Bull. Aust. Math. Soc. **95** (2017), 157–163
doi:10.1017/S0004972716000526

ON THE SUPPORT WEIGHT DISTRIBUTION OF LINEAR CODES OVER THE RING $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{d-1}\mathbb{F}_p$

MINJIA SHI✉, JIAQI FENG, JIAN GAO, ADEL ALAHMADI and PATRICK SOLÉ

(Received 17 May 2016; accepted 21 May 2016; first published online 27 September 2016)

Abstract

Let $R = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + \cdots + u^{d-1}\mathbb{F}_p$, where $u^d = u$ and p is a prime with $d-1$ dividing $p-1$. A relation between the support weight distribution of a linear code $\mathscr{C}$ of type p^{dk} over R and the dual code $\mathscr{C}^\perp$ is established.

2010 *Mathematics subject classification*: primary 94B05; secondary 94B15.

Keywords and phrases: codes over rings, support weight, support weight distribution.

1. Introduction

The support weight distribution of codes over fields has been known for a long time [4]. Sometimes called the Wei weight [6], this natural generalisation of the weight distribution is of great interest in cryptography (for example, the attack on the wiretap channel [6]), self-dual codes [2] and finite geometry [5]. More recently, the support weight distribution of codes over the ring of integers modulo 4, the smallest commutative ring with identity that is not a field, was studied in [1]. The case of codes over a special semilocal ring was considered in [3]. In the present note we extend the results of [3] to a larger family of semilocal rings.

The material is organised as follows. The next section contains the basic notions and notations that we need. Section 3 extends some lemmas of [3] to the present situation. Section 4 contains the main result, a MacWilliams-type identity on the support weight enumerator of codes over the ring in the title.

2. Preliminaries

Denote by $\mathbb{F}_p$ the finite field of order p, with p a prime. Let $R = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + \cdots + u^{d-1}\mathbb{F}_p$, where $u^d = u$ and $d-1$ divides $p-1$. This arithmetic condition implies

This research is supported by the National Natural Science Foundation of China (61672036, 61202068 and 11526045), the Open Research Fund of the National Mobile Communications Research Laboratory, Southeast University (2015D11), Technology Foundation for Selected Overseas Chinese Scholars, Ministry of Personnel of China (05015133) and Key Projects of Support Program for Outstanding Young Talents in Colleges and Universities (gxyqZD2016008).

that the polynomial $u^d - u$ can be factored into linear factors over $\mathbb{F}_p$ as follows:

$$u^d - u = u(u - a_1)(u - a_2)\cdots(u - a_{d-1})$$

for some distinct nonzero $a_1, a_2, \ldots, a_{d-1} \in \mathbb{F}_p$. Clearly, R is a commutative ring and has $(u), (u - a_1), \ldots, (u - a_{d-1})$ as its maximal ideals, which implies that R is *finite nonlocal*. Let $a_0 = 0$ and $f_i = u - a_i$ for $i = 0, 1, \ldots, d - 1$. Let $\widehat{f_i} = (u^d - u)/f_i$. Then, for each $i = 0, 1, \ldots, d - 1$, f_i and $\widehat{f_i}$ are coprime over $\mathbb{F}_p$, which implies that there are two polynomials m_i and t_i in $\mathbb{F}_p[u]$ such that

$$m_i f_i + t_i \widehat{f_i} = 1.$$

Let $e_i = m_i f_i$ for each $i = 0, 1, \ldots, d - 1$. From the above relation, we see that e_i is an idempotent. Further, it can be shown that $e_i e_j = 0$ for any $i \neq j$ and $\sum_{i=0}^{d-1} e_i = 1$ in R. Therefore, we have the ring decomposition

$$R = e_0 R \oplus e_1 R \oplus \cdots \oplus e_{d-1} R = e_0 \mathbb{F}_p \oplus e_1 \mathbb{F}_p \oplus \cdots \oplus e_{d-1} \mathbb{F}_p.$$

Let R^n be the set of n-tuples over R. Then $R^n = e_0 \mathbb{F}_p^n \oplus e_1 \mathbb{F}_p^n \oplus \cdots \oplus e_{d-1} \mathbb{F}_p^n$. Any nonempty R-submodule $\mathscr{C}$ of R^n is called a linear code of length n over R. According to the Chinese remainder theorem, $\mathscr{C} = e_0 \mathscr{C}_1 \oplus e_1 \mathscr{C}_2 \oplus \cdots \oplus e_{d-1} \mathscr{C}_d$, where $\mathscr{C}_1, \mathscr{C}_2, \ldots, \mathscr{C}_d$ are $\mathbb{F}_p$-subspaces of $\mathbb{F}_p^n$, that is, linear codes of length n over $\mathbb{F}_p$. Therefore, $|\mathscr{C}| = |\mathscr{C}_1||\mathscr{C}_2|\cdots|\mathscr{C}_d|$. For integers $0 \leq r_i \leq n$, let $|\mathscr{C}_1| = p^{r_1}$, $|\mathscr{C}_2| = p^{r_2}, \ldots, |\mathscr{C}_d| = p^{r_d}$. Then we say that $\mathscr{C}$ is a linear code of length n over R of type $p^{r_1 + r_2 + \cdots + r_d}$.

Let $\mathscr{B} \subseteq \mathscr{C}$ be a subcode. The support of $\mathscr{B}$ is defined as

$$\chi(\mathscr{B}) = \{i \mid c_i \neq 0 \text{ for some } (c_0, c_1, \ldots, c_{n-1}) \in \mathscr{B}\}.$$

The support weight of $\mathscr{B}$ is defined as

$$w_s(\mathscr{B}) = |\chi(\mathscr{B})|.$$

For any nonnegative integers $t_1 \leq r_1, t_2 \leq r_2, \ldots, t_d \leq r_d$, let $A_i^{(t_1, t_2, \ldots, t_d)}$ be the number of subcodes of type $p^{t_1 + t_2 + \cdots + t_d}$ with support weight i. The $A_i^{(t_1, t_2, \ldots, t_d)}$th support weight distribution is the polynomial

$$A^{(t_1, t_2, \ldots, t_d)}(z) = A_0^{(t_1, t_2, \ldots, t_d)} + A_1^{(t_1, t_2, \ldots, t_d)} z + \cdots + A_n^{(t_1, t_2, \ldots, t_d)} z^n.$$

3. Some lemmas

Let $\mathscr{C}$ be a linear code of length n and type $p^{k + \cdots + k}$, written p^{dk}, over R. Let $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ be a basis of $\mathscr{C}$ over R. Then, for any $i = 1, 2, \ldots, k$, there exist words $\mathbf{b}_{ji} \in \mathbb{F}_p^n$ such that

$$\mathbf{a}_i = e_1 \mathbf{b}_{1i} + e_2 \mathbf{b}_{2i} + \cdots + e_d \mathbf{b}_{di}.$$

Let G be the generator matrix of $\mathscr{C}$ and let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$ be its rows. Then, if $\mathscr{C}$ is viewed as an $\mathbb{F}_p$-subspace, it has a generator matrix $\widehat{G}$ with successive rows

$$e_1 \mathbf{b}_{11}, e_1 \mathbf{b}_{12}, \ldots, e_1 \mathbf{b}_{1k}, e_2 \mathbf{b}_{21}, e_2 \mathbf{b}_{22}, \ldots, e_2 \mathbf{b}_{2k}, \ldots, \ldots, e_d \mathbf{b}_{d1}, e_d \mathbf{b}_{d2}, \ldots, e_d \mathbf{b}_{dk}.$$

For any subcode $C \subseteq \mathscr{C}$ of type $p^{t_1+t_2+\cdots+t_d}$, where $t_1, t_2, \ldots, t_d \le k$, define

$$\mathcal{S}_C = \{(x_1, x_2, \ldots, x_k) \in R^k \mid (x_1, x_2, \ldots, x_k)G \in C\}.$$

Clearly, $\mathcal{S}_C$ is an R-submodule of R^k. Define

$$\mathcal{F}(t_1, t_2, \ldots, t_d) = \{C \mid C \text{ is a subcode of type } p^{t_1+t_2+\cdots+t_d} \text{ of } \mathscr{C}\}$$

and

$$\mathcal{T}(t_1, t_2, \ldots, t_d) = \{\mathcal{U} \mid \mathcal{U} \text{ is a submodule of type } p^{t_1+t_2+\cdots+t_d} \text{ of } R^k\}.$$

Define the map

$$\phi : R^k \to \mathscr{C}$$
$$(x_1, x_2, \ldots, x_k) \mapsto (x_1, x_2, \ldots, x_k)G.$$

One can verify that ϕ is an R-module isomorphism. Therefore, for any nonnegative integers $t_1, t_2, \ldots, t_d \le k$, if $C \subseteq \mathscr{C}$ is a subcode of type $p^{t_1+t_2+\cdots+t_d}$, then $\mathcal{S}_C \subseteq R^k$ is an R-submodule of type $p^{t_1+t_2+\cdots+t_d}$. Moreover, the map $C \to \mathcal{S}_C$ is bijective between the set $\mathcal{F}(t_1, t_2, \ldots, t_d)$ and the set $\mathcal{T}(t_1, t_2, \ldots, t_d)$.

Let $\mathcal{S}_C$ be a linear code of length k and type $p^{t_1+t_2+\cdots+t_d}$ over R, with $t_1, t_2, \ldots, t_d \le k$. Then the dual code

$$\mathcal{S}_C^{\perp} = \{(y_1, y_2, \ldots, y_k) \in R^k \mid (y_1, \ldots, y_k) \cdot (x_1, \ldots, x_k) = 0 \text{ for any } (x_1, \ldots, x_k) \in \mathcal{S}_C\}$$

is a linear code of length k and type $p^{k-t_1} p^{k-t_2} \cdots p^{k-t_d}$ over R.

From the discussion above, the next lemma follows immediately.

Lemma 3.1. *For any nonnegative integers $t_1, t_2, \ldots, t_d \le k$, $C \to \mathcal{S}_C^{\perp}$ is a bijection between the set $\mathcal{F}(t_1, t_2, \ldots, t_d)$ and the set $\mathcal{T}(k - t_1, k - t_2, \ldots, k - t_d)$.*

For any $\mathbf{x} \in R^k$, let $\mu(\mathbf{x})$ be the number of occurrences of $\mathbf{x}$ as a column in the generator matrix G of $\mathscr{C}$. More generally, for any $S \subseteq R^k$, let $\mu(S) = \sum_{x \in S} \mu(x)$. With this notation,

$$w_s(\mathscr{C}) = n - \mu(0).$$

Lemma 3.2. *Let $C \subseteq \mathscr{C}$ be a subcode of length n over R. Then $w_s(C) = n - \mu(\mathcal{S}_C^{\perp})$.*

Proof. Let $C \subseteq \mathscr{C}$ be a subcode of length n and type $p^{t_1+t_2+\cdots+t_d}$, where $t_1, t_2, \ldots, t_d \le k$. Then $\mathcal{S}_C \subseteq R^k$ is an R-submodule of type $p^{t_1+t_2+\cdots+t_d}$. As an $\mathbb{F}_p$-subspace, let

$$\{e_1\mathbf{b}_{11}, e_1\mathbf{b}_{12}, \ldots, e_1\mathbf{b}_{1t_1}, e_2\mathbf{b}_{21}, e_2\mathbf{b}_{22}, \ldots, e_2\mathbf{b}_{2t_2}, \ldots, e_d\mathbf{b}_{d1}, e_d\mathbf{b}_{d2}, \ldots, e_d\mathbf{b}_{dt_d}\}$$

be a basis of $\mathcal{S}_C$, where $\mathbf{b}_{1i}, \mathbf{b}_{2i}, \ldots, \mathbf{b}_{di} \in \mathbb{F}_p^k$. Let M be the $(r_1 + r_2 + \cdots + r_d) \times k$ matrix the rows of which are, successively,

$$e_1\mathbf{b}_{11}, e_1\mathbf{b}_{12}, \ldots, e_1\mathbf{b}_{1t_1}, e_2\mathbf{b}_{21}, e_2\mathbf{b}_{22}, \ldots, e_2\mathbf{b}_{2t_2}, \ldots, e_d\mathbf{b}_{d1}, e_d\mathbf{b}_{d2}, \ldots, e_d\mathbf{b}_{dt_d}.$$

Then $\{e_1\mathbf{b}_{11}^{\mathrm{T}}G, e_1\mathbf{b}_{12}^{\mathrm{T}}G, \ldots, e_1\mathbf{b}_{1t_1}^{\mathrm{T}}G, e_2\mathbf{b}_{21}^{\mathrm{T}}G, e_2\mathbf{b}_{22}^{\mathrm{T}}G, \ldots, e_2\mathbf{b}_{2t_2}^{\mathrm{T}}G, \ldots, e_d\mathbf{b}_{d1}^{\mathrm{T}}G, e_d\mathbf{b}_{d2}^{\mathrm{T}}G, \ldots, e_d\mathbf{b}_{dt_d}^{\mathrm{T}}G\}$ forms an $\mathbb{F}_p$-basis of C. Therefore, MG is a generator matrix of C, which implies that

$$w_s(C) = n - \sum_{M\mathbf{x}=0} \mu(x) = n - \sum_{\mathbf{x} \in \mathcal{S}_C^{\perp}} \mu(x) = n - \mu(\mathcal{S}_C^{\perp}).$$

□

https://doi.org/10.1017/S0004972716000526 Published online by Cambridge University Press

Let

$$[m]_{c_1,c_2,\dots,c_d} = \prod_{i_1=0}^{c_1-1}(p^m - p^{i_1}) \prod_{i_2=0}^{c_2-1}(p^m - p^{i_2}) \cdots \prod_{i_d=0}^{c_d-1}(p^m - p^{i_d}).$$

We make the convention that, for any integer a, the product $\prod_{i=0}^{a-1}(p^m - p^i) = 1$ if $a = 0$. Denote by $\mathrm{GR}(R, m) = e_1\mathbb{F}_{p^m} + e_2\mathbb{F}_{p^m} + \cdots + e_{d-1}\mathbb{F}_{p^m}$ the mth Galois extension ring of R. Let ξ be a primitive element of the finite field $\mathbb{F}_{p^m}$. Then, for any element $r \in \mathrm{GR}(R, m)$, r can be expressed uniquely as

$$r = r_0 + r_1\xi + \cdots + r_{m-1}\xi^{m-1},$$

where $r_0, r_1, \dots, r_{m-1} \in R$.

Lemma 3.3. *Let $\mathcal{U} \subseteq R^k$ be an R-module of type $p^{t_1+t_2+\cdots+t_d}$ and $\widehat{\mathcal{U}} = \{\mathbf{y} \in \mathrm{GR}(R, m) \mid \mathbf{y} \cdot \mathbf{x} = 0$ for $\mathbf{x} \in R^k$ if and only if $\mathbf{x} \in \mathcal{U}\}$. Then*

(i) $|\widehat{\mathcal{U}}| = [m]_{k-t_1,k-t_2,\dots,k-t_d}$;

(ii) $\{\widehat{\mathcal{U}} \mid \mathcal{U}$ *is a submodule of* $R^k\}$ *is a partition of* $\mathrm{GR}(R, m)^k$.

Proof. (i) This follows from the proof technique of [4, Lemma 3].

(ii) From the definition of $\widehat{\mathcal{U}}$, we have that if $\mathcal{U}_1 \neq \mathcal{U}_2$, then $\widehat{\mathcal{U}}_1 \cap \widehat{\mathcal{U}}_2 = \emptyset$. For any $(y_1, y_2, \dots, y_n) \in \mathrm{GR}(R, m)^k$, define

$$\mathcal{U} = \{(x_1, x_2, \dots, x_k) \in R^k \mid (x_1, x_2, \dots, x_k) \cdot (y_1, y_2, \dots, y_k) = 0\}.$$

Then $\mathcal{U}$ is an R-submodule of R^k and $(y_1, y_2, \dots, y_k) \in \widehat{\mathcal{U}}$, which implies that $\{\widehat{\mathcal{U}} \mid \mathcal{U}$ is a submodule of $R^k\}$ is a partition of $\mathrm{GR}(R, m)^k$. □

Similar to [1, Lemma 7], we also have the following result. We omit the proof.

Lemma 3.4. *If $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_k \in R^k$ are free over R, then $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_k$ are free over* $\mathrm{GR}(R, m)$.

4. Main results

Recall that $\mathscr{C}$ is a linear code of length n and type p^{dk} over R, and that $\{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_k\}$ is the basis of $\mathscr{C}$ with G as its generator matrix. Let $\mathscr{C}^{(m)}$ denote the linear code over $\mathrm{GR}(R, m)$ with generator matrix G.

Proposition 4.1. *The Hamming weight enumerator of $\mathscr{C}^{(m)}$ is*

$$W_H(z) = \sum_{t_1=0}^{m} \sum_{t_2=0}^{m} \cdots \sum_{t_d=0}^{m} [m]_{t_1,t_2,\dots,t_d} A^{(t_1,t_2,\dots,t_d)}(z).$$

Proof. From Lemma 3.4, for any $\mathbf{y}_1, \mathbf{y}_2 \in \mathrm{GR}(R, m)^k$ such that $\mathbf{y}_1 \neq \mathbf{y}_2$, we know that $\mathbf{y}_1 G \neq \mathbf{y}_2 G$, implying that $W_H(z) = \sum_{\mathbf{y}\in \mathrm{GR}(R,m)^k} z^{w(\mathbf{y}G)}$. From Lemma 3.3(ii),

$$W_H(z) = \sum_{t_1=0}^{k} \sum_{t_2=0}^{k} \cdots \sum_{t_d=0}^{k} \sum_{\mathcal{U}\in\mathcal{T}(t_1,t_2,\dots,t_d)} \sum_{\mathbf{y}\in\widehat{\mathcal{U}}} z^{w(\mathbf{y}G)}.$$

https://doi.org/10.1017/S0004972716000526 Published online by Cambridge University Press

For $\mathbf{y} \in \widehat{\mathcal{U}}$,

$$w(\mathbf{y}G) = \sum_{\mathbf{x}\in R^k} \mu(\mathbf{x}) w(\mathbf{y}\cdot\mathbf{x}) = n - \sum_{\mathbf{x}\in\mathcal{U}} \mu(\mathbf{x}) = n - \mu(\mathcal{U}).$$

Therefore,

$$\begin{aligned} W_H(z) &= \sum_{t_1=0}^{k}\sum_{t_2=0}^{k}\cdots\sum_{t_d=0}^{k}\sum_{\mathcal{U}\in\mathcal{T}(t_1,t_2,\ldots,t_d)}\sum_{\mathbf{y}\in\widehat{\mathcal{U}}} z^{n-\mu(\mathcal{U})} \\ &= \sum_{t_1=0}^{k}\sum_{t_2=0}^{k}\cdots\sum_{t_d=0}^{k}\sum_{\mathcal{U}\in\mathcal{T}(t_1,t_2,\ldots,t_d)} [m]_{k-t_1,k-t_2,\ldots,k-t_d} z^{n-\mu(\mathcal{U})} \\ &= \sum_{t_1=0}^{k}\sum_{t_2=0}^{k}\cdots\sum_{t_d=0}^{k}\sum_{\mathcal{U}\in\mathcal{T}(k-t_1,k-t_2,\ldots,k-t_d)} [m]_{t_1,t_2,\ldots,t_d} z^{n-\mu(\mathcal{U})} \end{aligned}$$

From Lemmas 3.1 and 3.2,

$$\sum_{\mathcal{U}\in\mathcal{T}(k-t_1,k-t_2,\ldots,k-t_d)} z^{n-\mu(\mathcal{U})} = \sum_{C\in\mathcal{F}(t_1,t_2,\ldots,t_d)} z^{n-\mu(\mathcal{S}_C^{\perp})} = \sum_{C\in\mathcal{F}(t_1,t_2,\ldots,t_d)} z^{w_s(C)} = A^{(t_1,t_2,\ldots,t_d)}(z),$$

which implies that

$$W_H(z) = \sum_{t_1=0}^{k}\sum_{t_2=0}^{k}\cdots\sum_{t_d=0}^{k}[m]_{t_1,t_2,\ldots,t_d} A^{(t_1,t_2,\ldots,t_d)}(z).$$

If $m \le k$ and $t_1, t_2, \ldots, t_d > m$, then $[m]_{t_1,t_2,\ldots,t_d} = 0$. If $m > k$ and $t_1, t_2, \ldots, t_d > k$, then $A^{(t_1,t_2,\ldots,t_d)} = 0$. Putting everything together,

$$\begin{aligned} W_H(z) &= \sum_{t_1=0}^{k}\sum_{t_2=0}^{k}\cdots\sum_{t_d=0}^{k}[m]_{t_1,t_2,\ldots,t_d} A^{(t_1,t_2,\ldots,t_d)}(z) \\ &= \sum_{t_1=0}^{m}\sum_{t_2=0}^{m}\cdots\sum_{t_d=0}^{m}[m]_{t_1,t_2,\ldots,t_d} A^{(t_1,t_2,\ldots,t_d)}(z). \end{aligned}$$ □

Let $\mathscr{C}^{\perp} \subseteq R^n$ be the dual code of $\mathscr{C}$ and $(\mathscr{C}^{(m)})^{\perp} \subseteq \mathrm{GR}(R, m)^n$ be the dual code of $\mathscr{C}^{(m)}$. Clearly, $(\mathscr{C}^{(m)})^{\perp}$ is also generated over $GR(R, m)$ by the parity-check matrix of $\mathscr{C}$. Denote by $W_H^m(z)$ the Hamming weight enumerator of $(\mathscr{C}^{(m)})^{\perp}$ and by $B^{(t_1,t_2,\ldots,t_d)}(z)$ the $(t_1, t_2, \ldots, t_d)$th support weight distribution of $\mathscr{C}^{\perp}$. Then, by Proposition 4.1,

$$W_H^m(z) = \sum_{t_1=0}^{m}\sum_{t_2=0}^{m}\cdots\sum_{t_d=0}^{m}[m]_{t_1,t_2,\ldots,t_d} B^{(t_1,t_2,\ldots,t_d)}(z). \tag{4.1}$$

Theorem 4.2. *For all $m \ge 1$,*

$$\begin{aligned} &\sum_{t_1=0}^{m}\sum_{t_2=0}^{m}\cdots\sum_{t_d=0}^{m}[m]_{t_1,t_2,\ldots,t_d} B^{(t_1,t_2,\ldots,t_d)}(z) \\ &\quad = \frac{1}{p^{dmk}}(1 + (p^{dm}-1)z)^n \sum_{t_1=0}^{m}\sum_{t_2=0}^{m}\cdots\sum_{t_d=0}^{m}[m]_{t_1,t_2,\ldots,t_d} A^{(t_1,t_2,\ldots,t_d)}\Big(\frac{1-z}{1+(p^{dm}-1)z}\Big). \end{aligned}$$

PROOF. Using the underlying additive group structure of the ring $\mathrm{GR}(R, m)$, we can write the following MacWilliams-type identity for the Hamming weight enumerator of the linear code $\mathscr{C}^{(m)}$ over that ring:

$$\mathrm{Ham}_{(\mathscr{C}^{(m)})^{\perp}}(x, z) = \frac{1}{|\mathscr{C}^{(m)}|}\mathrm{Ham}_{\mathscr{C}^{(m)}}(x + (p^{dm} - 1)z, x - z).$$

From this,

$$W_H^m(z) = \frac{1}{|\mathscr{C}^{(m)}|}(1 + (p^{dm} - 1)z)^n W_H\Big(\frac{1 - z}{1 + (p^{dm} - 1)z}\Big). \tag{4.2}$$

Substituting (4.2) into (4.1), the result follows. □

EXAMPLE 4.3. Assume that $p = d = 2$ and consider the code of length 2 obtained by taking the Cartesian product $C = R_2 \times R_2$, where R_2 is the repetition code of length 2, that is, $R_2 = \{00, 11\}$. By inspection,

$$\begin{aligned} B^{0,0} &= 1, \\ B^{1,0} &= 2z^2, \\ B^{0,1} &= 2z^2, \\ B^{1,1} &= z^2, \end{aligned}$$

while the definition of $[m]_{a,b}$ from above yields

$$[1]_{0,0} = [1]_{1,0} = [1]_{0,1} = [1]_{1,1} = 1,$$

leading to $W_H(z) = 1 + 3z^2 = B(z)$. Since C is self-dual, the polynomial $B(z)$ must be a fixed point of the MacWilliams transform. It can be checked by hand that equation (4.2) reduces to

$$(1 + 3z)^2 B\Big(\frac{1 - z}{1 + 3z}\Big) = |C|B(z) = 4 + 12z^2.$$

References

[1] J. Cui, 'Support weight distribution of $\mathbb{Z}_4$-linear codes', *Discrete Math.* **247** (2002), 135–145.

[2] S. Dougherty, A. Gulliver and M. Oura, 'Higher weights and graded rings for binary self-dual codes', *Discrete Appl. Math.* **128** (2003), 251–261.

[3] J. Gao, 'Note on support weight distribution of linear codes over $\mathbb{F}_p + u\mathbb{F}_p$', *Bull. Aust. Math. Soc.* **91** (2015), 345–350.

[4] T. Kløve, 'Support weight distribution of linear codes', *Discrete Math.* **106** (1992), 311–316.

[5] J. Simonis, 'The effective length of subcodes', *Applic. Algebra Eng. Common. Computing* **5** (1992), 371–377.

[6] V. K. Wei, 'Generalized Hamming weights for linear codes', *IEEE Trans. Inform. Theory* **37** (1991), 1412–1418.

https://doi.org/10.1017/S0004972716000526 Published online by Cambridge University Press

MINJIA SHI, Key Laboratory of Intelligent
Computing and Signal Processing, Ministry of Education,
Anhui University, No. 3 Feixi Road, Hefei,
Anhui Province 230039, PR China
and
National Mobile Communications Research Laboratory,
Southeast University, Nanjing 210096, PR China
and
School of Mathematical Sciences, Anhui University,
Hefei, Anhui 230601, PR China
e-mail: smjwcl.good@163.com

JIAQI FENG, School of Mathematical Sciences,
Anhui University, Hefei, Anhui 230601, PR China
e-mail: FengJQ1995@163.com

JIAN GAO, School of Science,
Shandong University of Technology, Zibo 255091, PR China
e-mail: jiangao@mail.nankai.edu.cn

ADEL ALAHMADI, Mathematics Department,
King Abdulaziz University, Jeddah, Saudi Arabia
e-mail: adelnife2@yahoo.com

PATRICK SOLÉ, CNRS/LTCI,
University of Paris-Saclay, 75013 Paris, France
e-mail: patrick.sole@telecom-paristech.fr