J Algebr Comb (2013) 38:197–208
DOI 10.1007/s10801-012-0399-4

On the permutation groups of cyclic codes

Kenza Guenda · T. Aaron Gulliver

Received: 20 November 2011 / Accepted: 11 September 2012 / Published online: 3 October 2012

Abstract We classify the permutation groups of cyclic codes over a finite field. As a special case, we find the permutation groups of non-primitive BCH codes of prime length. In addition, the Sylow p-subgroup of the permutation group is given for many cyclic codes of length p^m. Several examples are given to illustrate the results.

Keywords Permutation groups · Transitive groups · Doubly transitive groups · Non-primitive BCH codes

1 Introduction

The permutation groups of cyclic codes are of great theoretical and practical interest, e.g. the permutation group can be used to find the weight distribution of a code [19], and in decoding [16, 19]. They can also be used for cryptographic purposes such as the McEliece cryptosystem and its variants [20]. Despite the significance of this problem, the permutation groups of cyclic codes are known for only a few subclasses such as the Reed–Solomon codes, Reed–Muller codes and some BCH codes [3, 18]. The other cases remain open. Recently, Bienert and Klopsch [4] studied the permutation groups of cyclic codes in the binary case. They gave the primitive groups which can be the permutation group of a binary cyclic code. Dobson and Witte [13, 14] considered the cyclic codes invariant under some transitive groups. Furthermore in some cases they gave the Sylow p-subgroups of some transitive subgroups of S_{p^2} and S_{p^m}.

K. Guenda
Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algiers, Algeria

T. Aaron Gulliver (✉)
Department of Electrical and Computer Engineering, University of Victoria, PO Box 3055, STN CSC, Victoria, BC, V8W 3P6, Canada
e-mail: agullive@ece.uvic.ca

In this paper we classify the permutation groups of cyclic codes. First we generalize the results of [4] concerning the doubly transitive permutation groups with socle $PSL(d,q)$ to the non-binary case. Then we use the classification of the doubly transitive groups which contain a complete cycle, given by McSorley [21, 22], and our previous results to determine the permutation groups in the doubly transitive cases. This allows us to determine the permutation groups of the BCH codes in the prime length case. Further, we give conditions on the primitivity of the permutation groups which are based on the underlying field and the length of the code. For many cyclic codes, we explicitly give the Sylow p-subgroups of the permutation groups in the primitive and imprimitive cases. This is done using some subgroups of S_{p^m} introduced by Brand [5]. Several examples are given to illustrate the results.

2 Preliminaries

Let $\mathbb{F}_q$ be a finite field. A linear code C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. A vector $x = (x_0, \ldots, x_{n-1}) \in C$ is said to be a codeword of C. Let I denote the set $\{0, 1, \ldots, n-1\}$, and let S_n be the symmetric group acting on I. Then S_n acts naturally on a codeword of C as follows. If σ is a permutation of S_n, then

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

The permutation group of C is the subgroup of S_n given by

$$Per(C) = \{\sigma \in S_n \mid \sigma(C) = C\}.$$

A linear code C over $\mathbb{F}_q$ is cyclic if $T \in Per(C)$, where $T = (0, 1, \ldots, n-1)$ is a complete cycle of length n. If C is cyclic then $Per(C)$ is a transitive group. The group $AG(n) = \{\tau_{a,b} : a \neq 0, (a,n) = 1, b \in \mathbb{Z}_n\}$ is the subgroup of S_n formed by the permutation defined as follows:

$$\begin{aligned} \tau_{a,b} : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ x &\longmapsto (ax + b) \mod n. \end{aligned} \tag{1}$$

The group $AG(n)$ is called the group of affine transformations. The affine transformations $M_a = \tau_{a,0}$ are called a multiplier. The affine group $AGL(1,p)$ is the group of affine transformations over $\mathbb{Z}_p$. The projective semi-linear group $P\Gamma L(d,t)$ is the semi-direct product of the projective linear group $PGL(d,t)$ and the automorphism group $Z = Gal(\mathbb{F}_t/\mathbb{F}_p)$ of $\mathbb{F}_t$, where $t = p^s$, p prime, i.e.

$$P\Gamma L(d,t) = PGL(d,t) \rtimes Z.$$

Remark 1 The zero code, the entire space, and the repetition code and its dual are called elementary codes. The permutation group of these codes is S_n [16, p. 1410]. Further, it was proven in [16, p. 1410] that there is no cyclic code with permutation group equal to $Alt(n)$.

3 The permutation groups of cyclic codes

A doubly transitive group G has a unique minimal normal subgroup N which is either regular and elementary abelian, or simple and primitive, and the centralizer of N in G is equal to $C_G(N) = 1$ [8, p. 202]. All simple groups which can occur as a minimal normal subgroup of a doubly transitive group are known. This result is due to the classification of finite simple groups [9]. Using this classification, McSorley [21] gave the following result.

Lemma 1 *A group G of degree n which is doubly transitive and contains a complete cycle has socle N with $N \leq G \leq Aut(N)$, and is equal to one of the cases in Table 1.*

The arguments given in the following Lemma are similar to those for the binary case [4, Theorem E, Part 3].

Lemma 2 *Let C be a non-elementary cyclic code of length $n = \frac{t^d-1}{t-1}$ over a finite field $\mathbb{F}_q$, where $q = r^\alpha$ and t is a prime power. If the group $Per(C)$ satisfies*

$$PGL(d,t) \leq Per(C) \leq P\Gamma L(d,t),$$

then $t = r^a$ for some $a \geq 1$, $d \geq 3$, and $Per(C) = P\Gamma L(d,t)$.

Proof Assume $d = 2$. As the group $PGL(2,t)$ acts 3-transitively on the 1-dimensional projective space $\mathbb{P}^1(\mathbb{F}_t)$, we deduce from [22, Table 1 and Lemma 2], that the underlying code is elementary, which is a contradiction. Hence $d \geq 3$, and from [22, Table 1 and Lemma 2], it must be that since C is non-elementary, t must be equal to r^a. Now let V denote the permutation module over $\mathbb{F}_r$ associated with the natural action of $PGL(d,t)$ on the $(d-1)$-dimensional projective space $\mathbb{P}^{d-1}(\mathbb{F}_t)$. Let U_1 be a $PGL(d,t)$-submodule of V. Then U_1 is $P\Gamma L(d,t)$-invariant. This is because, if σ is a generator of the cyclic group $P\Gamma L(d,t)/PGL(d,t) \simeq Gal(\mathbb{F}_t/\mathbb{F}_r)$, then $U_2 = U_1^\sigma$, regarded as a $PGL(d,t)$-module, is simply a twist of U_1. Let $\overline{\mathbb{F}}_r$

Table 1 The doubly transitive groups that contain a complete cycle

G	n	N
$AGL(1,p)$	p	C_p
S_4	4	$C_2 \times C_2$
$S_n, n \geq 5$	n	$Alt(n)$
$Alt(n), n$ odd and ≥ 5	n	$Alt(n)$
$PGL(d,t) \leq G \leq P\Gamma L(d,t)$ $(d,t) \neq (2,2),(2,3),(2,4)$	$\frac{t^d-1}{t-1}$	$PSL(d,t)$
$PSL(2,11)$	11	$PSL(2,11)$
M_{11}(Mathieu)	11	M_{11}(Mathieu)
M_{23}(Mathieu)	23	M_{23}(Mathieu)

be the algebraic closure of $\mathbb{F}_r$. Then the composition factors of the $\overline{\mathbb{F}}_r PGL(d,t)$-modules $\overline{U}_1 = \overline{\mathbb{F}}_r \otimes U_1$ and $\overline{U}_2 = \overline{\mathbb{F}}_r \otimes U_2$ are the same. The submodules of the $\overline{\mathbb{F}}_r PGL(d,t)$-module $\overline{V} = \overline{\mathbb{F}}_r \otimes V$ are uniquely determined by their composition factors [1]. Then we have $\overline{U}_1 = \overline{U}_2$, which implies that $U_1 = U_2$, and therefore $Per(C) = P\Gamma L(d,t)$. □

The following theorem establishes the permutation group of a non-elementary cyclic code of prime length over $\mathbb{F}_q$, where $q = r^\alpha$.

Theorem 3 *Let C be a non-elementary cyclic code of length p over $\mathbb{F}_q$. Then $Per(C)$ is a primitive group, and one of the following holds*:

(i) *$Per(C)$ is a solvable group of order pm with m a divisor of $p-1$ and $C_p \leq Per(C) \leq AGL(1,p)$, with $p \geq 5$. Furthermore $Per(C)$ contains a normal Sylow p-subgroup.*
(ii) *If $p = q$, then $Per(C) = AGL(1,p)$.*
(iii) *$Per(C) = PSL(2,11)$ and q is a power of 3. C is either the $[11,6]$ or $[11,5]$ code that is equivalent to the $[11,6,5]$ ternary Golay code or its dual, respectively.*
(iv) *$Per(C) = M_{23}$ and q is a power of 2. C is either the $[23,12]$ or $[23,11]$ code that is equivalent to the $[23,12,7]$ binary Golay code or its dual, respectively.*
(v) *$Per(C) = P\Gamma L(d, r^{d^b})$ where $b \in \mathbb{N}$, $d \geq 3$ is a prime number such that $(d, r^{d^b} - 1) = 1$, and $p = (r^{d^{b+1}} - 1)/(r^{d^b} - 1)$.*

Proof A transitive group of prime degree is a primitive group [23, p. 195]. As a consequence of a result of Burnside [13, Theorem 2], a transitive group of prime degree is either a subgroup of $AGL(1,p)$ or a doubly transitive group. In the first case $C_p \leq Per(C) \leq AGL(1,p)$, and if $p = 2$ or 3, $AGL(1,p) = S_p$. In this case, C is elementary by Remark 1, which is a contradiction. Since C_p is normal in $AGL(1,p)$ and $AGL(1,p)/C_p$ is abelian, $Per(C)$ is a normal subgroup. By [11, Example 3.5.1] G is solvable. If $q = p$, Roth and Seroussi [24] proved that any cyclic code of prime length p over $\mathbb{F}_p$ must be an MDS code equivalent to an extended Reed–Solomon code. Berger [2] proved that the permutation group of such codes is the affine group $AGL(1,p)$. In the doubly transitive cases, as C is non-elementary of prime length p, by Lemma 1, Remark 1 and Lemma 2, we see that $Per(C)$ is one of M_{11}, with $p = 11$, $PSL(2,11)$ with $p = 11$, M_{23} with $p = 23$, or $P\Gamma L(d,t)$ of degree $p = (t^d - 1)/(t-1)$ and t a prime power. If $Per(C) = M_{11}$, from [22, Table 1, Lemma 2] C must be elementary, which is a contradiction. If $Per(C) = PSL(2,11)$, from [22, Table 1, Lemma 2 and (J)] q must be a power of 3, and there is a unique non-elementary code over $\mathbb{F}_q$ contained in the dual of the repetition code. The $[11,5,6]$ dual of the ternary Golay code is contained in the repetition code and has permutation group $PSL(2,11)$; its dual, an $[11,6,5]$ code, intersects the dual of the repetition code in this $[11,5,6]$ code and also has permutation group $PSL(2,11)$. Part (ii) then follows. Part (iii) is obtained in an analogous way from [22, Table 1, Lemma 2 and (I)]. For Part (iv), we have from Lemma 2 that $Per(C) = P\Gamma L(d,t)$, $t = r^a$ for some $a \geq 1$ and $d \geq 3$. A number theory argument [12, Lemma 3.1] gives the result

Table 2 Permutation groups of some BCH codes of length p

q	p	δ	$Per(C)$	$Per(C_2)$	$Per(C_3)$
2	17	2	$C_8 \ltimes C_{17}$	S_{17}	S_{17}
2	23	3	M_{23}	M_{23}	M_{23}
2	41	2	$C_{20} \ltimes C_{41}$	$C_{20} \ltimes C_{41}$	$C_{20} \ltimes C_{41}$
2	41	3	$C_{20} \ltimes C_{41}$	S_{41}	S_{41}
2	43	5	$C_{14} \ltimes C_{43}$	$C_{14} \ltimes C_{43}$	$C_{14} \ltimes C_{43}$
2	43	7	$C_{14} \ltimes C_{43}$	S_{43}	S_{43}
3	13	2	$C_3 \ltimes C_{13}$	$C_3 \ltimes C_{13}$	$C_3 \ltimes C_{13}$
3	13	4	$P\Gamma L(3,3)$	$C_3 \ltimes C_{13}$	$C_3 \ltimes C_{13}$
3	13	5	$C_3 \ltimes C_{13}$	$C_3 \ltimes C_{13}$	$C_3 \ltimes C_{13}$
3	23	3	$C_{11} \ltimes C_{23}$	$C_{11} \ltimes C_{23}$	$C_{11} \ltimes C_{23}$
3	41	5	$C_8 \ltimes C_{41}$	$C_8 \ltimes C_{41}$	$C_8 \ltimes C_{41}$
4	43	9	$C_7 \ltimes C_{43}$	S_{43}	S_{43}
5	11	5	$C_5 \ltimes C_{11}$	$C_5 \ltimes C_{11}$	$C_5 \ltimes C_{11}$
11	5	3	C_5	$C_2 \ltimes C_5$	C_5

that if p is prime, then d must be a prime such that $(d, r^a - 1) = 1$ and $a = b^d$. The result then follows. □

Remark 2 For p prime, the permutation group of a non-elementary BCH code of length p over $\mathbb{F}_q$ is one of those listed in Theorem 3.

In Table 2, we give examples of permutation groups of BCH codes of length p over $\mathbb{F}_q$. $Per(C)$ (respectively $Per(C_2)$ and $Per(C_3)$), denotes the permutation group of the narrow sense ($b = 1$) BCH code with designed distance δ (respectively BCH code with designed distance δ and $b = 2$ and $b = 3$).

The following result is obtained by considering the permutation groups of cyclic codes of composite length.

Theorem 4 *Let C be a non-elementary cyclic code over $\mathbb{F}_{r^\alpha}$ of composite length. Then $Per(C)$ is either*

(i) *an imprimitive group (in the case that $n = p^m$, p a prime, the orbit of the subgroup generated by $T^{p^{m-1}}$ and its conjugate form a complete block system of $Per(C)$);*
or
(ii) *$Per(C)$ is a doubly transitive group equal to*

$$P\Gamma L\big(d, r^a\big), \quad \text{with } n = \frac{r^{ad} - 1}{r^a - 1},\ d \geq 3,\ a \geq 1.$$

Proof The group $Per(C)$ contains a complete cycle and has composite degree. Hence from a theorem of Burnside and Schur [25, p. 65], $Per(C)$ is either imprimitive or doubly transitive. If it is imprimitive and $n = p^m$, by [7, Chap. XVI, Theo-

rem VIII] $Per(C)$ contains an intransitive normal subgroup generated by $T^{p^{m-1}}$ and its conjugates. By [25, Proposition 7.1] the orbit of such a subgroup forms a complete block system of $Per(C)$.

In the doubly transitive case, we have from Lemma 1 that the only cases when the socle can be abelian are $N = C_p$ and $N = C_2 \times C_2$. In these cases, $Per(C)$ must be equal to $AGL(1, p)$ or S_4, which is impossible. Since the socle is not abelian and the degree is not prime, this leads to the only solution given by row six of Table 1 in Lemma 1. Hence from Lemma 2, Part (ii) follows. □

4 The permutation group of cyclic codes of prime power length

In this section, we consider the permutation groups of cyclic codes of length p^m, where p is an odd prime.

Lemma 5 *Let q be a prime power, p an odd prime, and z the largest integer such that $p^z | (q^t - 1)$, with t the order of q modulo p. If $z = 1$ we have*

$$\mathrm{ord}_{p^m}(q) = p^{m-1}t.$$

Proof Let t be the order of q modulo p, and $u = q^t \equiv 1 \bmod p$. Assume that $z = 1$, or equivalently $u \neq 1 \bmod p^2$. It is well known from elementary number theory [10, p. 87] that $u \bmod p^m$ is an element of order p^{m-1} in the group $(\mathbb{Z}_{p^m})^*$ if and only if $u \neq 1 \bmod p^2$. Hence $\mathrm{ord}_{p^m}(q) = p^{m-1}t$. □

According to Brillhart et al. [6], it is unusual to have $z > 1$.

Proposition 6 *Let $n = p^m$ and $q = r^\alpha$ a prime power with $(q, n) = 1$, and C a cyclic code of length n over $\mathbb{F}_q$. Let M_q be the multiplier defined by $M_q(i) = iq \bmod p^m$. Then the group $Per(C)$ contains the subgroup $K = \langle T, M_q \rangle$ of order $p^m \,\mathrm{ord}_{p^m}(q)$. Let p^l, with $l \geq m$ be the p-part of the order of K. Then a Sylow p-subgroup P of $Per(C)$ has order p^s such that*

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

If $z = 1$, then $s \geq 2m - 1$.

Proof By the definition of a cyclic code, we have $T \in Per(C)$. It is obvious that each cyclotomic class modulo n over $\mathbb{F}_q$ is invariant under the permutation M_q. This can be deduced from the fact that the polynomial $f(x) \in \mathbb{F}_q[x]$ satisfies $f(x^q) = f(x)^q$. Thus $M_q \in Per(C)$. The order of M_q is equal to $\mathrm{ord}_n(q)$, hence $K = \langle T, M_q \rangle$ is a subgroup of $Per(C)$ of order $n \,\mathrm{ord}_n(q)$. Since $n = p^m$, the order of K has p-part p^l with $l \leq m$. Let P be a Sylow p-subgroup of $Per(C)$ which contains T. Then P is a p-subgroup of S_{p^m}. From Sylow's Theorem, P is contained in a Sylow p-subgroup of S_{p^m}. It is well known that a Sylow p-subgroup of S_{p^m} is of order $p^{p^{m-1}+p^{m-2}+\cdots+1}$ [23, Kalužnin's Theorem]. Since P also contains the subgroup of K of order p^l, then $l \leq s \leq p^{m-1} + p^{m-2} + \cdots + 1$. If $z = 1$, then by Lemma 5 the

order of the group K is $\mathrm{ord}_p(q)p^{2m-1}$. This shows that p^{2m-1} divides $|Per(C)|$, so $Per(C)$ contains a p-subgroup of order at least p^{2m-1}. □

Theorem 7 *Let C be a non-elementary cyclic code of length p^m over $\mathbb{F}_{r^\alpha}$, with $m \geq 1$. Then the following hold*:

(i) *If $p \nmid \alpha$ and $p \nmid (d, r^a - 1)$, then $Per(C) = P\Gamma L(d, r^a)$, $a \geq 1$, $d \geq 3$, if and only if the Sylow p-subgroup of $Per(C)$ is of order p^m.*

(ii) *If $p \geq 5$, $\alpha = 1$ and $r = p$, $m > 1$, then $Per(C)$ is an imprimitive group which admits a complete system formed by the orbit of the subgroup generated by $T^{p^{m-1}}$ and its conjugate. It also contains a transitive normal Sylow p-subgroup of order p^s with $m < s \leq p^{m-1} + p^{m-2} + \cdots + 1$.*

(iii) *If $z = 1$, $p \nmid \alpha$ and $p \nmid (d, r^a - 1)$, then $Per(C)$ is an imprimitive group which contains a transitive normal Sylow p-subgroup of order p^s, with $2m - 1 \leq s \leq p^{m-1} + p^{m-2} + \cdots + 1$. Furthermore, $Per(C)$ admits a complete block system formed by the orbit of the subgroup generated by $T^{p^{m-1}}$ and its conjugate.*

Proof For Part (i), we know that the socle of $P\Gamma L(d, r^a)$ is the group $PSL(d, r^a)$ of order $\frac{r^{ad(d-1)/2}}{(d, r^a-1)} \prod_{i=2}^{d} (r^{ai} - 1)$. From a lemma of Zsigmondy [17, Chap. IX, Theorem 8.3], except for the cases $d = 2$, $r^a = 2^b - 1$ and $d = 6$, $r^a = 2$, there exists a prime q_0 such that q_0 divides $r^{ad} - 1$, but does not divide $r^{ai} - 1$, for $1 \leq i < d$. From Lemma 2, we cannot have $d = 2$. The case $d = 6$ and $r^a = 2$ does not give a prime power. Hence if $n = p^m = \frac{r^{ad}-1}{r^a-1}$, there is a q_0 which divides $(r^{ad} - 1) = (r^a - 1)p^m$. Since q_0 does not divide $r^a - 1$, then q_0 divides p^m, and hence $q_0 = p$ and p^m is the p-part of the order of $PSL(d, r^a)$. Also, since $p \nmid r^a - 1$, we have $p \nmid (d, r^a - 1)$. Hence if $(\alpha, p) = 1$, p^m is also in the p-part of the order of $P\Gamma L(d, r^a)$, and the result follows.

Conversely, if $Per(C)$ has Sylow p-subgroup P of order p^m, we can assume that $T \in P$, which gives the equality $P = \langle T \rangle$. Assume that in this case $Per(C)$ is imprimitive. Then by [13, Theorem 33], P is normal. P is then the minimal normal subgroup which is transitive and abelian. From [25, p. 17] $Per(C)$ is primitive, which is impossible. Thus if $P = \langle T \rangle$, the group $Per(C)$ is equal to $P\Gamma L(d, r^a)$, which is possible only if $[P\Gamma L(d, r^a) : PSL(d, r^a)]$ is prime to p, i.e, $(p, \alpha) = 1$ and $p \nmid (d, r^a - 1)$.

For Part (ii), from Theorem 4 if $Per(C)$ is primitive, then it is doubly transitive and equal to $P\Gamma L(d, r^a)$ with $n = \frac{r^{ad}-1}{r^a-1}$, $d \geq 3$ and $a \geq 1$. From [13, Lemma 22], if $Per(C)$ is doubly transitive with non abelian socle, then $Soc(Per(C)) = Alt(p^m)$. Hence from Remark 1 the code is elementary, which is a contradiction. Therefore, $Per(C)$ is imprimitive, and then by Part (i) the order of the Sylow p-subgroup is p^s with $s > m$. The second inequality then follows by Proposition 6.

For Part (iii), if $z = 1$ then from Proposition 6, we find that the order of a Sylow p-subgroup of $Per(C)$ is at least p^{2m-1}. If $Per(C)$ is doubly transitive, by Theorem 4 it is equal to $P\Gamma L(d, r^a)$, with $d \geq 3$. By assuming $p \nmid \alpha$ and $p \nmid (d, r^a - 1)$, we obtain from Part (i) that a Sylow p-subgroup of $Per(C)$ has order p^m, which is impossible. Hence $Per(C)$ is an imprimitive group. From [13, Theorem 33] $Per(C)$ contains a transitive normal Sylow p-subgroup, hence the result follows. □

Example 1 The narrow sense BCH code of length 25 over $\mathbb{F}_3$ with designed distance 3 has a permutation group which is the imprimitive group $S_5 \wr S_5$. The narrow sense BCH code of length 9 over $\mathbb{F}_5$ with designed distance 2 has a permutation group which is the imprimitive group $S_3 \wr S_3$. The binary $[7, 4, 3]$ Hamming code has permutation group $P\Gamma L(3, 2)$, which contains a Sylow 7-subgroup of order 7.

We now give the Sylow p-group of $Per(C)$ for several cases. Let p be an odd prime. For $n < p - 1$, we define the following subsets of S_{p^m}:

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

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

The sets Q^n and Q_1^n are subgroups of S_{p^m} [5, Lemma 2.1]. Note that $Q^1 = AG(p^m)$.

The following lemma will be used later. Note that the proof is similar to that of [15, Lemmas 2.4, 2.5].

Lemma 8 *If* $1 \le n < p - 1$, *then*

(i) $|Q^n| = (p-1)p^{2m+n-2}$ *and* $|Q_1^n| = p^{m+n}$.
(ii) $AG(p^m) = N_{S_{p^m}}(\langle T \rangle)$.
(iii) $N_{S_{p^m}}(Q_1^n) = Q^{n+1}$.

Proof For Part (i), by [5, Lemma 3.2], the map $(a_0, \ldots, a_n) \longrightarrow f$, where $f(x) = \sum_{i=0}^{n} a_i x^i$ is injective if $n < p - 1$. Thus in Q^n, the coefficients of a_0 can take p^r different values, and a_1 can take $p^{m-1}(p-1)$ values. For $2 \le i \le n$, a_i can take p values. From these results we have $|Q^n| = p^{2m+n-2}(p-1)$. For Q_1^n, the coefficients of a_0 can take p^m different values, and a_i for $1 \le i \le n$ can take p values, hence $|Q_1^n| = p^{m+n}$.

Now we prove that $AG(p^m) = N_{S_{p^m}}(\langle T \rangle)$. Let σ be an element of $N_{S_{p^m}}(\langle T \rangle)$. 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 $\sigma T(1) = \sigma(1) + j = \sigma(0) + 2j$. Therefore $\sigma(k) = \sigma(0) + kj$ 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.

Now we prove Part (iii).

($\subseteq$ part) Let $h \in N_{p^m}(Q_1^n)$ 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^m), from [5, Lemma 3.6] there exists $f \in Q^{n+1}$ such that $f^{-1}gf = T$. Thus $f^{-1}h^{-1}Thf = T$. The only elements of S_{p^m} which commute with T (a complete cycle of length p^m), are the powers of T. Thus $hf = T^j$ for some j. Since Q^{n+1} is a subgroup of S_{p^m} and $\langle T \rangle \le Q^{n+1}$, then $h \in Q^{n+1}$. Hence $N_{p^m}(Q_1^n) \le Q^{n+1}$.

($\supseteq$ part) Let $h \in Q_1^n$, where $h(x) = \sum_{i=0}^{n} h_i x^i$, with $h_1 \equiv 1 \bmod p^{m-1}$ and $p^{m-1} | h_i$, for $2 \le i \le n$. Let $g \in Q^{n+1}$ where $g(x) = \sum_{i=0}^{n+1} g_i x^i$, with $p \nmid g_1$ and $p^{m-1} | g_i$ for $2 \le i \le n$. 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 $p^{m-1}|h_i$, for $i \geq 2$ and $p^{m-1}|g_j$ for $j \geq 2$, any terms in $\sum_{i=2}^{n} h_i(\sum_{j=0}^{n+1} g_j x^j)^i$ involving g_j for $j \geq 2$ vanish modulo p^m. Therefore we have

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

By [5, Lemma 2.1], we have

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

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

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

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

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

Let $g^{-1}hg(x) = \sum_{m=0}^{n+1} c_m x^m$, and note that $c_{n+1} = b_1 h_1 g_{n+1} + b_{n+1}(h_1 g_1)n + 1$. Then by replacing the b_i with their values from (2), we obtain

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

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

Lemma 9 *Let $1 \leq n < p-1$. If P is a p-subgroup of S_{p^m} with $Q_1^n \lneq P \leq Q^{n+1}$, then $P = Q_1^{n+1}$.*

Proof By Lemma 8 Part (ii), we have $Q_1^n \lhd Q^{n+1}$. Hence we can consider $\overline{Q} = Q^{n+1}/Q_1^n$, which is of order $p^{m-1}(p-1)$ by Lemma 8. Let N be the number of Sylow p-subgroups of $\overline{Q}$. Then by Sylow's Theorem, $N \equiv 1 \bmod p$ and N divides $p^{m-1}(p-1)$. Hence $N = 1$, so there exists a unique Sylow p-subgroup $\overline{P'}$ of $\overline{Q}$ which is normal. From the condition on P above, the image $\overline{P}$ of P in $\overline{Q}$ is also a Sylow p-subgroup of $\overline{Q}$. Since there is a unique Sylow p-subgroup $\overline{P'} = \overline{P}$, by Lemma 8 the image $\overline{Q}_1^{n+1}$ of Q_1^{n+1} in $\overline{Q}$ is a Sylow p-subgroup of $\overline{Q}$. Hence $\overline{Q}_1^{n+1} = \overline{P} = \overline{P'}$. As $Q_1^n \leq P$ and $Q_1^n \leq Q_1^{n+1}$, the result follows. □

Theorem 10 *The group Q_1^1 is a normal subgroup of Q^1 and is the unique subgroup of S_{p^m} of order p^{m+1} which contains T.*

Proof It is obvious that $T \in Q_1^1$. By Lemma 8, $|Q_1^1| = p^{m+1}$. Consider now an element g of Q^1, $g(x) = b_0 + b_1 x$ with $b_0, b_1 \in \mathbb{Z}_{p^m}$ and $(b_1, p) = 1$. It is not difficult to check that the inverse of g in Q^1 is given by $g^{-1}(x) = -b_1^{-1}b_0 + b_1^{-1}x$. Consider $f \in Q_1^1$, so that $f(x) = a_0 + a_1 x$ with $a_0, a_1 \in \mathbb{Z}_{p^m}$, $(a_1, p) = 1$ and $a_1 \equiv 1 \bmod p^m$. We then have $g^{-1}fg(x) = g^{-1}(a_0 + a_1(b_0 + b_1 x)) = (-b_0 + a_0 + a_1 b_0)b_1^{-1} + a_1 x$. This proves that $g^{-1}fg(x) \in Q_1^1$. Hence Q_1^1 is normal in Q^1. Now let S be a subgroup of Q^1 of order p^{m+1} which contains T. Thus $\langle T\rangle$ has index p in S, and thus $\langle T\rangle$ is maximal in S. Furthermore, $\langle T\rangle \lhd S$, because any subgroup of a p-group of index p must be normal. Therefore we have $S = N_S(T) \leq N_{S_{p^m}}(T)$, and by Lemma 8, $S \leq N_{S_{p^m}}(T) = AG(p^m) = Q^1$. Thus, such an S must be a subgroup of Q^1. It is clear that Q_1^1 is not abelian, and S cannot be abelian since it is a transitive group. If this were the case it would have to be a regular group [23, Theorem 1.6.3], and thus $|S| = p^m$, which is impossible. Furthermore, the p-groups which contain a cyclic maximal subgroup are known [23, Theorem 5.3.4]. If these groups are not abelian or $p \neq 2$, they have the following special forms:

$$Q_1^1 = \left\langle x, T \;\middle|\; x^p = 1;\ x^{-1}Tx = T^{1+p^{m-1}} \right\rangle,$$

and

$$S = \left\langle y, T \;\middle|\; y^p = 1;\ y^{-1}Ty = T^{1+p^{m-1}} \right\rangle.$$

However, the conditions on x and y give

$$x^{-1}Tx = y^{-1}Ty \quad \Longleftrightarrow \quad Tyx^{-1} = yx^{-1}T,$$

so the only elements of S_{p^m} which commute with T (a complete cycle of length p^m), are the powers of T. Thus $yx^{-1} = T^j$ for some j. Since the order of yx^{-1} is p, the only choices for j are $j = p^m$ or $j = p^{m-1}$. For both choices we get $S = Q_1^1$, namely $j = p^m$ gives $x = y^{-1}$ (so $S = Q_1^1$), and $j = p^{m-1}$ gives $x = T^{-p^{m-1}}y$. Thus we have $x \in \langle y, T\rangle$, so that $\langle x, T\rangle = \langle y, T\rangle$, and hence $S = Q_1^1$. □

Theorem 11 *Let p be an odd prime, $q = r^\alpha$ a prime power, C a cyclic code over $\mathbb{F}_q$ of length p^m, and P a Sylow p-subgroup of $Per(C)$ of order p^s such that $T \in P$. Then the following hold*:

(a) *If* $p \nmid \alpha$ *and* $p \nmid (d, r^a - 1)$, *then* $s = m$, *and* $P = \langle T \rangle$ *if and only if* $Per(C) = P\Gamma L(d, r^a)$, $d \geq 3$,
(b) *If* $p \geq 5$, $\alpha = 1$ *and* $r = p$, $m > 1$, *then* $Per(C)$ *is an imprimitve group and* P *is normal of order* p^s, $s > m$. *If* $m < s \leq p + m - 1$, *then we have* $P = Q_1^{s-m}$.
(c) *If* $z = 1$, $p \nmid \alpha$ *and* $p \nmid (d, r^a - 1)$, *then* $Per(C)$ *is an imprimitve group and* P *is normal of order* $p^s \geq p^{2m-1}$. *Furthermore, if* $2m - 1 < s \leq p + m - 1$, *then we have* $P = Q_1^{s-m}$.

Proof Statement (a) and the first parts of (b) and (c) follow from Theorem 7. We thus only need prove that if $s < p + m - 1$, then $P = Q_1^{s-m}$. Assume $s \leq p + m - 1$, so that P contains a p-subgroup P' of order p^{m+1}. By Theorem 10, we obtain $P' = Q_1^1$. Let $j \geq 1$ be the largest integer such that $Q_1^j \leq P$. If $j = p - 1$, by Lemma 8 we have $|Q_1^{p-1}| = p^{p+m-1}$. Thus Q_1^{p-1} is a subgroup of P of the same order as P, and hence $P = Q_1^{p-1}$, so we can assume that $1 \leq j < p - 1$. If $Q_1^j \lneq P$, then $Q_1^j \lneq N_P(Q_1^j)$ and by Lemma 8, $N_P(Q_1^j) \leq Q_1^{j+1}$. Since $Q_1^j \lneq N_P(Q_1^j) \leq Q_1^{j+1}$, by Lemma 8 $N_p(Q_1^j) = Q_1^{j+1}$, which contradicts the choice of j. □

References

1. Bardoe, M., Sin, P.: The permutation modules for $GL(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$. J. Lond. Math. Soc. **61**, 58–80 (2000)
2. Berger, T.P.: A direct proof for the automorphism group of Reed–Solomon codes. In: Cohen, G., Charpin, P. (eds.) Proc. Eurocode 90. Lecture Notes in Computer Science, vol. 514, pp. 21–29. Springer, Berlin (1991)
3. Berger, T.P., Charpin, P.: The permutation group of affine invariant extended cyclic codes. IEEE Trans. Inf. Theory **62**(6), 2194–2209 (1996)
4. Bienert, R., Klopsch, B.: Automorphism group of cyclic codes. J. Algebr. Comb. **31**, 33–52 (2010)
5. Brand, N.: Polynomial isomorphisms of combinatorial objects. Graphs Comb. **7**(1), 7–14 (1991)
6. Brillhart, J., Tonascia, J., Weinberger, P.: On the Fermat quotient. In: Atkin, A.O.L., Birch, B. (eds.) Computers in Number Theory. Academic Press, New York (1991)
7. Burnside, W.: On some properties of groups of odd order. J. Lond. Math. Soc. **33**, 162–185 (1901)
8. Burnside, W.: Theory of Groups of Finite Order. Dover, Mineola (1955)
9. Cameron, P.J.: Finite permutation groups and finite simple groups. Bull. Lond. Math. Soc. **13**, 1–22 (1981)
10. Demazure, M.: Cours D'Algèbre: Primalité, Divisibilité, Codes. Cassini, Paris (1997)
11. Dixon, J.D., Mortimer, B.: Permutation Groups. Graduate Texts in Mathematics, vol. 163. Springer, Berlin (1996)
12. Dixon, J.D., Zalesskii, A.: Finite primitive linear groups of prime degree. J. Lond. Math. Soc. **57**(2), 126–134 (1998)
13. Dobson, E.D.: On groups of odd prime-power degree that contain a full cycle. Discrete Math. **299**, 65–78 (2005)
14. Dobson, E.D., Witte, D.: Transitive permutation groups of prime-squared degree. J. Algebr. Comb. **16**(1), 43–69 (2002)
15. Huffman, W.C., Job, V., Pless, V.: Multiplier and generalized multipliers of cyclic objects and cyclic codes. J. Comb. Theory, Ser. A **62**, 183–215 (1993)
16. Huffman, W.C.: Codes and groups. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, vol. II, pp. 1345–1439. Elsevier, Amsterdam (1998)
17. Huppert, B., Blackburn, N.: Finite Groups II. Grundlehren Math. Wiss., vol. 242. Springer, Berlin (1982)
18. Lim, F., Fossorier, M., Kavcić, A.: Notes on the automorphism group of Reed–Solomon binary images. In: Proc. IEEE Int. Symp. Inform. Theory, Toronto, Canada, July 2008, pp. 1813–1817 (2008)

19. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting-Codes. North-Holland, Amsterdam (1977)
20. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, pp. 114–116, Jan.–Feb. 1978
21. McSorley, J.P.: Cyclic permutation groups in doubly-transitive groups. Commun. Algebra **25**, 33–35 (1997)
22. Mortimer, B.: The modular permutation representations of the known doubly transitive groups. Proc. Lond. Math. Soc. **41**, 1–20 (1980)
23. Robinson, D.J.S.: A Course in the Theory of Groups. Graduate Texts in Mathematics, vol. 80. Springer, Berlin (1980)
24. Roth, R., Seroussi, G.: On cyclic MDS codes of length q over $GF(q)$. IEEE Trans. Inf. Theory **32**(2), 284–285 (1986)
25. Wielandt, H.: Finite Permutation Groups. Academic Press, New York (1964)