Hyper-Cyclotomic Algebra

Solomon W. Golomb[1] and Guang Gong[2]

[1] Department of Electrical Engineering-Systems,
University of Southern California, Los Angeles, CA 90089-2565 USA
[2] Department of Electrical and Computer Engineering,
University of Waterloo, Waterloo, Ontario N2L 3G1 CANADA

Abstract. Two new operators imposed on the set of cyclotomic cosets modulo $p^n - 1$ and their algebraic structure are discussed. These two new operators can be performed on the cyclotomic algebra in a field. The resulting algebraic structure is called *hyper cyclotomic algebra*. It is shown that there exist distributive laws which connect these new operators to the ordinary operations of a field. An application of this new algebraic system to cyclic invariant sequences is provided.

1 Introduction

The cyclotomic algebra was studied by Golomb in [2] [3] for use with computation of correlation of binary sequences having period $2^n - 1$. In this paper, we investigate two new operators imposed on the set of cyclotomic cosets modulo $p^n - 1$ and their algebraic structure. These two new operators can be performed on the cyclotomic algebra in a field. The resulting algebraic structure is called a *hyper cyclotomic algebra*. We show that there are distributive laws which connect these new operators to the ordinary operations of a field. An application of this new algebraic system is to facilitate computation of the linear span and the correlation of sequences having period $p^n - 1$ via the computation with *Gauss periods*, the elements in the cyclotomic algebra, using these new operators.

The following notation will be used throughout this paper.

- $\mathcal{F}$, a field.
- $\mathbb{Z}$ represents the integer ring.
- p is a prime number, n a positive integer, and $q = p^n$.
- $\mathbb{F}_{p^n} = GF(p^n)$.
- $\mathbb{Z}_m$ is the ring of integers modulo m.

2 Cyclotomic Set Monoid

The following definition is taken from [1]

Definition 1. *A* monoid *is a triple* $(M, o, 1)$ *in which* M *is a non-vacuous set,* o *is an associative binary composition (or product) in* M*, and 1 is an element of* M *such that*

$$o(1, a) = a = o(a, 1) \textit{ for all } a \in M. \tag{1}$$

An element 1 of M such that (1) holds is called a *unit* in (M, o). A unit in M is unique.

A cyclotomic coset C_s modulo $q-1$ (with respect to p) is defined by

$$C_s = \{s, sp, \cdots, sp^{n_s - 1}\},$$

where n_s is the smallest positive integer such that $s \equiv sp^{n_s} \pmod{q-1}$. The subscript s is chosen as the smallest integer in C_s, and s is called the *coset leader* of C_s. Let

$$\Omega_n = \{ \text{ all cosets } C_s \text{ in } Z_{q-1} \}, \text{ and}$$
$$\Omega_n^- = \{C_s \in \Omega_n | s \neq 0\}.$$

We define two operations in Ω_n as follows:

$$C_r \oplus C_s = C_{r+s}$$
$$C_r \circ C_s = C_{rs}$$

where $s+r$ and sr are in the cosets containing $s+r$ and sr respectively. We still call these operations *addition* and *multiplication* in Ω_n.

Note that the product $C_r \circ C_s = C_{rs}$, when $r \in C_r$, $s \in C_s$, and $rs \in C_{rs}$, is independent of which representative elements are selected from the cosets C_r, C_s and C_{rs}. To see this, suppose that we have picked r' from C_r and s' from C_s. Then $r' = m_1 r$ and $s' = m_2 s$, whre m_1 and m_2 are multiples which do not effect coset membership. (A cyclotomic coset is, by construction, a minimal set which is closed under multiplication by multipliers.) Then $r's' = (m_1 m_2) rs$, which is in the same coset as rs because $m_1 m_2$ is again a multiplier. (The multipliers from a subgroup of the multiplicative group of the integers modulo $q-1$.) On the other hand, the sum $C_r \oplus C_s = C_{r+s}$ depends on the representatives picked from C_r and C_s. We achieve uniqueness by requiring r and s to be the leaders of the cosets C_r and C_s, respectively, and then interpreting C_{r+s} to be the coset containing the element $r+s$. Thus we have proved the following lemma.

Lemma 1. *The operators $\oplus$ and $\circ$ are well defined in Ω_n.*

Theorem 1. *With the above notation, both $(\Omega_n, \oplus, C_0)$ and $(\Omega_n^-, \cdot, C_1)$ are monoids. Moreover, these two operations satisfy the following distributive law*

$$C_r \circ (C_s \oplus C_t) = (C_r \circ C_s) \oplus (C_r \circ C_t).$$

Proof. From Lemma 1, the operators $\oplus$ and $\circ$ are well defined in Ω_n. It is easy to check C_0 and C_1 are the additive unit and multiplicative unit of Ω_n respectively. According to Definition 1, both $(\Omega_n, \oplus, C_0)$ and $(\Omega_n^-, \cdot, C_1)$ are monoids. For the distributive law, since

$$\begin{aligned} C_r \circ (C_s \oplus C_t) &= C_r \circ C_{s+t} = C_{r(s+t)} \\ (C_r \circ C_s) \oplus (C_r \circ C_t) &= C_{rs} \oplus C_{rs} = C_{rs+rt}, \end{aligned}$$

and $r(s+t)$ and $rs+rt$ belong to the same coset, the assertion is established. $\square$

Remark 1. The multiplicative group in Ω_n is $(\Omega_n^*, \cdot, C_1)$, where Ω_n^*, is the set of nonzero elements in Ω_n with indexes coprime to $p^n - 1$.

We will call Ω_n a *cyclotomic coset monoid*, which is different from the cyclotomic algebra in [3] which we will discuss in the next section.

In the following, we will introduce an isomorphic image of Ω_n. Let $I_n = \{r \in \mathbb{Z}_{q-1} | r,$ a coset leader $\}$ and let

$$\sigma : \Omega_n \to I_n \text{ by } \sigma : C_r \mapsto r. \tag{2}$$

The following proposition is immediate from the definition of σ.

Proposition 1. *$\sigma : \Omega_n \to I_n$ is a one-to-one correspondence between Ω_n and I_n, and I_n is the isomorphic image of Ω_n under σ, i.e., $\sigma(\Omega_n) = I_n$.*

The fact that $\sigma(\Omega_n) = I_n$ induces that $(I_n, \oplus, 0)$ and $(I_n^-, \circ, 1)$ are also monoids where the two operations $\oplus$ and $\circ$ are induced from the operations in Ω_n. I.e., we have

$$r \oplus s = t \tag{3}$$

where t is the coset leader of the coset C_{r+s} and the multiplication is the ordinary one since the product rs is also a coset leader modulo $q-1$ if both r and s are coset leaders modulo $q-1$, and I_n^* is the multiiplication group in I_n.

In the following, we will consider that I_n and Ω_n are interchangeable.

Example 1. Let $p = 2$ and $n = 4$. Then $q = 2^4 - 1 = 15$. The elements in Ω_4 are:

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8\} \\ C_3 &= \{3, 6, 12, 9\} \\ C_5 &= \{5, 10\} \\ C_7 &= \{7, 14, 13, 11\} \end{aligned}$$

and $I_4 = \{0, 1, 3, 5, 7\}$. We have the following addition table and multiplication table for I_4.

Table 1

$\oplus$	0	1	3	5	7
0	0	1	3	5	7
1	1	1	1	3	1
3	3	1	3	1	5
5	5	3	1	5	3
7	7	1	5	3	7

$\circ$	1	3	5	7
1	1	3	5	7
3	3	3	0	3
5	5	0	5	5
7	7	3	5	1

3 Cyclotomic Algebra Ψ_n and New Operators on Ψ_n

Let ξ be a primitive $(q-1)$st root of unity in $\mathcal{F}$. For any $r \in I_n$, let

$$\eta_r = \sum_{i=0}^{n_r-1} \xi^{rp^i} \tag{4}$$

where $n_r = |C_r|$. This notation was introduced by Gauss for r coprime to $q-1$, and is called a *Gauss period* in [6]. Here we will consider all coset leaders modulo $q-1$. Let

$$\Psi_n = \{\eta_r | r \in I_n\}. \tag{5}$$

Thus the elements in Ψ_n have the following ordinary addition and multiplication in $\mathcal{F}$.

$$\eta_r + \eta_s = \sum_{i=0}^{n_r-1} \alpha^{rp^i} + \sum_{i=0}^{n_s-1} \alpha^{rp^i} \tag{6}$$

$$\eta_r \cdot \eta_s = \sum_{i=0}^{n_r-1} \alpha^{rp^i} \cdot \sum_{i=0}^{n_s-1} \alpha^{rp^i} \tag{7}$$

$$= \sum_{k=0}^{M} c_k \eta_k \tag{8}$$

where c_k are non-negative integers. Thus Ψ_n forms an algebra under $+$ and $\cdot$. Sometimes we also write the product of η_r and η_s as $\eta_r\eta_s$ for short. Golomb studied this product $\eta_r\eta_s$ in [2] [3]. Here we will give an explicit formula to compute c_k's in the above representation.

Theorem 2. *Let $n_j = C_j, j \in I_n$. Then the indices k and the coefficients of η_k in the representation of $\eta_r \cdot \eta_s$ can be determined as follows.*

Case 1. *One of n_r and n_s is equal to n.*

1. $n_r = n_s = n$

$$\eta_r \cdot \eta_s = \sum_{k=0}^{n-1} c_k \eta_{r+2^k s}, \ \textit{where } c_k = n/n_{t+2^k s}.$$

2. $n_r | n_s = n$ *and* $n_r < n$.

$$\eta_r \cdot \eta_s = \sum_{k=0}^{n_r-1} c_k \eta_{r+2^k s}, \ \textit{where } c_k = n/n_{t+2^k s}.$$

Case 2. *Both n_r and n_s are less than n.*

1. $(n_r, n_s) = 1$. *Then* $\eta_r \cdot \eta_s = \frac{n_r n_s}{n_{r+s}} \eta_{r+s}$.

2. $(n_r, n_s) = d > 1$. *If* $n_r = n_s = d$, *then*

$$\eta_r \cdot \eta_s = \sum_{k=0}^{d-1} c_k \eta_{r+2^k s}, \ \textit{where } c_k = d/n_{r+2^k s}.$$

If $n_r \neq n_s$, *then*

$$\eta_r \cdot \eta_s = \sum_{k=0}^{d-1} c_k \eta_{r+2^k s}, \ \textit{where } c_k = lcm(n_r, n_s)/n_{r+2^k s}.$$

Proof. Let $t_k = t + 2^k s$.

Case 1. One of n_r and n_s is equal to n.

1. $n_r = n_s = n$. In this case,

$$C_{t_k} \subset \{2^j t_k | 0 \leq j < n\}.$$

Hence all C_{t_k}, $k = 0, \cdots, n-1$ are different elements in Ω_n and the coset size of C_{t_k} is a factor of n. Thus the result follows.

2. If $n_r | n_s = n$ and $n_r < n_s$, then

$$C_{t_k} \subset \{2^i t_{k+jn_r} | 0 \le j \le n/n_r, 0 \le i < n_r\}$$

where $0 \le k < n_r$. Applying the same argument as Case 1-1, the result follows.

Case 2. Both n_r and n_s are less than n.

1. $(n_r, n_s) = 1$. We have $n_r n_s | n$ and

$$C_{r+s} \subset \{2^j(r + s2^i) | 0 \le j \le n_r; 0 \le i \le n_s\}.$$

Thus $n_{r+s} | n_r n_s$ which establishes the assertion.

2. If $(n_r, n_s) = d > 1$ and $n_r = n_s$, this is similar as in Case 1-1. If $n_r \neq n_s$, then

$$C_{t_k} \subset \{2^{id} t_{k+jd} | 0 \le j < n_s/d; 0 \le i < n_r\}$$

where $0 \le k < d$. Thus the result follows. □

From the proof of Theorem 2, the computation of $\eta_r \eta_s$ is essentially carried out on the coset monoid Ω_n. We have the following two new operators which are induced from the monoid Ω_n.

$$\eta_r \oplus \eta_s = \eta_{r+s} \tag{9}$$

$$\eta_r \circ \eta_s = \eta_{rs} = \sum_{j=0}^{n_{rs}-1} \xi^{rsp^j} \tag{10}$$

For the sum of any $m > 0$ elements in Ψ_n, we define

$$\eta_r \oplus \left(\sum_{i=1}^{m} \eta_i\right) = \sum_{i=1}^{m} (\eta_r \oplus \eta_i) \tag{11}$$

$$\eta_r \circ \left(\sum_{i=1}^{m} \eta_i\right) = \sum_{i=1}^{m} (\eta_r \circ \eta_i) \tag{12}$$

Now we have four operations in Ψ_n. How does $\oplus$ interact with $+$ and $\cdot$? How does $\circ$ interact with $\oplus$, $+$ and $\cdot$? What distributive laws (if any) connect $\oplus$ and $\circ$ with $+$ and $\cdot$? From the identities (11) and (12), both the new operators $\oplus$ and $\circ$ satisfy the distributive law for the ordinary addition operator. Next we will prove that

Theorem 3. *The operator* $\circ$ *in* Ψ_n *has the following distributive law for the ordinary multiplication operation and* $\oplus$*:*

$$\eta_r \circ (\eta_s \cdot \eta_t) = (\eta_r \circ \eta_s) \cdot (\eta_r \circ \eta_t), \text{ for } r \in \Omega_n^*, s, t \in \Omega_n \tag{13}$$
$$\eta_r \circ (\eta_s \oplus \eta_t) = (\eta_r \circ \eta_s) \oplus (\eta_r \circ \eta_t), r, s, t \in \Omega_n. \tag{14}$$

In order to prove this result, we need the following lemma. We write $\eta_s = \eta_s(\xi)$ for its dependence on ξ.

Lemma 2. *If* $(r, q-1) = 1$*, then*

$$\eta_s(\xi^r) = \eta_{rs}(\xi) = \eta_{rs}.$$

Proof. Note that

$$\eta_s(\xi^r) = \sum_{i=0}^{n_s - 1} \xi^{rsp^i}.$$

Since $(r, q-1) = 1$, the cosets containing s and rs have the same size. I.e., $n_s = n_{rs}$. Substituting this into the above identity, we get

$$\eta_s(\xi^r) = \sum_{i=0}^{n_{rs} - 1} \xi^{rsp^i} = \eta_{rs}(\xi) = \eta_{rs}.$$

Proof of Theorem 3. From Theorem 2, we can write

$$\eta_s \cdot \eta_t = \sum_k c_k \eta_k$$

where the c_k's are positive integers. Thus

$$\begin{aligned} \eta_r \circ (\eta_s \cdot \eta_t) &= \eta_r \circ \left(\sum_k c_k \eta_k \right) \\ &= \sum_k c_k (\eta_r \circ \eta_k) \\ &= \sum_k c_k \eta_{rk} \end{aligned}$$

where the second to last identity is from the definition (11). On the other hand, for $r \in \Omega_n^*$, according to Lemma 2,

$$\begin{aligned}(\eta_r \circ \eta_s) \cdot (\eta_r \circ \eta_t) &= \eta_{rs} \cdot \eta_{rt} \\ &= \eta_s(\xi^r)\eta_t(\xi^r) \\ &= \sum_k c_k \eta_k(\xi^r) \\ &= \sum_k c_k \eta_{rk}\end{aligned}$$

which establishes the assertion (13). The second distributive law is a direct result from Theorem 1. □

Example 2. We will use Example 1. Here ξ is a primitive 15th root of unity, and

$$\begin{aligned}&\eta_0 = 1 \\ &\eta_1 = \xi + \xi^2 + \xi^4 + \xi^8 \\ &\eta_3 = \xi^3 + \xi^6 + \xi^{12} + \xi^9 \\ &\eta_5 = \xi^5 + \xi^{10} \\ &\eta_7 = \xi^7 + \xi^{14} + \xi^{13} + \xi^{11}\end{aligned}$$

The multiplication tables for $\cdot$ and $\circ$ of Ψ_4 are shown as Tables 2 and 3.

Table 2

$\cdot$	η_0	η_1	η_3	η_5	η_7
η_0	η_0	η_1	η_3	η_5	η_7
η_1	η_1	$\eta_1 + 2\eta_3 + 2\eta_5$	$\eta_1 + 2\eta_5 + 2\eta_7$	$\eta_3 + \eta_7$	$4\eta_0 + \eta_1 + \eta_3 + \eta_7$
η_3	η_3	$2\eta_7 + \eta_1 + 2\eta_5$	$4\eta_0 + 3\eta_3$	$\eta_1 + \eta_7$	$2\eta_1 + 2\eta_5 + \eta_7$
η_5	η_5	$\eta_3 + \eta_7$	$\eta_1 + \eta_7$	$2\eta_0 + \eta_5$	$\eta_1 + \eta_3$
η_7	η_7	$4\eta_0 + \eta_1 + \eta_3 + \eta_7$	$2\eta_1 + 2\eta_5 + \eta_7$	$\eta_1 + \eta_3$	$2\eta_3 + 2\eta_5 + \eta_7$

Table 3

$\circ$	η_1	η_3	η_5	η_7
η_1	η_1	η_3	η_5	η_7
η_3	η_3	η_3	η_0	η_3
η_5	η_5	η_0	η_5	η_5
η_7	η_7	η_3	η_5	η_1

From Tables 2 and 3, we have

$$\eta_7 \circ (\eta_3 \cdot \eta_7) = \eta_7 \circ (2\eta_1 + 2\eta_5 + \eta_7) = 2\eta_7 + 2\eta_5 + \eta_1$$

and

$$(\eta_7 \circ \eta_3) \cdot (\eta_7 \circ \eta_7) = \eta_3 \cdot \eta_1 = 2\eta_7 + 2\eta_5 + \eta_1$$

Thus

$$\eta_7 \circ (\eta_3 \cdot \eta_7) = (\eta_7 \circ \eta_3) \cdot (\eta_7 \circ \eta_7)$$

as stated in Theorem 3 since $7 \in \Omega_4^*$.

Remark 2. Theorem 3 shows that the new operator $\circ$ in the cyclotomic algebra Ψ_n is analogous to the exponential operation in the field $\mathcal{F}$. I.e., it is analogous to $(a \cdot b)^c = a^c \cdot b^c$ for $a, b \in \mathcal{F}$ and c an integer.

4 Applications to Cyclic Invariant Sequences

Before we introduce this connection, we restate here that the number of elements in Ψ_n is equal to the number of elements in Ω_n [2]. Let $I_p(d)$ be the number of irreducible polynomials over $\mathbb{F}_p$ of degree d. Then

$$|\Omega_n| = \sum_{d|n} I_p(d)$$

and

$$|\Omega_n^*| = \phi(p^n - 1)/n.$$

where $\phi(x)$ is the Euler function, representing the number of integers coprime to $p^n - 1$ in the range of 1 to $p^n - 1$.

From the theory of linear feedback shift register (LFSR) sequences, $|\Omega_n|$ is the number of shift distinct linear feedback shift register (LFSR) sequences over $\mathbb{F}_p$ with irreducible feedback polynomials of degree dividing n. Moreover $|\Omega_n^*|$ is the number of all shift distinct m-sequences over $\mathbb{F}_p$ of degree n. Any sequence over $\mathbb{F}_p$ can be decomposed into a sum of phase shifts of these LFSR sequences.

Let $A = \{a_i\}$ be a sequence over $\mathbb{F}_p$ of period dividing $p^n - 1$. Then the sequence A has the following trace representation

$$a_i = f(\xi^i) \text{ where } f(x) = \sum_{r \in \Omega_n} Tr_p^{n_r}(\beta_r \xi^{ri})$$

where ξ is a primitive element in $\mathbb{F}_{p^n}$, $\beta_r \in \mathbb{F}_{p^{n_r}}$, and $Tr_p^{n_r}(x)$ is the trace function from $\mathbb{F}_{p^{n_r}}$ to $\mathbb{F}_p$. Under this assumption, we can take $\mathcal{F} = \mathbb{F}_{p^n}$. From Section 3, we have

$$\eta_r = \eta_r(\xi) = Tr_p^{n_r}(\xi)$$

If the elements of A satisfy the cyclic invariant condition, i.e., $a_i = a_{ip}, i = 0, 1, \cdots$, then we say that A is *cyclic invariant.* In this case, the trace representation of A becomes

$$f(x) = \sum_{r \in \Omega_n} d_r Tr_p^{n_r}(\xi^{ri}), \; d_r \in \mathbb{F}_p.$$

(This can be verified directly using the trace representation and the cyclic invariant condition, so we omit it here.)

Decimation Operator and Shift Operator. Let s be an integer. A sequence $B = \{b_i\}$ whose elements are given by

$$b_i = a_{si}, i = 0, 1, \cdots,$$

is called an s-decimation of A, denoted by $B = A^{(s)}$. For the case $(s, q-1) = 1$, applying Theorem 3 to the s-decimation of A, we have

$$\begin{aligned}
b_i &= a_{si} = f(\xi^{si}) \\
&= \sum_{r \in \Omega_n} d_r Tr_p^{n_r}(\xi^{sri}) \\
&= \sum_{r \in \Omega_n} c_{r,i} Tr_p^{n_{ri}}(\xi^{sri}), \; \text{where } c_{r,i} = d_r \frac{n_r}{n_{ri}} \\
&= \sum_{r \in \Omega_n} c_{r,i} \eta_{sri} \\
&= \sum_{r \in \Omega_n} c_{r,i} (\eta_s \circ \eta_{ri}) \\
&= \eta_s \circ \left(\sum_{r \in \Omega_n} c_{r,i} \eta_{ri} \right).
\end{aligned}$$

Thus

$$a_{si} = \eta_s \circ \left(\sum_{r \in \Omega_n} c_{r,i} \eta_{ti} \right), i = 0, 1, \cdots. \tag{15}$$

Hence the new operator $\circ$ on the cyclotomic algebra Ψ_n corresponds to the decimation operator on cyclic invariant sequences. The formula (15) provides a new insight for computing correlation between the sequence and its decimation in terms of the cyclotomic formulas provided in [3].

Next we will show that the new operator $\oplus$ on Ψ_n corresponds to the (left) shift operator on the sequence A. Let L be the shift operator, i.e., $L^t(A) = a_t, a_{t+1}, \cdots$. Here we only present the special case of n is prime. The same approach used here can apply to general n, but it needs a more complicated formula for justification of the coefficients. Applying (11), we now have

$$\begin{aligned} a_{t+i} &= f(\xi^{i+t}) \\ &= \sum_{r \in \Omega_n} d_r Tr_p^{n_r}(\xi^{r(i+t)}) \\ &= \sum_{r \in \Omega_n} d_r \eta_{ri+rt} \\ &= \sum_{r \in \Omega_n} d_r (\eta_{rt} \oplus \eta_{ri}) \\ &= \sum_{r \in \Omega_n} d_r ((\eta_t \circ \eta_r) \oplus \eta_{ri}) \end{aligned}$$

i.e., we have

$$a_{t+i} = \sum_{r \in \Omega_n} d_r ((\eta_t \circ \eta_r) \oplus \eta_{ri}), i = 0, 1, \cdots. \tag{16}$$

Remark 3. Any 2-level autocorrelation sequence over $\mathbb{F}_2$ is a cyclic invariant sequence for $p = 2$ [4], [5], and for $p > 2$, we have found that all known 2-level autocorrelation sequences are cyclic invariant. However, it has not been proved whether the 2-level autocorrelation condition implies the cyclic invariant condition. The formulae (15) and (16) provide another representation of the decimated sequences and the shifted sequences in terms of cyclotomic algebra with the new operators $\oplus$ and $\circ$. These representations will facilitate computation of the linear span and the correlation of cyclic invariant sequences and may enable one to characterize families of 2-level autocorrelation sequences and low crosscorrelation sequences.

References

1. N. Jacobson, *Basic Algebra I*, W.H. Freeman and Company, San Francisco, 1974.
2. S.W. Golomb, *Shift Register Sequences,* Holden-Day, Inc., 1967. Revised edition, Aegean Park Press, 1982.
3. S.W. Golomb, Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences, *Information Sciences*, vol.1, no. 1, December 1968, pp.87-109.
4. S. W. Golomb, "On the classification of balanced binary sequences of period 2^n-1," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 730-732, Nov. 1980.
5. G. Gong and S.W. Golomb, Binary sequences with two-level autocorrelation, *IEEE Trans. on Inform. Theory*, vol. 45, No.2, March 1999, pp.692-693.
6. B.L. van der Waerden, *Modern Algebra*, Volume I, Frederick Ungar Publishing Co, 1950.