Foundational Aspects of Linear Codes: 3. Extension property: sufficient conditions

Jay A. Wood

Department of Mathematics
Western Michigan University
http://homepages.wmich.edu/∼jwood/

On the Algebraic and Geometric Classifications of Projective Varieties
University of Messina
June 22, 2016

3. Extension property: sufficient conditions

- Extension property (EP)
- EP for Hamming weight over Frobenius bimodules via linear independence of characters
- Egalitarian weights for module alphabets
- General weight: reducing to egalitarian weight
- Weights with maximal symmetry
- Lee and Euclidean weights on $\mathbb{Z}/N\mathbb{Z}$

Notation

- Let R be a finite associative ring with 1.
- Let A be a finite unital left R-module: the **alphabet**.
- Let $w : A \to \mathbb{C}$ be a **weight**: $w(0) = 0$. Extend to A^n by

$$w(a_1, \ldots, a_n) = \sum_{i=1}^{n} w(a_i).$$

- **Hamming weight**: $\mathrm{wt}(0) = 0$; $\mathrm{wt}(a) = 1$ for $a \neq 0$.

Symmetry groups

- Recall the **symmetry groups** of w:

$$G_{\mathrm{lt}} = \{u \in \mathcal{U}(R) : w(ua) = w(a), a \in A\},$$
$$G_{\mathrm{rt}} = \{\phi \in GL_R(A) : w(a\phi) = w(a), a \in A\}.$$

- $\mathcal{U}(R)$ is the group of units of R, and $GL_R(A)$ is the group of invertible R-linear homomorphisms $A \to A$.
- Hamming weight: $G_{\mathrm{lt}} = \mathcal{U}(R)$, $G_{\mathrm{rt}} = GL_R(A)$.
- Recall that I will usually write homomorphisms of left modules on the right side.

Monomial transformations

- Recall: if $G \subseteq GL_R(A)$ is a subgroup, then a G-**monomial transformation** of A^n is an invertible R-linear homomorphism $T : A^n \to A^n$ of the form

$$(a_1, a_2, \ldots, a_n)T = (a_{\sigma(1)}\phi_1, a_{\sigma(2)}\phi_2, \ldots, a_{\sigma(n)}\phi_n),$$

  for $(a_1, a_2, \ldots, a_n) \in A^n$.
- Here, σ is a permutation of $\{1, 2, \ldots, n\}$ and $\phi_i \in G$ for $i = 1, 2, \ldots, n$.

Isometries

- Let $C_1, C_2 \subseteq A^n$ be two linear codes. Recall that an R-linear isomorphism $f : C_1 \to C_2$ is a linear **isometry** with respect to w if $w(xf) = w(x)$ for all $x \in C_1$.
- Every G_{rt}-monomial transformation is an isometry from A^n to itself.

Extension property (EP)

- Given ring R, alphabet A, and weight w on A.
- The alphabet has the **extension property** (EP) with respect to w if the following holds: For any left linear codes $C_1, C_2 \subseteq A^n$, if $f : C_1 \to C_2$ is a linear isometry, then f extends to a G_{rt}-monomial transformation $A^n \to A^n$.
- That is, there exists a G_{rt}-monomial transformation $T : A^n \to A^n$ such that $xT = xf$ for all $x \in C_1$.

Slightly different point of view

- Linear codes are often presented by generator matrices. A generator matrix serves as a linear encoder from an information space to a message space.
- If $f : C_1 \to C_2$ is a linear isometry, then C_1 and C_2 are isomorphic as R-modules. Let M be a left R-module isomorphic to C_1 and C_2. Call M the **information module**.
- Then C_1 and C_2 are the images of R-linear homomorphisms $\Lambda : M \to A^n$ and $N : M \to A^n$, respectively. Then, $N = \Lambda f$: inputs on left!

Coordinate functionals

- C_1 was given by $\Lambda : M \to A^n$. Write the individual components as $\Lambda = (\lambda_1, \ldots, \lambda_n)$, with $\lambda_i \in \mathrm{Hom}_R(M, A)$. Call the λ_i **coordinate functionals**.
- Similarly, $N = (\nu_1, \ldots, \nu_n)$, $\nu_i \in \mathrm{Hom}_R(M, A)$.
- The isometry f extends to a monomial transformation if there exists a permutation σ and $\phi_i \in G_{\mathrm{rt}}$ such that $\nu_i = \lambda_{\sigma(i)}\phi_i$ for all $i = 1, \ldots, n$.

Case of $\widehat{R}$

- Our first result will show that, for any finite ring R, $A = \widehat{R}$ has EP with respect to the Hamming weight.
- It follows that $A = R$ itself has EP with respect to the Hamming weight when R is Frobenius.
- The Frobenius ring case came first (JW, 1999).
- The more general $A = \widehat{R}$ case is due to Greferath, Nechaev, and Wisbauer (2004).

Techniques

- For any alphabet A, the summation formulas for characters imply that the Hamming weight wt satisfies

$$\mathrm{wt}(a) = 1 - \frac{1}{|A|} \sum_{\pi \in \widehat{A}} \pi(a), \quad a \in A.$$

- Characters are linearly independent over $\mathbb{C}$.

Symmetry groups for the Hamming weight

- Consider the Hamming weight wt on $A = \widehat{R}$, which is an (R, R)-bimodule.
- Both symmetry groups G_{lt} and G_{rt} equal $\mathcal{U}(R)$.

A preorder

- Define a preorder $\preceq$ on $\mathrm{Hom}_R(M, \widehat{R})$ by $\lambda \preceq \nu$ if there exists $r \in R$ such that $\lambda = \nu r$.
- It follows from a result of Bass that if $\lambda \preceq \nu$ and $\nu \preceq \lambda$, then $\lambda = \nu u$, where $u \in \mathcal{U}(R)$.

Proof (a)

- R, $A = \widehat{R}$, with Hamming weight. $C_1, C_2 \subseteq \widehat{R}^n$, with $f : C_1 \to C_2$ linear isometry.
- $\widehat{R}$ has a generating character: $\rho : \widehat{R} \to \mathbb{C}$, $\rho(\pi) = \pi(1)$ for $\pi \in \widehat{R}$. (Evaluate at $1 \in R$.) Every $\pi \in \widehat{R}$ has the form $\pi = {}^r\rho$ for some unique $r \in R$.
- C_1 is image of $\Lambda : M \to \widehat{R}^n$; C_2 is image of $N : M \to \widehat{R}^n$. $N = \lambda f$.
- Isometry: $\mathrm{wt}(x\Lambda) = \mathrm{wt}(xN)$, for all $x \in M$.

Proof (b)

- Hamming weight as character sum:

$$\sum_{i=1}^{n} \sum_{r \in R} {}^{r}\rho(x\lambda_i) = \sum_{j=1}^{n} \sum_{s \in R} {}^{s}\rho(x\nu_j), \quad x \in M.$$

- That is,

$$\sum_{i=1}^{n} \sum_{r \in R} \rho(x\lambda_i r) = \sum_{j=1}^{n} \sum_{s \in R} \rho(x\nu_j s), \quad x \in M.$$

- This is an equation of characters on M.

Proof (c)

- Among the λ_i, ν_j, choose one that is maximal for $\preceq$. Say, ν_1.
- Let $j = 1$ and $s = 1$ on the right side of the character equation.
- By linear independence of characters, there exists i and $r \in R$ so that $\rho(x\lambda_i r) = \rho(x\nu_1)$ for all $x \in M$.
- Thus $\rho(x(\nu_1 - \lambda_i r)) = 1$ for all $x \in M$. I.e., $M(\nu_1 - \lambda_i r) \subseteq \ker \rho$.

Proof (d)

- By ρ a generating character, $\nu_1 = \lambda_i r$. Thus, $\nu_1 \preceq \lambda_i$.
- By maximality, $\nu_1 \preceq \lambda_i$ and $\lambda_i \preceq \nu_1$. Thus, $\nu_1 = \lambda_i u_1$, for some $u_1 \in \mathcal{U}(R)$.
- Then inner sums agree: $\sum_{r \in R} \rho(x\lambda_i r) = \sum_{s \in R} \rho(x\nu_1 s)$, $x \in M$.
- Set $\sigma(1) = i$. Subtract inner sums to reduce the size of the outer sums by 1. Proceed by induction.

Generalize to module alphabets

- For ring R, alphabet A, and Hamming weight wt, EP holds if A: (1) is pseudo-injective and (2) has a cyclic socle (embeds into $\widehat{R}$).
- Pseudo-injective means injective with respect to submodules. That is, if B is a submodule of A and $h : B \to A$ is any module homomorphism, then h extends to $\tilde{h} : A \to A$.
- Main idea: use $\widehat{R}$-case to get $GL_R(\widehat{R})$-monomial extension. Use pseudo-injectivity to show existence of $GL_R(A)$-monomial extension.

Using generating character to define a weight

- Suppose the alphabet A admits a generating character ρ: $\mathrm{Soc}(A)$ is cyclic.
- Fix a subgroup $U \subseteq GL_R(A)$.
- Define a weight $w_U : A \to \mathbb{C}$:

$$w_U(a) = 1 - \frac{1}{|U|} \sum_{\phi \in U} \rho(a\phi), \quad a \in A.$$

- When $A = R$, the ring must be Frobenius.

Properties of w_U

- $w_U(0) = 0$.
- Re-index: $U \subseteq G_{\mathrm{rt}}(w_U)$.
- By the summation formulas and ρ generating: for any nonzero left R-submodule $B \subseteq A$, and any $a_0 \in A$,
$$\sum_{b \in B} w_U(a_0 + b) = |B|.$$
- We say that w_U is **egalitarian** on cosets of B.

A little history

- w_U is similar a formula of Honold's for the homogeneous weight.
- Homogeneous weight was developed first for $\mathbb{Z}/m\mathbb{Z}$, then for more general rings and modules.
- Constantinescu, Heise, Greferath, Schmidt, Honold, Nechaev.
- The following proof is due essentially to Barra and Gluesing-Luerssen (2014).

w_U has EP

- Suppose $w_U(x\Lambda) = w_U(xN)$ for all $x \in M$.
- Equation of characters: for all $x \in M$,

$$\sum_{i=1}^{n} \sum_{\phi \in U} \rho(x\lambda_i \phi) = \sum_{j=1}^{n} \sum_{\psi \in U} \rho(x\nu_j \psi).$$

- Use linear independence of characters: for $j = 1$, $\psi = \mathrm{id}_A$, there exist $i = \sigma(1)$ and $\phi_1 \in U$ with $\rho(x\lambda_{\sigma(1)}\phi_1) = \rho(x\nu_1)$ for all $x \in M$.
- ρ generating: $\nu_1 = \lambda_{\sigma(1)}\phi_1$. Inner sums agree, reduce outer sum, and continue by induction.

Correlation action (Greferath-Honold)

- Let $\alpha : R \to \mathbb{C}$ and $w : A \to \mathbb{C}$.
- Define the **correlation** $w\alpha : A \to \mathbb{C}$ by

$$(w\alpha)(a) = \sum_{r \in R} w(ra)\alpha(r), \quad a \in A.$$

- If $w(0) = 0$, then $(w\alpha)(0) = 0$.
- $G_{\mathrm{rt}}(w) \subseteq G_{\mathrm{rt}}(w\alpha)$.

Comparing isometries

Lemma

If $f : C \to A^n$ is a w-isometry, then f is a $w\alpha$-isometry for any α.

Proof.

For $x \in C$,

$$(w\alpha)(xf) = \sum_{r \in R} w(rxf)\alpha(r)$$

$$= \sum_{r \in R} w(rx)\alpha(r) = (w\alpha)(x). \qquad \square$$

A sufficient condition for EP

Theorem

Let $U = G_{\mathrm{rt}}(w)$. If $w\alpha = w_U$ for some α, then w has EP.

Proof.

Suppose $f : C \to A^n$ is a w-isometry. By the previous lemma, f is a w_U-isometry. Since w_U has EP, f extends to a U-monomial transformation. Thus w has EP. □

Matrix representing correlation

- Recall that $(w\alpha)(a) = \sum_{r \in R} w(ra)\alpha(r)$, for $a \in A$.
- By symmetry, values of $w(ra)$ depend only on orbit $[r]$ of r under G_{lt} and orbit $[a]$ of a under G_{rt}.
- Define a complex matrix $W = (w(ra))$, $[0] \neq [r] \in G_{\mathrm{lt}} \backslash R$, $[0] \neq [a] \in A/G_{\mathrm{rt}}$.
- w has EP when $\operatorname{rk} W = |A/G_{\mathrm{rt}}| - 1$.
- When W is square (e.g., when $A = R$ is commutative), w has EP when W is invertible or $\det W \neq 0$.

Cases of maximal symmetry

- There has been progress on finding more explicit conditions over ring alphabets ($A = R$) when the weight w has maximal symmetry: $G_{\mathrm{lt}} = G_{\mathrm{rt}} = \mathcal{U}(R)$.
- When R is a product of chain rings: Greferath, Mc Fadden, Zumbrägel, 2013.
- When R is a principal ideal ring: Greferath, Honold, Mc Fadden, Wood, Zumbrägel, 2014. Here $\det W$ is factored into terms $\sum_{0<dR\leq aR} w(d)\mu(0, dR)$, for $a \in R$, where μ is the Möbius function for the poset of principal right ideals of R.

Case of commutative chain rings

- A finite ring is a **chain ring** if all its left ideals form a chain under inclusion. In that case, every ideal is two-sided. A chain ring is Frobenius.
- In the commutative case, a chain ring is a local principal ideal ring.
- Examples: fields; $\mathbb{Z}/p^k\mathbb{Z}$, p prime; Galois rings (Galois extensions of $\mathbb{Z}/p^k\mathbb{Z}$).

det W factors over chain rings

- Let R be a finite commutative chain ring with weight w. Let U be the symmetry group of w.
- When R is a finite field $\mathbb{F}$, det W factors as a product of Fourier transforms of w with respect to characters of the quotient group $G = \mathbb{F}^\times / U$. This is due to Dedekind and Frobenius, 1896.
- This generalizes for finite commutative chain rings, 1998: det W factors as a product of character sums of w over $\mathcal{U}(R)/U$ that reflect the conductors of the characters.

Examples over $\mathbb{Z}/N\mathbb{Z}$

- In addition to the Hamming weight, there are three additional weights that are easy to define on $\mathbb{Z}/NZ$.
- Lee weight: viewing $\mathbb{Z}/NZ = \{0, 1, \ldots, N-1\}$, Lee weight is $w_L(a) = \min\{a, N-a\}$.
- Euclidean weight: $w_E(a) = w_L(a)^2$.
- Complex Euclidean weight:

$$w(a) = |\exp(2\pi ia/N) - 1|^2 = 2 - 2\cos(2\pi a/N),$$

the square of distance to 1 in $\mathbb{C}$.

Facts about EP over $\mathbb{Z}/N\mathbb{Z}$

- The complex Euclidean weight is easy: it is the egalitarian weight using $U = \{\pm 1\}$.
- EP for w_L and w_E have been numerically verified (W invertible via SVD) for $N \leq 2048$.
- Proofs of EP for w_L and w_E using the form of cyclotomic polynomials for $N = 2^k, 3^k$ and $N = p = 2q + 1$ (Langevin-JW) or $p = 4q + 1$ (Barra) where p and q are prime.

EP over $\mathbb{Z}/p^k\mathbb{Z}$

- Recent work of Dyshko, Langevin and JW.

Theorem

Let $R = \mathbb{Z}/p^k\mathbb{Z}$, p prime. Then R has EP for the Lee and the Euclidean weights.

Sketch of proof (a)

- $R = \mathbb{Z}/p^k\mathbb{Z}$ is a chain ring. The symmetry group $U = \{\pm 1\}$.
- $\det W$ factors into a product of character sums over $G_{p^k} = \mathcal{U}(R)/U$.
- General character sums reduce to understanding Fourier transforms of w over G_{p^j} for (perhaps) smaller $j \leq k$.
- The characters involved are primitive even characters modulo p^j.

Sketch of proof (b)

- Easy: $\widehat{w}_L(\chi) \neq 0$ and $\widehat{w}_E(\chi) \neq 0$ for $\chi = 1$: sums of positive terms.
- The specific form of w_L and w_E, together with a Fourier transform calculation, implies that $\widehat{w}_L(\chi) = 0$ if and only if $\widehat{w}_E(\chi) = 0$ for every primitive even character $\chi \neq 1$.

Sketch of proof (c)

- If $\widehat{w}_L(\chi) = 0$ or $\widehat{w}_E(\chi) = 0$, then the other also vanishes.
- Calculate that the second generalized Bernoulli number $B_2(\chi) = 0$.
- This implies that the Dirichlet L-function $L(s, \chi)$ vanishes at $s = -1$ for a primitive even character, which contradicts known behavior of $L(s, \chi)$.
- Thus $\widehat{w}_L(\chi) \neq 0$ and $\widehat{w}_E(\chi) \neq 0$, so $\det W \neq 0$ in both cases.

Relation between the determinants

- For $\mathbb{Z}/2^k\mathbb{Z}$,

$$\det W_E = 2^{(k-1)2^{k-1}} \det W_L.$$

- For odd primes there is a similar relation.
- Special case: when 2 is a primitive root modulo p^k,

$$\prod_{j=1}^{k} (2^{p^{j-1}(p-1)/2} + 1) \cdot \det W_E = p^{k(p^k-1)/2} \det W_L.$$

What about $\mathbb{Z}/N\mathbb{Z}$?

- We expect w_L and w_E to have EP for all N.
- What's missing is a factorization of $\det W$, or some other decomposition, for general N.