Malaysian Journal of Mathematical Sciences 11(S) August: 59 - 73 (2017)
Special Issue: The 5th International Cryptology and Information Security Conference (New Ideas in Cryptology)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES
Journal homepage: http://einspem.upm.edu.my/journal

Cyclotomic Cosets, Codes and Secret Sharing

Wong, D. C. K.

Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Jalan Sungai Long, Cheras, 43000 Kajang, Selangor Darul Ehsan, Malaysia.

E-mail: deniswong@utar.edu.my

ABSTRACT

In this paper, all 2-cyclotomic cosets modulo p^n are constructed when 2 is a primitive root modulo p^n. When the order of 2 is $\frac{p-1}{2}$ modulo p and the order of 2 is $\frac{p(p-1)}{2}$ modulo p^2, we construct all 2-cyclotomic cosets modulo p^2. Also, when 2 has order $\frac{p^2(p-1)}{2}$ modulo p^3, we derive all 2-cyclotomic cosets modulo p^3. Furthermore, four results on all s-cyclotomic cosets modulo pq are obtained by considering three different possible orders of s modulo p and q, for distinct odd primes p, q. Finally, we use the 2-cyclotomic cosets modulo 9, 25 and 49 to construct binary codes of length 9, 15 and 49, respectively, and hence the access sets for the secret sharing scheme based on some of these families of binary codes are discussed.

Keywords: Cyclotomic cosets, minimum distance, secret sharing, cyclic codes, idempotents.

1. Introduction

Throughout this paper, we let q be a prime, n a positive integer and $gcd(q,n) = 1$. The $q-$cyclotomic coset modulo n containing i is defined by $C_i = \{iq^j (\text{mod } n) \in Z_n \mid j = 0, 1, 2, \dots\}$. A subset $\{i_1, \dots, i_t\}$ of Z_n is called a complete set of representatives of $q-$cyclotomic cosets modulo n if $C_{i_1}, C_{i_2}, \dots, C_{i_t}$ are distinct and $\bigcup_{j=1}^{t} C_{i_j} = Z_n$. Furthermore, any two cyclotomic cosets are either equal or disjoint. Hence, we see that $C_{i_1}, C_{i_2}, \dots, C_{i_t}$ partition Z_n.

Dating back to 1948, the birth of coding theory was inspired by the paper called "A Mathematical Theory of Communication" written by Shannon (Shannon, 1948). Coding theory is the study of the properties of error-correcting codes which are used for data compression, cryptography and network coding. A special type of linear code is cyclic code which was first studied by Prange in 1957. In recent years, many authors have used the cyclotomic cosets approach to construct various families of cyclic codes, see MacWilliams and Sloane (1977), Wong and Ang (2013). Construction of binary idempotents from the cyclotomic cosets is easy. However, there is not much information can be obtained from the generated codes. In years 1997 and 2003, respectively, Arora and Pruthi gave an explicit expression for all q-cyclotomic cosets modulo p^n when q is a primitive root modulo p^n (Arora and Pruthi, 1997) and when q has order $\frac{\phi(p^n)}{2}$ modulo p^n (Arora and Pruthi, 1999). Then, in Sharma et al. (2004), the authors obtained all q-cyclotomic cosets modulo p^n with a more subtle conditions. Later in year 2012, Sharma and Bakshi (Sharma and G.K.Bakshi, 2012) considered a more general type of q-cyclotomic cosets modulo p^m to compute the weight distribution of some irreducible cyclic codes. In Singh and Arora (2010), q-cyclotomic cosets modulo 2^n when q is quadratic residue modulo 2^n is obtained. More recently, l-cyclotomic cosets modulo the product of two distinct primes power are studied in Arora et al. (2002) and Sahni and Sehgal (2012).

This paper is organized as follows: In section 2, we construct 2-cyclotomic cosets modulo p^n when 2 is a primitive root modulo p^n and when the order of 2 modulo p is $\frac{p-1}{2}$. Furthermore, we investigate the structures of all s-cyclotomic cosets modulo pq when s is a primitive root modulo q and s is a primitive root modulo p, s has order $\frac{q-1}{2}$ modulo q and s has order $\frac{p-1}{2}$ modulo p, and s has order $\frac{q-1}{2}$ modulo q and s is a primitive root modulo p. For all these cases, p and q are distinct odd primes. In section 3, we construct three families of binary cyclic codes of length 9, 25 and 49 from 2-cyclotomic cosets modulo 9, modulo 25 and modulo 49, respectively. Hence, we investigate the access sets for the secret sharing based on some of these families of binary cyclic codes.

Finally, in section 4 we give a conclusion and future research directions.

2. Cyclotomic Cosets

Let n be an integer > 1 and $gcd(a, n) = 1$. The order of a modulo n is the smallest integer k such that $a^k \equiv 1(\text{mod } n)$. When $k = \phi(n)$, where ϕ is the Euler-phi function, then a is called a primitive root of the integer n. We need the following result from Sharma and G.K.Bakshi (2012).

Lemma 2.1. *Suppose α is a primitive root modulo p^n. Then, α is a primitive root modulo p^{n-j} also, for all j, $0 \leq j \leq n-1$.*

We start by showing all 2-cyclotomic cosets modulo p^n when 2 is a primitive root modulo p^n in the following theorem.

Theorem 2.1. *Let p be an odd prime and $n \geq 2$. Suppose 2 is a primitive root modulo p^n. Then, there are exactly n nonzero 2-cyclotomic cosets modulo p^n with $|C_1| = p^n - p^{n-1}, |C_p| = p^{n-1} - p^{n-2}, \ldots, |C_{p^{n-1}}| = p - 1$.*

Proof. Given 2 is a primitive root modulo p^n, then $2^{p^n - p^{n-1}} \equiv 1(\text{mod } p^n)$. By Lemma 2.1, we have $2^{p^{n-1} - p^{n-2}} \equiv 1(\text{mod } p^{n-1})$, $2^{p^{n-2} - p^{n-3}} \equiv 1(\text{mod } p^{n-2})$, $\ldots$, $2^{p^2 - p} \equiv 1(\text{mod } p^2)$ and $2^{p-1} \equiv 1(\text{mod } p)$.

The 2-cyclotomic coset modulo p^n with coset representative 1 is $C_1 = \{1, 2, 2^2, ..., 2^{t_1 - 1}\}$, where $2^{t_1} \equiv 1(\text{mod } p^n)$. Clearly, $t_1 = p^n - p^{n-1}$ and so $|C_1| = p^n - p^{n-1}$. Next, since $p \notin C_1$, we construct $C_p = \{p, 2p, 2^2p, ..., 2^{t_p - 1}p\}$, where $2^{t_p}p \equiv p(\text{mod } p^n)$ which is equivalent to $2^{t_p} \equiv 1(\text{mod } p^{n-1})$ and so $t_p = p^{n-1} - p^{n-2} = |C_p|$. Now, we suppose that $p^2 \in C_p$. Then, $p^2 = 2^i p$ for some i implies that $p = 2^i$ which is a contradiction. Hence, $p^2 \notin C_p$. Since $p^2 \notin C_1$ and $p^2 \notin C_p$, we consider $C_{p^2} = \{p^2, 2p^2, 2^2p^2, ..., 2^{t_{p^2} - 1}p^2\}$, where $2^{t_{p^2}}p^2 \equiv p^2(\text{mod } p^n)$ which is equivalent to $2^{t_{p^2}} \equiv 1(\text{mod } p^{n-2})$ and so $t_{p^2} = p^{n-2} - p^{n-3} = |C_{p^2}|$. Continue in this way, we obtain the rest of the 2-cyclotomic cosets modulo p^n.

Finally, note that $|C_1| + |C_p| + |C_{p^2}| + \cdots + |C_{p^{n-1}}| + |\{0\}| = |\mathbb{Z}_{p^n}|$. Therefore, we conclude that $\mathbb{Z}_{p^n} = C_1 \cup C_p \cup \cdots \cup C_{p^{n-1}} \cup \{0\}$ and $C_i \cap C_j = \emptyset$ for all $i,\ j \in \{1, p, p^2, \ldots, p^{n-1}\}$. □

Next, we construct 2-cyclotomic cosets modulo p^n when the order of 2 modulo p is $\frac{p-1}{2}$ for the cases when $n = 2$ and 3. Also, we assume q is an odd

prime such that $q < p$.

Theorem 2.2. *Suppose* 2 *has order* $\frac{p-1}{2}$ *modulo* p *and* 2 *has order* $\frac{p(p-1)}{2}$ *modulo* p^2. *Then, there are exactly* 4 *distinct nonzero 2-cyclotomic cosets modulo* p^2.

Proof. The cyclotomic coset modulo p^2 with coset representative 1 is $C_1 = \{1, 2, 2^2, ..., 2^{t_1-1}\}$, where $2^{t_1} \equiv 1 (\text{mod } p^2)$. Since 2 has order $\frac{p(p-1)}{2}$ modulo p^2, then we have $t_1 = \frac{p(p-1)}{2}$ and so $|C_1| = \frac{p(p-1)}{2}$. Next, we construct the second 2-cyclotomic coset modulo p^2 with coset representative q, that is, $C_q = \{q, 2q, 2^2q, ..., 2^{t_q-1}q\}$, where $2^{t_q}q \equiv q (\text{mod } p^2)$. The condition $2^{t_q}q \equiv q (\text{mod } p^2)$ can be reduced to $2^{t_q} \equiv 1 (\text{mod } p^2)$ since p, q are distinct odd primes, which gives us $t_q = \frac{p(p-1)}{2}$ and so $|C_q| = \frac{p(p-1)}{2}$.

Now, since $p \notin C_1$ and $p \notin C_q$, we consider $C_p = \{p, 2p, ..., 2^{t_p-1}p\}$, where $2^{t_p}p \equiv p (\text{mod } p^2)$ which is equivalent to $2^{t_p} \equiv 1 (\text{mod } p)$. Since 2 has order $\frac{p-1}{2}$ modulo p, then we have $t_p = \frac{p-1}{2}$ and so $|C_p| = \frac{p-1}{2}$. Finally, as $pq \notin C_1 \cup C_q \cup C_p$, we construct the last nonzero cyclotomic coset modulo p^2, that is, $C_{pq} = \{pq, 2pq, ..., 2^{t_{pq}-1}pq\}$, where $2^{t_{pq}}pq \equiv pq (\text{mod } p^2)$ which is equivalent to $2^{t_{pq}}q \equiv q (\text{mod } p)$. Similarly, it can be reduced to $2^{t_{pq}} \equiv 1 (\text{mod } p)$. Then, we have $t_{pq} = \frac{p-1}{2}$ and so $|C_{pq}| = \frac{p-1}{2}$.

Combining all above, we have $|C_1| = |C_q| = \frac{p(p-1)}{2}$ and $|C_p| = |C_{pq}| = \frac{p-1}{2}$. Clearly, $|C_1| + |C_q| + |C_p| + |C_{pq}| + |\{0\}| = |\mathbb{Z}_{p^2}|$. Hence, C_1, C_q, C_p and C_{pq} are the required 2-cyclotomic cosets modulo p^2. □

As an illustration, we list all 2-cyclotomic cosets modulo 7^2.

$C_0 = \{0\}$,
$C_1 = \{1, 2, 4, 8, 16, 32, 15, 30, 11, 22, 44, 39, 29, 9, 18, 36, 23, 46, 43, 37, 25\}$,
$C_3 = \{3, 6, 12, 24, 48, 47, 45, 41, 33, 17, 34, 19, 38, 27, 5, 10, 20, 40, 31, 13, 26\}$,
$C_7 = \{7, 14, 28\}$ and
$C_{21} = \{21, 42, 35\}$.

Theorem 2.3. *Suppose* 2 *has order* $\frac{p^2(p-1)}{2}$ *modulo* p^3. *Then, there are exactly* 6 *distinct nonzero 2-cyclotomic cosets modulo* p^3.

Proof. Given 2 has order $\frac{p^2(p-1)}{2}$ modulo p^3, then $2^{\frac{p^2(p-1)}{2}} \equiv 1 (mod\ p^3)$. Thus, by Euler's Theorem together with the definition of order, we have $2^{\frac{p(p-1)}{2}} \equiv 1 (mod\ p^2)$ and $2^{\frac{p-1}{2}} \equiv 1 (mod\ p)$. The cyclotomic coset modulo p^3 with

coset representative 1 is $C_1 = \{1, 2, 2^2, ..., 2^{t_1-1}\}$, where $2^{t_1} \equiv 1 (\text{mod } p^3)$. From above, we have $t_1 = \frac{p^2(p-1)}{2}$ and so $|C_1| = \frac{p^2(p-1)}{2}$.

Clearly, $q \notin C_1$, so we construct $C_q = \{q, 2q, 2^2q, ..., 2^{t_q-1}q\}$, where $2^{t_q}q \equiv q (\text{mod } p^3)$ which can be reduced to $2^{t_q} \equiv 1 (\text{mod } p^3)$, which gives us $t_q = \frac{p^2(p-1)}{2}$ and so $|C_q| = \frac{p^2(p-1)}{2}$. Since $p \notin C_1 \cup C_q$, we consider the third cyclotomic coset modulo p^3 with coset representative p, that is, $C_p = \{p, 2p, 2^2p, ..., 2^{t_p-1}p\}$, where $2^{t_p}p \equiv p (\text{mod } p^3)$ which is equivalent to $2^{t_p} \equiv 1 (\text{mod } p^2)$. Then, we have $t_p = \frac{p(p-1)}{2}$ and so $|C_p| = \frac{p(p-1)}{2}$.

Similar to previous theorem, we consider pq which is not in all the previous cyclotomic cosets and construct $C_{pq} = \{pq, 2pq, ..., 2^{t_{pq}-1}pq\}$, where $2^{t_{pq}}pq \equiv pq (\text{mod } p^3)$ which is equivalent to $2^{t_{pq}}q \equiv q (\text{mod } p^2)$. It can be reduced to $2^{t_{pq}} \equiv 1 (\text{mod } p^2)$. Then, we have that $t_{pq} = \frac{p(p-1)}{2}$ and so $|C_{pq}| = \frac{p(p-1)}{2}$. As $p^2 \notin C_1 \cup C_q \cup C_p \cup C_{pq}$, we consider $C_{p^2} = \{p^2, 2p^2, ..., 2^{t_{p^2}-1}p^2\}$, where $2^{t_{p^2}}p^2 \equiv p^2 (\text{mod } p^3)$ which is equivalent to $2^{t_{p^2}} \equiv 1 (\text{mod } p)$ and so $t_{p^2} = \frac{p-1}{2}$. Finally, we consider p^2q as it is also not in the other five cyclotomic cosets modulo p^3 and hereby construct the cyclotomic coset modulo p^3, that is, $C_{p^2q} = \{p^2q, 2p^2q, ..., 2^{t_{p^2q}-1}p^2q\}$, where $2^{t_{p^2q}}p^2q \equiv p^2q (\text{mod } p^3)$ which is equivalent to $2^{t_{p^2q}}q \equiv q (\text{mod } p)$. Later, it is reduced to $2^{t_{p^2q}} \equiv 1 (\text{mod } p)$. Clearly, we see that $t_{p^2q} = \frac{p-1}{2} = |C_{p^2q}|$. The rest of the properties will then follow immediately. □

Here, we list all 2-cyclotomic cosets modulo 7^3, which is the smallest case covered by previous theorem.

C_0 ={0},
C_1 ={1, 2, 4, 8, 16, 32, 64, 128, 256, 169, 338, 333, 323, 303, 263, 183, 23,
46, 92, 184, 25, 50, 100, 200, 57, 114, 228, 113, 226, 109, 218, 93, 186, 29, 58,
116, 232, 121, 242, 141, 282, 221, 99, 198, 53, 106, 212, 81, 162, 324, 305, 267,
191, 39, 78, 156, 312, 281, 219, 95, 190, 37, 74, 148, 296, 249, 155, 310, 277, 211
79, 158, 316, 289, 235, 127, 254, 165, 330, 317, 291, 239, 135, 270, 197, 51, 102,
204, 65, 130, 260, 177, 11, 22, 44, 88, 176, 9, 18, 36, 72, 144, 288, 233, 123, 246,
149, 298, 253, 163, 326, 309, 275, 207, 71, 142, 284, 225, 107, 214, 85, 170, 340,
337, 331, 319, 295, 247, 151, 302, 261, 179, 15, 30, 60, 120, 240, 137, 274, 205,
67, 134, 268, 193, 43, 86, 172},
C_3 ={3, 6, 12, 24, 48, 96, 192, 41, 82, 164, 328, 313, 283, 223, 103,
206, 69, 138, 276, 209, 75, 150, 300, 257, 171, 342, 341, 339, 335, 327, 311,
279, 215, 87, 174, 5, 10, 20, 40, 80, 160, 320, 297, 251, 159, 318, 293, 243, 143,
286, 229, 115, 230, 117, 234, 125, 250, 157, 314, 285, 227, 111, 222, 101, 202,
61, 122, 244, 145, 290, 237, 131, 262, 181, 19, 38, 76, 152, 304, 265, 187, 31, 62,
124, 248, 153, 306, 269, 195, 47, 94, 188, 33, 66, 132, 264, 185, 27, 54, 108, 216,
89, 178, 13, 26, 52, 104, 208, 73, 146, 292, 241, 139, 278, 213, 83, 166, 332, 321,
299, 255, 167, 334, 325, 307, 271, 199, 55, 110, 220, 97, 194, 45, 90, 180, 17, 34,
68, 136, 272, 201, 59, 118, 236, 129, 258, 173},
C_7 ={7, 14, 28, 56, 112, 224, 105, 210, 77, 154, 308, 273, 203, 63, 126, 252, 161, 322, 301, 259, 175},
C_{21} ={21, 42, 84, 168, 336, 329, 315, 287, 231, 119, 238, 133, 266, 189, 35, 70, 140, 280, 217, 91, 182},
C_{49} ={49, 98, 196},
C_{147} ={147, 294, 245}

Finally, we drawn our attention to study all $s-$ cyclotomic cosets modulo pq, where p, q and s are distinct odd primes.

Theorem 2.4. *Let p, q, s be distinct odd primes. Suppose s is a primitive root modulo q and s is a primitive root modulo p. Then there are $2 + h$ distinct nonzero s-cyclotomic cosets modulo pq, where $h = gcd(p-1, q-1)$. Furthermore, the h distinct nonzero s-cyclotomic cosets modulo pq have size $m = lcm(p-1, q-1)$.*

Proof. We first construct the s-cyclotomic coset modulo pq which contains p. Note that $C_p = \{p, sp, \ldots, s^{t_p-1}p\}$, where $s^{t_p}p \equiv p(\text{mod } pq)$. The condition $s^{t_p}p \equiv p(\text{mod } pq)$ implies $q \mid s^{t_p} - 1$. Since s has order $q-1$ modulo q, then we have $t_p = q-1$ and so $|C_p| = q-1$. A similar argument shows that $|C_q| = p-1$.

Next, we consider any $a \in \{1, 2, \ldots, pq\}$ with $gcd(a, pq) = 1$. Then, we see that $gcd(a, p) = 1$ and $gcd(a, q) = 1$. The s-cyclotomic coset modulo n containing a is $C_a = \{a, as, \ldots, as^{t_a} - 1\}$, where $s^{t_a}a \equiv a(\text{mod } pq)$. The choice of a ensures that $pq \mid s^{t_a} - 1$ which implies $p \mid s^{t_a} - 1$ and $q \mid s^{t_a} - 1$. Since s is a primitive root modulo p and modulo q, we obtain $t_a = lcm(p-1, q-1)$. Therefore, we obtained $|C_a| = lcm(p-1, q-1)$ for any $a \in \{1, 2, \ldots, pq\}$ with $gcd(a, pq) = 1$.

Finally, we let h be the number of s-cyclotomic cosets modulo pq containing a and note that $|C_0| = |\{0\}| = 1$. Hence, $|C_0| + |C_p| + |C_q| + \sum_a |C_a| = pq$. We then have $1 + (q-1) + (p-1) + h.lcm(p-1, q-1) = pq$ and so $h = \frac{pq-q-p+1}{lcm(p-1,q-1)} = gcd(p-1, q-1)$. □

Theorem 2.5. *Let p, q, s be distinct odd primes. Suppose s has order $\frac{q-1}{2}$ modulo q and s has order $\frac{p-1}{2}$ modulo p. Then there are $4+h$ distinct nonzero s-cyclotomic cosets modulo pq, where $h = \frac{(p-1)(q-1)}{lcm(\frac{q-1}{2}, \frac{p-1}{2})}$. Furthermore, the h distinct nonzero s-cyclotomic cosets modulo pq have size $m = lcm(\frac{q-1}{2}, \frac{p-1}{2})$.*

Proof. Since s has order $\frac{q-1}{2}$ modulo q, then we have $|C_p| = \frac{q-1}{2}$. Also, as s has order $\frac{p-1}{2}$ modulo p, then we have $|C_q| = \frac{p-1}{2}$. Next, let k be a prime such that $q \nmid k$. The s-cyclotomic coset modulo pq containing kp is $C_{kp} = \{kp, skp, s^2kp, \ldots, s^{t_{kp}-1}k_p\}$, where $s^{t_{kp}}k_p \equiv kp (\mathrm{mod}\ pq)$ which implies $q \mid (s^{t_{kp}} - 1)$ and so $t_{kp} = \frac{q-1}{2}$. Thus, $|C_{kp}| = \frac{q-1}{2}$. Similarly, if $p \nmid j$, then $|C_{jq}| = \frac{p-1}{2}$.

Next, we let h be the nonzero s-cyclotomic cosets modulo pq of size m, then we have $1 + 2.\frac{q-1}{2} + 2.\frac{p-1}{2} + h.m = pq$, that is, $hm = (p-1)(q-1)$. Finally, we consider any $a \notin \{p, q, kp, jq\}$. The s-cyclotomic coset modulo pq containing a is $C_a = \{a, as, as^2, \ldots, as^{t_a-1}\}$, where $as^{t_a} \equiv a (\mathrm{mod}\ pq)$ which is equivalent to $pq|(s^{t_a} - 1)$. Thus, $t_a = m = lcm(\frac{q-1}{2}, \frac{p-1}{2})$ and so $h = \frac{(p-1)(q-1)}{m}$. □

The following theorem can be proved in the similar way as theorems above.

Theorem 2.6. *Let p, q, s be distinct odd primes. Suppose s has order $\frac{q-1}{2}$ modulo q and s is a primitive root modulo p. Then there are $3+h$ distinct nonzero s-cyclotomic cosets modulo pq, where $h = \frac{(p-1)(q-1)}{lcm(\frac{q-1}{2}, p-1)}$. Furthermore, the h distinct nonzero s-cyclotomic cosets modulo pq have size $m = lcm(\frac{q-1}{2}, p-1)$.*

3. Codes and Secret Sharing

In coding theory, a code C of length n and size M over $\mathbb{F}_q$ is called a $q-$ary (n, M)-code. The Hamming distance of two codewords x and y in C, denoted by $d(x, y)$ is defined as the number of symbols at which x and y differ. The minimum distance of a code is denoted by d or $d(C)$. When the d is known, we call C a $q-$ ary (n, M, d)-code over $\mathbb{F}_q$. The minimum distance is a very important parameter as it tell us the number of errors it can correct or detect when transmitting codewords across a noisy channel, refer MacWilliams and

Sloane (1977). In general, there are two main types of codes which are linear code and nonlinear code. A code C of length n is called a linear code if C is a subspace of the vector space $\mathbb{F}_q^n$, else, it is a nonlinear code. Since linear code is a subspace, it is also a vector space and is spanned by a basis. The basis for a linear code is often represented in the form of a matrix which is known as the generator matrix where the rows of the matrix form a basis of the linear code. We often called linear code as $[n, k]$-code or if the d is known, it is called a $[n, k, d]$-code, where k is the dimension of the subspace. Next, the weight of a codeword is defined as the number of nonzero symbols in a nonzero codeword. The minimum distance d is equals to the minimum weight of a nonzero codeword in C if C is a linear code. This property is advantageous as we do not need to compare every codeword to find the distance, instead we just look at each nonzero codeword for the weight which saves more steps and time. In this paper, we are interested in constructing a special type of linear code which is know as the cyclic codes. A linear code C is cyclic if any cyclic shift of a codeword is also a codeword, i.e., whenever $(c_0, c_1, ..., c_{n-1})$ is in C then so is $(c_{n-1}, c_0, ..., c_{n-2})$. For more information on cyclic codes, refer to MacWilliams and Sloane (1977).

3.1 Binary Cyclic Codes of length 9

In this section, we construct binary cyclic codes with length $n = 9$. Since 2 is a primitive root modulo 3, by Theorem 2.1, there are exactly two nonzero 2−cyclotomic cosets modulo 9 which is listed as follows:

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 7, 5\} \text{ and } C_3 = \{3, 6\}.$$

To represent these cyclotomic cosets in term of group ring, we let $\Omega_1 = \sum_{s \in C_1} g^s \in \mathbb{F}_2[\mathbb{Z}_9]$ and $\Omega_2 = \sum_{r \in C_3} g^r \in \mathbb{F}_2[\mathbb{Z}_9]$. In term of group ring, the cyclotomic cosets of $\mathbb{F}_2[\mathbb{Z}_9]$ are

$$\Omega_0 = 1, \Omega_1 = g^1 + g^2 + g^4 + g^8 + g^7 + g^5, \text{ and } \Omega_2 = g^3 + g^6.$$

We see that $\Omega_0^2 = 1^2 = 1 = \Omega_0$ and easily verify that $\Omega_1^2 = \Omega_1$ and $\Omega_2^2 = \Omega_2$ as well as the union of different idempotents are also idempotent. These idempotent are called the generating idempotent as each of them can generate a cyclic code. For the following calculations, we are using the methods and theorems derived in MacWilliams and Sloane (1977).

Clearly, the generator polynomial for Ω_0 is 1, so $\langle \Omega_0 \rangle$ is a $[9, 9, 1]$-cyclic

code. For Ω_1, the generator matrix G is found as follows:

$$\begin{pmatrix} 1&0&1&1&0&1&1&0&1\\ 1&1&0&1&1&0&1&1&0\\ 0&1&1&0&1&1&0&1&1 \end{pmatrix} \xrightarrow{R_2\to R_2+R_1} \begin{pmatrix} 1&0&1&1&0&1&1&0&1\\ 0&1&1&0&1&1&0&1&1\\ 0&1&1&0&1&1&0&1&1 \end{pmatrix}$$
$$\xrightarrow{R_3\to R_3+R_2} \begin{pmatrix} 1&0&1&1&0&1&1&0&1\\ 0&1&1&0&1&1&0&1&1\\ 0&0&0&0&0&0&0&0&0 \end{pmatrix} = \begin{pmatrix} G\\ 0 \end{pmatrix}$$

From above, we see that the dimension of the cyclic code is 2 and the minimum distance is 6. Thus, $\langle\Omega_1\rangle$ is a $[9,2,6]$- binary cyclic code.

Next, the generator polynomial for $\langle\Omega_2\rangle$ is obtained as follows:

$$g(x) = gcd(g^9+1, g^3+g^6) = gcd(g^3+g^6, 1+g^3) = 1+g^3.$$

The dimension of the cyclic code is 6 and the minimum distance is 2. Hence, $\langle\Omega_2\rangle$ is a $[9,6,2]$-cyclic code.

Since $\Omega_0+\Omega_1$ is also a generating idempotent, the corresponding generator polynomial is determined as follows:

$$\begin{aligned} g(x) =& gcd(g^9+1, 1+g^1+g^2+g^4+g^8+g^7+g^5)\\ =& gcd(1+g^1+g^2+g^4+g^8+g^7+g^5, g^3+g^4+g^6+g^7)\\ =& gcd(g^3+g^4+g^6+g^7, 1+g+g^2)\\ =& 1+g+g^2. \end{aligned}$$

The dimension of this code is 7 and the minimum distance is 2. $\langle\Omega_0+\Omega_1\rangle$ is a $[9,7,2]$-cyclic code. Similarly, we found that $\langle\Omega_0+\Omega_2\rangle$ is a $[9,3,3]$-cyclic code.

Next, the generator polynomial for $\langle\Omega_1+\Omega_2\rangle$ is

$$\begin{aligned} g(x) =& gcd(g^9-1, g^1+g^2+g^3+g^4+g^5+g^6+g^7+g^8)\\ =& gcd(g^1+g^2+g^3+g^4+g^5+g^6+g^7+g^8, 1+g)\\ =& 1+g. \end{aligned}$$

Clearly, the dimension of the code is 8 while the minimum distance is 2. Hence, $\langle\Omega_1+\Omega_2\rangle$ is a $[9,8,2]$-cyclic code. Finally, by using a similar argument $\langle\Omega_0+\Omega_1+\Omega_2\rangle$=$\{000000000, 111111111\}$ which is a $[9,1,9]$-binary cyclic code.

Secret sharing scheme is used to break down a secret into smaller portions call shares and later distributed to other participants by a dealer. The group of participants who hold the shares that can reconstruct the secret is called the access set. If a group of participants can recover the secret by combining their

shares, then any group of participants containing this group can also recover the secret. The group of participants is known as the minimal access set if they can recover the secret with their shares, while any of its proper subgroups cannot do so.

Next, we randomly choose $\langle \Omega_1 \rangle$ to construct a secret sharing scheme. $\langle \Omega_1 \rangle$ is a $[9, 2, 6]$-binary cyclic code which have the following codewords:

$$\{000000000, 101101101, 110110110, 011011011\}.$$

In the secret sharing scheme based on $[9, 2, 6]$-cyclic code, there are 8 participants and a dealer involved. There are only two access sets as follows:

$$\{1, 3, 4, 6, 7\} \text{ and } \{2, 3, 5, 6, 8\}$$

$\{1, 3, 4, 6, 7\}$ denotes the access set $\{P_1, P_3, P_4, P_6, P_7\}$. From above, we can see that participants 3 and 6 are involved in all the access sets. Hence, whoever who need to find the secret must include these two participants. In each access set, there are exactly 5 participants. Every participant in the set $\{1, 2, 4, 5, 7, 8\}$ is in exactly one access set.

Now, we consider $\langle \Omega_2 \rangle$, a $[9, 6, 2]-$ binary cyclic code which have the following codewords:

$\{000000000, 010010000, 001001000, 000100100, 000010010, 000001001,$
$100000100, 010000010, 001000001, 100100000, 010111101, 101011110,$
$010101111, 101010111, 110101011, 111010101, 111101010, 011110101,$
$101111010, 101100001, 110110000, 011011000, 001101100, 000110110,$
$000011011, 100001101, 110000110, 011000011, 110100010, 011010001,$
$101101000, 010110100, 001011010, 000101101, 100010110, 010001011,$
$101000101, 100111011, 110011101, 111001110, 011100111, 101110011,$
$110111001, 111011100, 011101110, 001110111, 100011111, 110001111,$
$111000111, 111100011, 111110001, 111111000, 011111100, 001111110,$
$000111111, 101001100, 010100110, 001010011, 100101001, 110010100,$
$011001010, 001100101, 100110010, 010011001\}$

Throughout all these codewords, there are only two minimal codewords. So, there are only 2 access sets as follows:$\{3\}$ and $\{6\}$. Both participants 3 and 6 can solely determine the secret. If participant 3 cheats and recover the secret by himself, there is no one to govern his actions. Hence, this secret sharing scheme may expose the secret easily. To describe in a more business-related way, there are two business partner A and B which represent participants 3 and 6 here where both of them have full access right to their shared account. Since A has the full access right, if A became greedy, he can take all the money invested and run away.

3.2 Binary Cyclic Codes of length 25

Next, we consider the case $p = 5$. From Theorem 2.1, we verified that 2 is a primitive root modulo 5, so there are exactly two nonzero cyclotomic cosets modulo 25. Hence, we let $\Omega_1 = \sum_{h \in C_1} g^h \in \mathbb{F}_2[\mathbb{Z}_{25}]$ and $\Omega_2 = \sum_{k \in C_5} g^k \in \mathbb{F}_2[\mathbb{Z}_{25}]$. Then, we see that all 2-cyclotomic cosets modulo 25 are as follows:

$$C_0 = \{0\}, C_5 = \{5, 10, 20, 15\} \text{ and}$$
$$C_1 = \{1, 2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 18, 11, 22, 19, 13\}.$$

In term of group ring, the cyclotomic cosets of $\mathbb{F}_2[\mathbb{Z}_{25}]$ are

$$\begin{aligned}\Omega_0 =& g^0,\\ \Omega_1 =& g^1 + g^2 + g^4 + g^8 + g^{16} + g^7 + g^{14} + g^3 + g^6 + g^{12} +\\ & g^{24} + g^{23} + g^{21} + g^{17} + g^9 + g^{18} + g^{11} + g^{22} + g^{19} + g^{13},\\ \Omega_2 =& g^5 + g^{10} + g^{20} + g^{15}.\end{aligned}$$

Next, we use Ω_1 to construct a cyclic code of length 9, we perform Gaussian elimination on the matrix formed by the generating idempotent to obtain the following generator matrix:

$$G = \begin{pmatrix} 0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1\\ 1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\ 1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1\\ 1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1 \end{pmatrix}.$$

Clearly, the dimension is 4. Then we have $2^4 = 16$ codewords. We easily list down all the codewords as follows:

$$\begin{aligned}\langle \Omega_1 \rangle = \{&0000000000000000000000000, 1101111011110111101111011,\\ &1110111101111011110111101, 1111011110111101111011110,\\ &0111101111011110111101111, 1011110111101111011110111,\\ &1010010100101001010010100, 0101001010010100101001010,\\ &0010100101001010010100101, 1001010010100101001010010,\\ &0100101001010010100101001, 1000110001100011000110001,\\ &1100011000110001100011000, 0110001100011000110001100,\\ &0011000110001100011000110, 0001100011000110001100011\}.\end{aligned}$$

We easily deduced that $\langle \Omega_1 \rangle$ is a 2-constant weight code as it only has two type of weight which are 10 and 20.

Now, we construct the secret sharing scheme based on a $[25, 4, 10]$-code where the secrets are shared among 24 participants. One of the 25 participants

is a trusted dealer that distributes the secrets so he is excluded. The access set corresponding to the minimal codewords are as follows:

$$\{4,5,9,10,14,15,19,20,24\},\{1,5,6,10,11,15,16,20,21\},$$
$$\{2,5,7,10,12,15,17,20,22\},\{3,5,8,10,13,15,18,20,23\}.$$

Only the participants $P_5, P_{10}, P_{15}, P_{20}$ is in all the 4 access sets. So in order to recover the secret, these four participants must be included. Each access set contains exactly 9 participants.

3.3 Binary Cyclic Codes of length 49

In this section, we construct binary cyclic codes of length 49 by using the 2-cyclotomic cosets modulo 7^2 obtained from the previous section. Recall that all 2-cyclotomic cosets modulo 49 are listed in section 2. In term of group ring $\mathbb{F}_2[\mathbb{Z}_{49}]$, we let $\Omega_1 = \sum_{s\in C_1} g^s$, $\Omega_2 = \sum_{r\in C_3} g^r$, $\Omega_3 = \sum_{t\in C_7} g^t$ and $\Omega_4 = \sum_{v\in C_{21}} g^v$. Then, we have

$$\begin{aligned}
\Omega_0 =& g^0,\\
\Omega_1 =& g^1+g^2+g^4+g^8+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+g^{22}+g^{44}+\\
& g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+g^{25},\\
\Omega_2 =& g^3+g^6+g^{12}+g^{24}+g^{48}+g^{47}+g^{45}+g^{41}+g^{33}+g^{17}+g^{34}+\\
& g^{19}+g^{38}+g^{27}+g^5+g^{10}+g^{20}+g^{40}+g^{31}+g^{13}+g^{26},\\
\Omega_3 =& g^7+g^{14}+g^{28} \text{ and } \Omega_4 = g^{21}+g^{42}+g^{35}.
\end{aligned}$$

Let $\Omega_1 = \sum_{s\in C_1} g^s \in \mathbb{F}_2[\mathbb{Z}_{49}]$. The generator polynomial for $C = \langle\Omega_1\rangle$ is computed as follows :

$$\begin{aligned}
g(x) =& gcd(g^{49}+1, \Omega_1)\\
=& 1+g+g^3+g^7+g^8+g^{10}+g^{14}+g^{15}+g^{17}+g^{21}+g^{22}+g^{24}+\\
& g^{28}+g^{29}+g^{31}+g^{35}+g^{36}+g^{38}+g^{42}+g^{43}+g^{45}.
\end{aligned}$$

From above, we see that the dimension of C is 4 and so C has the following 16 codewords.

0000000000000000000000000000000000000000000000000,
1111111111111111111111111111111111111111111111111,
1101000110100011010001101000110100011010001101000,
0110100011010001101000110100011010001101000110100,
0011010001101000110100011010001101000110100011010,
0001101000110100011010001101000110100011010001101,
1000110100011010001101000110100011010001101000110,
0100011010001101000110100011010001101000110100011,

1010001101000110100011010001101000110100011010001,
0101110010111001011100101110010111001011100101110,
0010111001011100101110010111001011100101110010111,
1001011100101110010111001011100101110010111001011,
1100101110010111001011100101110010111001011100101,
1110010111001011100101110010111001011100101110010,
0111001011100101110010111001011100101110010111001,
1011100101110010111001011100101110010111001011100.

From above, we see that the minimum distance of C is 21. Hence, we have a $[49, 4, 21]$-binary code. For the secret sharing scheme based on $[49, 4, 21]$-code, the 7 access sets are as follows:

$\{1, 3, 7, 8, 10, 14, 15, 17, 21, 22, 24, 28, 29, 31, 35, 36, 38, 42, 43, 45\}$,
$\{4, 5, 7, 11, 12, 14, 18, 19, 21, 25, 26, 28, 32, 33, 35, 39, 40, 42, 46, 47\}$,
$\{2, 6, 7, 9, 13, 14, 16, 20, 21, 23, 27, 28, 30, 34, 35, 37, 41, 42, 44, 48\}$,
$\{1, 4, 6, 7, 8, 11, 13, 14, 15, 18, 20, 21, 22, 25, 27, 28, 29, 32, 34, 35, 36, 39,$
$41, 42, 43, 46, 48\}$, $\{1, 2, 5, 7, 8, 9, 12, 14, 15, 16, 19, 21, 22, 23, 26, 28, 29,$
$30, 33, 35, 36, 37, 40, 42, 43, 44, 47\}$, $\{2, 3, 4, 7, 9, 10, 11, 14, 16, 17, 18, 21,$
$23, 24, 25, 28, 30, 31, 32, 35, 37, 38, 39, 42, 44, 45, 46\}$, $\{3, 5, 6, 7, 10, 12, 13,$
$14, 17, 19, 20, 21, 24, 26, 27, 28, 31, 33, 34, 35, 38, 40, 41, 42, 45, 47, 48\}$.

Participants $7, 14, 21, 28, 35, 42$ appears in all access sets. Hence, any group who can determine the secret must include these 6 participants. The remaining participants must be in exactly 3 access sets.

Next, we use $\langle \Omega_1 + \Omega_2 \rangle$ which is a $[49, 6, 14]$- code to construct a secret sharing scheme. As the dimension is 6, there are 64 codewords. The dealer distributes the shares of the secret among 48 participants. The 6 access sets are as follows:

$\{1, 7, 8, 14, 15, 21, 22, 28, 29, 35, 36, 42, 43\}$,
$\{2, 7, 9, 14, 16, 21, 23, 28, 30, 35, 37, 42, 44\}$,
$\{3, 7, 10, 14, 17, 21, 24, 28, 31, 35, 38, 42, 45\}$,
$\{4, 7, 11, 14, 18, 21, 25, 28, 32, 35, 39, 42, 46\}$,
$\{5, 7, 12, 14, 19, 21, 26, 28, 33, 35, 40, 42, 47\}$,
$\{6, 7, 13, 14, 20, 21, 27, 28, 34, 35, 41, 42, 48\}$.

Clearly, participants $7, 14, 21, 28, 35, 42$ appears in all access sets. Hence, any group who can determine the secret must include these 6 participants. Each participant in the set $\{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19,$

20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48} is in exactly one access set. The number of participants in each access set is 13.

For secret sharing based on $[49, 3, 28]$-code, secret are distributed as shares to 48 participants by a dealer. The minimal codeword are listed below:

$$\{0000000000000000000000000000000000000000000000000,$$
$$0111010011101001110100111010011101001110100111010,$$
$$0011101001110100111010011101001110100111010011101,$$
$$0100111010011101001110100111010011101001110100111,$$
$$1001110100111010011101001110100111010011101001110,$$
$$1010011101001110100111010011101001110100111010011,$$
$$1101001110100111010011101001110100111010011101001,$$
$$1110100111010011101001110100111010011101001110100\}$$

In the secret sharing constructed based on $[49, 3, 28]$- cyclic code, the four access sets are as follows:

$\{3, 4, 5, 7, 10, 11, 12, 14, 17, 18, 19, 21, 24, 25, 26, 28, 31, 32, 33, 35, 38, 39, 40, 42, 45, 46, 47\}$,
$\{2, 5, 6, 7, 8, 12, 13, 14, 16, 19, 20, 21, 23, 26, 27, 28, 30, 33, 34, 35, 37, 40, 41, 42, 44, 47, 48\}$,
$\{1, 3, 6, 7, 8, 10, 13, 14, 15, 17, 20, 21, 22, 24, 27, 28, 29, 31, 34, 35, 36, 38, 41, 42, 43, 45, 48\}$,
$\{1, 2, 4, 7, 8, 9, 11, 14, 15, 16, 18, 21, 22, 23, 25, 28, 29, 30, 32, 35, 36, 37, 39, 42, 43, 44, 46\}$.

Participants $7, 14, 21, 28, 35, 42$ appears in all access sets. Hence, any group who can determine the secret must include these 6 participants. Each participant in the set $\{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48\}$ is in exactly 2 access sets. In each access set, there are 27 participants. Such a secret sharing scheme can be useful in big corporate where there are a few major shareholders to make a decision.

4. Conclusions

In this paper, all 2-cyclotomic cosets modulo p^n are constructed, when 2 is a primitive root modulo p^n and when the order of 2 is $\frac{p-1}{2}$ modulo p. Also, some results on s-cyclotomic cosets modulo pq are obtained for three possible orders of s modulo p and q, respectively, for distinct odd primes p, q. Note that not much know results on 3-cyclotomic cosets modulo $2^n rs$, where r, s are distinct

primes greater than 3, and $n \geq 1$. Suppose 3 is a primitive root modulo r and is also a primitive root modulo s. Furthermore, $gcd(\phi(r), \phi(s)) = 2$. Then, by the help of computer we obtain four results; there are 9 3-cyclotomic cosets modulo $2rs$, there are 18 3-cyclotomic cosets modulo 2^2rs, there are 36 3-cyclotomic cosets modulo 2^3rs and there are 66 3-cyclotomic cosets modulo 2^4rs. Research can be continued in proving the validity of these observations. Here, we also used families of cyclotomic cosets to construct some codes of length 9, 25 and 49 with different minimum distance and dimension, and hence used these codes to define some secret sharing together with their corresponding access structures. The initial secret sharing results above are not comprehensive, further work in subsequent papers should provide a more substantiate outcome.

References

Arora, S., Batraa, S., and Cohen, S. (2002). The primitive idempotents of a cyclic group algebra. *Southeast Asian Bulletin of Mathematics*, 26:549–557.

Arora, S. and Pruthi, M. (1997). Minimal codes of prime-power length. *Finite fields and applications*, 3:99–113.

Arora, S. and Pruthi, M. (1999). Minimal cyclic codes of length $2p^n$. *Finite fields and applications*, 5:177–187.

MacWilliams, F. and Sloane, N. (1977). The theory of error-correcting codes. *North-Holland*.

Sahni, A. and Sehgal, P. T. (2012). Minimal cyclic codes of length p^nq. *Finite fields and applications*, 18:1017–1036.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423.

Sharma, A., Bakshi, G., Dumir, V., and Raka, M. (2004). Cyclotomic numbers and primitive idempotents in the ring $\mathrm{gf}(q)[x]/(x^(p^n) - 1)$. *Finite fields and applications*, 10:653–673.

Sharma, A. and G.K.Bakshi (2012). The weight distribution of some irreducible cyclic codes. *Finite fields and applications*, 18:144–159.

Singh, K. and Arora, S. (2010). The primitive idempotents in $fc_(2^n)$. *International Journal of algebra*, 4:1231–1241.

Wong, D. C. and Ang, M. (2013). Group codes define over dihedral groups of small order. *Malaysian Journal of Mathematical Sciences*, 7(s):101–116.