NOTE

THE WEIGHT DISTRIBUTION FOR A CLASS OF IRREDUCIBLE CYCLIC CODES*

Torleiv KLOVE
University of Bergen, N-5014 Bergen -U, Norway

We show that the weight enumerator for the irreducible cyclic code of length fn over GF(q) is
the fth power of the weight enumerator for the code of length n for all f in a set we characterize.

1. Statement of results

Let q be a prime power and let ord, (q) denote the multiplicative order of q
modulo n. Let

\[ F(n, q) = \{ f \mid f \text{ is a positive integer, } \gcd(f, q) = 1, \text{ and } \text{ord}_q (f) = f \text{ ord}_q (q) \}. \]

Let \( \gcd(n, q) = 1 \). There is a unique (up to isomorphism) irreducible cyclic code
(with no repeated coordinates) of length n over GF(q). Let \( A_n (Z) \) be it's weight
enumerator. The following theorem is a direct consequence of results (Lemma 4.5
(iii) and Theorem 5.1) given in [1].

Theorem 1.1. If \( f \in F(n, q) \) and \( \gcd(f, ((q - 1)/\gcd(n, q - 1))) = 1 \), then \( A_n (Z) = A_n (Z)^f \).

The next two theorems characterize \( F(n, q) \).

In the following p and P denote primes, \( v_p (m) \) is the exponent of the highest
power of p dividing m, \( n^* = \Pi_{p \mid n} p \), \( \gamma = v_2 (q + 1) \), and \( z_p = v_p (q^{\text{ord}_p (q)} - 1) \).

Theorem 1.2. (i) If \( q \equiv 3 \pmod{4} \), \( n \not\equiv 0 \pmod{2} \), or P \# 2, then \( P \in F(n, q) \) if and
only if \( v_p (n) \leq z_p + v_p (\text{ord}_p (q)) \).

(ii) If \( q \equiv 3 \pmod{4} \) and \( n = 0 \pmod{4} \), then \( 2 \in F(n, q) \) if and only if \( v_2 (n) \geq \gamma + \max \{ 1, v_2 (\text{ord}_2 (q)) \} \).

(iii) If \( q \equiv 3 \pmod{4} \) and \( n = 2 \pmod{4} \), then \( 2 \in F(n, q) \) if and only if \( v_2 (\text{ord}_2 (q)) = 0 \).

Theorem 1.3. Let \( P_1 < P_2 < \cdots < P \) be the primes in \( F(n, q) \). Then \( f \in F(n, q) \) if

* This research was supported in part by The Norwegian Research Council for Science and the

Humanities.
and only if \( f = P_1^{\alpha_1}P_2^{\alpha_2} \cdots P_r^{\alpha_r} \) where \( \alpha_i \geq 0 \) for \( 1 \leq i \leq r \), and, if \( q \equiv 3 \pmod{4} \) and \( n \equiv 2 \pmod{4} \), \( v_2(f) \leq 1 \).

We note that Theorem 1.2 implies that if \( P \in F(n, q) \), then \( P \mid n \).

**Example.** Let \( q = 2 \) and \( n = 15 \). Then \( n^* = 15 \), \( \text{ord}_{n^*}(q) = 4 \), \( z_5 = 1 \), and \( z_5 = 1 \). Hence the primes in \( F(15, 2) \) are 3 and 5 and so \( F(15, 2) = \{3^*5^\alpha \mid \alpha, \beta \geq 0\} \). The \((15,4)\) code is a maximal-length shift-register code and so \( A_{15}(Z) = 1 + 15Z^e \). Therefore, we get

\[
A_{15+15^*4^*}(Z) = (1 + 15Z^e)^{3*5^\alpha} \quad \text{for all } \alpha, \beta \geq 0.
\]

**2. Proofs of Theorems 1.2 and 1.3**

We shall use some well-known facts on \( \text{ord}_n(q) \). We give them in the following lemma.

**Lemma 2.1.** (i) If \( \gcd(m, n) = 1 \), then \( \text{ord}_{mn}(q) = \text{lcm}(\text{ord}_m(q), \text{ord}_n(q)) \).

(ii) If \( q \not\equiv 3 \pmod{4} \) or \( P \not\equiv 2 \), then \( \text{ord}_{q^r}(q) = P^{\max(0, z_p-1, z_p)} \text{ord}_P(q) \).

(iii) If \( q \equiv 3 \pmod{4} \) and \( \alpha > 1 \), then \( \text{ord}_{q^r}(q) = 2^{\max(1, z_p-\gamma)} \).

**Lemma 2.2.** We have \( \text{ord}_{q^r}(q) \leq P \text{ord}_n(q) \).

**Proof of Lemma 2.2 and Theorem 1.2.** If \( P \not\mid n \), then \( \text{ord}_{q^r}(q) = \text{lcm}(\text{ord}_P(q), \text{ord}_n(q)) < P \text{ord}_n(q) \). If \( P \mid n \), let \( n = P^m \text{m} \) where \( P \not\mid \text{m} \). Suppose first that \( q \not\equiv 3 \pmod{4} \) or \( P \not\equiv 2 \). Then, by Lemma 2.1,

\[
\text{ord}_{q^r}(q) = \text{lcm}(\text{ord}_{q^r}(q), \text{ord}_m(q))
\]

\[
= \text{lcm}(P^{\max(0, z_p-1, z_p)} \text{ord}_P(q), \text{ord}_m(q))
\]

\[
= \begin{cases} 
\text{ord}_n(q) \quad \text{if } \alpha - z_p < v_p(\text{ord}_m(q)), \\
P \text{ord}_n(q) \quad \text{if } \alpha - z_p \geq v_p(\text{ord}_m(q)).
\end{cases}
\]

This proves Lemma 2.2 in this case. Further, by Lemma 2.1,

\[
v_P(\text{ord}_m(q)) = v_P\left( \text{lcm}\left( \text{ord}_{q^r}(q), \text{ord}_m(q) \right) \right)
\]

\[
= v_P\left( \text{lcm}\left( \text{ord}_n(q) \right) \right)
\]

\[
= v_P\left( \text{lcm}\left( \text{ord}_P(q) \right) \right) = v_P(\text{ord}_n(q)),
\]
since $v_p(\text{ord}_p(q)) = 0$. This proves Theorem 1.2(i). The proof is similar in the case $q \equiv 3 \pmod{4}$ and $P = 2$.

**Lemma 2.3.** We have $\text{ord}_{m^k}(q) \leq m^k \text{ord}_n(q)$ for $m \geq 1$.

**Proof.** This follows from Lemma 2.2 by induction on the number of prime factors of $m$.

**Lemma 2.4.** If $f \in F(n, q)$ and $P | f$, then $P \in F(n, q)$.

**Proof.** Let $f = gP$. Then, by Lemma 2.3,

$$gP \text{ord}_n(q) = \text{ord}_{p^k}(q) \leq g \text{ord}_{p^m}(q) \leq gP \text{ord}_n(q).$$

Hence

$$P \text{ord}_n(q) = \text{ord}_{p^m}(q).$$

**Lemma 2.5.** If $q \equiv 3 \pmod{4}$, $n \equiv 2 \pmod{4}$, and $f \in F(n, q)$, then $v_2(f) \leq 1$.

**Proof.** Suppose $f = 2^\gamma g$ where $\alpha > 0$ and $g$ is odd. Let $n = 2m$. Then, by Lemma 2.1 $\text{ord}_n(q) = \text{ord}_m(q)$. Hence, by Lemmata 2.1 and 2.3,

$$f \text{ord}_n(q) = \text{ord}_m(q) = \text{ord}_{p^m}(q)$$

$$= \text{lcm}(2^{\max(1,\alpha + 1 - \gamma)}, \text{ord}_{p^m}(q))$$

$$\leq 2^{\max(1,\alpha + 1 - \gamma)} \text{ord}_m(q)$$

$$= 2^{\max(1 - \alpha, 1 - \gamma)}f \text{ord}_n(q).$$

Since $\gamma \geq 2$, this is possible only if $\alpha \leq 1$.

**Lemma 2.6.** Suppose $q \not\equiv 3 \pmod{4}$, $n \not\equiv 2 \pmod{4}$, $P \not= 2$, or $v_2(f) = 0$. If $Pf \in F(n, q)$, then $Pf \in F(n, q)$.

**Proof.** Suppose first that $q \not\equiv 3 \pmod{4}$ or $P \not= 2$. Then, by Theorem 1.2(i),

$$v_p(n) \geq z_p + v_p(\text{ord}_{n^*}(q)).$$

Since all the primes dividing $f$ also divide $n$, we have $(fn)^* = n^*$. Hence

$$v_p(fn) \geq z_p + v_p(\text{ord}_{(fn)^*}(q))$$

and so, by Theorem 1.2(i),

$$\text{ord}_{p^m}(q) = P \text{ord}_{p^m}(q) = Pf \text{ord}_n(q).$$

The cases where $q \equiv 3 \pmod{4}$ and $P = 2$ are similar.

We can now prove Theorem 1.3. The "only if" part follows from Lemmata 2.4 and 2.5 and the "if" part follows from Lemma 2.6 by induction.
Acknowledgement

Due to good criticism by the anonymous referee, proofs have been simplified and exposition improved.

Reference