Bull. Aust. Math. Soc. **91** (2015), 345–350
doi:10.1017/S0004972715000052

NOTE ON SUPPORT WEIGHT DISTRIBUTION OF LINEAR CODES OVER $\mathbb{F}_p + u\mathbb{F}_p$

JIAN GAO

(Received 20 June 2014; accepted 22 December 2014)

Abstract

Let $R = \mathbb{F}_p + u\mathbb{F}_p$, where $u^2 = u$. A relation between the support weight distribution of a linear code $\mathscr{C}$ of type p^{2k} over R and its dual code $\mathscr{C}^\perp$ is established.

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

Keywords and phrases: finite nonchain ring, support weight, support weight distribution.

1. Introduction

Let $R = \mathbb{F}_p + u\mathbb{F}_p$, where $u^2 = u$. Then R is a commutative ring and has ideals (u) and $(1-u)$ as its maximal ideals, which implies that R is a *finite nonchain ring*. By the Chinese remainder theorem, we have that $R = uR \oplus (1-u)R = u\mathbb{F}_p \oplus (1-u)\mathbb{F}_p$. Let R^n be the set of n-tuples over R. Then $R^n = u\mathbb{F}_p^n \oplus (1-u)\mathbb{F}_p^n$. 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, $\mathscr{C} = u\mathscr{C}_1 \oplus (1-u)\mathscr{C}_2$, where $\mathscr{C}_1$ and $\mathscr{C}_2$ are $\mathbb{F}_p$-subspaces of $\mathbb{F}_p^n$, that is, linear codes of length n over $\mathbb{F}_p$. Therefore, we have that $|\mathscr{C}| = |\mathscr{C}_1||\mathscr{C}_2|$. Let $|\mathscr{C}_1| = p^{r_1}$ and $|\mathscr{C}_2| = p^{r_2}$. Then we say that $\mathscr{C}$ is a linear code of length n over R of *type* $p^{r_1+r_2}$.

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 $t_1 \leq r_1$ and $t_2 \leq r_2$, let $A_i^{(t_1,t_2)}$ be the number of subcodes of type $p^{t_1+t_2}$ with support weight i. The (t_1, t_2)th support weight distribution is the polynomial

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

Wei [6] introduced the notion of generalised Hamming weights, that is, the support weights in his analysis of the wire-tap channel of type II. His paper has sparked renewed interest in the subject, indicating its importance in both the theory and the applications of coding theory. Kløve [4] gave the relation between the support weight distribution of a linear code over the finite field $\mathbb{F}_q$ and that of its dual code. Simonis [5] gave another method for deriving the relation obtained in [4]. Following the approaches given in [4] and [5], Cui [1, 2] obtained the relation between the support weight distribution of a linear code over the ring $\mathbb{Z}_4$ and that of its dual code.

Recently, much work on the coding theory over the finite nonchain ring $\mathbb{F}_p + u\mathbb{F}_p$ has appeared (see, for example, [3, 7, 8]). It is natural to ask if there is similar relation between the support weight distribution of a linear code over the ring $\mathbb{F}_p + u\mathbb{F}_p$ and that of its dual code. The goal of this short note is to give such a relation.

2. Some lemmas

Let $\mathscr{C}$ be a linear code of length n and type p^{2k} over R. Let $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ be a free basis of $\mathscr{C}$ over R. Then, for any $i = 1, 2, \ldots, k$, there exist $\mathbf{b}_i, \mathbf{c}_i \in \mathbb{F}_p^n$ such that $\mathbf{a}_i = u\mathbf{b}_i + (1-u)\mathbf{c}_i$. Let

$$G = \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_k \end{pmatrix}$$

be the generator matrix of $\mathscr{C}$. If $\mathscr{C}$ has an $\mathbb{F}_p$-subspace, it has the following matrix as its generator matrix:

$$\widehat{G} = \begin{pmatrix} u\mathbf{b}_1 \\ u\mathbf{b}_2 \\ \vdots \\ u\mathbf{b}_k \\ (1-u)\mathbf{c}_1 \\ (1-u)\mathbf{c}_2 \\ \vdots \\ (1-u)\mathbf{c}_k \end{pmatrix}.$$

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

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

and

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

https://doi.org/10.1017/S0004972715000052 Published online by Cambridge University Press

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 $t_1, t_2 \le k$, if $C \subseteq \mathscr{C}$ is a subcode of type $p^{t_1+t_2}$, then $\mathcal{S}_C \subseteq R^k$ is an R-submodule of type $p^{t_1+t_2}$. Moreover, the map $C \to \mathcal{S}_C$ is bijective between the set $\mathcal{F}(t_1, t_2)$ and the set $\mathcal{T}(t_1, t_2)$.

Let $\mathcal{S}_C$ be a linear code of length k and type $p^{t_1+t_2}$ over R, where $t_1, t_2 \le k$. 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 $p^{k-t_1}p^{k-t_2} = p^{2k-t_1-t_2}$ over R.

The above discussion immediately gives the following lemma.

Lemma 2.1. *For any nonnegative integers $t_1, t_2 \le k$, $C \to \mathcal{S}_C^{\perp}$ is a bijection between the set $\mathcal{F}(t_1, t_2)$ and the set $\mathcal{T}(k - t_1, k - t_2)$.*

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 $\mathscr{C}$. Then

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

Lemma 2.2. *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 $p^{t_1+t_2}$, where $t_1, t_2 \le k$. Then $\mathcal{S}_C \subseteq R^k$ is an R-submodule of type $p^{t_1+t_2}$. As an $\mathbb{F}_p$-subspace, let

$$\{u\mathbf{b}_1, u\mathbf{b}_2, \ldots, u\mathbf{b}_{t_1}, (1-u)\mathbf{c}_1, (1-u)\mathbf{c}_2, \ldots, (1-u)\mathbf{c}_{t_2}\} \tag{2.1}$$

be a basis of $\mathcal{S}_C$, where $\mathbf{b}_i$ and $\mathbf{c}_j \in \mathbb{F}_p^k$. Let M be the $(t_1 + t_2) \times k$ matrix whose rows are the transposes, $u\mathbf{b}_1^{\mathrm{T}}, \ldots, (1-u)\mathbf{c}_{t_2}^{\mathrm{T}}$, of the column vectors in (2.1). Then the columns of the matrix

$$MG = \{u\mathbf{b}_1^{\mathrm{T}}G, u\mathbf{b}_2^{\mathrm{T}}G, \ldots, u\mathbf{b}_{t_1}^{\mathrm{T}}G, (1-u)\mathbf{c}_1^{\mathrm{T}}G, (1-u)\mathbf{c}_2^{\mathrm{T}}G, (1-u)\mathbf{c}_{t_2}^{\mathrm{T}}G\}$$

form an $\mathbb{F}_p$-basis of C and MG is a generator matrix of C, which implies that

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

□

https://doi.org/10.1017/S0004972715000052 Published online by Cambridge University Press

Let

$$[m]_{a,b} = \prod_{i=0}^{a-1}(p^m - p^i)\prod_{j=0}^{b-1}(p^m - p^j).$$

We make the convention that $\prod_{i=0}^{a-1}(p^m - p^i) = 1$ if $a = 0$ and that $\prod_{j=0}^{b-1}(p^m - p^j) = 1$ if $b = 0$. Denote by $\mathrm{GR}(R, m) = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ the mth Galois extension ring of R. Let ξ be a primitive element of the finite field $\mathbb{F}_{p^m}$. Any element $r \in \mathrm{GR}(R, m)$ can be expressed uniquely as

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

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

Lemma 2.3. *Let $\mathcal{U} \subseteq R^k$ be an R-module of type $p^{t_1+t_2}$ 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) $|\widehat{\mathcal{U}}| = [m]_{k-t_1,k-t_2}$.

(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 process of Lemma 3 in [4].

(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 $(y_1, y_2, \ldots, y_n) \in \mathrm{GR}(R, m)^k$, define

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

Then $\mathcal{U}$ is an R-submodule of R^k and $(y_1, y_2, \ldots, y_k) \in \widehat{\mathcal{U}}$, 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.

Lemma 2.4. *If $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in R^k$ are free over R, then $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$ are free over* $\mathrm{GR}(R, m)$.

3. Main results

Recall that $\mathscr{C}$ is a linear code of length n and type p^{2k} over R, and $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ is the free basis of $\mathscr{C}$ with G as its generator matrix. Denote by $\mathcal{D}$ the linear code over $\mathrm{GR}(R, m)$ with generator matrix G.

Proposition 3.1. *The Hamming weight enumerator of $\mathcal{D}$ is*

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

Proof. From Lemma 2.4, we know that for any $\mathbf{y}_1, \mathbf{y}_2 \in \mathrm{GR}(R, m)^k$ with $\mathbf{y}_1 \neq \mathbf{y}_2$, we have $\mathbf{y}_1 G \neq \mathbf{y}_2 G$, whence $W_H(z) = \sum_{\mathbf{y}\in\mathrm{GR}(R,m)^k} z^{w(\mathbf{y}G)}$. From Lemma 2.3(ii),

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

https://doi.org/10.1017/S0004972715000052 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,

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

From Lemmas 2.1 and 2.2,

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

which implies that

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

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

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

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 by the parity-check matrix of $\mathscr{C}$. Denote by $W_H^m(z)$ the Hamming weight enumerator of $(\mathscr{C}^{(m)})^{\perp}$ and $B^{(t_1,t_2)}(z)$ the (t_1,t_2)th support weight distribution of $\mathscr{C}^{\perp}$. Then, by Proposition 3.1,

$$W_H^m(z) = \sum_{t_1=0}^{m}\sum_{t_2=0}^{m} [m]_{t_1,t_2} B^{(t_1,t_2)}(z). \tag{3.1}$$

THEOREM 3.2. *For all $m \ge 1$,*

$$\sum_{t_1=0}^{m}\sum_{t_2=0}^{m} [m]_{t_1,t_2} B^{(t_1,t_2)}(z) = \frac{1}{p^{2mk}}(1 + (p^{2m}-1)z)^n \sum_{t_1=0}^{m}\sum_{t_2=0}^{m} [m]_{t_1,t_2} A^{(t_1,t_2)}\Big(\frac{1-z}{1+(p^{2m}-1)z}\Big).$$

https://doi.org/10.1017/S0004972715000052 Published online by Cambridge University Press

PROOF. Recall the MacWilliams-type identity for the Hamming weight of the linear code over GR(R, m):

$$\mathrm{Ham}_{(\mathscr{C}^{(m)})^{\perp}}(x, z) = \frac{1}{|\mathscr{C}^{(m)}|}\mathrm{Ham}_{\mathscr{C}^{(m)}}(x + (p^{2m} - 1)z, x - z).$$

From this identity,

$$W_H^m(z) = \frac{1}{|\mathscr{C}^{(m)}|}(1 + (p^{2m} - 1)z)^n W_H\Big(\frac{1 - z}{1 + (p^{2m} - 1)z}\Big) \tag{3.2}$$

and the desired result follows by substituting (3.2) into (3.1). □

Acknowledgements

This research is supported by the National Key Basic Research Program of China (Grant No. 2013CB834204) and the National Natural Science Foundation of China (Grant No. 61171082).

References

[1] J. Cui, 'Support weight distribution of $\mathbb{Z}_4$-linear codes', *Discrete Math.* **247** (2002), 135–145.
[2] J. Cui and J. Pei, 'Generalized MacWilliams identities for $\mathbb{Z}_4$-linear codes', *IEEE Trans. Inform. Theory* **50** (2004), 3302–3305.
[3] A. Kaya, B. Yildiz and I. Siap, 'Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p$ and their Gray images', *J. Pure Appl. Algebra* **218** (2014), 1999–2011.
[4] T. Kløve, 'Support weight distribution of linear codes', *Discrete Math.* **106** (1992), 311–316.
[5] J. Simonis, 'The effective length of subcodes', *Appl. Algebra Engrg. Comm. Comput.* **5** (1992), 371–377.
[6] V. K. Wei, 'Generalized Hamming weights for linear codes', *IEEE Trans. Inform. Theory* **37** (1991), 1412–1418.
[7] S. Zhu and L. Wang, 'A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image', *Discrete Math.* **311** (2011), 2677–2682.
[8] S. Zhu, Y. Wang and M. Shi, 'Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$', *IEEE Trans. Inform. Theory* **56** (2010), 1680–1684.

JIAN GAO, Chern Institute of Mathematics and LPMC,
Nankai University, China
e-mail: dezhougaojian@163.com