in Chapter-1. For details, one may refer to any standard text on Algebra as also Peterson & Weldon [1972], Chapters 2 & 6.
DEFINITION: RING OF POLYNOMIALS

Given a field $F$, a polynomial is given by

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1},$$

where coefficients $a_1, a_2, \ldots, a_{n-1} \in F$. The collection of all polynomials over field $F$, denoted by $F[x]$ under usual addition and product of polynomials, forms a ring, called ‘ring of polynomials over $F$’.

ALGEBRA OF POLYNOMIAL RESIDUE CLASSES (Refer Peterson & Weldon [1972])

The residue classes of the ring of polynomials $F[x]$ modulo a polynomial $f(x)$ of degree $n$ form a commutative linear algebra of dimension $n$ over the coefficient field $F$.

DEFINITION: CYCLIC CODE: An $(n,k)$ block code $C$ is said to be cyclic if it is linear and if for every code word $c_0, c_1, c_2, \ldots, c_n \in C$, its right cyclic shift $c_{n-1}, c_0, c_1, \ldots, c_{n-2} \in C$. An $(n,k)$ cyclic code is generated by a polynomial $g(x)$ of degree $n - k$ that is a factor of $x^n - 1$.

DEFINITION: QUASI CYCLIC CODE: A code is said to be quasi-cyclic (QC) if a cyclic shift of any code word by $p$ positions is still a code word. Thus a cyclic code is a QC code with $p=1$. The block length $n$ of a QC code is a multiple of $p$, or $n = mp$.

Further, there are other classes of QC codes as given below.

1-GENERATOR QC: A 1-generator QC code has the following form of generator matrix;

$$G = [G_0, G_1, \ldots, G_{p-1}]$$

where each $G_i$, $i = 0, 1, 2, \ldots, p-1$, is a circulant matrix of order $m$. Also if $g_0(x), g_1(x), \ldots, g_{p-1}(x)$ are the corresponding defining polynomials of $G_i$, then, $g(x)$ generator is given by
\[ g(x) = g_0(x), g_1(x), ..., g_{p-1}(x) \]

or in the extended form

\[ g(x) = \left( c_{0,0} + c_{0,1}x + ... + c_{0,m-1}, c_{1,0} + c_{1,1}x + ... + c_{1,m-1}, ..., c_{p-1,0} + c_{p-1,1}x + ... + c_{p-1,m-1} \right) \]

is the generator polynomial of \( G \).

Corresponding to above expanded form of \( g(x) \), a code word may be written in following form

\[ C = \left( c_{0,0}, c_{1,0}, ..., c_{p-1,0}, c_{0,1}, ..., c_{p-1,1}, ..., c_{0,m-1}, c_{1,m-1}, ..., c_{p-1,m-1} \right). \]

**2-GENERATOR QC**: A 2 generator Quasi Cyclic code has the generator matrix of the form:

\[
G = \begin{bmatrix}
G_{00}, G_{01}, ..., G_{0,p-1} \\
G_{10}, G_{11}, ..., G_{1,p-1} \\
... & ... & ...
\end{bmatrix}
\]

where \( G_{ij} \) are circulants matrices, for \( i = 0 \) and \( j = 0, 1, 2, ..., p-1 \).

In line of the above definitions, a **T-Generator Quasi Cyclic Code** \((T < p)\) has the generator matrix of the following form:

\[
G = \begin{bmatrix}
G_{00} & G_{01} & ... & G_{0,p-1} \\
G_{10} & G_{11} & ... & G_{1,p-1} \\
... & ... & ... & ...
\end{bmatrix}
\]

**6.3 NEW PRODUCT-ORDERED POWER PRODUCT OF POLYNOMIALS (OPP)**

Linear algebraic structures, as is well known, are studied with advantage through polynomials. While direct polynomial addition and multiplications are commonly used as the operations on polynomials, wider algebraic structures and applications are done by considering polynomial algebra over a field. Here we shall consider polynomials over a field \( F \), and consider the set of all polynomials \( F[x] \). We will be considering structure of \( F[x] \) modulo some polynomial, say, \( g(x) \).

It is proposed to define a new type of composition on polynomials, in which order of the polynomials multiplied is retained and segments of the product arise in terms of rising
powers, we name it as ‘Ordered Power product’. To motivate the new product, let us look at ordinary product of two polynomials

\[ \lambda(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1} x^{m-1} \quad \text{and} \quad \nu(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}. \]

Then \( \lambda(x) \nu(x) = c_0 \nu(x) + c_1 x \nu(x) + a_2 x^2 \nu(x) + \ldots + a_{n-1} x^{n-1} \nu(x) \).

Generalizing this by considering suitably indexed powers of \( x \) in the segments above, we arrive at the following what we call as the ‘Ordered power Product’ (OPP).

**ORDERED POWER PRODUCT OF POLYNOMIALS IN NON-OVERLAPPING SIFTING SEGMENTS**

**DEFINITION: ORDERED POWER PRODUCT OF POLYNOMIALS (OPP)**

Let \( \lambda(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1} x^{m-1} \quad \text{and} \quad \nu(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}, \) be two polynomials of degree \( m-1 \) and \( n-1 \) respectively over a field \( F \). The ordered power product of \( \lambda(x) \) and \( \nu(x) \), (in \( n \)th power of \( x \) in different segments), denoted by \( \lambda(x) \otimes \nu(x) \), is defined as:

\[ \lambda(x) \otimes \nu(x) = c_0 \nu(x) + c_1 x \nu(x)^x + c_2 x^{2n} \nu(x) + \ldots + c_{m-1} x^{(m-1)n} \nu(x) \]

or \( \lambda(x) \otimes \nu(x) = \sum_{i=0}^{m-1} c_i x^i \nu(x) \)

In short we shall call it ‘Ordered Power Product’ (OPP) or \( \otimes - \)product of \( \lambda(x) \) and \( \nu(x) \).

**NOTE 1:** Clearly, the degree of the product polynomial \( \lambda(x) \otimes \nu(x) \) is

\[ (m - 1)n + (n - 1) = mn - 1. \]

**NOTE 2:** We call it ‘ordered’ because as proved below, unlike ordinary product it is not commutative.
**NOTE 3:** Just for convenience, in the product so defined, we will refer to $\lambda(x)$ as outer polynomial and $\nu(x)$ as inner the polynomial.

**EXAMPLE 6.1:** Let $\lambda(x) = 1 + 2x + 4x^3 + 5x^4$ be a polynomial (outer) of degree 4, with $m = 5$, and $\nu(x) = 2 + x^2 + x^6$ be the another polynomial of degrees 6, with $n = 7$ then

$$\lambda(x) \otimes \nu(x) = 1(2 + x^2 + x^6) + 2x^7(2 + x^2 + x^6) + 0x^{14}(2 + x^2 + x^6) + 4x^{21}(2 + x^2 + x^6) + 5x^{28}(2 + x^2 + x^6)$$

$$= 2 + x^2 + 5x^6 + 2x^9 + 10x^{13} + 8x^{21} + 4x^{23} + 20x^{27} + 10x^{28} + 5x^{30} + 5x^{34}$$

This example also verifies the degree of outer product of two polynomials $\lambda(x) \otimes \nu(x)$ mentioned above.

**VECTOR EQUIVALENCE OF OPP**

Interestingly, if polynomials are replaced by their equivalent vectors:

$$\lambda(x) = c_0 + c_1x + c_2x^2 + ... + c_{m-1}x^{m-1} = (c_0, c_1, c_2, ..., c_{m-1}) = \lambda$$

and

$$\nu(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} = (a_0, a_1, a_2, ..., a_{n-1}) = \nu$$

Then it can be easily seen that $\lambda \otimes \nu$ is straight forwardly the Kronecker product of vectors $\lambda$ and $\nu$.

**PROPERTIES OF ORDERED POWER PRODUCT OF POLYNOMIALS**

i. **NON COMMUTATIVITY**

The $\otimes$ product of two polynomials is in general non-commutative, i.e.

$$\lambda(x) \otimes \nu(x) \neq \nu(x) \otimes \lambda(x)$$

**PROOF:** Choosing $\lambda(x)$ and $\nu(x)$ as above, we have

$$\lambda(x) \otimes \nu(x) = (c_0 + c_1x + c_2x^2 + ... + c_{m-1}x^{m-1}) \otimes \nu(x)$$
\[ (c_0v(x) + c_1x^2v(x) + c_2x^{2n}(x) + \ldots + c_{m-1}x^{(m-1)n}v(x)) \quad (6.1) \]

Also, \( v(x) \otimes \lambda(x) = (a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}) \otimes \lambda(x) \)
\[ = (a_0 \lambda(x) + a_1x \lambda(x) + a_2x^{2n} \lambda(x) + \ldots + a_{n-1}x^{(n-1)n} \lambda(x)) \quad (6.2) \]

In general (6.1) and (6.2) are different and this proves the result.

ii. ASSOCIATIVITY

The \( \otimes \) product of two polynomials is in general associative, i.e.
\[ \lambda(x) \otimes (u(x) \otimes v(x)) = (\lambda(x) \otimes u(x)) \otimes v(x) \]

PROOF: Let us consider the three polynomials as,
\[ \lambda(x) = (c_0 + c_1x + c_2x^2 + \ldots + c_{m-1}x^{m-1}), \]
\[ u(x) = (b_0 + b_1x + b_2x^2 + \ldots + b_{k-1}x^{k-1}) \]
and
\[ v(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} \]
of degrees \( m - 1, k - 1 \) and \( n - 1 \) respectively. We then have:
\[ \lambda(x) \otimes (u(x) \otimes v(x)) = \lambda(x) \otimes \left( b_0\left( a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} \right) \right. \\
+ b_1x^n\left( a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} \right) \\
+ b_2x^{2n}\left( a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} \right) + \ldots \\
+ b_{k-1}x^{(k-1)n}\left( a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} \right) \]
\[ = \lambda(x) \otimes \left( b_0a_0 + b_0a_1x + b_0a_2x^2 + \ldots + b_0a_{n-1}x^{n-1} \right) \\
+ x^n\left( b_0a_0 + b_1a_1x + b_1a_2x^2 + \ldots + b_1a_{n-1}x^{n-1} \right) \\
+ x^{2n}\left( b_2a_0 + b_2a_1x + b_2a_2x^2 + \ldots + b_2a_{n-1}x^{n-1} \right) + \ldots \\
+ x^{(k-1)n}\left( b_{k-1}a_0 + b_{k-1}a_1x + b_{k-1}a_2x^2 + \ldots + b_{k-1}a_{n-1}x^{n-1} \right) \]
\[ = (c_0 + c_1x + c_2x^2 + \ldots + c_{m-1}x^{m-1}) \otimes \left( b_0a_0 + b_0a_1x + b_0a_2x^2 + \ldots + b_0a_{n-1}x^{n-1} \right) \\
+ x^n\left( b_0a_0 + b_1a_1x + b_1a_2x^2 + \ldots + b_1a_{n-1}x^{n-1} \right) \\
+ x^{2n}\left( b_2a_0 + b_2a_1x + b_2a_2x^2 + \ldots + b_2a_{n-1}x^{n-1} \right) + \ldots \\
+ x^{(k-1)n}\left( b_{k-1}a_0 + b_{k-1}a_1x + b_{k-1}a_2x^2 + \ldots + b_{k-1}a_{n-1}x^{n-1} \right) \]
\[ + x^{2kn} \left( \begin{align*}
&\left( c_0 b_0 a_0 + c_2 b_0 a_0 x + c_2 b_0 a_2 x^2 + \ldots + c_2 b_0 a_{n-1}x^{n-1} \right) \\
&+ x^n \left( c_0 b_0 a_0 + c_2 b_0 a_0 x + c_2 b_0 a_2 x^2 + \ldots + c_2 b_0 a_{n-1}x^{n-1} \right) \\
&+ x^{2n} \left( c_0 b_0 a_0 + c_2 b_0 a_0 x + c_2 b_0 a_2 x^2 + \ldots + c_2 b_0 a_{n-1}x^{n-1} \right) \\
&+ x^{k-1n} \left( c_0 b_0 a_0 + c_2 b_0 a_0 x + c_2 b_0 a_2 x^2 + \ldots + c_2 b_0 a_{n-1}x^{n-1} \right) \\
&+ \ldots
\end{align*} \right) + \ldots
\]

\[ + x^{(m-1)kn} \left( \begin{align*}
&\left( c_m b_0 a_0 + c_m b_0 a_1 x + c_m b_0 a_2 x^2 + \ldots + c_m b_0 a_{n-1}x^{n-1} \right) \\
&+ x^n \left( c_m b_0 a_0 + c_m b_0 a_1 x + c_m b_0 a_2 x^2 + \ldots + c_m b_0 a_{n-1}x^{n-1} \right) \\
&+ x^{2n} \left( c_m b_0 a_0 + c_m b_0 a_1 x + c_m b_0 a_2 x^2 + \ldots + c_m b_0 a_{n-1}x^{n-1} \right) \\
&+ x^{k-1n} \left( c_m b_0 a_0 + c_m b_0 a_1 x + c_m b_0 a_2 x^2 + \ldots + c_m b_0 a_{n-1}x^{n-1} \right) \\
&+ \ldots
\end{align*} \right) + \ldots
\]

\[ = \left( c_0 b_0 a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + c_0 b_1 x^n \left( a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + \ldots
\]

\[ + x^{kn} \left( c_0 b_0 a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + c_0 b_1 x^n \left( a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + \ldots
\]

\[ + x^{2kn} \left( c_0 b_0 a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + c_0 b_1 x^n \left( a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + \ldots
\]

\[ + x^{k-1n} \left( c_0 b_0 a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + c_0 b_1 x^n \left( a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + \ldots
\]

\[ + x^{(m-1)kn} \left( c_0 b_0 a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + c_0 b_1 x^n \left( a_0 + ax_1 + a_2 x^2 + \ldots + b_{n-1} x^{n-1} \right) + \ldots
\]

\[ = \left( c_0 b_0 a_0 + c_0 b_1 x + c_2 b_0 a_2 x^2 + \ldots + c_0 b_{k-1} x^{k-1} \right) \otimes v(x) +
\]

\[ x^{kn} \left( c_0 b_0 a_0 + c_0 b_1 x + c_2 b_0 a_2 x^2 + \ldots + c_0 b_{k-1} x^{k-1} \right) \otimes v(x) +
\]

\[ + x^{2kn} \left( c_0 b_0 a_0 + c_0 b_1 x + c_2 b_0 a_2 x^2 + \ldots + c_0 b_{k-1} x^{k-1} \right) \otimes v(x) +
\]

\[ = \left( c_0 u(x) \right) \otimes v(x) \]
This proves the result.

iii. **DISTRIBUTIVE OVER ADDITION**

The ⊗ product of two polynomials is such that:

(a) The outer polynomial distributes over the sum of inner polynomials,

\[ \lambda(x) \otimes (u(x) + v(x)) = (\lambda(x) \otimes u(x)) + (\lambda(x) \otimes v(x)). \]

(b) The inner polynomial distributing over the sum of outer polynomials,

\[ (c(x) + d(x)) \otimes v(x) = c(x) \otimes v(x) + d(x) \otimes v(x). \]

**PROOF:** We prove both the forms

\[
\begin{align*}
(a) \lambda(x) \otimes (u(x) + v(x)) &= \left( c_0 + c_1 x + c_2 x^2 + ... + c_m x^{m-1} \right) \otimes \\
&= \left( c_0 \left( b_0 + a_0 \right) + \left( b_1 + a_1 \right) x + \left( b_2 + a_2 \right) x^2 + ... + \left( b_{n-1} + a_{n-1} \right) x^{n-1} \right) \\
&\quad + x^n \left( c_0 \left( b_0 + a_0 \right) + \left( b_1 + a_1 \right) x + \left( b_2 + a_2 \right) x^2 + ... + \left( b_{n-1} + a_{n-1} \right) x^{n-1} \right) \\
&\quad + x^{2n} \left( c_0 \left( b_0 + a_0 \right) + \left( b_1 + a_1 \right) x + \left( b_2 + a_2 \right) x^2 + ... + \left( b_{n-1} + a_{n-1} \right) x^{n-1} \right) + ... \\
&\quad + x^{(m-1)n} \left( c_0 \left( b_0 + a_0 \right) + \left( b_1 + a_1 \right) x + \left( b_2 + a_2 \right) x^2 + ... + \left( b_{n-1} + a_{n-1} \right) x^{n-1} \right) \\
&= \left( c_0 b_0 + c_0 a_0 \right) + \left( c_0 b_1 + c_0 a_1 \right) x + \left( c_0 b_2 + c_0 a_2 \right) x^2 + ... + \left( c_0 b_{n-1} + c_0 a_{n-1} \right) x^{n-1} \\
&\quad + x^n \left( c_1 b_0 + c_1 a_0 \right) + \left( c_1 b_1 + c_1 a_1 \right) x + \left( c_1 b_2 + c_1 a_2 \right) x^2 + ... + \left( c_1 b_{n-1} + c_1 a_{n-1} \right) x^{n-1} \\
&\quad + x^{2n} \left( c_2 b_0 + c_2 a_0 \right) + \left( c_2 b_1 + c_2 a_1 \right) x + \left( c_2 b_2 + c_2 a_2 \right) x^2 + ... + \left( c_2 b_{n-1} + c_2 a_{n-1} \right) x^{n-1} + ... \\
&\quad + x^{(m-1)n} \left( c_m b_0 + c_m a_0 \right) + \left( c_m b_1 + c_m a_1 \right) x + \left( c_m b_2 + c_m a_2 \right) x^2 + ... + \left( c_m b_{n-1} + c_m a_{n-1} \right) x^{n-1} + ...
\end{align*}
\]
In this section we extend the idea considered above to product of two sets of polynomials defined over the same field $F$. In particular, let us consider two rings of polynomials namely

$$
R_m[x] = F[x] \text{ modulo } (x^n - 1) \quad \text{and} \quad R_n[x] = F[x] \text{ modulo } (x^n - 1),
$$

where $m$ and $n$ are any positive integers. Obviously these rings contain respectively all polynomials of degree $m-1$ and $n-1$, and less.

**DEFINITION:** Let $\lambda_j(x) = c_{0,j}x + c_{1,j}x^2 + \ldots + c_{m-1,j}x^{m-1} \in R_m[x]$ for different values of $j$ be polynomials of degree $m-1$ or less and $\nu_i(x) = a_{0,i}x + a_{1,i}x^2 + \ldots + a_{n-1,i}x^{n-1} \in R_n[x]$, where $i = 0, 1, 2, \ldots, m-1$.

This proves the results.

### 6.4 ORDERED POWER PRODUCT OF RINGS OF POLYNOMIALS

The collection of polynomials

$$
\{ (c_0 + c_{1}x + c_{2}x^2 + \ldots + c_{m-1}x^{m-1}) \otimes v(x) + (c_0 + c_{1}x + c_{2}x^2 + \ldots + c_{m-1}x^{m-1}) \otimes v(x) \}
$$

is an $R_m[x] \otimes R_n[x]$-module.

The ordered product of two polynomials $c(x)$ and $d(x)$ is defined as

$$
(c(x) + d(x)) \otimes v(x) = \left( (c_0 + d_0) + (c_1 + d_1)x + (c_2 + d_2)x^2 + \ldots + (c_{m-1} + d_{m-1})x^{m-1} \right) \otimes v(x)
$$

This proves the results.
for different values of \(i\), be polynomials of degree \(n-1\) or less. We define the set of ordered power product of \(R_m[x]\) and \(R_n[x]\), as

\[
\Gamma[x] = R_m[x] \otimes R_n[x] = \{ \lambda_j(x) \otimes v_i(x) \mid \lambda_j \in R_m[x], v_i \in R_n[x] \}.
\]

**THEOREM 6.1:** If \(R_m[x] = F[x]\) modulo \((x^m - 1)\) and \(R_n[x] = F[x]\) modulo \((x^n - 1)\), \(m\) and \(n\) being any positive integers are two rings of polynomial over a field \(F\), then

\[
\Gamma[x] = R_m[x] \otimes R_n[x] = \{ \lambda_j(x) \otimes v_i(x) \mid \lambda_j \in R_m[x], v_i \in R_n[x] \}.
\]

is a ring of polynomials of degree \(mn - 1\), under ordinary addition and ordered product of elements of \(\Gamma[x]\) modulo \((x^m - 1, x^n - 1)\), over \(F\).

**PROOF:** First we show that \(\Gamma[x]\) is a group under *addition* of polynomials:

**CLOSE UNDER ADDITION:** Let \(\lambda_j(x) \otimes v_i(x)\) and \(\lambda_l(x) \otimes v_s(x) \in \Gamma[x]\) then

\[
\lambda_j(x) \otimes v_i(x) + \lambda_l(x) \otimes v_s(x) = \left( (\lambda_{0,j} + \lambda_{1,j}x + \lambda_{2,j}x^2 + \ldots + \lambda_{(m-1),j}x^{(m-1)}) \otimes v_i(x) \right)
+ \left( (\lambda_{0,l} + \lambda_{1,l}x + \lambda_{2,l}x^2 + \ldots + \lambda_{(m-1),l}x^{(m-1)}) \otimes v_s(x) \right)
\]

\[
= \left( \lambda_{0,j}v_i(x) + \lambda_{1,j}x^nv_i(x) + \lambda_{2,j}x^{2n}v_i(x) + \ldots + \lambda_{(m-1),j}x^{(m-1)n}v_i(x) \right)
+ \left( \lambda_{0,l}v_s(x) + \lambda_{1,l}x^nv_s(x) + \lambda_{2,l}x^{2n}v_s(x) + \ldots + \lambda_{(m-1),l}x^{(m-1)n}v_s(x) \right)
\]

\[
= \left( \lambda_{0,j}v_i(x) + \lambda_{0,l}v_s(x) + \lambda_{1,j}x^nv_i(x) + \lambda_{1,l}x^nv_s(x) + \lambda_{2,j}x^{2n}v_i(x) + \lambda_{2,l}x^{2n}v_s(x) + \ldots + \lambda_{(m-1),j}x^{(m-1)n}v_i(x) + \lambda_{(m-1),l}x^{(m-1)n}v_s(x) \right)
\]
\[ \left( \lambda_0 v_f(x) + \lambda_0 v_s(x) \right) + \left( \lambda_1 v_f(x) + \lambda_s v_s(x) \right) x \]
\[ + \left( \lambda_2 v_f(x) + \lambda_2 v_s(x) \right) x^2 + \ldots \]
\[ + \left( \lambda_{m-1} v_f(x) + \lambda_{m-1} v_s(x) \right) x^{(m-1)} \]
\[ \otimes \left( 1 + x + x^2 + \ldots + x^{m-1} \right) \]
\[ = \lambda_f(x) \otimes v_f(x) \]

\[ \lambda_f(x) \otimes v_f(x) \in \Gamma[x] \]

**ASSOCIATIVE UNDER ADDITION:** Let \( \lambda_f(x) \otimes v_f(x), \lambda_l(x) \otimes v_s(x) \) and \( \lambda_r(x) \otimes v_r(x) \) then

\[ \left( \lambda_f(x) \otimes v_f(x) + \lambda_l(x) \otimes v_s(x) + \lambda_r(x) \otimes v_r(x) \right) = \left( \left( \lambda_0 v_f(x) + \lambda_0 v_s(x) \right) + \left( \lambda_1 v_f(x) + \lambda_s v_s(x) \right) x^n \right) \]
\[ + \left( \lambda_2 v_f(x) + \lambda_2 v_s(x) \right) x^{2n} + \ldots \]
\[ + \left( \lambda_{m-1} v_f(x) + \lambda_{m-1} v_s(x) \right) x^{(m-1)n} \]
\[ + \lambda_f(x) v_f(x) + \lambda_l(x) x^n v_f(x) + \lambda_r(x) x^{2n} v_r(x) + \ldots + \lambda_r(x) x^{(m-1)n} v_r(x) \]

\[ = \left[ \left( \lambda_0 v_f(x) + \lambda_0 v_s(x) \right) + \left( \lambda_1 v_f(x) + \lambda_s v_s(x) \right) x^n \right] \]
\[ + \left( \lambda_2 v_f(x) + \lambda_2 v_s(x) \right) x^{2n} + \ldots \]
\[ + \left( \lambda_{m-1} v_f(x) + \lambda_{m-1} v_s(x) \right) x^{(m-1)n} \]
\[ + \lambda_f(x) v_f(x) + \lambda_l(x) x^n v_f(x) + \lambda_r(x) x^{2n} v_r(x) + \ldots + \lambda_r(x) x^{(m-1)n} v_r(x) \]
\[
\begin{align*}
&= \left( \lambda_j(x)v_i(x) + \lambda_j(x)x^n v_i(x) + \lambda_j(x)x^{2n} v_i(x) + \ldots + \lambda_j(x)x^{(m-1)n} v_i(x) \right) \\
&= \left( \lambda_{0j} v_i(x) + \lambda_{1j} x + \lambda_{2j} x^2 + \ldots + \lambda_{(m-1)j} x^{(m-1)} \right) v_i(x) \\
&= \left( \lambda_j(x) \otimes v_i(x) \right) + \left( \lambda_j(x) \otimes v_i(x) \right) + \ldots + \left( \lambda_j(x) \otimes v_i(x) \right)
\end{align*}
\]

**EXISTENCE OF ADDITIVE IDENTITY:**

Let \( \lambda_j(x) \otimes v_i(x) \in \Gamma[x] \) then exists \( 0_j(x) \otimes 0_i(x) \) such that

\( (\lambda_j(x) \otimes v_i(x)) + (0_j(x) \otimes 0_i(x)) = (\lambda_j(x) \otimes v_i(x)) \).

**EXISTENCE OF ADDITIVE INVERSE:**

Let \( \lambda_j(x) \otimes v_i(x) \in \Gamma[x] \) then exists \( -(\lambda_j(x) \otimes v_i(x)) \in \Gamma[x] \) such that

\( \lambda_j(x) \otimes v_i(x) + (-(\lambda_j(x) \otimes v_i(x))) = 0_j(x) \otimes 0_i(x) \).

Next we show that \( \Gamma[x] \) is a semi group under ordinary polynomial multiplication.

**CLOSE UNDER MULTIPLICATION:** Let \( \lambda_j(x) \otimes v_i(x) \) and \( \lambda_j(x) \otimes v_i(x) \) in \( \Gamma[x] \) then

\[
\begin{align*}
&= \left( \left( \lambda_{0j} v_i(x) + \lambda_{1j} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x) \right) \otimes v_i(x) \right) \mod (x^n - 1, x^n - 1)
\end{align*}
\]

99
\[
\begin{align*}
\lambda_{0j} v_j(x)
\left(\lambda_{0i} v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x)\right) \\
+ \lambda_{ij} x^n v_i(x)
\left(\lambda_{0i} v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x)\right) \\
+ \lambda_{2j} x^{2n} v_i(x)
\left(\lambda_{0i} v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x)\right) \\
+ \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x)
\left(\lambda_{0i} v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x)\right)
\end{align*}
\mod(x^m - 1, x^n - 1)
\]

\[
\begin{align*}
\left(\lambda_{0j} v_j(x) + \lambda_{ij} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x)\right)
\left(\lambda_{0i} v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x)\right)
\end{align*}
\mod(x^m - 1, x^n - 1)
\]
ASSOCIATIVE UNDER MULTIPLICATION:

Let \( \lambda_j(x) \otimes v_s(x) \), \( \lambda_i(x) \otimes v_s(x) \) and \( \lambda_r(x) \otimes v_s(x) \) then

\[
(\lambda_j(x) \otimes v_s(x))(\lambda_i(x) \otimes v_s(x))(\lambda_r(x) \otimes v_s(x)) = \left( \lambda_{0j} v_s(x) + \lambda_{ij} x^n v_s(x) + \ldots + \lambda_{(m-1)i} x^{(m-1)n} v_s(x) \right) \\
+ \lambda_{j} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x) \\
+ \lambda_{0i} v_s(x) + \lambda_{il} x^n v_s(x) + \lambda_{2i} x^{2n} v_s(x) + \ldots + \lambda_{(m-1)i} x^{(m-1)n} v_s(x) \\
+ \lambda_{0r} v_s(x) + \lambda_{rm} x^n v_s(x) + \lambda_{2r} x^{2n} v_s(x) + \ldots + \lambda_{(m-1)r} x^{(m-1)n} v_s(x) \\
\text{mod}(x^m - 1, x^n - 1) \\
\otimes \left( \lambda_{0s} v_s(x) + \lambda_{im} x^n v_s(x) + \lambda_{2s} x^{2n} v_s(x) + \ldots + \lambda_{(m-1)s} x^{(m-1)n} v_s(x) \right)
\]
\[
\begin{align*}
&= \left( \lambda_{0i} v_r(x) \left( \lambda_{0j} v_i(x) \lambda_{0o} v_s(x) + \lambda_{0j} v_i(x) \lambda_{0l} x^n v_s(x) + \lambda_{0j} v_i(x) \lambda_{0m} x^{(m-1)n} v_s(x) \right) + \\
&+ \lambda_{1i} x^n v_r(x) \left( \lambda_{1j} x^n v_i(x) \lambda_{1l} x^n v_s(x) + \lambda_{1j} x^n v_i(x) \lambda_{1l} x^{(m-1)n} v_s(x) \right) + \\
&+ \lambda_{2i} x^{2n} v_r(x) \left( \lambda_{2j} x^{2n} v_i(x) \lambda_{2l} x^{2n} v_s(x) + \lambda_{2j} x^{2n} v_i(x) \lambda_{2l} x^{2n} v_s(x) \right) + \cdots \right) \pmod{(x^m - 1, x^n - 1)}
\end{align*}
\]
\[
\begin{aligned}
\left( \lambda_{ij} v_i(x) \lambda_{0j} v_j(x) \lambda_{00} v_s(x) + \lambda_{ij} v_i(x) \lambda_{2j} x^{2n} v_s(x) + \ldots + \right. \\
\left. \lambda_{ij} v_i(x) \lambda_{2j} x^{2n} v_s(x) \lambda_{(m-1)j} x^{(m-1)n} v_s(x) \right) \\
+ \left( \lambda_{ij} x^n v_r(x) \lambda_{ij} x^n v_j(x) \lambda_{0j} v_s(x) + \lambda_{ij} x^n v_j(x) \lambda_{2j} x^{2n} v_s(x) + \ldots + \right. \\
\left. \lambda_{ij} x^n v_j(x) \lambda_{ij} x^n v_j(x) \lambda_{2j} x^{2n} v_s(x) + \ldots + \right. \\
\left. \lambda_{ij} x^n v_j(x) \lambda_{ij} x^n v_j(x) \lambda_{(m-1)j} x^{(m-1)n} v_r(x) \right)
\end{aligned}
\]

\[
\equiv \mod(x^m - 1, x^n - 1)
\]

\[
\begin{aligned}
\left( \lambda_{ij} v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{ij} x^n v_i(x) + \ldots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x) \right) \\
\left( \lambda_{0j} v_j(x) \lambda_{00} v_s(x) + \lambda_{ij} x^n v_r(x) + \lambda_{ij} x^n v_r(x) + \ldots + \right. \\
\left. \lambda_{ij} x^n v_r(x) \lambda_{(m-1)j} x^{(m-1)n} v_r(x) \right) \\
+ \lambda_{ij} x^n v_s(x) \left( \lambda_{0j} v_j(x) + \lambda_{ij} x^n v_s(x) + \lambda_{ij} x^n v_s(x) + \ldots + \right. \\
\left. \lambda_{ij} x^n v_s(x) \lambda_{(m-1)j} x^{(m-1)n} v_s(x) \right) \\
+ \lambda_{ij} x^n v_s(x) \left( \lambda_{0j} v_j(x) + \lambda_{ij} x^n v_r(x) + \lambda_{ij} x^n v_r(x) + \ldots + \right. \\
\left. \lambda_{ij} x^n v_r(x) \lambda_{(m-1)j} x^{(m-1)n} v_r(x) \right)
\end{aligned}
\]

\[
\equiv \mod(x^m - 1, x^n - 1)
\]

\[
= \lambda_j(x) \otimes v_j(x) ( \lambda_j(x) \otimes v_s(x) ) ( \lambda_j(x) \otimes v_r(x) )
\]
DISTRIBUTIVE LAW MULTIPLICATION OVER ADDITION:

Let \( \lambda_j(x) \otimes v_i(x), \lambda_i(x) \otimes v_s(x) \) and \( \lambda_i(x) \otimes v_r(x) \) then

\[
\left( (\lambda_j(x) \otimes v_i(x)), (\lambda_i(x) \otimes v_s(x)) \right) + (\lambda_i(x) \otimes v_r(x)) =
\]

\[
\left( \lambda_0 v_i(x) + \lambda_{1j} x^n v_i(x) + \lambda_{2j} x^{2n} v_i(x) + \cdots + \lambda_{(m-1)j} x^{(m-1)n} v_i(x) \right)
\]

\[
\left( \lambda_0 v_s(x) + \lambda_{0r} v_r(x) + \lambda_{1r} v_r(x)) x^n + \cdots + \lambda_{(m-1)r} v_r(x)) x^{(m-1)n} \right)
\]

\[
\cdots + \left( \lambda_0 v_s(x) + \lambda_{0r} v_r(x) + \lambda_{1r} v_r(x)) x^n + \cdots + \lambda_{(m-1)r} v_r(x)) x^{(m-1)n} \right)
\]

\[
\mod(x^n - 1, x^n - 1)
\]
\[
\left( \lambda_{ij} v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{ij} x^2 v_i(x) \right) + \ldots + \lambda_{ij} x^{(m-1)n} v_i(x)
\]
\[
\left( \lambda_{ij} x^n v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{ij} x^2 v_i(x) \right) + \ldots + \lambda_{ij} x^{(m-1)n} v_i(x)
\]
\[
\left( \lambda_{ij} x^n v_i(x) + \lambda_{ij} x^n v_i(x) + \lambda_{ij} x^2 v_i(x) \right) + \ldots + \lambda_{ij} x^{(m-1)n} v_i(x)
\]
\[
\left( \lambda_{ij} x^{(m-1)n} v_i(x) + \lambda_{ij} x^{(m-1)n} v_i(x) \right) + \ldots + \lambda_{ij} x^{(m-1)n} v_i(x)
\]
\[
\mod(x^n - 1, x^n - 1)
\]
6.5 APPLICATIONS OF OPP OF POLYNOMIALS IN CODING THEORY

In this section, we consider cyclic binary codes represented by their generator polynomials and study codes obtained by their OPP-composition. It may be pointed out that in the binary case, $x^n - 1$ may be taken as $x^n + 1$, and that $1 + 1 = 0$. Since cyclic codes of length $n$ are generated by factors of $x^n - 1$, we next give some useful results for getting its factors.

**Lemma 6.1:** For $p$ and $q$ distinct prime numbers and $r$ and $s$ are natural numbers, we have:

(i)  \[ x^p + 1 = (1 + x)(1 + x + x^2 + ... + x^{p-1}) \]

(ii)  \[ x^{p^r} + 1 = \left( \left( \left( 1 + x \right) \left( 1 + x + x^2 + ... + x^{p-1} \right) \right) \left( 1 + x^{p} + x^{2p} + ... + x^{(p-1)p} \right) \right) \]

\[ = (1 + x) \prod_{a=1}^{\alpha} \left[ 1 + x^{r^{a-1}} + x^{2r^{a-1}} + ... + x^{(p-1)r^{a-1}} \right] \]

(iii)  \[ x^{p^aq^r} + 1 = \left( (1 + x) \left( 1 + x + x^2 + ... + x^{p-1} \right) \left( 1 + x^{p} + x^{2p} + ... + x^{(p-1)p} \right) \right) \]

\[ = (1 + x) \prod_{a=1}^{\alpha} \left( 1 + x^{r^{a-1}} + x^{2r^{a-1}} + ... + x^{(p-1)r^{a-1}} \right) \]

\[ = \left( \prod_{a=1}^{\alpha} \left( 1 + x^{r^{a-1}} + x^{2r^{a-1}} + ... + x^{(p-1)r^{a-1}} \right) \right) \cdot \left( \prod_{b=1}^{\beta} \left( 1 + x^{q^{b-1}} + x^{2q^{b-1}} + ... + x^{(q-1)q^{b-1}} \right) \right) \]

**Note:** These results can be easily verified, and extended for $x^n - 1$, for any $n$ when $n$ is expressed as product of powers of primes.
THEOREM 6.2: If \((n_1, k_1)\) and \((n_2, k_2)\) are two cyclic codes with \(g_1(x)\) and \(g_2(x)\) as their generator polynomials then the \(\otimes\)-product of their generator polynomials given by

\[
g(x) = g_1(x) \otimes g_2(x),
\]

of degree \((n_1 - k_1)n_2 + (n_2 - k_2)\), will generate a cyclic \((n, k)\) code, where \(n = n_1n_2\), and \(k = (k_1 - 1)n_2 + k_2\), whenever \(g_2(x)\) divides \(x^n - 1\).

PROOF: Let

\[
g(x) = g_1(x) \otimes g_2(x).
\]

It can be written as a following simple product:

\[
g(x) = g_1(x^{n_2}) \cdot g_2(x)
\]

where \(g_1(x)\) and \(g_2(x)\) are divisors of \(x^{n_1} - 1\) and \(x^{n_2} - 1\) respectively.

For \(g(x)\) to represent a cyclic code of length \(n_1n_2\), \(g(x)\) must a factor of \(x^{n_1n_2} - 1\). So we examine the conditions under which \(g(x) = g_1(x) \otimes g_2(x)\) is a divisor of \(x^{n_1n_2} - 1\).

First we show that \(g_1(x^{n_2})\) is a divisor of \(x^{n_1n_2} - 1\). This follows from the fact that \(g_1(x)\) is a divisor of \(x^n - 1\), and by replacing \(x\) by \(x^{n_2}\). Thus we get that \(g_1(x^{n_2})\) is a divisor of \((x^{n_2})^{n_1} - 1 = x^{n_1n_2} - 1\) or of \(x^n - 1\).

It remains to investigate the conditions for \(g_2(x)\) is a factor of \(x^{n_1n_2} - 1\). This will not happen for all choices of \(n_1, n_2\), as is evident by the Example 2 below. We therefore can use the result of the Lemma above for determining if \(g_2(x)\) divides \(x^{n_1n_2} - 1\). In fact any one or products of any numbers of these factors can be taken for \(g_2(x)\) to get the \(\otimes\)-product cyclic code from generator polynomials of component codes.
Note: It may have been noted that while choice of $g_2(x)$, the inner-polynomial, is limited, there is no limitation on choice of outer polynomial $g_1(x)$ in forming OPP codes.

**THEOREM 6.3:** If $(n_1, k_1)$ and $(n_2, k_2)$ are two cyclic codes with $g_1(x)$ and $g_2(x)$ as their generator polynomials and $g_2(x)$ divides $x^{n_2} - 1$ then the $\otimes$-product $g(x) = g_1(x) \otimes g_2(x)$ generates $(n_1n_2, k)$ code, where $k = (k_1 - 1)n_2 + k_2$. Also then the $k - 1$ code polynomials $g(x), xg(x), x^2g(x), ..., x^{k-1}g(x)$ span the complete cyclic code $C$.

**PROOF:** The proof follows directly from the definition of cyclic code generated by $g(x)$.

**EXAMPLE 6.2:** Let us consider two cyclic codes $C_1$ and $C_2$ where $C_1$ is $(7, 4)$ code and $C_2$ is $(3, 1)$ cyclic code with generator polynomials $g_1(x) = (1 + x + x^3)$ and $g_2(x) = (1 + x + x^2)$ respectively. Then

\[
g_1(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{10} + x^{11}
\]

\[
xg_1(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 + x^{10} + x^{11} + x^{12}
\]

\[
x^2g_1(x) = x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^{11} + x^{12} + x^{13}
\]

\[
x^3g_1(x) = x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{12} + x^{13} + x^{14}
\]

\[
x^4g_1(x) = x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{13} + x^{14} + x^{15}
\]

\[
x^5g_1(x) = x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{14} + x^{15} + x^{16}
\]

\[
x^6g_1(x) = x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{14} + x^{15} + x^{16} + x^{17}
\]

\[
x^7g_1(x) = x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{16} + x^{17} + x^{18}
\]

\[
x^8g_1(x) = x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{17} + x^{18} + x^{19}
\]

\[
x^9g_1(x) = x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{18} + x^{19} + x^{20}.
\]
Above polynomials gave a (21, 9) cyclic code.

**EXAMPLE 6.3:** Let us consider two cyclic codes $C_1$ and $C_2$ where $C_1$ is (3, 2) code and $C_2$ is (7, 4) cyclic code with generator polynomials $g_1(x) = (1 + x)$ and $g_2(x) = (1 + x + x^3)$ respectively. Then

$$g(x) = g_1(x) \otimes g_2(x) = 1 + x^3 + x^7 + x^8 + x^{10}$$

Here $g_2(x) = (1 + x + x^3)$ is not a divisor of $x^{21} - 1$, therefore $g(x)$ will not generate a cyclic code of length 21.

**THEOREM 6.4:** If two linear binary cyclic codes $(n_1, k_1)$ and $(n_2, k_2)$ have rates $R_1$ and $R_2$ then the rate $R$ of their component cyclic Code is an increasing function of the rate of either component code.

**PROOF:** Let $R$ be the rate of the product cyclic code. Then, we have

$$R = \frac{(k_1 - 1)n_2 + k_2}{n_1n_2} = \frac{(k_1 - 1)n_2}{n_1n_2} + \frac{k_2}{n_1n_2}$$

$$= R_1 + \frac{(R_2 - 1)R_1}{k_1}$$

$$= \frac{1}{k_1} \left( R_1 (k_1 - 1) + R_1 R_2 \right)$$

$$R - R_1 R_2 = \frac{1}{k_1} \left( R_1 (k_1 - 1) + R_1 R_2 \right) - R_1 R_2$$

$$= \frac{(k_1 - 1)}{k_1} R_1 (1 + R_2) \text{ and } k_1 \geq 1$$

Trivially, $R = R_1 R_2$, when $k = 1$. In general the difference is directly proportional to $R_1$ and increases with $R_2$. This shows that the newly introduced OPP cyclic codes are a new class of codes that have rates better than those that be obtained by their Kronecker product codes.
THEOREM 6.5: If \( (n_1p_1,k_1) \) and \( (n_2p_2,k_2) \) are two quasi cyclic codes with
\[
g_1(x) = \{g_0(x), g_1(x), \ldots, g_{n_1-1}(x)\} \quad \text{and} \quad g_2(x) = \{g'_0(x), g'_1(x), \ldots, g'_{p_2-1}(x)\},
\]
as their generator polynomials and \( g_2(x) \) divides \( x^{n_2} - 1 \) then the \( \otimes \)-product
\[
g(x) = g_1(x) \otimes g_2(x),
\]
generates \( (n_1n_2p_1p_2,k) \) code, where \( k = (k_1 - 1)n_2 + k_2. \) Also then \( k-1 \) code polynomials
\( g(x), xg(x), x^2g(x), \ldots, x^{k-1}g(x) \) span cyclic code \( C. \)

PROOF: Let \( (n_1p_1,k_1) \) and \( (n_2p_2,k_2) \) be two quasi cyclic codes with,
\[
g_1(x) = \{g_0(x), g_1(x), \ldots, g_{n_1-1}(x)\} \quad \text{and} \quad g_2(x) = \{g'_0(x), g'_1(x), \ldots, g'_{p_2-1}(x)\},
\]
as their generator polynomials then the \( \otimes \) product \( (n_1n_2p_1p_2,k) \), \( k = (k_1 - 1)n_2 + k_2 \), code
generated by \( g(x) = g_1(x) \otimes g_2(x) \) define as
\[
g(x) = \prod_{i=0}^{n_1-1} \prod_{j=0}^{p_2-1} g_i(x) \otimes g'_j(x),
\]
and the \( \otimes \) product of \( g_1(x) \) and \( g_2(x) \) given as follows
\[
g_1(x) \otimes g_2(x) = \left( \begin{array}{c} g_0(x) \otimes g'_0(x), g_0(x) \otimes g'_1(x), \ldots, g_0(x) \otimes g'_{p_2-1}(x) \\ g_1(x) \otimes g'_0(x), g_1(x) \otimes g'_1(x), \ldots, g_1(x) \otimes g'_{p_2-1}(x) \\ \vdots \end{array} \right)
\]
\[
= \left( \begin{array}{c} g_0(x) \otimes g'_0(x), g_0(x) \otimes g'_1(x), \ldots, g_0(x) \otimes g'_{p_2-1}(x) \\ \ldots \\ \ldots \\ g_p(x) \otimes g'_0(x), g_p(x) \otimes g'_1(x), \ldots, g_p(x) \otimes g'_{p_2-1}(x) \end{array} \right)
\]
\[
g(x) = \prod_{i=0}^{n_1-1} \prod_{j=0}^{p_2-1} g_i(x) \otimes g'_j(x).
\]
**THEOREM 6.6:** If two quasi cyclic codes \((n_1, p_1, k_1)\) and \((n_2, p_2, k_2)\) have rates \(R_1\) and \(R_2\) then the rate \(R\) of product quasi cyclic Code is an increasing function of the rate of either component code.

**PROOF:** Let \(R\) be the rate of the product cyclic code. Then, we have

\[
R = \frac{(k_1-1)n_2 + k_2}{n_1 n_2 P} = \frac{(k_1-1)n_2}{n_1 n_2 P} + \frac{k_2}{n_1 n_2 P}
\]

\[
= \frac{R_1}{p_1 p_2} + \frac{(R_2 - 1)R_1}{k_1 p_1 p_2}
\]

\[
= \frac{1}{k_1 p_1 p_2} (R_1(k_1 - 1) + R_1 R_2)
\]

\[
R - R_1 R_2 = \frac{1}{k_1 p_1 p_2} (R_1(k_1 - 1) + R_1 R_2) - R_1 R_2
\]

\[
R - R_1 R_2 = \frac{(k_1 - 1)}{k_1 p_1 p_2} R_1 (1 + R_2) \text{ and } k_1 \geq 1
\]

Trivially, \(R = R_1 R_2\), when \(k = 1\). In general the difference is directly proportional to \(R_1\) and increases with \(R_2\). This shows that the product quasi cyclic codes are a new class of codes that have rates better than existing product cyclic codes.

**EXAMPLE 6.4:** Let us consider two cyclic codes \(C_1\) and \(C_2\) where \(C_1\) is \((7, 4)\) code and \(C_2\) is \((3, 1)\) cyclic code, then \((14, 4)\) and \((6, 1)\) be two quasi cyclic codes where \(p=2\), with generator polynomials,

\[
g_1(x) = \{1 + x + x^3, 1 + x^2 + x^3\} \quad \text{and} \quad g_2(x) = \{1 + x + x^2, 1 + x + x^2\}
\]

then \(\text{OPP}\) of \(g_1(x)\) and \(g_2(x)\) given as follows:

\[
g_1(x) \odot g_2(x) = \{1 + x + x^3, 1 + x^2 + x^3\} \odot \{1 + x + x^2, 1 + x + x^2\}
\]

\[
= \{(1 + x + x^3) \odot (1 + x + x^2, 1 + x + x^2)\} \odot \{1 + x + x^2, 1 + x + x^2\}
\]
(1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{10} + x^{11},
1 + x + x^2 + x^3 + x^4 + x^5 + x^9 + x^{10} + x^{11}),
\{ (1 + x + x^2 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11},
1 + x + x^2 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11}) \}

\begin{align*}
&= (x + x^2 + x^3 + x^4 + x^5 + x^6 + x^{10} + x^{11} + x^{12},
&\quad x + x^2 + x^3 + x^4 + x^5 + x^6 + x^{10} + x^{11} + x^{12})
\end{align*}
\begin{align*}
&\quad x + x^2 + x^3 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12},
&\quad x + x^2 + x^3 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12})
\end{align*}

\begin{align*}
&= (x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^{11} + x^{12} + x^3,
&\quad x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^{11} + x^{12} + x^3)
\end{align*}
\begin{align*}
&\quad x^2 + x^3 + x^4 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13},
&\quad x^2 + x^3 + x^4 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13})
\end{align*}

\begin{align*}
&= (x^3 + x^4 + x^5 + x^6 + x^7 + x^{12} + x^{13} + x^4,
&\quad x^3 + x^4 + x^5 + x^6 + x^7 + x^{12} + x^{13} + x^4)
\end{align*}
\begin{align*}
&\quad x^3 + x^4 + x^5 + x^6 + x^7 + x^{12} + x^{13} + x^4,
&\quad x^3 + x^4 + x^5 + x^6 + x^7 + x^{12} + x^{13} + x^4)
\end{align*}

\begin{align*}
&= (x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{13} + x^{14},
&\quad x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{13} + x^{14})
\end{align*}
\begin{align*}
&\quad x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{13} + x^{14} + x^{15},
&\quad x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{13} + x^{14} + x^{15})
\end{align*}

\begin{align*}
&= (x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{14} + x^{15},
&\quad x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{14} + x^{15})
\end{align*}
\begin{align*}
&\quad x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{14} + x^{15} + x^{16},
&\quad x^5 + x^6 + x^7 + x^{11} + x^{12} + x^{14} + x^{15} + x^{16},
\end{align*}
\begin{align*}
&\quad x^5 + x^6 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{15} + x^{16})
\end{align*}

\begin{align*}
&= (x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{15} + x^{16} + x^{17},
&\quad x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{15} + x^{16} + x^{17})
\end{align*}
\begin{align*}
&\quad x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{15} + x^{16} + x^{17},
&\quad x^6 + x^7 + x^8 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17},
\end{align*}
\begin{align*}
&\quad x^6 + x^7 + x^8 + x^{12} + x^{13} + x^{14} + x^{15} + x^{16} + x^{17})
\end{align*}
Above polynomials gave a (84, 9) quasi cyclic code.

6.6 CONCLUDING REMARK

We have considered ordered power product of two polynomials in such powers of $x$ that the various segments of the inner polynomial are laterally advanced without having overlaps amongst them, with coefficients multiplied by those of the outer polynomial. For this choice the motivation was to consider a new composition suitable for developing new product type of codes, which are more efficient. However, an ordered power product may be defined more generally, when this is not the case, that is when

$$\lambda(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{m-1} x^{m-1} \text{ and } v(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1};$$

but

$$\lambda(x) \otimes v(x) = c_0(v(x)) + c_1 x^k(v(x)) + c_2 x^{2k}(v(x)), \ldots, a_{m-1} x^{(m-1)k}(v(x))$$

where $k < n$, or even when $k > n$. In such cases we can perhaps use the notation for OPP using an index, like $\otimes^k – OPP$. These interesting cases are being studied separately.