J. Algebra Comb. Discrete Appl.
4(3) • 261–269

Received: 21 February 2016
Accepted: 21 March 2017

Journal of Algebra Combinatorics Discrete Structures and Applications

On the equivalence of cyclic and quasi-cyclic codes over finite fields

Research Article

Kenza Guenda, T. Aaron Gulliver

Abstract: This paper studies the equivalence problem for cyclic codes of length p^r and quasi-cyclic codes of length $p^r l$. In particular, we generalize the results of Huffman, Job, and Pless (J. Combin. Theory. A, 62, 183–215, 1993), who considered the special case p^2. This is achieved by explicitly giving the permutations by which two cyclic codes of prime power length are equivalent. This allows us to obtain an algorithm which solves the problem of equivalency for cyclic codes of length p^r in polynomial time. Further, we characterize the set by which two quasi-cyclic codes of length $p^r l$ can be equivalent, and prove that the affine group is one of its subsets.

2010 MSC: 94B05, 94B15, 94B60

Keywords: Cyclic code, Quasi-cyclic code, Equivalence, Automorphism, Permutation

1. Introduction

The equivalence problem for codes has many practical applications such as code-based cryptography [8, 9, 12, 13]. As a consequence, this problem has received considerable attention in the literature [2, 3, 6, 11, 12]. However, progress in obtaining results has been slow. Brand ([3]) characterized the set of permutations by which two combinatorial cyclic objects on p^r elements are equivalent. Using these results, Huffman et al. ([6]) explicitly gave this set for the case p^2, and constructed algorithms to find the equivalence between cyclic objects and extended cyclic objects. In [6], a negative answer was given to the generalization of their results to the case p^r, $r > 2$. This is due to the fact that the permutations of Brand that are crucial to the proofs do not generate a Sylow subgroup of S_{p^r}. Babai et al. ([2]) gave an exponential time algorithm for determining the equivalence of codes. Sendrier ([11]) proposed the support splitting algorithm to solve the problem of code equivalence in the binary case. However, in [12]

Kenza Guenda (Corresponding Author); Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algeria (email: ken.guenda@gmail.com).
T. Aaron Gulliver; Department of Electrical and Computer Engineering, University of Victoria, PO Box 1700, STN CSC, Victoria, BC, Canada V8W 2Y2 (email: agullive@ece.uvic.ca).

http://dx.doi.org/10.13069/jacodesmath.327375

ISSN 2148-838X

the authors showed that extending the support splitting algorithm to $q \geq 5$ results in an exponential growth in complexity, which makes this approach impractical.

In this paper, we study the equivalence problem for cyclic codes of length p^r and quasi-cyclic codes of length $p^r l$ over finite fields. We generalize the results of [6] (which are only for the special case p^2), by explicitly giving the permutations by which two cyclic codes of prime power length are equivalent. Further, the set of Brand is extended to the class of quasi-cyclic codes of length $p^r l$.

The remainder of this paper is organized as follows. In Section 2, some preliminary results are presented. Section 3 considers the equivalence of cyclic codes, in particular cyclic codes of length p^r. Then in Section 4, the equivalence of quasi-cyclic codes of length $p^r l$ is investigated.

2. Preliminaries

Let C be a linear code of length n over the finite field of q elements, $\mathbb{F}_q$, and σ a permutation of the symmetric group S_n, acting on $\{0, 1, \ldots, n-1\}$. For a code C, we associate another linear code $\sigma(C)$ defined by

$$\sigma(C) = \{(x_{\sigma^{-1}(0)}, \ldots, x_{\sigma^{-1}(n-1)})\,;(x_0, \ldots x_{n-1}) \in C\}.$$

We say that the codes C and C' are permutation equivalent if there exists a permutation $\sigma \in S_n$ such that $C' = \sigma(C)$. The automorphism group of C is the subgroup of S_n given by

$$Aut(C) = \{\sigma \in S_n\,; \sigma(C) = C\}.$$

A linear code C of length n over $\mathbb{F}_q$ is called quasi-cyclic of index l or an l-quasi-cyclic code if its automorphism group contains the permutation T^l given by

$$\begin{aligned} T^l : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ i &\longmapsto i + l \bmod n, \end{aligned} \tag{1}$$

where $T : i \mapsto i + 1$ is the cyclic shift. This definition is equivalent to saying that for all $c \in C$ we have $T^l(c) \in C$. The index l of C is the smallest integer satisfying this property. It can easily be proven that l is a divisor of n. In the case $l = 1$, the code is called a cyclic code. This is a code with an automorphism group that contains the cyclic shift T.

3. Equivalence of cyclic codes

In this section, we consider the permutation equivalence of cyclic codes. Later we will show that there is a very close link between the equivalence of some quasi-cyclic codes and cyclic codes. This provides further motivation to study the equivalence of cyclic codes.

We begin with some well known results. Let n be a positive integer. The set of permutations $AG(n) = \{\tau_{a,b} : a \neq 0, (a, n) = 1, b \in \mathbb{Z}_n\}$ is the subgroup of S_n formed by the permutations defined as follows

$$\begin{aligned} \tau_{a,b} : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ x &\longmapsto (ax + b) \bmod n. \end{aligned} \tag{2}$$

The group $AG(n)$ is called the group of affine transformations. The affine transformations

$$M_a = \tau_{a,0}, \tag{3}$$

are called multipliers. The affine group $AGL(1, p)$ is the group of affine transformations over $\mathbb{Z}_p$.

For $d \in \mathbb{Z}_p^*$, the generalized multiplier $\mu_d \in S_{p^2}$ was defined in [6] as follows. Let $k \in \mathbb{Z}_{p^2}$ and $k = i + jp$ for some $0 \leq i, j \leq p-1$, so that $k\mu_d = (id) \bmod p + pj$. Then from Palfy ([10]) and Alspach and Parson ([1]), we have the following results.

Theorem 3.1. [6, Theorem 1] *Let C and C' be cyclic codes of length n over a finite field. Suppose one of the following holds for n:*

(i) $gcd(n, \phi(n)) = 1$ or $n = 4$, or

(ii) $n = pr, p > r$ are primes and the p-Sylow subgroup of the automorphism group of C has order p.

Then C and C' are equivalent by a multiplier.

In the case $n = p^2$, Huffman et al. ([6]) gave the following result.

Theorem 3.2. [6, Theorem 3.1] *Let C and C' be cyclic codes of length p^2 with p an odd prime, where $T \in Aut(C)$ and $T \in Aut(C')$. Then if C and C' are equivalent, they are equivalent by a multiplier or a generalized multiplier times a multiplier.*

For $n = p^r$, $r > 2$ the equivalence of cyclic codes of length n is very complex, but in the next section this problem is partially solved.

3.1. Equivalence of cyclic codes of length p^r

Let C be a cyclic code of length p^r, p an odd prime and $r > 1$. Further let T be the cyclic shift modulo p^r and P a p-Sylow subgroup of $Aut(C)$. The following subset of S_{p^r} was introduced by Brand ([3])

$$H(P) = \{\sigma \in S_{p^r} | \sigma^{-1} T \sigma \in P\}.$$

The set $H(P)$ is well defined since $\langle T \rangle$ is a subgroup of $Aut(C)$ of order p^r, so it is a p-group of $Aut(C)$. From Sylow's Theorem, there exists a p-Sylow subgroup P of $Aut(C)$ such that $\langle T \rangle \leq P$. Furthermore, in some cases the set $H(P)$ is a group.

Lemma 3.3. [3, Lemma 3.1] *Let C and C' be cyclic codes of length p^r, and P be a p-Sylow subgroup of $Aut(C)$ which contains T. Then C and C' are equivalent if and only if C and C' are equivalent by an element of $H(P)$.*

Lemma 3.3 shows the importance of having information on the p-Sylow subgroup of $Aut(C)$. The following results provide some of this information.

Proposition 3.4. [4, Proposition 9] *Let C be a cyclic code of length p^r with $r > 1$, and M_q be the multiplier defined by $M_q(i) = iq \bmod p^r$. Then the group $Aut(C)$ contains the subgroup $K = \langle T, M_q \rangle$ of order $p^r ord_{p^r}(q)$. Let p^l, $l \geq r$, be the p-part of the order of K. Then a p-Sylow subgroup P of $Aut(C)$ has order p^s such that*

$$l \leq s \leq p^{r-1} + p^{r-2} + \cdots + 1.$$

Now we define the sets of Brand. Let p be an odd prime. For $n < p$, we define the following subsets of S_{p^r}

$$Q^n = \{f : \mathbb{Z}_{p^r} \to \mathbb{Z}_{p^r} | f(x) = \sum_{i=0}^{n} a_i x^i, a_i \in \mathbb{Z}_{p^r} \text{ for each } i, (p, a_1) = 1,$$
$$\text{and } p^{r-1} \text{ divides } a_i \text{ for } i = 2, 3, \ldots, n\}.$$

$$Q_1^n = \{f \in Q^n | f(x) = \sum_{i=0}^{n} a_i x^i, \text{ with } a_1 \equiv 1 \bmod p^{r-1}\}.$$

The sets Q^n and Q_1^n are subgroups of S_{p^r} [3, Lemma 2.1]. Note that $Q^1 = AG(p^r)$.

Lemma 3.5. *Let C be a cyclic code of length p^r where p is odd and $m > 1$. Let P be a p-Sylow subgroup of $Aut(C)$ which contains T. If $1 \leq n < p$, then:*

(i) $|Q^n| = (p-1)p^{2r+n-2}$ *and* $|Q_1^n| = p^{r+n}$,

(ii) $AG(p^r) = N_{S_{p^r}}(\langle T \rangle) \subset H(P)$,

(iii) $Q^{n+1} = H(Q_1^n)$,

(iv) $N_{S_{p^r}}(Q_1^n) = Q^{n+1}$.

Proof. For part (i), from [3, Lemma 3.2] we have the map $(a_0, \dots, a_n) \longrightarrow f$ where $f(x) = \sum_{i=0}^{n} a_i x^i$ is injective if $n < p-1$. Thus in Q^n, the coefficient a_0 can take p^r different values, and a_1 can take $p^{r-1}(p-1)$ values. For $2 \leq i \leq n$, a_i can take p values. From these results we have $|Q^n| = p^{2r+n-2}(p-1)$. For Q_1^n, the coefficient of a_0 can take p^r different values, and a_i for $1 \leq i \leq n$ can take p values, so that $|Q_1^n| = p^{r+n}$.

Now we prove that $AG(p^r) = N_{S_{p^r}}(\langle T \rangle)$. Let σ be an element of $N_{S_{p^r}}(\langle T \rangle)$. Then there is a $j \in \mathbb{Z}_n \setminus \{0\}$ such that $\sigma T \sigma^{-1} = T^j$, or equivalently $\sigma T = T^j \sigma$. Hence $\sigma T(0) = \sigma(1) = T^j \sigma(0) = \sigma(0) + j$ and $\sigma T(1) = \sigma(1) + j = \sigma(0) + 2j$, so that $\sigma(k) = \sigma(0) + kj$ for any $k \in \mathbb{Z}_n$. Then $(j, n) = 1$ follows from the fact that the order of T equals the order of T^j. The last inclusion is obvious.

Part (iii) follows from [3, Lemma 3.7].

For part (iv), we begin with the $\leq$ condition. Let $h \in N_{S_{p^r}}(Q_1^n)$ and $g = h^{-1}Th$. As $T \in Q_1^n$, it must be that $g \in Q_1^n$. Since the order of g is equal to the order of T (which is p^r), from [3, Lemma 3.6] there exists $f \in Q^{n+1}$ such that $f^{-1}gf = T$, so then $f^{-1}h^{-1}Thf = T$. The only elements of S_{p^r} which commute with T (a complete cycle of length p^r), are the powers of T. Thus $hf = T^j$ for some j. Since Q^{n+1} is a subgroup of S_{p^r} and $\langle T \rangle \leq Q^{n+1}$, $h \in Q^{n+1}$, and hence $N_{S_{p^r}}(Q_1^n) \leq Q^{n+1}$.

Now consider the $\geq$ condition. Let $g \in Q^{n+1}$ where $g(x) = \sum_{i=0}^{n+1} g_i x^i$ with $p \nmid g_1$ and $p^{r-1} | g_i$ for $2 \leq i \leq n$. Further, let $h \in Q_1^n$, where $h(x) = \sum_{i=0}^{n} h_i x^i$ with $h_1 \equiv 1 \bmod p^{r-1}$ and $p^{r-1} | h_i$ for $2 \leq i \leq n$. We have

$$hg(x) = \sum_{i=0}^{n} h_i \left(\sum_{j=0}^{n+1} g_j x^j \right)^i = h_0 + h_1 \sum_{i=0}^{n+1} g_j x^j + \sum_{i=2}^{n} h_i \left(\sum_{j=0}^{n+1} g_j x^j \right)^i.$$

Since $p^{r-1} | h_i$, for $i \geq 2$ and $p^{r-1} | g_j$ for $j \geq 2$, any terms in $\sum_{i=2}^{n} h_i \left(\sum_{j=0}^{n+1} g_j x^j \right)^i$ involving g_j for $j \geq 2$ vanish modulo p^r, so that

$$hg(x) = h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^{n} h_i \left(g_0 + g_1 x \right)^i.$$

By [3, Lemma 2.1]

$$g^{-1}(x) = \sum_{i=1}^{n+1} b_i x^i, \text{ with } b_1 = g_1^{-1} \text{ and } b_i = -g_i g_1^{-(i+1)} \text{ for } 2 \leq j \leq n+1. \tag{4}$$

We now determine $g^{-1}hg$ in order to prove that it is in Q_1^n. This is given by

$$g^{-1}hg(x) = \sum_{k=1}^{n+1} b_k \left(h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^{n} h_i (g_0 + g_1 x)^i - g_0 \right)^k$$

$$= b_1 \left(h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^{n} h_i \left(g_0 + g_1 x\right)^i - g_0 \right)$$

$$+ \sum_{k=2}^{n+1} b_k \left(h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^{n} h_i (g_0 + g_1 x)^i - g_0 \right)^k .$$

As $p^{r-1}|g_j$ for $j \geq 2$, hence $p^{r-1}|b_k$ for $k \geq 2$. Furthermore, we have $p^{r-1}|h_i$ for $i \geq 2$, and thus

$$g^{-1}hg(x) = b_1 \left(h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{j=0}^{n+1} h_i (g_0 + g_1 x)^i - g_0 \right) + \sum_{k=2}^{n+1} b_k \left(h_0 + h_1 \left(g_0 + g_1 x\right) - g_0\right)^k .$$

Let $g^{-1}hg(x) = \sum_{r=0}^{n+1} c_r x^r$, and note that $c_{n+1} = b_1 h_1 g_{n+1} + b_{n+1}(h_1 g_1)n + 1$. Then replacing the b_i with their values from (4), we obtain

$$c_{n+1} = g_1^{-1} h_1 g_{n+1} - g_{n+1} g_1^{-(n+2)} h_1^{n+1} g_1^{n+1} = g_1^{-1} h_1 (g_{n+1} - g_{n+1} h_1^n).$$

As $h_1 \equiv 1 \bmod p^{r-1}$, we have that $h_1^n \equiv 1 \bmod p^{r-1}$. In addition, as $p^{r-1}|g_{n+1}$, it must be that $g_{n+1}h_1^n \equiv g_{n+1} \bmod p^r$. Therefore, $c_{n+1} = 0$, and $p^{r-1}|c_i$ for $2 \leq i \leq n$. Then we only need to show that $c_1 \equiv 1 \bmod p^{r-1}$. As $g_j \equiv 0 \bmod p^{r-1}$ for $j \geq 2$, $h_i \equiv 0 \bmod p^{r-1}$ for $i \geq 2$, and $b_k \equiv 0 \bmod p^{r-1}$ for $k \geq 2$, so then $c_1 \equiv b_1 h_1 g_1 \bmod p^{r-1}$. Finally, since $b_1 = g_1^{-1}$, we have that $c_1 \equiv h_1 \equiv 1 \bmod p^{r-1}$. □

Next, we require the following theorems which characterize some p subgroups of S_{p^r}.

Theorem 3.6. [4, Theorem 10] *Let n be a positive integer less than $p-1$. If P is a p subgroup of S_{p^r} with $Q_1^n \lneq P \leq Q^{n+1}$, then $P = Q_1^{n+1}$. Further, the group Q_1^1 is a normal subgroup of Q^1 and is the unique p subgroup of S_{p^r} of order p^{r+1} which contains T.*

Theorem 3.7. [4, Theorem 11] *Let G be a subgroup of S_{p^r} and P a p-Sylow subgroup of G of order p^s such that $T \in P$. Then the following hold:*

(i) if $s = r$, then $P = \langle T \rangle$,

(ii) if $r < s \leq p + r - 1$, then we have $P = Q_1^{s-r}$.

Corollary 3.8. *Let C and C' be two cyclic codes of length p^r, and let P be a p-Sylow subgroup of $Aut(C)$ such that $T \in P$. If $|P| = p^s$ and $s \leq p + r - 1$, then C and C' can be equivalent only under the action of a permutation of the following subgroups of S_{p^r}:*

(i) $AG(p^r)$ if $s = r$,

(ii) Q^{s-r+1} if $s > r$.

Proof. The result follows from Lemmas 3.3 and 3.5, and Theorem 3.7. □

Remark 3.9. *Since each affine transformation can be written as the product of a power of T and a multiplier, and $T \in Aut(C)$, we must have $\tau_{a,b} \in C$ whenever $M_a \in C$. Hence from Corollary 3.8, if $s = r$ then two cyclic codes of length p^r are equivalent if and only if they are equivalent by a multiplier.*

In order to solve the equivalence problem for cyclic codes, we need the p-Sylow subgroup of $Aut(C)$. To determine this, for $i \leq i \leq p-1$ consider the polynomial $f_i \in Q_1^i$ defined by

$$f_i(x) = x + p^{r-1}(x + x^2 + \ldots + x^i).$$

Theorem 3.10. *Let G be a subgroup of S_{p^r} with a p-Sylow subgroup P which contains T. Then the following hold:*

(i) if there is no $f_i \in G$, then $P = \langle T \rangle$,

(ii) if I is the largest value of i such that $f_i \in G$ and $I \leq p-2$, then $P = Q_1^I$.

Proof. If there is no $f_i \in G$, then there is no f_i in P. If $|P| = p^r$, we can take $P = \langle T \rangle$, but then from Theorem 3.6 any p-Sylow subgroup of p^s, $s > r$, must contain Q_1^1, which is impossible. Assume that I is the largest i such that $f_i \in G$ and $I \leq p-2$. Let P be a p-Sylow subgroup of G of order s, and s be such that $I + r \leq s < p + r - 1$. From Theorem 3.7, we have that a p-Sylow subgroup of any subgroup of $G \leq S_{p^r}$ which contains T has order p^s with $m < s \leq p + r - 1$. Then we have $P = Q_1^{s-r}$, so that $s - r = I$. Now if $s \leq I + r \leq p + r - 1$, we have from Theorem 3.7 that $P = Q_1^{s-r}$, so $Q_1^I \cap G \leq Q_1^{s-r}$. The assumption on I gives $I = s - r$.

Assume now that $s > p + r - 1$. Since $I \leq p - 2$, we have that $s > p + r - 1 > r + I$. We will prove that this case cannot occur. Further, as $T = f_1 \in Q_1^1$, from Theorem 3.6 Q_1^1 is the unique subgroup of S_{p^r} of order p^{r+1} which contains T, so that $Q_1^1 \lneq P$. Since $Q_1^1 \lneq Q_1^2$, it must be that $Q_1^1 \lneq Q_1^2 \cap P \leq Q^2$. Hence we have that $Q_1^2 \cap P = Q_1^2$, which gives $Q_1^2 \leq P$. Using the same approach for $2 \leq i \leq I$, we obtain $Q_I \leq P$. The assumption on s gives that $Q_I \lneq P$, so $Q_1^I \lneq Q_1^{I+1} \cap P \leq Q^{I+1}$ (Q^{I+1} can be considered as it was assumed that $I \leq p - 2$). Hence from Theorem 3.6, we obtain that $Q_1^{I+1} \cap P = Q_1^{I+1}$, which contradicts the assumption on I. □

This theorem suggests the following algorithm for $I \leq p - 2$.

Algorithm A: Let p be an odd prime and C and C' be two cyclic codes of length p^m. Then the equivalence of C and C' can be determined as follows.

Step 1: Find the order of the p-Sylow subgroup of $Aut(C)$ as follows. Find the largest I such that $f_I \in Aut(C)$, and set $s = I + r$.
Step 2: Find $f \in Q^{I+1}$ such that $C' = fC$.

Remark 3.11. *To find the required I in Algorithm A we can use (for example), a binary search which requires checking at most $\lceil \log_2(p-1) \rceil + 1$ of the f_i. Furthermore, the cardinality of Q^{I+1} is $(p-1)p^{2r+I-2}$. This proves that the algorithm has polynomial time complexity.*

4. Equivalence of quasi-cyclic codes

In this section, we characterize the equivalence problem for quasi-cyclic codes. Consider the cycles $\sigma_i = (i, i + l, i + 2l, \ldots, i + (m-1)l)$ for $0 \leq i \leq l - 1$. The cycles σ_i have order m and satisfy

$$T^l = \sigma_0 \ldots \sigma_{l-1}. \tag{5}$$

This gives that $|(T^l)| = \mathrm{lcm}(|\sigma_0|, \ldots, |\sigma_{l-1}|) = m$.

Proposition 4.1. *Let $n = lm$ with $(m, l) = 1$, and $\langle T^l \rangle$ be the subgroup of S_n generated by the permutation T^l. Therefore the normalizer of $\langle T^l \rangle$ in S_n contains the following groups:*

(i) $Q = \langle \sigma_0, \ldots, \sigma_{l-1}, T \rangle$,

(ii) $AG(n)$.

Proof. It is obvious that $T \in N_{S_n}(\langle T^l \rangle)$. As the cycles in (5) are pairwise disjoint, it must be that $\sigma_0 \ldots \sigma_{l-1} = T^l$. Furthermore, as the cycles σ_i are disjoint, we have that $\sigma_i^{-1} T^l \sigma_i = T^l$.

We consider the affine transformation $\tau_{a,b} \in AG(n)$, which shows that $\tau_{a,b} \in N_{S_n}(\langle T^l \rangle)$ is equivalent to proving the existence of an $\alpha \in \mathbb{N}^*$ such that

$$\tau_{a,b} T^l \tau_{a,b}^{-1} = T^{l\alpha}.$$

The permutation $\tau_{a,b}$ can be decomposed as $\tau_{a,b} = \tau_{1,b}\tau_{a,0}$. Then combining this decomposition with (5), we obtain the following equality

$$\tau_{a,b} T^l \tau_{a,b}^{-1} = \tau_{1,b}\tau_{a,0}\sigma_0 \dots \sigma_{l-1}\tau_{a,0}^{-1}\tau_{1,b}^{-1}. \tag{6}$$

A well known result [5, Lemma 5.1] gives that if $\sigma = \sigma_0 \dots \sigma_{l-1}$ is a product of disjoint cycles and S is a permutation from S_n, then $S\sigma S^{-1} = S(\sigma_0)S(\sigma_1)\dots S(\sigma_{l-1})$, where $S(\sigma_i) = (S(\sigma_{1i}), \dots, S(\sigma_{mi}))$ for the cycle $\sigma_i = (\sigma_{1i}, \dots, \sigma_{mi})$. For $r_a = a \bmod l$, we obtain that $\tau_{a,0}(\sigma_i) = \sigma_{ir_a}^a$. This gives

$$\tau_{a,0}(\sigma_0)\tau_{a,0}(\sigma_1)\dots\tau_{a,0}(\sigma_{l-1}) = \sigma_0^a \sigma_{ra}^a \dots \sigma_{ra(l-1)}^a = T^{la}.$$

For $r_b = b \bmod l$, we obtain

$$\tau_{1,b}\sigma_i\tau_{1,b}^{-1} = \tau_{i+r_b},$$

and hence

$$\tau_{1,b}T^l\tau_{1,b}^{-1} = \prod_{i=0}^{l-1}\sigma_{i+r_b} = T^l.$$

Finally, we obtain

$$\tau_{a,b}T^l\tau_{a,b}^{-1} = \tau_{1,b}\tau_{a,0}T^l\tau_{a,0}^{-1}\tau_{1,b}^{-1} = \tau_{1,b}T^{la}\tau_{1,b}^{-1} = T^{la}.$$

This gives $\alpha = a$, so that $\tau_{a,b} \in N_{S_n}(< T^l >)$. □

4.1. Quasi-cyclic codes of length $p^r l$

We now consider quasi-cyclic codes of length $n = p^r l$ with p a prime number such that $(p, l) = (p, q) = 1$. In this case, $\langle T^l \rangle \leq Aut(C)$ is a subgroup of order p^r. Hence it is contained in a p-Sylow subgroup P.

Lemma 4.2. *Let C and C' be two quasi-cyclic codes of length $n = p^r l$, and P be a p-Sylow subgroup of $Aut(C)$ such that $T^l \in P$. Then C and C' are equivalent only if they are equivalent by the elements of the set*

$$H'(P) = \{\sigma \in S_n | \sigma^{-1}T^l\sigma \in P\}.$$

Proof. Since C and C' are equivalent, there exists a permutation $\sigma \in S_n$ such that $C' = \sigma(C)$. This gives the following relationship between the automorphism groups $Aut(C)$ and $Aut(C')$

$$Aut(C') = \sigma Aut(C)\sigma^{-1}. \tag{7}$$

Let P be a Sylow subgroup of $Aut(C)$. Then from (7) we have that $\sigma P \sigma^{-1} = P''$ is a Sylow p-subgroup of $Aut(C')$. From Sylow's Theorem, there exists $\tau \in Aut(C')$ such that $\tau P' \tau^{-1} = P''$. We can assume that $\langle T^l \rangle \leq P'$ since $\langle T^l \rangle$ is a p-group. Let $\gamma = \tau^{-1}\sigma$, then γ is an isomorphism between C and C' because $\gamma(C) = \tau^{-1}\sigma(C) = \tau^{-1}C' = C'$. Then $\gamma^{-1}T^l\gamma = \sigma^{-1}\tau T^l \tau^{-1}\sigma \in \sigma^{-1}P''\sigma = P$ as $\tau T^l \tau^{-1} \in \tau P' \tau^{-1}$, and hence $\gamma \in H'(P)$. □

It is obvious that if $P = \langle T^l \rangle$, then we have

$$N_{S_n}(\langle T^l \rangle) = H'(\langle T^l \rangle).$$

The following proposition gives other properties of $H'(P)$.

Proposition 4.3. *Let P be a Sylow p-subgroup of $Aut(C)$. Then the group $H'(P)$ has the following properties:*

(i) if $P = \langle T^l \rangle$, then $N_{S_n}(\langle T^l \rangle) = H'(\langle T^l \rangle)$,

(ii) $N_{S_n}(\langle T^l \rangle) \subset H'(P)$,

(iii) $N_{S_n}(P) \subset H'(P)$.

Proof. The first property is obtained from the definition of $H'(P)$. To prove the second property we consider a permutation σ in $N_{S_n}(\langle T^l \rangle)$, the normalizer of $\langle T^l \rangle$ in S_n. Then permutation σ satisfies $\sigma^{-1}\langle T^l \rangle \sigma = \langle T^l \rangle \subset P$. Hence, we have that

$$N_{S_n}(\langle T^l \rangle) \subset H'(P). \tag{8}$$

Now consider $N_{S_n}(P)$, the normalizer of P in S_n. The permutation $\sigma \in N_{S_n}(P)$ shows that $\sigma^{-1}P\sigma = P$. Thus for $T^l \in P$ we have $\sigma^{-1}T^l\sigma \in P$, so that

$$N_{S_n}(P) \subset H'(P). \tag{9}$$

□

Corollary 4.4. *The set $H'(P)$ satisfies $AG(n) \subset H'(P)$.*

Proof. From Proposition 4.1 we have $AG(n) \leq N_{S_n}(\langle T^l \rangle)$. Furthermore, Proposition 4.3 gives that $N_{S_n}(\langle T^l \rangle) \subset H'(P)$, which completes the proof. □

From Corollary 4.4, we have $AG(n) \subset H'(P)$. As the multipliers are elements of $AG(n)$, this proves that two quasi-cyclic codes of length n can be equivalent by a multiplier. This extends the results on 1-generator quasi-cyclic codes in [7].

References

[1] B. Alspach, T. D. Parson, Isomorphism of circulant graphs and digraphs, Discrete Math. 25(2) (1979) 97–108.

[2] L. Babai, P. Codenotti, J. A. Groshow, Y. Qiao, Code equivalence and group isomorphism, in Proc. ACM-SIAM Symp. on Discr. Algorithms, San Francisco, CA, (2011) 1395–1408.

[3] N. Brand, Polynomial isomorphisms of combinatorial objects, Graphs Combin. 7(1) (1991) 7–14.

[4] K. Guenda, T. A. Gulliver, On the permutation groups of cyclic codes, J. Algebraic Combin. 38(1) (2013) 197–208.

[5] M. Hall, Jr., The Theory of Groups, MacMillan, New York, 1970.

[6] W. C. Huffman, V. Job, V. Pless, Multipliers and generalized multipliers of cyclic objects and cyclic codes, J. Combin. Theory Ser. A 62(2) (1993) 183–215.

[7] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes III: Generator theory, IEEE Trans. Inform. Theory 51(7) (2005) 2692–2700.

[8] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, DSN Progress Report 42-44, (1978) 114–116.

[9] A. Otmani, J.–P. Tillich, L. Dallot, Cryptanalysis of a McEliece cryptosystem based on quasi-cyclic LDPC codes, in Proc. Conf. on Symbolic Computation and Crypt., Beijing, China, (2008) 69–81.

[10] P. P. Palfy, Isomorphism problem for relational structures with a cyclic automorphism, European J. Combin. 8(1) (1987) 35–43.

[11] N. Sendrier, Finding the permutation between equivalent linear codes: The support splitting algorithm, IEEE Trans. Inform. Theory 46(4) (2000) 1193–1203.

[12] N. Sendrier, D.E. Simos, How easy is code equivalence over $\mathbb{F}_q$?, in Proc. Int. Workshop on Coding Theory and Crypt., Bergen, Norway, 2013.

[13] N. Sendrier, D. E. Simos, The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography, in P. Gaborit (Ed.), Post-Quantum Cryptography, Springer Lecture Notes in Computer Science 7932, Limoges, France (2013) 203–216.