Journal of Algebraic Combinatorics **12** (2000), 95–99

Singleton Bounds for Codes over Finite Rings*

KEISUKE SHIROMOTO keisuke@math.sci.kumamoto-u.ac.jp
Department of Mathematics, Kumamoto University, 2-39-1, Kurokami, Kumamoto 860-8555, Japan

Received April 22, 1998; Revised May 6, 1999

Abstract. We introduce the Singleton bounds for codes over a finite commutative quasi-Frobenius ring.

Keywords: code, QF ring, module, bound, support, weight

1. Introduction

Let R be a finite commutative quasi-Frobenius (QF) ring (see [1]), and let $V := R^n$ be the free module of rank n consisting of all n-tuples of elements of R. A *code* C of length n over R is an R-submodule of V. An element of C is called a *codeword* of C.

In this paper, we will use a general notion of weight, abstracted from the Hamming, the Lee and the Euclidean weights. For every $x = (x_1, \dots, x_n) \in V$ and $r \in R$, the *complete weight* of x is defined by

$$n_r(x) := |\{i \mid x_i = r\}|.$$

To define a *general weight function* $w(x)$, let a_r, $(0 \neq)r \in R$, be positive real numbers, and set $a_0 = 0$. Set

$$w(x) := \sum_{r \in R} a_r n_r(x). \tag{1}$$

If we set $a_r = 1$, $(0 \neq)\forall r \in R$, then $w(x)$ is just the Hamming weight of x. For later use, we denote

$$A := \max\{a_r \mid r \in R\}. \tag{2}$$

For example, if $R = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, then setting $a_1 = a_3 = 1$ and $a_2 = 2$ yields the Lee weight, while setting $a_1 = a_3 = 1$ and $a_2 = 4$ yields the Euclidean weight.

Put $N := \{1, 2, \dots, n\}$. Define the *support* $\mathrm{supp}(x)$ of a vector $x = (x_1, \dots, x_n) \in V$ by

$$\mathrm{supp}(x) := \{i \in N \mid x_i \neq 0\}.$$

*Supported in part by the Japan Society for the Promotion of Science.

The *minimum weight* of a code C, denoted by d, is

$$d := \min\{w(x) \mid (0 \neq)x \in C\}.$$

We make the important (and elementary) observation that

$$w(x) \leq A|\mathrm{supp}(x)|. \tag{3}$$

The *inner product* of vectors $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in V$ is defined by

$$\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n.$$

The *dual code* of C is defined by

$$C^{\perp} := \{y \in V \mid \langle x, y\rangle = 0 \quad (\forall x \in C)\}.$$

The following proposition is well-known as the Singleton bound (see [4]).

Proposition 1 *Let C be a linear $[n, k, d]$-code over $GF(q)$, where d is the minimum Hamming weight of C. Then*,

$$d \leq n - k + 1.$$

The main purpose of this paper is to find a similar bound for the minimum weight of a general weight function $w(x)$ over R.

2. Singleton bound

For a submodule D of V and a subset $M \subseteq N = \{1, 2, \ldots, n\}$, let

$$D(M) := \{x \in D \mid \mathrm{supp}(x) \subseteq M\},$$
$$D^* := \mathrm{Hom}_R(D, R).$$

Clearly $D(M) = D \cap V(M)$ is a submodule of V, and $|V(M)| = |R|^{|M|}$. It is also the case that $|D| = |D^*|$ for any submodule of V. The following lemma is essential. (There is a similar result over $GF(q)$ in [6]).

Lemma 1 *Let C be a code of length n over R and $M \subseteq N$. Then there is an exact sequence of R-modules*:

$$0 \to C^{\perp}(M) \xrightarrow{\mathrm{inc}} V(M) \xrightarrow{f} C^* \xrightarrow{\mathrm{res}} C(N - M)^* \to 0,$$

where the maps inc, res *denote the inclusion map*, *restriction map*, *respectively*, *and the map f is defined by*

$$f : y \mapsto (\hat{y} : x \mapsto \langle x, y\rangle).$$

Proof: The exactness of the sequence at $C^{\perp}(M)$ and at $V(M)$ is clear. That the map res is surjective follows from R being an injective module over itself (the meaning of R being QF).

Clearly we note that $\mathrm{Im}\, f \subseteq \ker(\mathrm{res})$. Conversely, if we take any $\lambda \in \ker(\mathrm{res})$, then

$$\lambda(x) = 0 \quad (\forall x \in C(N - M)).$$

Note that $V \to C^*; v \mapsto \hat{v}$ is surjective, so there exists $y \in V$ with $\lambda = \hat{y}$. For any $x \in C(N - M)$, $\langle x, y\rangle = 0$, so that,

$$\begin{aligned} y &\in (C(N - M))^{\perp} = (C \cap V(N - M))^{\perp} \\ &= C^{\perp} + V(N - M)^{\perp} = C^{\perp} + V(M). \end{aligned}$$

Since $\hat{z} = 0$ for any $z \in C^{\perp}$, we have

$$\ker(\mathrm{res}) \subseteq \mathrm{Im}\, f.$$

Thus the sequence is also exact at C^*, and the lemma follows. □

We remark that we can prove the MacWilliams identity for codes over $\mathbb{Z}_4$ ([3]) by using Lemma 1 (there are similar results over $GF(q)$ in [5] and [6]).

Using the above lemma, we establish the Singleton bound for a general weight function over R.

Theorem 1 *Let C be a code of length n over a finite commutative QF ring R. Let $w(x)$ be a general weight function on C, as in* (1), *and with maximum a_r-value A, as in* (2). *Suppose the minimum weight of $w(x)$ on C is d. Then*

$$\left[\frac{d-1}{A}\right] \leq n - \log_{|R|} |C|,$$

where $[b]$ is the integer part of b.

Proof: By Lemma 1, we have

$$|C| \cdot |C^{\perp}(N - \tilde{M})| = |V(N - \tilde{M})| \cdot |C(\tilde{M})|,$$

where $\tilde{M} = N - M$. If we take a subset M of N with $|\tilde{M}| = [\frac{d-1}{A}]$, then $|C(\tilde{M})| = 1$ by (3). Since we always have $|C^{\perp}(N - \tilde{M})| \geq 1$, we see that

$$|C| \leq |V(N - \tilde{M})| = |R|^{|N - \tilde{M}|}.$$

Hence the theorem follows. □

3. An application to codes over $\mathbb{Z}_l$

The ring $R = \mathbb{Z}_l$ is a good example of a finite commutative QF ring. Let $k := [l/2]$, and regard $\mathbb{Z}_l$ as the set $\{0, \pm 1, \ldots, \pm k\}$ (with $k = -k$, when $l = 2k$ is even). On codes over $\mathbb{Z}_l$, there are three special weight functions:

1. the *Hamming weight*, where each $a_i = 1$, $i \neq 0$,
2. the *Lee weight*, where $a_i = |i|$, and
3. the *Euclidean weight*, where $a_i = |i|^2$.

Denote the minimum weight of a code C with respect to these three weights by d_H, d_L and d_E, respectively. It is clear that the maximum a_r-value A is 1, k and k^2, respectively. The next result follows immediately from Theorem 1.

Theorem 2 *Using the above notation for a code C of length n over $\mathbb{Z}_l$, there are the following bounds on minimum weights*:

$$d_H \leq n - \log_l |C| + 1,$$
$$\left\lceil \frac{d_L - 1}{k} \right\rceil \leq n - \log_l |C|,$$
$$\left\lceil \frac{d_E - 1}{k^2} \right\rceil \leq n - \log_l |C|.$$

The Gray map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ is defined by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, and $\phi(3) = 10$. It is well-known that ϕ is a weight-preserving map from ($\mathbb{Z}_4^n$, Lee weight) to ($\mathbb{Z}_2^{2n}$, Hamming weight) (see [2]). Using the above theorem, we have the Singleton bound for certain binary nonlinear codes.

Corollary 1 *If a binary nonlinear $(2n, M, d)$-code B, where $M := |B|$ and d is the minimum Hamming weight of B, is the Gray map image of a code C of length n over $\mathbb{Z}_4$, then*

$$\left\lceil \frac{d - 1}{2} \right\rceil \leq n - \log_4 M.$$

Proof: Since $M = |C|$ and d is also the minimum Lee weight of C, the corollary follows from Theorem 2. □

Acknowledgment

The author would like to thank the referee for his helpful advice on QF rings and general weight functions and other helpful suggestions. The author would like to thank adviser Professor Tomoyuki Yoshida for his helpful suggestions and Dr. Masaaki Harada for his helpful comments on codes over $\mathbb{Z}_4$.

References

1. C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, New York, 1962.
2. A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory* **40** (1994), 301–319.
3. M. Klemm, "Über die Identität von MacWilliams für die Gewichtsfunktion von Codes," *Arch. Math.* **49** (1987), 400–406.
4. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.
5. K. Shiromoto, "A new MacWilliams type identity for linear codes," *Hokkaido Math. J*. **25** (1996), 651–656.
6. T. Yoshida, "MacWilliams identities for linear codes with group action," *Kumamoto Math. J*. **6** (1993), 29–45.