Witt Theorems for Linear Codes over Finite Frobenius Rings

Jay A. Wood*
Department of Mathematics
Purdue University Calumet†
Hammond, IN 46323
wood@calumet.purdue.edu
http://www.calumet.purdue.edu/public/math/wood

ICAA
Athens, Ohio
March 27, 1999

*Supported in part by Purdue University Calumet Scholarly Research Awards.

†A regional campus in the Purdue University system, located in northwest Indiana, about 30 miles southeast of downtown Chicago.

Thanks to Claude Carlet and Thann Ward.

1. Extension theorems.

For nondegenerate bilinear and quadratic forms, E. Witt and C. Arf proved extension theorems. For W a subspace of V, any linear isometry $W \to V$ extends to an isometry $V \to V$.

For codes, F. J. MacWilliams proved:

Theorem *Let F be any finite field, and set $V = F^n$. Suppose C is a subspace of V and that $f : C \to V$ is linear and preserves Hamming weight. Then f extends to a monomial transformation on V.*

2. Finite Frobenius rings.

Let R be a finite ring. For any (right) R-module M, the *character module* of M is the (left) module

$$\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{T}),$$

where $\mathbb{T}$ is the group of unit complex numbers.

A finite ring R is *Frobenius* if $\widehat{R} \cong R$ as one-sided R-modules. In particular, there exists a character χ of R such that every character π of R has the form $\pi(x) = \chi^a(x) = \chi(ax)$ ($x \in R$), for some $a \in R$. Such a χ is called a *generating character*. Example: $R = \mathbb{Z}/(k)$, $\chi(x) = \exp(2\pi i x/k)$.

Theorem *Let R be any finite Frobenius ring, and set $V = R^n$. Suppose C is a (right) submodule of V and that $f : C \to V$ is linear and preserves Hamming weight. Then f extends to a monomial transformation on V.*

3. Sketch of proof.

The inclusion $C \subset V$ and f are given by coordinate functionals $\lambda = (\lambda_1, \ldots, \lambda_n)$ and $\mu = (\mu_1, \ldots, \mu_n)$. Write weight preservation as an equation of characters:

$$\sum_{i=1}^{n} \sum_{\pi \in \widehat{R}} \pi(\lambda_i(x)) = \sum_{j=1}^{n} \sum_{\psi \in \widehat{R}} \psi(\mu_j(x)).$$

Since R is Frobenius, every character has the form χ^a, where χ is a generating character. Thus

$$\sum_{i=1}^{n} \sum_{a \in R} \chi^a(\lambda_i(x)) = \sum_{j=1}^{n} \sum_{b \in R} \chi^b(\mu_j(x)).$$

By linear independence of characters, terms must match up: $\chi \circ \lambda_i = \chi \circ b_i \mu_{\sigma(i)}$. Additional arguments show that $\lambda_i = b_i \mu_{\sigma(i)}$ and that b_i can be taken to be units. (σ: permutation.)

4. Symmetrized weight compositions.

Fix a subgroup U of the group of units of R. Write $s \approx r$ if $s = ur$ for some $u \in U$. Define the *symmetrized weight composition* of $x \in V$ by

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

We emphasize that swc depends on U.

Theorem *Let R be any finite Frobenius ring, with $V = R^n$. Suppose C is a submodule of V and that $f : C \to V$ is linear and preserves* swc. *Then f extends to a monomial transformation on V with units belonging to U.*

5. General weight functions.

For every nonzero $r \in R$, assign a weight $a_r > 0$; set $a_0 = 0$. Define a *weight function* w on V by

$$w(x) = \sum_{i=1}^{n} a_{x_i}.$$

The *symmetry group* of w is

$$\mathrm{Sym}(w) = \{\text{units } u : a_{ur} = a_r, r \in R\}.$$

We now require that R be a finite commutative chain ring (local, principal ideals). Examples: $\mathbb{Z}/(p^k)$, Galois rings $GR(p^k, m)$.

Theorem *Let R be any finite commutative chain ring, with $V = R^n$, and assume certain technical hypotheses on the a_r. Suppose C is a submodule of V and that $f : C \to V$ is linear and preserves w. Then f extends to a monomial transformation on V with units belonging to* $\mathrm{Sym}(w)$.

6. Sufficient conditions. The technical hypotheses on the a_r are that certain Fourier coefficients of the a_r are nonzero. Under these hypotheses, preserving w implies preserving swc, with $U = \mathrm{Sym}(w)$.

Here's an easy way to state the hypotheses. Construct a square matrix $\mathcal{A}$ indexed by nonzero elements r, s of R/U. The entry in position (r, s) is the weight a_{rs} of the product rs.

The technical hypotheses are that $\det \mathcal{A} \neq 0$. Like the group determinant of a finite abelian group, $\det \mathcal{A}$ factors into linear factors, expressible as certain Fourier coefficients with respect to characters.

Example: $\det \mathcal{A} \neq 0$ for Lee and Euclidean weight functions over $\mathbb{Z}/(p^k)$ for $p^k \leq 125$. (A Maple computation.)

7. Linear codes of constant weight.

Continue to assume that R is a finite commutative chain ring, equipped with a weight function w for which the extension theorem holds. Also need $a_r \in \mathbb{Q}$.

A linear code $C \subset V$ has *constant weight* if there exists $L > 0$ with $w(x) = L$ for all nonzero $x \in C$.

Write $\mathrm{Aut}(C)$ for the group of linear automorphisms of C. If C has constant weight, then every $f \in \mathrm{Aut}(C)$ preserves w, and hence extends to a monomial transformation with units from $U = \mathrm{Sym}(w)$.

Proposition *Assume C has constant weight. Then the multiset of cooordinate functionals of C consists of $\mathrm{Aut}(C)$-orbits, modulo scaling by units in U.*

8. Uniqueness and existence.

Theorem *(Uniqueness) Fix a finite module M over R. If M admits an embedding of constant weight, then there is a unique shortest embedding, and every other embedding is a replication of the shortest one.*

Theorem *(Existence) Constant weight embeddings exist over finite commutative chain rings as follows.*

(a) Hamming weight: Any dimension over fields (Bonisoli). At most rank one, otherwise.
(b) Homogeneous weight (Schmidt's talk): Any M over any R.
(c) Lee weight: Any M over $\mathbb{Z}/(2^k)$ (Carlet). Any dimension over $\mathbb{F}_p$; at most rank 2 over $\mathbb{Z}/(p^k)$, $k > 1$, p odd prime.
(d) Euclidean weight: Any M over $\mathbb{Z}/(2^k)$. Equivalent to constant Lee weight over $\mathbb{Z}/(p^k)$, p odd.

9. Euclidean example.

Over $R = \mathbb{Z}/(4)$, consider the generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 \\ 0 & 1 & 2 & -1 & 1 & 1 & 0 & 2 & 2 \end{pmatrix}.$$

Then G generates a code C which is a free R-module of rank 2. This code has constant Euclidean weight 16.

Aut$(C) = GL_2(R)$, i.e., det $= \pm 1$.
Sym$(w) = \{\pm 1\}$.

Nonzero orbits:

$$\left(\begin{array}{cccccc|cccccc} 1 & 1 & 1 & 1 & 0 & 2 & 2 & 0 & -1 & -1 & -1 & -1 \\ 0 & 1 & 2 & -1 & 1 & 1 & -1 & -1 & 1 & 2 & -1 & 0 \end{array}\right)$$

$$\begin{matrix} 2 & 2 & 0 \\ 0 & 2 & 2 \end{matrix}$$