Homogeneous Weight Enumerators

Jay A. Wood

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

NCRA VII
Lens, France (virtually)
Traverse City, Michigan (actually)
5 July 2021

Main Result

- The MacWilliams identities fail to hold for the homogeneous weight enumerator over $\mathbb{Z}/m\mathbb{Z}$, with m composite and greater than 5.

Outline

- MacWilliams identities for Hamming weight
- Homogeneous weight
- Prime powers: $m = p^a$, $a \geq 2$
- Two primes: $m = pq$, primes $p < q$
- Going from $\mathbb{Z}/pq\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$
- Analyzing dual codewords of small weight

Historical context

- F. J. MacWilliams, “A theorem on the distribution of weights in a systematic code,” Bell System Tech J, 1963. Also, her 1962 Radcliffe PhD dissertation.
- Linear codes over finite fields
- Dual codes defined using the standard dot product
- Uses Hamming weight and Hamming weight enumerator hwe.

MacWilliams identities

- For a linear code $C \subseteq \mathbb{F}_q^n$, with dual code $C^\perp \subseteq \mathbb{F}_q^n$,

$$\mathrm{hwe}_{C^\perp}(X, Y) = \frac{1}{|C|}\,\mathrm{hwe}_C(X + (q-1)Y, X - Y).$$

- Need to know only hwe_C, not C itself, in order to know $\mathrm{hwe}_{C^\perp}$.
- Also true for Lee weight enumerator over $\mathbb{Z}/4\mathbb{Z}$, using $X + Y$ and $X - Y$ substitutions (famous $\mathbb{Z}/4\mathbb{Z}$ paper, Hammons, et al., 1994).

Commutative diagram

- The following diagram commutes:

$$\begin{tikzcd}
\{[n,k]\text{-linear codes}\} \arrow[r, "\perp"] \arrow[d, "\mathrm{hwe}"'] & \{[n,n-k]\text{-linear codes}\} \arrow[d, "\mathrm{hwe}"] \\
\mathbb{C}[X,Y]_n \arrow[r, "MW"] & \mathbb{C}[X,Y]_n
\end{tikzcd}$$

- MW is the MacWilliams transform, induced by:

$$(X,Y) \mapsto ((X+(q-1)Y)/q^{k/n}, (X-Y)/q^{k/n}).$$

Failure of MacWilliams identities

- Suppose there is a different weight w, with its weight enumerator for a linear code C: $\mathrm{wwe}_C = \sum_{c \in C} t^{w(c)} = \sum_j A_j^w(C) t^j$.
- The MacWilliams identities will fail for wwe if there exist two linear codes C and D such that $\mathrm{wwe}_C = \mathrm{wwe}_D$ and $\mathrm{wwe}_{C^\perp} \neq \mathrm{wwe}_{D^\perp}$.
- For the latter, it is enough to have $A_j^w(C^\perp) \neq A_j^w(D^\perp)$, for some j.
- There is no way to complete the commutative diagram with a well-defined map.

Some failures

- Lee weight over $\mathbb{Z}/m\mathbb{Z}$, $m \geq 5$: Abdelghany and Wood, Discrete Math, 2020. (Noha's talk.)
- Euclidean weight over $\mathbb{Z}/m\mathbb{Z}$, m divisible by $4, 6, 9$ or by a prime p in the range $5 \leq p < 2^{13}$: computational results. Conjecture: any $m \geq 4$.
- Homogeneous weight over $\mathbb{Z}/m\mathbb{Z}$, excluding primes and 4. (The rest of this talk.)
- Homogeneous weight over $M_{2\times 2}(\mathbb{F}_q)$, $q > 2$.

Homogeneous weight

- Homogeneous weight: Constantinescu-Heise 1997, Honold-Nechaev 1999, Greferath-Schmidt 2000
- Characterization: $\mathrm{w}(0) = 0$; w is constant on any left orbit of the group of units; same average weight ζ on any nonzero left principal ideal.
- Greferath-Schmidt: w exists for any finite ring (a formula!); unique up to a scalar multiple (ζ).

Homogeneous weight enumerator

- An appropriate choice of ζ yields non-negative integer values for w.
- For $\mathbb{Z}/m\mathbb{Z}$, $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, choose $\zeta = \prod_{i=1}^{k}(p_i - 1)$.
- Extend w to vectors:

$$\mathrm{w}(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \mathrm{w}(x_i).$$

- Then $\mathrm{wwe}_C(t) = \sum_{c \in C} t^{\mathrm{w}(c)} = \sum_j A_j^{\mathrm{w}}(C) t^j$.

Main Theorem

Theorem

Suppose m is not prime and $m \geq 6$. Then there exist linear codes C and D over $\mathbb{Z}/m\mathbb{Z}$ satisfying

$$\mathrm{wwe}_C = \mathrm{wwe}_D,$$

but with

$$A_j^{\mathrm{W}}(C^\perp) \neq A_j^{\mathrm{W}}(D^\perp)$$

for some $j > 0$.

- There are no MacWilliams identities for W over $\mathbb{Z}/m\mathbb{Z}$ for those m.

Examples of homogeneous weight (1)

- Over $\mathbb{F}_q$, choosing $\zeta = q - 1$ yields $\mathrm{w}(r) = q$, $r \neq 0$.
- Over $\mathbb{F}_q$, w is q times the Hamming weight.
- MacWilliams identities hold for Hamming weight.
- This is why we exclude primes in Main Theorem.

Examples of homogeneous weight (2)

- Over $\mathbb{Z}/p^a\mathbb{Z}$, p prime, $a \geq 2$; ideals are

$$(1) \supset (p) \supset (p^2) \supset \cdots \supset (p^{a-1}) \supset (0).$$

- Choosing $\zeta = p - 1$:

$$\mathrm{w}(r) = \begin{cases} 0, & r = 0, \\ p, & r \in (p^{a-1}) - (0), \\ p - 1, & r \in (1) - (p^{a-1}). \end{cases}$$

Prime power case: $m = p^a$, $a \geq 2$

- Two linear codes C_1, C_2 with generator matrices of sizes $1 \times (p+1)$ and $2 \times (p+1)$.

$$G_1 = \begin{bmatrix} p^{a-1} & p^{a-2} & p^{a-2} & p^{a-2} & \cdots & p^{a-2} \end{bmatrix}$$
$$G_2 = \begin{bmatrix} 0 & p^{a-1} & p^{a-1} & p^{a-1} & \cdots & p^{a-1} \\ p^{a-1} & 0 & p^{a-1} & 2p^{a-1} & \cdots & (p-1)p^{a-1} \end{bmatrix}$$

Result in prime power case

- Same wwe: $1 + (p^2 - 1)t^{p^2}$.
- For duals, counting singleton vectors that annihilate columns is enough in most cases.
- Dual A_p^{W}: $p - 1$ versus $p^2 - 1$, for $p \geq 3$, $a = 2$.
- Dual A_{p-1}^{W}: $2p^{a-1} - p^2 - p$ versus $p^a + p^{a-1} - p^2 - p$, for $p \geq 2$, $a \geq 3$.
- But, when $p = 2$, doubleton vectors can have weight p (the $m = 4$ exception, where weight enumerators are equal).

Outline of proof of Main Theorem (1)

- Already did prime power case (except $m = 4$).
- Now assume $m = pq$, for primes $p < q$.
- Can show, when $p > 2$, that $1 \times n$ generator matrices do not yield examples.
- So, use $2 \times n$ generator matrix. Assume second row is multiple of p.

Outline of proof of Main Theorem (2)

- Primes $p < q$.
- Code C has generator matrix G of size $2 \times (2q + 3)$:

$$G = \left[\begin{array}{cccc|c|cccc} q & \dots & 1 & \dots & q & 0 & \dots & p & \dots \\ p & \dots & rp & \dots & 0 & p & \dots & rp & \dots \end{array} \right]$$

- Twice in the second row, $r = 0, 1, \dots, q - 1$.
- Column **groupings** by gcd of entries: 1, q, p.
- $C \cong \mathbb{Z}/pq\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, as q annihilates the second row. Think of $[x\ y] \mapsto [x\ y]G$.

Weight enumerator of C

- p odd: computation shows

  $$\mathrm{wwe}_C = 1+(p-1)t^\beta+(q^2-1)t^\gamma+(p-1)(q^2-1)t^\alpha,$$

  with $\beta < \gamma < \alpha$:

  $$\begin{aligned} \alpha &= 2pq^2 - 2q^2 + pq - 2p, \\ \beta &= pq^2 + pq - 2p, \\ \gamma &= 2pq^2 - 2q^2. \end{aligned}$$

- $p = 2$: $\beta = \alpha$ and $\mathrm{wwe}_C = 1 + (q^2 - 1)t^\gamma + q^2 t^\alpha$.

Orbit structure of C

- The group of units $\mathcal{U}_{pq}$ of $\mathbb{Z}/pq\mathbb{Z}$ acts on the linear code C by scalar multiplication. Think $u[x\ y]$.
- Representatives of the nonzero orbits are just the transposes of the columns of G. Use the same **groupings** as for the columns.
- Each orbit has a gcd: $1, q, p$, for left, middle, right groupings.

Orbit analysis

- wwe $= 1 + (p-1)t^\beta + (q^2-1)t^\gamma + (p-1)(q^2-1)t^\alpha$.
- The $p-1$ codewords of weight β come from one orbit of size $p-1$: grouping II.
- The q^2-1 codewords of weight γ come from $q+1$ orbits of size $q-1$: grouping III.
- The $(p-1)(q^2-1)$ codewords of weight α come from $q+1$ orbits of size $(p-1)(q-1)$: grouping I.

The second code

- Swap: assign weight β to the first orbit of size $(p-1)(q-1)$; assign weight α to the last $p-1$ orbits of size $q-1$.
- Original orbit weight listing is $(\alpha, \ldots, \alpha; \beta; \gamma, \ldots, \gamma)$.
- Second code has orbit weight listing $(\gamma, \alpha, \ldots, \alpha; \beta; \gamma, \ldots, \gamma, \alpha, \ldots, \alpha)$.
- Makes use of different sizes of orbits.
- Same weight enumerators.

Second code D exists!

- Detailed analysis of map that associates multiplicities of columns in a generator matrix to orbit weight listing.
- Explicit form of inverse.
- Nonnegative multiplicities for second code.
- Need to clear denominators: multiply all multiplicities by same factor. Do the same for C.
- New codes have same weight enumerators.

Features of multiplicities

- Can clear denominators with $(p-1)q^2$.
- Comparing multiplicities for C and D yields ...
- Sum of grouping III multiplicities: **same**.
- Grouping II: **different**.
- Sum of all (length): **same**.
- Remember the same/different pattern for later.

Other values of m

- Suppose m is not a prime or a prime power.
- Pick two primes $p < q$ that divide m.
- Form generator matrices over $\mathbb{Z}/pq\mathbb{Z}$, as above.
- Multiply all entries by $m/(pq)$.
- Generate codes over $\mathbb{Z}/m\mathbb{Z}$.
- Form of W implies codes still have same weight enumerators.

Small weight codewords in the dual

- Except when $6 \mid m$, small weight nonzero vectors are singletons (only one nonzero entry).
- We look for singletons that annihilate the corresponding column of the generator matrix of C or D.
- Special argument needed for $6 \mid m$ case: omitted.

Annihilators

- Singletons can annihilate: no columns; grouping II columns only; grouping III columns only; all columns, depending on divisibility by p or q.
- Singletons that annihilate grouping II columns only will contribute **differently** to $\mathrm{wwe}_{C^\perp}$ and $\mathrm{wwe}_{D^\perp}$.
- All other singletons contribute the **same**.
- Can always find singletons that annihilate grouping II columns only. (Which proves the theorem!)

Exercises

- Figure out the formula for the homogeneous weight on $\mathbb{Z}/6\mathbb{Z}$.
- Let $G_1 = [1\ 1\ 1]$ and $G_2 = [1\ 3\ 3]$ generate two linear codes over $\mathbb{Z}/6\mathbb{Z}$. Find their dual codes.
- Find the homogeneous weight enumerators of the linear codes and their duals.
- Look up the **eighth** edition of the Oxford Essential World Atlas. What location is on the cover?

Thank you

- Thank you for your kind attention.
- Thanks to André for his organizing acumen and hospitality!