A characterization of two-weight projective cyclic codes

Tao Feng

Abstract—We give necessary conditions for a two-weight projective cyclic code to be the direct sum of two one-weight irreducible cyclic subcodes of the same dimension, following the work of Wolfmann and Vega. This confirms Vega’s conjecture that all the two-weight cyclic codes of this type are the known ones in the projective case.

Index Terms—cyclic code, two-weight code, projective code, Gauss sum sum

I. INTRODUCTION

A projective code is a linear code such that the minimum weight of its dual code is at least 3. A cyclic code is irreducible if its check polynomial is irreducible. Cyclic codes have important applications in digital communication, so it is of theoretical interest to determine the weight distribution of cyclic codes. We refer the reader to the classical textbooks [8] and [11] for basic facts on cyclic codes. When a cyclic code has exactly one nonzero weight, a nice characterization is given by Vega in [12], which we will describe later.

The class of two-weight cyclic codes was extensively studied in [3], [5], [7], [15], [17], [18]. Schmidt and White obtained in [10] the necessary and sufficient conditions for an irreducible cyclic code to have at most two weights, and they also explored the connections with other combinatorial objects.

We fix the following notations throughout this note:

(i) The number $p$ is a prime and $q$ is a power of $p$. Let $k \geq 1$ be a positive integer and $r = q^k$. Write $\Delta = \frac{r-1}{q-1}$.
(ii) Let $\gamma$ be a fixed primitive element of $\mathbb{F}_q$. For an integer $a$, we use $h_a(x)$ for the minimal polynomial of $\gamma^a$ over $\mathbb{F}_q$.
(iii) Let $\xi_N$ be the complex primitive $N$-th root of unity $e^{2\pi i/N}$ for any positive integer $N$.

It was once conjectured that two-weight projective cyclic codes must be irreducible. Wolfmann [17] proved that this is true when $q = 2$, but false when $q > 2$. To be more specific, he proved that if $C$ is an $[n,k]$ two-weight projective cyclic code over $\mathbb{F}_q$ with $\gcd(n,q) = 1$, then either

1. $C$ is irreducible, or
2. $q > 2$, $C$ is the direct sum of two one-weight irreducible cyclic subcodes of the same dimension, and $n = \lambda q^{k-1}$, where $\lambda |q-1$, $\lambda \neq 1$. Additionally, the two nonzero weights are $\lambda q^{k-1}$ and $(\lambda - 1)q^{k-1}$.

After Wolfmann’s work, several infinite families of two-weight cyclic codes of the second type were discovered, and a unified explanation is given by Vega in [13]. We state his result below.

Theorem 1: [13, Theorem 10] Let $a_1, a_2, v$ be integers such that $a_1q^i \neq a_2$ (mod $q^k-1$) for all $i \geq 0$, $v = \gcd(a_1 - a_2, q-1)$, $a_2 \in \mathbb{Z}_q^\times$, and let $\tilde{a}_2$ be the inverse of $a_2$ in $\mathbb{Z}_q^\times$. For an integer $\ell$ which divides $\gcd(a_1, a_2, q-1)$, we set $\lambda = \frac{v}{\gcd(a_1, a_2, q-1)}$, $n = \lambda \Delta$ and $\mu = \frac{q^k-1}{n}$. Suppose that at least one of the following two conditions holds:

- $p = 2, k = 2, v = 1$, and $a_1$ is a unit in the ring $\mathbb{Z}_\Delta$, or
- $p$ is an odd prime and $k\geq 3$, $a_1$ is a unit in $\mathbb{Z}_\Delta$, $a_2$ is a unit in $\mathbb{Z}_\Delta$, and $\lambda > v/\mu$.

Then the following four assertions are true:

(a) $h_{a_1}(x), h_{a_2}(x)$ are the check polynomials for two different one-weight cyclic codes of length $n$ and dimension $k$; 
(b) $\mu | v$, and $\lambda > v/\mu$;
(c) If $C$ is the cyclic code with check polynomial $h_{a_1}(x)h_{a_2}(x)$, then $C$ is an $[n,2k]$ two-weight cyclic code with nonzero weights $\lambda q^{k-1}$ and $(\lambda - v/\mu)q^{k-1}$;
(d) $C$ is a projective code if and only if $v = \mu$.

It is not hard to show that under condition (1) in the above theorem, the code $C$ cannot be projective. It is the purpose of this note to prove the following characterization of two-weight projective cyclic codes.

Theorem 2: Let $C$ be an $[n,k]$ two-weight projective cyclic code over $\mathbb{F}_q$ with $\gcd(n,q) = 1$. Then $C$ is either irreducible, or the direct sum of two one-weight irreducible cyclic subcodes of the same dimension. Let $\gamma$ be a fixed primitive element of $\mathbb{F}_q^\times$. In the latter case, $q > 2$, and there exist integers $a_1, a_2$ such that

1. $a_1 \neq a_2q^j$ (mod $q^k-1$) for any integer $j$;
2. $a_1, a_2 \in \mathbb{Z}_\Delta$;
3. $\gcd(a_1, a_2, q - 1) = \gcd(a_1 - a_2, q - 1) = \frac{v}{n}$;
4. $1 + \tilde{a}_2(a_1 - a_2) \equiv p^j (\text{mod } \ell \Delta)$ for some integer $j$, where $\tilde{a}_2$ is the inverse of $a_2$ in $\mathbb{Z}_\Delta$;
5. The minimal polynomials of $\gamma^{a_1}, \gamma^{a_2}$ over $\mathbb{F}_q$, denoted by $h_{a_1}(x)$ and $h_{a_2}(x)$, have the same degree.

Moreover, the product $h_{a_1}(x)h_{a_2}(x)$ is the check polynomial of the cyclic code $C$.

We shall need the following well-known characterization of one-weight cyclic code, c.f. [12]. This will serve as the ingredient for the two-weight projective cyclic codes of the second type as described by Wolfmann.

Lemma 3: With the same notation as specified before, $h_a(x)$ is the check polynomial of a one-weight irreducible cyclic code if and only if $\gcd(a, \Delta) = 1$.

II. PRELIMINARIES

In this section, we introduce the necessary backgrounds that we shall use in this note.

A. Group rings, characters

Let $G$ be a (multiplicatively written) finite Abelian group with identity $1_G$. The group ring $\mathbb{C}[G]$ is a ring, consisting of all the formal sums of the free basis $\{g \in G\}$ over $\mathbb{C}$, with the multiplication extending that of $G$ by linearity and distributivity. We identify a subset $D$ of $G$ with the corresponding group ring element, namely $D = \sum_{g \in D} g \in \mathbb{C}[G]$. For a group ring element $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$, and an integer $m$, we use the notation $A^{(m)} := \sum_{g \in G} a_g g^m$. Please refer to [21] for more details.

We use $\bar{G}$ for the character group of $G$, consisting of all the homomorphisms from $G$ to $\mathbb{C}^\times$. We use $\chi_0$ for the principal character
of $G$, namely the homomorphism which maps each of $G$ to 1. We have the following orthogonality relation:

$$\sum_{x \in G} \chi(g) = \begin{cases} |G|, & \text{if } g = 1_G, \\ 0, & \text{otherwise}. \end{cases}$$

The inversion formula follows from this relation: If $A = \sum_{g \in G} a_g g \in \mathbb{C}[G]$, then

$$a_g = \frac{1}{|G|} \sum_{x \in G} (\chi(A)\chi^{-1}(g)).$$

where $\chi(A) = \sum_{g \in G} a_g \chi(g)$. A direct consequence is that two elements $A, B \in \mathbb{C}[G]$ are equal if and only if $\chi(A) = \chi(B)$ for each character $\chi$.

Let $Tr$ be the trace function from $F_r$ to $F_q$, and use $Tr_{p/q}/F_p$ for the trace function from $F_q$ to $F_p$. Let $\psi$ be the canonical character of $F_q$ defined by $\psi(x) = e^{2\pi i/\sqrt{q}}(x)$, $x \in F_q$. For each $a \in F_r$, we can define an additive character $\psi_a$ of $F_r$, by $\psi_a(x) = \psi(Tr(ax))$ $(x \in F_r)$. Let $\varphi$ be the multiplicative character of $F^*_r$ which maps $\gamma$ to $\xi_{\gamma-1}$.

Each character of $F_r \times F_r$ is of the form $\psi_a \otimes \psi_b$ $(a, b \in F_r)$ which is defined as

$$\psi_a \otimes \psi_b((x, y)) = \psi_a(x)\psi_b(y), \forall(x, y) \in F_r \times F_r.$$

Each character of the quotient group $F^*_r/F^*_q$ can be viewed as a multiplicative character of $F^*_r$, which is principal on $F^*_q$, and vice versa. Please refer to [6] for details.

### B. Gauss sums

Let $\chi$ be a multiplicative character of $F^*_r$. The Gauss sum $G(\chi)$ is defined as

$$G(\chi) = \sum_{x \in F^*_r} \psi(Tr(x))\chi(x).$$

Clearly, $G(\chi) = -1$ if $\chi = \chi_0$, and $|G(\chi)| = \sqrt{r}$ otherwise. One important property of Gauss sums we shall use is the following

$$\psi(Tr(x)) = \frac{1}{r-1} \sum_{\chi \in \mathbb{F}_r^*} G(\chi)\chi^{-1}(x), \forall x \in F^*_r.$$


### C. Singer difference sets, multipliers

Let $G$ be the quotient group $F^*_r/F^*_q$, and $D$ be the image of $\{x \in F^*_r | Tr(x) = 1\}$ in $G$. It is well known that $D$ is the classical Singer difference set, which satisfies that

$$DD^{-1} = q^{k-2} + q^{k-2} - (q-1)G.$$

For a nontrivial character $\chi$ of $G$, we have ([23])

$$\chi(D) = -\frac{G(\chi)}{q}.$$

In particular, $D$ is an invertible element in the ring $\mathbb{C}[G]$. Under the character $\chi$, its inverse $D^{-1}$ has character value $\chi(D^{-1}) = \frac{1}{\chi(D)}$, so $D^{-1}$ can be computed using the inversion formula. We can show that $D^{(-1)}$ is invertible, since $\chi(D^{(-1)}) = \chi(D)$.

If $t$ is an integer relatively prime with $|G|$, then $t$ is called a multiplier of $D$ if there exists $g \in G$ such that $D^t = Dg$. By [9, Proposition 3.1.1], the only multipliers of the classical Singer difference sets are the powers of $p$.

Please refer to [9] or [19] for more details on difference sets.

### D. Stieltjes’s theorem

Let $a$ be any integer not divisible by $r - 1$. We use $L(a)$ for the least positive integer such that $L(a) \equiv 0 \pmod{r - 1}$. Let $L(a) = a_0 + a_1p + \cdots + a_{m-1}p^{m-1} \equiv r \equiv 0 \pmod{p^m}$ be the $p$-adic expansion of $L(a)$, with $0 \leq a_i \leq p - 1$ for each $i$. We define the function

$$s(a) = \sum_{i=0}^{m-1} a_i.$$

Let $\varphi$ be the prime ideal in $\mathbb{Z}[\xi_{r-1}]$ such that

$$\xi_{r-1} \equiv \gamma, \pmod{\varphi},$$

and $\Psi$ be the prime ideal in $\mathbb{Z}[\xi_{r-1}, \xi_{|\Psi|}]$ lying over $\varphi$. Stieltjes’s theorem tells us that the highest power of $\Psi$ that divides $G(\varphi^{-n})$ is $s(a)$, for any integer $a$ not divisible by $r - 1$. Please refer to [4].

### III. Proof of the Main Result

#### Proof of Theorem 2

Let $C$ be an $[n, k]$, two-weight projective cyclic code, and assume that $C$ is not irreducible. Then by Wolfmann’s result [17], $C$ is the direct sum of two one-weight irreducible cyclic subcodes of the same dimension; moreover, $q > 2$, $n = \lambda q - 1$, where $\lambda q - 1$, $\lambda > 1$, and the two nonzero weights are $\lambda q - 1$ and $(\lambda - 1)q - 1$. By Lemma 3, there exist $a_1, a_2 \in \mathbb{Z}_\Delta$ such that $h_{a_1}(x), h_{a_2}(x)$ have the same degree and their product $h_{a_1}(x)h_{a_2}(x)$ is the check polynomial of $C$. Since $x^n - 1$ has no repeated root, $a_1 \neq a_2 q^i \pmod{r - 1}$ for any integer $i$. Therefore, $a_1, a_2$ satisfy the conditions (1), (2), (5), and we only need to prove that $a_1, a_2$ satisfy the conditions (3) and (4).

Write $\beta := \gamma^{-1}$; in the trace form, the cyclic code $C$ consists of codewords of the form

$$c_{a,b} := (Tr(a+b), Tr(a\beta^{a_1}+b\beta^{a_2}), \ldots, Tr(a\beta^{a(n-1)a_1}+b\beta^{a(n-1)a_2}))$$

with $a, b \in F_r$ (see [11, p. 89]). We use wt$(c_{a,b})$ for the Hamming weight of the codeword $c_{a,b}$.

From $\gamma^{a_1n} = \gamma^{a_2n} = 1$, we see that the length $n$ is divisible by $r - 1$, i.e.,

$$\ell := n \cdot \text{gcd}(a_1, a_2, q - 1) \equiv \frac{\lambda \cdot \text{gcd}(a_1, a_2, q - 1)}{r - 1} \equiv 1 \pmod{q - 1}$$

is an integer. Write $\tilde{a}_2$ for the inverse of $a_2$ in $\mathbb{Z}_\Delta$. Also, we define

$$v := \text{gcd}(a_1 - a_2, q - 1), \quad \tilde{w} := 1 + \tilde{a}_2(a_1 - a_2).$$

**Lemma 4**: We have $\ell = 1$, $v = \text{gcd}(a_1, a_2, q - 1) = \frac{q - 1}{v}$, and $\text{gcd}(v, \Delta) = 1$.

**Proof**: Since $C$ is projective, the existence of $0 \leq i \leq j \leq n - 1, \mu \in \mathbb{F}_q$ such that $Tr(a\beta^{i\mu} + b\beta^{j\mu}) = \mu Tr(a\beta^{i\mu} + b\beta^{j\mu})$ for any $a, b \in F_r$, implies that $i = j$. To put it another way, if there exists $0 \leq i \leq j \leq n - 1$ and $\mu \in \mathbb{F}_q$ such that $\beta^{i\mu} = \mu \beta^{j\mu}$, then $i = j$. Since $\beta(i - j) = \mu$ is in $\mathbb{F}_q$, we have that $\Delta$ divides $a_1(i - j)$. Since $\text{gcd}(a_1, \Delta) = 1$, we have $i - j = u\Delta$ for some integer $u$. From $\beta(i - j) = \beta(i - j)\mu$, we get $r - 1 | u\Delta(a_1 - a_2)$, i.e., $r - 1 | u(a_1 - a_2)$. Since $v = \text{gcd}(a_1 - a_2, q - 1)$, $u$ is a multiple of $q - 1$. If $\frac{r - 1}{v} < q - 1$, then the pair $(i, j) = (\frac{r - 1}{v}, 0)$ would contradict the fact $C$ is projective. Hence $\frac{r - 1}{v} \geq n$. On the other hand, $n$ is divisible by $\text{gcd}(a_1, a_2, q - 1)$, so

$$\frac{r - 1}{\text{gcd}(a_1, a_2, q - 1)} \leq n \leq \frac{r - 1}{v}.$$

Since $v \geq \text{gcd}(a_1, a_2, q - 1)$, we immediately get $v = \text{gcd}(a_1, a_2, q - 1), n = \frac{r - 1}{v}, \ell = 1$. Since $a_1$ is relatively prime with $\Delta$, we have $\text{gcd}(v, \Delta) = 1$. 

\[\boxed{}\]
It follows from the above lemma that \(a_1, a_2\) satisfy condition (3). We break the remaining part of the proof into a series of lemmas.

**Lemma 5:** The product \(G(\varphi^{\frac{x_1}{q}a})G(\varphi^{\frac{x_2}{q}w})\) is divisible by \(r\), for any \(s \not\equiv 0 \pmod{v\Delta}\).

**Proof:** We define the following subset \(R \subset (\mathbb{F}_r, +) \times (\mathbb{F}_r, +)\) as in [17]:

\[
R := \{(y\beta^{ja_2}, y\beta^{ja_2}) | 0 \leq i \leq n - 1, y \in \mathbb{F}_r^*\}.
\]

Let \(a, b\) be two nonzero elements of \(\mathbb{F}_r^*\), and we associate the weight of \(c_{a,b}\) to the value \(\psi \circ \psi(R)\) as follows:

\[
\psi_a \otimes \psi_b(R) = \sum_{i=0}^{n-1} \sum_{y \in \mathbb{F}_r^*} \psi(yTr(a\beta^{ja_2} + b\beta^{ja_2})) = (-1)^{i} \cdot wt(c_{a,b}) + (q - 1)(n - wt(c_{a,b})) = n(q - 1) - qwt(c_{a,b}).
\]

This takes only two values, namely \(-\lambda\) and \(-\lambda\), since \(wt(c_{a,b}) \in \{\lambda q^{k-1}, (\lambda - 1)q^{k-1}\}\). Now we compute it again in the McLiece way:

\[
\psi_a \otimes \psi_b(R) = \frac{n}{r - 1} \sum_{x \in \mathbb{F}_r^*} \psi(Tr(axa_1 + bxa_2)) = \frac{1}{v(r - 1)^2} \sum_{x \in \mathbb{F}_r^*} \sum_{y \in \mathbb{F}_r^*} \sum_{\chi, \phi} G(\chi)G(\phi)\chi^{-1}(axa_1)\phi^{-1}(bxa_2)
\]

where the last summation is over those \(\chi, \phi\) such that

\[
\chi \phi | x_r^* = 1, \quad \chi^{a_1} \phi^{a_2} = 1.
\]

Here we use \(x_0\) for the trivial character of \(\mathbb{F}_q^*\) and \(\mathbb{F}_r^*\), which we do not make a distinction. Write \(\chi = \varphi^x, \phi = \varphi^y\) (recall that \(\varphi\) is a fixed multiplicative character of order \(r - 1\)). Then the above condition is translated to

\[
i + j \equiv 0 \pmod{q - 1}, \quad a_1i + a_2j \equiv 0 \pmod{r - 1}.
\]

By exactly the same argument as in the proof of [13, Lemma 7], we see that this is equivalent to

\[
i = \frac{q - 1}{v}t, \quad j = -iw, \quad 0 \leq t \leq v\Delta - 1.
\]

We thus have

\[
\psi_a \otimes \psi_b(R) = \frac{1}{v\Delta} \sum_{t=0}^{v\Delta - 1} \sum_{i=0}^{v\Delta - 1} G(\varphi^{\frac{x_1}{q}a})G(\varphi^{\frac{x_2}{q}w})\varphi^{-\frac{1}{v\Delta}(ab^{-w})} = \frac{1}{v\Delta} \sum_{t=0}^{v\Delta - 1} G(\varphi^{\frac{x_1}{q}a})G(\varphi^{\frac{x_2}{q}w})\varphi^{-\frac{1}{v\Delta}(ab^{-w})} + \frac{1}{v\Delta}
\]

where we define

\[
B_z := \sum_{t=0}^{v\Delta - 1} G(\varphi^{\frac{x_1}{q}a})G(\varphi^{\frac{x_2}{q}w})\varphi^{-\frac{1}{v\Delta}(x)}, \quad x \in \mathbb{F}_r^*.
\]

We thus have \(B_z \in \{-r, v\Delta r\}\) for any \(x \in \mathbb{F}_r^*\), by letting \(b = 1, a = x\) above. An easy consequence is that \(r\) divides each of \(B_z, x \in \mathbb{F}_r^*\).

For each integer \(1 \leq s \leq v\Delta - 1\), we compute that

\[
\begin{align*}
\frac{1}{r - 1} \sum_{x \in \mathbb{F}_r^*} B_x \varphi^{\frac{-1}{v\Delta}x} = \frac{1}{r - 1} \sum_{x \in \mathbb{F}_r^*} \sum_{t=0}^{v\Delta - 1} G(\varphi^{\frac{x_1}{q}a})G(\varphi^{\frac{x_2}{q}w})\varphi^{-\frac{1}{v\Delta}(x)} = \frac{1}{r - 1} \sum_{x \in \mathbb{F}_r^*} \sum_{t=0}^{v\Delta - 1} G(\varphi^{\frac{x_1}{q}a})G(\varphi^{\frac{x_2}{q}w})\varphi^{-\frac{1}{v\Delta}(x)} = G(\varphi^{\frac{x_1}{q}a})G(\varphi^{\frac{x_2}{q}w}).
\end{align*}
\]

Since \(gcd(r - 1, r) = 1\) and \(r\) divides each of \(B_z, x \in \mathbb{F}_r^*\), this product is divisible by \(r\). By the properties of Gauss sums, it also has modulus \(r\).

**Remark:** The subset \(R\) here is a partial difference set in the group \((\mathbb{F}_r, +) \times (\mathbb{F}_r, +), \) c.f. [1].

**Lemma 6:** We have \(G(\varphi^{\frac{-1}{q}w}) = G(\varphi^{\frac{-1}{q}w})\eta_s\) for some root of unity \(\eta_s\), for any \(s \not\equiv 0 \pmod{v\Delta}\).

**Proof:** Define the set \(X\) as

\[
\mathbb{X}_s = \left\{ \pm \xi_{s-1}G(\varphi^{\frac{-1}{q}w}) | s, i \in \mathbb{Z}, s \not\equiv 0 \pmod{v\Delta} \right\}.
\]

Each element in the set \(X\) is divisible by \(r\) as well as has modulus \(r\) by Lemma 5. We show that this set is fixed by \(Gal(\mathbb{Q}(\xi, \xi^{r-1}/\mathbb{Q})\), so that each element of \(X\) has all its algebraic conjugates in \(X\). Let \(\sigma_{u_1, u_2}\) be the automorphism which maps \(\xi_{s} \to \xi^{u_1}, \xi_{s} \to \xi^{u_2}\), where \(gcd(p, u_1) = 1, gcd(r - 1, u_2) = 1\). For each multiplicative character \(\chi\), we have

\[
\sigma_{u_1, u_2}(G(\chi)) = \chi^{-u_2(u_1)}G(\chi^{u_1}).
\]

The verification is now routine.

Now we have shown that each element of \(X\) is divisible by \(r\) and all its algebraic conjugates have modulus \(r\). By a classical result of Kronecker (see [4]), it is equal to \(r\) times a root of unity. Since

\[
G(\chi)G(\chi^{-1}) = r, \quad G(\chi^{-1}) = (\chi(-1))G(\chi)
\]

for any nonprincipal character \(\chi\), we get the claim.

In the case \(s\) is a multiple of \(v\), the above lemma shows that \(G(\varphi^{w}) = G(\chi)\eta_s\) for some root of unity \(\eta_s\), where \(\chi\) is any nonprincipal character of \(\mathbb{F}_q^*\) which is principal on \(\mathbb{F}_q^*\).

**Lemma 7:** \(w\) is a power of \(p\) modulo \(\Delta\), i.e., \(a_1 \equiv a_2p^j \pmod{\Delta}\) for some integer \(j\).

**Proof:** Let \(G\) be the quotient group \(\mathbb{F}_r^*/\mathbb{F}_q^*\), and \(D\) be the classical Singer difference set in \(G\). Recall that for a nontrivial character \(\chi\) of \(G\), we have \([23])

\[
\chi(D) = -\frac{G(\chi)}{q}\cdot
\]

By the previous lemma, we see that \(\chi(D(w)) = \sum_{x \in D} \chi(d^x) = \chi(D)\) and \(\chi(D)\) differ by a root of unity. We shall show that \(w\) is a multiplier of \(D\), and hence by [9, Proposition 3.1.1], \(w\) is a power of \(p\) modulo \(\Delta\). The following argument is a standard trick in the proofs of various multiplier theorems.
First define $F := D^{(w)} D^{(-1)} - q^{k-2}(q-1)G \in \mathbb{Z}[G]$. For each nonprincipal character $\chi$ of $G$, we have

$$\chi(F) = \frac{G(\chi^w) G(\chi^{-1})}{q^2} = q^{k-2} \eta_\chi,$$

for some root of unity $\eta_\chi$. If $\chi_0$ is the principal character, then $\chi_0(F) = |D|^2 - q^{k-2}G = q^{k-2} \eta_{\chi_0}$, with $\eta_{\chi_0} = 1$.

Let $q$ be an element of $G$ which has nonzero coefficient in $F$. By the inversion formula, this coefficient is

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(F) \chi^{-1}(g) = q^{k-2} \sum_{\chi \in \hat{G}} \eta_\chi \chi^{-1}(g) \in \mathbb{Z}.$$

Now since $q^{k-2}$ and $|G|$ are relatively prime, $\sum_{\chi \in \hat{G}} \eta_\chi \chi^{-1}(g)$ is a rational integer. This number has modulus not exceeding 1 and not equal to zero, so is either 1 or $-1$. We deduce that $\eta_\chi = \epsilon_\chi(g)$ for each $\chi \in \hat{G}$, where $\epsilon \in \{\pm 1\}$. Since $\eta_{\chi_0} = 1$, we must have $\epsilon = 1$. Now, for any $h \in G \setminus \{g\}$, its coefficient in $F$ is equal to

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(F) \chi^{-1}(h) = \frac{q^{k-2}}{|G|} \sum_{\chi \in \hat{G}} \chi(gh^{-1}) = 0$$

by the orthogonality relation. We thus have $F = q^{k-2}g$. Comparing this with

$$D^{(w)} D^{(-1)} = q^{k-2} + q^{k-2} - 1,$$

and using the fact that $D^{(-1)}$ is invertible in the ring $\mathbb{C}[G]$, we conclude that $D^{(w)} = D_g$. Hence $w$ is a multiplier of the difference set $D$. The claim then follows.

Using Stickelberger’s theorem, we deduce from Lemma 6 that

$$s\left(\frac{q-1}{v} - wt\right) = s\left(\frac{q-1}{v} - t\right), \quad \forall t \neq 0 \pmod{v \Delta}.$$  

(1)

The set of integers $x$’s relatively prime with $v \Delta$ that satisfy the above equation with $w$ replaced by $x$ is clearly closed under multiplication, so forms a multiplicative subgroup of $\mathbb{Z}_{x\Delta}$ after taking them modulo $v \Delta$. Moreover, $p$ is such an integer.

By Lemma 7, we have $w \equiv p^i (\text{mod } \Delta)$ for some integer $0 \leq j \leq m - 1$ (here $r = p^m$). Since $v = \gcd(a_1 - a_2, q - 1)$, we naturally have $w \equiv 1 \pmod v$, recalling that $w = 1 + a_2(a_1 - a_2)$. In order to show that $w \equiv p^j \pmod{v \Delta}$, we only need to prove that $p^j \equiv 1 \pmod{v \Delta}$, using the Chinese Remainder Theorem and the fact that $\gcd(v, \Delta) = 1$.

**Lemma 8:** $w$ is a power of $p$ modulo $v \Delta$.

**Proof:** Let $d := \gcd(j, m_0)$, where $q = p^{m_0}, r = p^m = p^{m_0}$ and $j$ is the same as in the previous lemma. There exist positive integers $u_0, v_0$ such that $u_0 j + v_0 m_0 \equiv d \pmod{m}$. Define $w_0 := w^{u_0} q^{v_0} \pmod{v \Delta}$. Then Eqn. (1) also holds with $w$ replaced by $w_0$, and $w_0 \equiv 1 \pmod{v}, w_0 \equiv p^j \pmod{\Delta}$. We aim to show that $w \equiv p^j \pmod{v \Delta}$ and thus $p^j \equiv 1 \pmod{v \Delta}$, which is what we need. Let $m_0 = r o d$. Since $v | q - 1$, we only need to deal with the case $r o > 1$. The case $d = 1$ and $d > 1$ can be dealt with in much the same way, but only for clarity we deal with them separately.

First we consider the case $d = 1$. Write

$$\frac{q-1}{v} = a_0 + a_1 p + \cdots + a_{r o - 1} p^{r o - 1}, \quad 0 \leq a_i \leq p - 1.$$

If $a_0 = a_1 = \cdots = a_{r o - 1}$, then $\frac{q-1}{v}$ divides $\frac{q-1}{p^l}$, so $v | p^l$ and we are done. Assume that the $a_i$’s are not all equal. Let $i_0$ be such that $a_{i_0}$ is smallest among all $a_i$’s and $a_{i_0} < a_{i_0 + 1}$, where the subscript is taken modulo $r o$; similarly, let $j_0$ be such that $a_{j_0}$ is largest among all $a_i$’s and $a_{j_0} > a_{j_0 + 1}$. This guarantees that $a_{j_0 + 1} + 1 < p$, $a_{i_0} + 1 > 0$. Set $x := j_0 - i_0 (\text{mod } m)$. We have

$$\frac{q-1}{v} w_0^x \Delta \pmod{\Delta} = \frac{q-1}{v} \Delta,$$

which is equal to $\sum_{i=0}^{r o - 1}(a_0 + a_1 p + \cdots + a_{r o - 1} p^{r o - 1}) p^{l o}$. Take $t = \Delta + v p^{l_0} \delta$, with $0 \leq \delta \leq p - 1$ to be specified later. Then $\frac{q-1}{v} t$ is congruent to the sum of

$$(a_0 + a_1 p + \cdots + a_{r o - 1} p^{r o - 1}),$$

and $\sum_{j=0}^{r o - 1}(a_0 + a_1 p + \cdots + a_{r o - 1} p^{r o - 1}) p^{l_0} \pmod{\Delta}$. Similarly, $\frac{q-1}{v} t$ is congruent to the sum of

$$(a_0 + a_1 p + \cdots + a_{r o - 1} p^{r o - 1}),$$

and $\sum_{j=0}^{r o - 1}(a_0 + a_1 p + \cdots + a_{r o - 1} p^{r o - 1}) p^{l_0} \pmod{\Delta}$.

Now let us assume that $d > 1$. Write

$$\frac{q-1}{v} = a_0 + a_1 p^d + \cdots + a_{d-1} p^{d-1}, \quad 0 \leq a_i \leq p - 1,$$

for each $i$ we write

$$a_i = a_{i_0} + a_{i_1} p + \cdots + a_{i_d-1} p^{d-1}, \quad 0 \leq a_{i_0} \leq p - 1.$$

The idea is to show that $a_{i_0} = a_{i_1} = \cdots = a_{i_{r o - 1}}$ for each $0 \leq i \leq d - 1$, using the same argument as in the case $d = 1$. Because the proof is a slight modification of the $d = 1$ case, we do not include all the details here.

Take any $k_0 \in \{0, \cdots, d-1\}$ such that $a_{i_0} = 0 \leq i \leq r o - 1$, and not all the same. Let $i_0$ (resp. $j_0$) be such that $a_{i_0} = a_{i_0} (resp. a_{i_0} = a_{i_0} = a_{i_0} = a_{i_0}$) is smallest (resp. largest) among all $a_{i_0}$’s and $a_{i_0} = a_{i_0} = a_{i_0} = a_{i_0}$, where the first subscript is taken modulo $r o$. Let $N$ be the digit sum $s\left(\frac{q-1}{v} \Delta\right)$ before $\Delta$. Let $x := j_0 - i_0 \pmod{m}$.

Take $t = \Delta + v p^{l_1} \delta$, with $\delta$ the smallest among the numbers $a_{i_0} + 1, a_{i_0} + 1, p - a_{i_0}$, and $p - a_{i_0}$. Assume that $\delta$ occurs only once among these four values. If $\delta = a_{i_0} + 1$, then $s\left(\frac{q-1}{v} w_0^x \Delta\right) = N$, and $s\left(\frac{q-1}{v} t\right) = N + (l_1 + 1) (p - 1)$, where $l_1$ counts the number of consecutive $p - 1$’s immediately following $a_0, a_1, a_2, \cdots, a_{r o - 1} p^{r o - 1}$ in the $p$-adic expansion of $\frac{q-1}{v} \Delta + q \cdot p^{l_1} \delta \pmod{\Delta}$. Similarly,
$0 \leq l_1 \leq d - 1$. In both cases, the two digit sums are not equal, which is a contradiction. Hence $\delta = a_{0_{l_{1}}} + 1 = p - a_{0_{l_{1}}} + 1$, but in this case, $s \left( \frac{d-1}{u} \right) < N$, and $s \left( \frac{d-1}{u} \right) > N$ by arguing as in the $d = 1$ case. This is also a contradiction.

We conclude that $a_{0_{i}} = a_{1_{i}} = \cdots = a_{r_{0_{i}} - 1}$, for each $0 \leq i \leq d - 1$, and so $a_0 = a_1 = \cdots = a_{r_0 - 1}$. It follows that $p^{d - 1}$ divides $p^{d - 1} - 1$, i.e., $v$ divides $p^d - 1$. Hence $p^d \equiv 1 \pmod{v}$, and the desired congruence $w \equiv p^d \pmod{v}$ follows. This proves (4), and completes the proof of Theorem 2. $\square$

IV. CONCLUSION

In this note, we give necessary conditions for a two-weight projective cyclic code to be the direct sum of two one-weight irreducible cyclic subcodes of the same dimension, following the work of Wolfmann and Vega. In particular, these necessary conditions are also sufficient in view of Theorem 1. Based on computer search evidence, Vega [14] conjectured that all two-weight cyclic codes which are the direct sum of two one-weight irreducible cyclic subcodes of the same dimension are the known ones. Our result confirms the conjecture in the projective case.

Finally, we mention that the weight distributions of cyclic codes with two zeros $\gamma^d, \gamma^{d+D}$ were recently studied in several papers ([2], [7], [16], [22]), where $D = \frac{d-1}{e}, ed|q-1$, and $ed > 1$. These codes are never projective. It is of interest to determine the two-weight codes among all such cyclic codes. This will provide further verification to Vega’s conjecture.

ACKNOWLEDGMENTS

The author is indebted to the referees for helpful comments and suggestions which led to the current form of Theorem 2 and helped to improve the presentation of the paper.

REFERENCES