# Highly symmetric weight functions on matrix rings

Jay A. Wood
Western Michigan University
1903 W. Michigan Ave.
Kalamazoo, MI 49008
http://homepages.wmich.edu/∼jwood
jay.wood@wmich.edu

AMS Sectional Meeting
Evanston, IL
October 23, 2004

For which rings $R$ and weight functions $w$ on $R$ does the extension theorem of MacWilliams hold?

Summary of concepts

Summary of earlier results

Case of matrix rings over finite fields

Linear codes over finite rings

Let $R$ be a finite ring with 1. (Later: $R = M_n(\mathbb{F}_q)$.) Let $\mathcal{U}$ be the group of units of $R$.

A (left) *linear code* $C$ over $R$ of length $n$ is a (left) submodule $C \subset R^n$.

A *weight function* on $R$ is a function $w : R \to \mathbb{C}$ satisfying $w(0) = 0$. One extends $w$ to a function $w : R^n \to \mathbb{C}$, $w(x) = \sum_{i=1}^{n} w(x_i)$.

Two *symmetry groups*:

$$\begin{aligned} G_l &= \{u \in \mathcal{U} : w(ur) = w(r), r \in R\}, \\ G_r &= \{v \in \mathcal{U} : w(rv) = w(r), r \in R\}. \end{aligned}$$

Extension property

A ring $R$ with weight function $w$ has the *extension property* if the following condition holds for every submodule $W \subset R^n$ and every injective linear transformation $f : W \to R^n$: if $f$ preserves $w$ (i.e., $w(f(x)) = w(x)$, all $x \in W$), then $f$ extends to a right $G_r$-monomial transformation of $R^n$.

Right $G_r$-monomial transformation:

$$f(x_1, \ldots, x_n) = (x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n),$$

with $u_i \in G_r$ and $\sigma$ a permutation of $\{1, 2, \ldots, n\}$.

Summary of earlier results

The extension property holds in the following situations.

Hamming weight: finite fields (MacWilliams; Bogart, Goldberg, Gordon; Ward, W.), finite Frobenius rings (W; Greferath, Schmidt).

Homogeneous weights: integer residue rings $\mathbb{Z}/m\mathbb{Z}$ (Constantinescu, Heise, Honold), finite commutative chain rings (W), finite Frobenius rings (Greferath, Schmidt).

Symmetrized weight compositions: finite fields (Goldberg), finite Frobenius rings (W.). Fix a subgroup $U \subset \mathcal{U}$ (later: $U = G_r$); $r \sim s$, if $r = su$, some $u \in U$. For $x \in R^n$, $r \in R$,

$$\mathsf{swc}_r(x) = |\{i : x_i \sim r\}|.$$

General situation

Finite ring $R$ with weight function $w$ and symmetry groups $G_l, G_r$. Elementary manipulations yield

$$w(tx) = \sum w(ts)\mathrm{swc}_s(x), \qquad (1)$$

where the sum is over the non-zero $\sim$-equivalence classes (i.e., $R/G_r$ minus zero). Note that $w(tx)$ involves the $G_l$-class only of $t$.

For fixed $x \in R^n$, (1) can be viewed as a linear transformation from a vector space of dimension $|R/G_r| - 1$ to one of dimension $|R/G_l| - 1$, represented by a $(|R/G_l| - 1) \times (|R/G_r| - 1)$ matrix $A$ with $(t, s)$-entry equal to $w(ts)$. (Note that $t, s$ are multiplied here.)

**Theorem (W., 1997)** *Let $R$ be a finite Frobenius ring with weight function $w$. If the matrix $A$ above has trivial kernel, then the extension property holds for $w$.*

*Proof.* Use (1) and the extension property for swc. $\square$

The example of matrix rings

Let $R = M_n(\mathbb{F}_q)$. Fix an $n$-dimensional vector space $V$ over $\mathbb{F}_q$, and view $R = \mathrm{End}_{\mathbb{F}_q}(V) = \mathrm{Hom}_{\mathbb{F}_q}(V, V)$.

Assume the symmetry groups $G_l, G_r$ are as large as possible; i.e., $G_l = G_r = GL_n(\mathbb{F}_q)$.

Right $GL_n$-orbits correspond to all $f : V \to V$ with a fixed subspace as range. Left $GL_n$-orbits correspond to all $f : V \to V$ with a fixed subspace as kernel.

**Proposition** *If $G_l = G_r = GL_n(\mathbb{F}_q)$, then $w(P)$, $P \in M_n(\mathbb{F}_q)$, depends only on the rank of $P$.*

*Proof.* Suppose $P, Q$ have the same rank. One can find invertible matrices $U_1, U_2$ such that $Q = U_1 P U_2$. Then $w(P) = w(Q)$. $\square$

So, $w(P) = w(\mathrm{rank}(P))$. Write $w_0 = 0, w_1, \ldots, w_n$ for the values of $w$, indexed by the rank.

Form of matrix $A$

Rows and columns of $A$ are parameterized by non-zero subspaces of $V$. The entry in row $W_1$, column $W_2$ is $w(\mathrm{rank}(PQ))$, where $\ker P = W_1^\perp$ and range $Q = W_2$. One verifies that

$$\mathrm{rank}(PQ) = \dim W_2 - \dim(W_1^\perp \cap W_2).$$

Example. $R = M_2(\mathbb{F}_2)$. The space $V$ (dimension 2) has four non-zero subspaces: $V$ itself, and three lines.

$$A = \begin{pmatrix} w_2 & w_1 & w_1 & w_1 \\ w_1 & w_1 & 0 & w_1 \\ w_1 & 0 & w_1 & w_1 \\ w_1 & w_1 & w_1 & 0 \end{pmatrix}.$$

One verifies that $\det A = w_1^3(3w_1 - 2w_2)$.

In general, we can factor $\det A$ into linear expressions.

Factoring $\det A$

**Theorem** *For $R = M_n(\mathbb{F}_q)$,*

$$\det A = c \prod_{l=1}^{n} \left( \sum_{m=1}^{l} (-1)^m \begin{bmatrix} l \\ m \end{bmatrix}_q q^{\frac{m(m-1)}{2}} w_m \right)^{\begin{bmatrix} n \\ l \end{bmatrix}_q},$$

*where*

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \frac{(1-q^a)(1-q^{a-1})\cdots(1-q^{a-b+1})}{(1-q^b)(1-q^{b-1})\cdots(1-q)}$$

*is the $q$-binomial coefficient.*

**Corollary** *$R = M_n(\mathbb{F}_q)$, $w$ with $G_l = G_r = GL_n(\mathbb{F}_q)$, satisfy the extension property if and only if*

$$R_l := \sum_{m=1}^{l} (-1)^m \begin{bmatrix} l \\ m \end{bmatrix}_q q^{\frac{m(m-1)}{2}} w_m \neq 0,$$

*for all $l = 1, 2, \ldots, n$.*

Examples:

$$\begin{aligned} R_1 &= w_1; \\ R_2 &= (q+1)w_1 - qw_2; \\ R_3 &= (q^2+q+1)w_1 \\ &\quad -q(q^2+q+1)w_2 + q^3 w_3. \end{aligned}$$

Idea of proof

View $A$ as a linear transformation. Input and output vectors are indexed by non-zero subspaces of $V$. By assuming $R_l = 0$, we write down $\begin{bmatrix} n \\ l \end{bmatrix}_q$ linearly independent solutions of $Ax = 0$. We conclude that $R_l^{\begin{bmatrix} n \\ l \end{bmatrix}_q}$ divides $\det A$.

In order to write down those solutions, we assume a certain format—in part, that the input vectors depend only on the dimension of the indexing subspace and that entries for dimensions $> l$ vanish. By carefully adjusting the constants in the input vector, we get the desired solutions.

To verify the solutions, the Cauchy Binomial Theorem is used:

$$\prod_{k=1}^{n}(1+yq^k)=\sum_{m=0}^{n}y^m q^{m(m+1)/2}\left[\begin{array}{c} n \\ m \end{array}\right]_q.$$

Example of $R = M_2(\mathbb{F}_2)$

$$A = \begin{pmatrix} w_2 & w_1 & w_1 & w_1 \\ w_1 & w_1 & 0 & w_1 \\ w_1 & 0 & w_1 & w_1 \\ w_1 & w_1 & w_1 & 0 \end{pmatrix}.$$

$l = 1$: input vector $x = (0, b, 0, 0)^t$, $b \neq 0$. $Ax = (w_1 b, w_1 b, 0, w_1 b)^t$, which equals 0 if $w_1 = 0$. Similarly for $x = (0, 0, b, 0)^t$ or $(0, 0, 0, b)^t$. There are three independent solutions of $Ax = 0$, if $w_1 = 0$.

$l = 2$: Now use $x = (b_2, b_1, b_1, b_1)^t$.

$$\begin{aligned} Ax &= (w_2 b_2 + 3 w_1 b_1, w_1(b_2 + 2b_1), \\ &\quad w_1(b_2 + 2b_1), w_1(b_2 + 2b_1))^t. \end{aligned}$$

Take $b_2 = -2b_1$ to kill the last three entries. Then the first entry is $(-2w_2 + 3w_1)b_1$, which vanishes if $3w_1 - 2w_2 = 0$.

$$\det A = w_1^3(3w_1 - 2w_2).$$

In general, we fix a subspace $W$ of dimension $l$ in $V$ and set input vector

$$x^W = (x^W)_U = \begin{cases} 0, & U \not\subset W, \\ b_i, & U \subset W, \dim U = i. \end{cases}$$

By setting $b_i = (-1)^i q^{i(i-1)/2}$, we get most of the entries of $Ax$ to vanish (by Cauchy). By assuming $R_l = 0$, the remaining entries vanish, too. Thus we get one solution $x^W$ for $Ax = 0$ (if $R_l = 0$) for each subspace $W$ of dimension $l$. There are $\begin{bmatrix} n \\ l \end{bmatrix}_q$ such subspaces.

Hamming weight

What if $w_1 = w_2 = \cdots = w_n = 1$?

$$\begin{aligned}
R_l &= \sum_{m=1}^{l} (-1)^m \begin{bmatrix} l \\ m \end{bmatrix}_q q^{m(m-1)/2} \\
&= -1 + \sum_{m=0}^{l} (-1)^m \begin{bmatrix} l \\ m \end{bmatrix}_q q^{m(m-1)/2} \\
&= -1 + \sum_{m=0}^{l} (-1)^m \begin{bmatrix} l \\ m \end{bmatrix}_q q^{m(m+1)/2} q^{-m} \\
&= -1 + \sum_{m=0}^{l} \left(-\frac{1}{q}\right)^m \begin{bmatrix} l \\ m \end{bmatrix}_q q^{m(m+1)/2} \\
&= -1 + 0 = -1,
\end{aligned}$$

by Cauchy.