Restrictions on Two-Weight Projective Linear Codes

Jay A. Wood
Department of Mathematics
Western Michigan University
1903 W Michigan Ave
Kalamazoo MI 49008-5248 USA
jay.wood@wmich.edu
http://homepages.wmich.edu/∼jwood

WCC2003, INRIA
March 28, 2003

Two years ago, at WCC2001, I gave a talk entitled *The Structure of Linear Codes of Constant Weight* in which I presented some results about one-weight linear codes over $\mathbb{Z}/N\mathbb{Z}$ for the Hamming, Lee, or Euclidean weights. At the end of that talk I made some comments about linear two-weight codes. That will be the subject of today's talk.

Disclaimer: There is very little that is new in this talk. Most of the results have been discovered by others using similar techniques. I am hopeful that my point of view may shed some additional light on the subject.

Outline:

- Preliminaries
- Isomorphism theorem
- Restrictions

Preliminaries

Ground field is $\mathbb{F} = \mathbb{F}_q$.

Linear code $C = (M, \eta)$, where M is a finite-dimensional $\mathbb{F}$-vector space, and

$$\eta : M^\sharp := \mathsf{Hom}_{\mathbb{F}}(M, \mathbb{F}) \to \mathbb{N}$$

is a *multiplicity function*.

Think of columns of a generator matrix.

Non-degenerate: $\eta(0) = 0$. No zero columns.

There is a notion of equivalence, which will be discussed later.

Weights

A *weight function* w on $\mathbb{F}$ assigns weights $w(r)$ to $r \in \mathbb{F}$; $w(0) = 0$. We assume $w(r) \in \mathbb{Q}$. Later in this talk we will concentrate on Hamming weight, where $w(r) = 1$ for nonzero $r \in \mathbb{F}$.

The *symmetry group* of w is defined to be

$$\mathrm{Sym}(w) := \{u \in \mathbb{F}^\times : w(ur) = w(r) \text{ for all } r \in \mathbb{F}\}.$$

For a code $C = (M, \eta)$, $x \in M$ has *weight*

$$w_\eta(x) := \sum_{\lambda \in M^\sharp} \eta(\lambda) w(\lambda(x)).$$

Orbits

The group Sym(w) acts on M and $M^\sharp$ by scalar multiplication. Orbits are denoted orb(x) or orb(λ), for $x \in M$, $\lambda \in M^\sharp$.

Denote the sets of non-zero orbits by $\mathcal{O}$ and $\mathcal{O}^\sharp$, respectively.

Given a linear code (M, η) and $\lambda \in M^\sharp$, define

$$\eta_S(\lambda) := \sum_{\mu \in \mathrm{orb}(\lambda)} \eta(\mu).$$

Then $\eta_S(\mu) = \eta_S(\lambda)$ when $\mu \in \mathrm{orb}(\lambda)$, and

$$w_\eta(x) = \sum_{\lambda \in \mathcal{O}^\sharp} \eta_S(\lambda) w(\lambda(x)).$$

Equivalence

Two linear codes (M, η), (M, η') are said to be *scale equivalent* if $\eta'_S = \eta_S$.

Denote the set of all functions $\mathcal{O}^\sharp \to \mathbb{N}$ by $\mathbb{N}[\mathcal{O}^\sharp]$.

Theorem *There is a bijection between the set of all nondegenerate linear codes (M, η), up to scale equivalence, and the function space $\mathbb{N}[\mathcal{O}^\sharp]$.*

Equivalence (more)

Two linear codes (M', η'), (M, η) are *equivalent* if there is an isomorphism $f : M' \to M$ such that $(M, \eta' \circ f^\sharp)$ and (M, η) are scale equivalent.

The general linear group $GL(M)$ acts on M, $M^\sharp$, $\mathcal{O}$, and $\mathcal{O}^\sharp$. The space of $GL(M)$-orbits in $\mathbb{N}[\mathcal{O}^\sharp]$ corresponds to equivalence classes of linear codes (M, η).

Slepian, Peterson: modular representation.
Assmus and Mattson: use linear functionals.
Tsfasman and Vlāduţ: projective systems.
Calderbank and Kantor: projective sets.
Dodunekov and Simonis: projective multisets.

Weight mapping

Fix an $\mathbb{F}$-vector space M.

$$\eta \in \mathbb{N}[M^\sharp] \mapsto w_\eta \in \mathbb{Q}[M].$$

Passing to Sym(w)-orbits:

$$\eta_S \in \mathbb{N}[\mathcal{O}^\sharp] \mapsto w_{\eta_S} \in \mathbb{Q}[\mathcal{O}].$$

For Hamming weight, this map is injective

$$W : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$$

(MacWilliams Equivalence Theorem).

The map W is also $GL(M)$-equivariant.

Virtual linear codes

A *virtual linear code* $C = (M, \eta)$, where now

$$\eta : M^\sharp \to \mathbb{Q}.$$

Classical codes: where η takes values in $\mathbb{N}$.

Theorem *For Hamming weight, the mapping*

$$W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}], \quad \eta_S \mapsto w_{\eta_S}$$

is a $GL(M)$-equivariant isomorphism of vector spaces.

Isomorphism (again)

We assume Hamming weight from now on.

Theorem *Suppose that M has dimension k over $\mathbb{F}$. The isomorphism*

$$W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$$

has an inverse which is represented by a specific matrix W', with

$$W'_{\lambda,x} = \begin{cases} \frac{-(q-1)}{q^{k-1}}, & \lambda(x) = 0, \\ \frac{1}{q^{k-1}}, & \lambda(x) \neq 0. \end{cases}$$

This result goes back to MacWilliams and to Bogart, Goldberg, and Gordon.

Can extend to generalized Hamming weights.

(Slide from WCC2001)

Comments on linear two-weight codes

Suppose the nonzero elements $x \in M$ have one of two weights, a or b. In

$$\eta_S \in \mathbb{Q}[\mathcal{O}^\sharp] \mapsto w_{\eta_S} \in \mathbb{Q}[\mathcal{O}],$$

the difficulty lies in determining which orbits in M have weight a, say. This leads directly to the "projective sets" of Calderbank and Kantor.

Two-weight Codes

Suppose $C = (M, \eta)$ is a two-weight linear code. That is, there exist two natural numbers $0 < a_1 < a_2$ such that, for all non-zero $x \in M$, $w_\eta(x) = a_1$ or a_2.

Let $S_i = \{x \in \mathcal{O} : w_\eta(x) = a_i\}$, for $i = 1, 2$.

Let $P_i = (M^\sharp, 1_{S_i})$ be the projective codes determined by the S_i. (Dual transforms of Dodunekov and Simonis.) Let ω_1 be the weight function of P_1, and let s_1 be the number of elements of S_1.

Theorem *The multiplicity function η satisfies*

$$\begin{aligned}\eta(\lambda) =& \frac{a_1}{q^{k-1}}\left(q\omega_1(\lambda) - (q-1)s_1\right) \\ &+ \frac{a_2}{q^{k-1}}\left(1 + (q-1)s_1 - q\omega_1(\lambda)\right).\end{aligned}$$

Projectivity

Theorem *If a two-weight code $C = (M, \eta)$ is projective, then its associated projective codes P_1 and P_2 are two-weight codes. Conversely, given a projective two-weight code P_1, there are unique values for $a_1 < a_2$ so that C is a projective two-weight code with associated code P_1.*

One manipulates the equations relating η and ω_1.

Restrictions

Suppose $C = (M, \eta)$ is a projective two-weight linear code, with associated projective two-weight code P_1. Denote the weights of P_1 by $b_1 < b_2$, and let $T_i = \{\lambda \in M^\sharp : \omega_1(\lambda) = b_i\}$, with t_i equaling the number of elements of T_i.

Theorem *The following equations hold, relating the parameters of C and P_1.*

$$(a_2 - a_1)(b_2 - b_1) = q^{k-2}$$

$$s_1 a_1 + (\frac{q^k - 1}{q - 1} - s_1)a_2 = q^{k-1} t_1$$

$$t_1 b_1 + (\frac{q^k - 1}{q - 1} - t_1)b_2 = q^{k-1} s_1$$

This again follows from manipulating earlier equations.

Calderbank-Kantor.

Self-Associated Codes

When C is equivalent to its associated code P_1 (or to its complement P_2), the previous theorem implies additional restrictions on the parameters of C.

See printed version for details.

Example M of dimension $k = 2t$ over $\mathbb{F}_2$. $E_1, E_2, \ldots, E_N$ $(1 < N < 2^t + 1)$ pairwise disjoint linear subspaces of dimension t. Projective code $C = (M, \eta)$ with $\eta = 1$ on the union of the E_i, and η equaling 0 elsewhere. Then C has the same parameters as P_1.

Dillon's partial spread family of bent functions.