Homogeneous Weight Enumerators (Slight Return)

Jay A. Wood

Department of Mathematics
Western Michigan University
jay.wood@wmich.edu

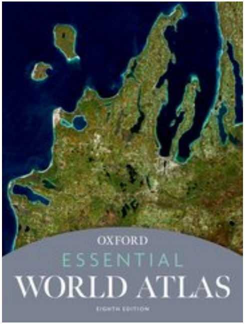
NCRA VIII
Lens, France (virtually)
Traverse City, Michigan, USA (actually)
28 August 2023

Exercise from 2021

Look up the eighth edition of the Oxford Essential World Atlas. What location is on the cover?

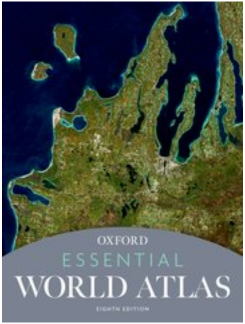
Exercise from 2021

Look up the eighth edition of the Oxford Essential World Atlas. What location is on the cover?



Exercise from 2021

Look up the eighth edition of the Oxford Essential World Atlas. What location is on the cover?



Leelanau Peninsula, Michigan, with Traverse City at center right

Our main speaker, 2012

With Hai Dinh

MacWilliams identities (1962–63)

- Linear codes over $\mathbb{F}_q$, Hamming weight enumerator:

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

- If $\mathrm{hwe}_C = \mathrm{hwe}_D$, then $\mathrm{hwe}_{C^\perp} = \mathrm{hwe}_{D^\perp}$.
- The Hamming weight **respects duality**.
- Need only hwe_C, not C itself, to get $\mathrm{hwe}_{C^\perp}$.

Other rings? Other weights?

- MacWilliams identities are true for Lee (homogeneous) 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).
- Also true for homogeneous weight enumerator over $\mathbb{F}_2 + u\mathbb{F}_2 = \mathbb{F}_2[u]/(u^2)$ and over $M_{2\times 2}(\mathbb{F}_2)$.

Some failures

- Rosenbloom-Tsfasman weight, Dougherty, Skriganov, 2002.
- Lee and homogeneous weights on $\mathbb{Z}/8\mathbb{Z}$, referee, and Shi, Shiromoto, Solé, 2015.
- Restrictions on Lee, Euclidean on $\mathbb{Z}/m\mathbb{Z}$, Tang, Zhu, Kai, 2017
- Lee on $\mathbb{Z}/m\mathbb{Z}$, $m \geq 5$: Abdelghany, W., 2020.
- Homogeneous weight over $\mathbb{Z}/m\mathbb{Z}$, excluding primes and 4, W., 2023. (Subject of 2021 NCRA talk.)

Main Result

- Context: R is finite chain ring or $M_{k\times k}(\mathbb{F}_q)$, with a positive integer weight w having maximal symmetry.
- The MacWilliams identities fail to hold for many* w-weight enumerators over a finite chain ring R, except for the Hamming weight (any R) or the homogeneous weight ($|R| = 4$ only).

But wait, there's more

- Failure for all weights over $M_{2\times 2}(\mathbb{F}_q)$, except for Hamming (any q) or homogeneous ($q = 2$ only).
- Failure for the homogeneous weight enumerator over $M_{k\times k}(\mathbb{F}_q)$, $k \geq 2$, except for $k = q = 2$.
- Conjecture: Failure for all weights over $M_{k\times k}(\mathbb{F}_q)$, except Hamming (any k, q) or homogeneous ($k = q = 2$ only).

Context for today

- Finite ring R: a chain ring or $M_{k\times k}(\mathbb{F}_q)$.
- An integer-valued weight w on R, $w(0) = 0$, and $w(r) > 0$ for $r \neq 0$.
- The weight is extended additively to R^n: $w(x_1, \ldots, x_n) = \sum_i w(x_i) \in \mathbb{Z}$.
- Codes are left R-submodules of R^n.
- Use standard R-valued dot product on R^n.
- Dual code is $C^\perp = \mathcal{R}(C) = \{y \in R^n : C \cdot y = 0\}$.

Failure of MacWilliams identities

- Given a weight w, the w-weight enumerator of a linear code C is: $\mathrm{wwe}_C = \sum_j A_j^w(C) X^{nw_{\max}-j} Y^j$.
- 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 $\mathrm{wwe}_{C^\perp} \neq \mathrm{wwe}_{D^\perp}$.
- We say that w **does not respect duality**.
- For the latter, it is enough to have $A_j^w(C^\perp) \neq A_j^w(D^\perp)$, for some j.

Maximal symmetry

- We assume that the weight w has maximal symmetry; i.e., $w(u_1 r u_2) = w(r)$ for all $r \in R$ and units $u_1, u_2 \in \mathcal{U} = \mathcal{U}(R)$.
- This is a crucial hypothesis: cf., 'Lee' weight on $\mathbb{Z}_4 + u\mathbb{Z}_4$, Yildiz, Karadeniz, 2014.

Main idea

- Build one code C. (Keep it simple.)
- Each codeword of C has a weight.
- Tweak the locations of those weights.
- Find a code D that realizes the tweaked weights.
- Try to detect differences $A_j(C^\perp) - A_j(D^\perp)$.

Chain rings

- In a chain ring the (left) ideals form a chain and are principal. Maximal ideal $\mathfrak{m} = (\theta)$, $R/\mathfrak{m} \cong \mathbb{F}_q$:

$$R = (\theta^0) \supset (\theta) \supset \cdots \supset (\theta^{m-1}) \supset (\theta^m) = (0).$$

- Cyclic modules $Z_k = R/(\theta^k)$ vs. semi-simple modules $S_k = Z_1 \oplus \cdots \oplus Z_1$ (k summands).
- Both have size $|Z_k| = |S_k| = q^k$.

Example: $\mathbb{Z}/8\mathbb{Z}$

- $\mathcal{U}$ is group of units, $w_i = w(2^i)$, $w(0) = w_3 = 0$.
- For code C, use $1 \times$ '3' generator matrix, with same multiplicity τ, so length is 3τ:

$$G_C = \frac{\tau \quad \tau \quad \tau}{1 \quad 2 \quad 4}.$$

- The weights of codewords, $w(xG_C)$, $x \in \mathbb{Z}/8\mathbb{Z}$, are

x	0	$1u$	$2u$	$4u$
$\lvert x\mathcal{U}\rvert$	1	4	2	1
$w(xG_C)$	0	$(w_0 + w_1 + w_2)\tau$	$(w_1 + w_2)\tau$	$w_2\tau$

$\mathbb{Z}/8\mathbb{Z}$, continued

- For D, use $3 \times$ '7' generator matrix, with multiplicities listed:

$$G_D = \begin{array}{cccc|cc|c} a_0 & a_0 & a_0 & a_0 & a_1 & a_1 & a_2 \\ \hline 0 & 4 & 0 & 4 & 0 & 4 & 4 \\ 0 & 0 & 4 & 4 & 4 & 4 & 0 \\ 4 & 4 & 4 & 4 & 0 & 0 & 0 \end{array}.$$

- Length is $4a_0 + 2a_1 + a_2$.

$\mathbb{Z}/8\mathbb{Z}$, continued more

- Number and weights of nonzero codewords of D:

x	number	$w(xG_D)$
$1{*}{*}$	4	$(2a_0 + a_1 + a_2)w_2$
$01{*}$	2	$(2a_0 + 2a_1)w_2$
001	1	$4a_0w_2$

- $x \in (\mathbb{Z}/2\mathbb{Z})^3$ because of the 4's in G_D.

$\mathbb{Z}/8\mathbb{Z}$, continued even more

- Match up, and solve for integers τ, a_i:

$$\begin{aligned}(2a_0 + a_1 + a_2)w_2 &= (w_0 + w_1 + w_2)\tau \\ (2a_0 + 2a_1)w_2 &= (w_1 + w_2)\tau \\ 4a_0 w_2 &= w_2\tau\end{aligned}$$

- $\tau = 4w_2$, $a_0 = w_2$, $a_1 = 2w_1 + w_2$, $a_2 = 4w_0 + 2w_1 + w_2$.
- Pad the shorter code with 0's.
- With these choices, $\mathrm{wwe}_C = \mathrm{wwe}_D$.

What about dual codes?

- In general, calculating $\mathrm{wwe}_{C^\perp}$ and $\mathrm{wwe}_{D^\perp}$ is nasty.
- But we can calculate the singletons in $C^\perp$ and $D^\perp$.
- *Singleton*: a vector with exactly one nonzero entry.
- A singleton r is in $C^\perp$ if r annihilates the functional (column) λ in its position: $\lambda r = 0$.
- Let $\mathring{w} = \min\{w_0, w_1, \ldots, w_{m-1}\}$.
- If $\mathring{w} \leq j < 2\mathring{w}$, then any vector in R^n of weight j must be a singleton.
- For $\mathring{w} \leq j < 2\mathring{w}$, $A_j(C^\perp) = A_j^{\mathrm{sing}}(C^\perp)$.

Back to $\mathbb{Z}/8\mathbb{Z}$

- Over $\mathbb{Z}/8\mathbb{Z}$, $\lambda = 4$ is killed by $r = 2, 4$; $\lambda = 2$ by $r = 4$; $\lambda = 1$ by none; $\lambda = 0$ by all.
- Net contributions by singleton ur's, $r = 2^i$:

i	r	to $A_{w_i}(C^\perp) - A_{w_i}(D^\perp)$
0	1	$4(4w_0 + 6w_1 - 5w_2)$
1	2	$-16w_2$
2	4	$-4w_2$

Other details for $\mathbb{Z}/8\mathbb{Z}$

- Similar construction at size 4: cyclic vs. semisimple.
- Net contributions:

i	r	to $A_{w_i}(C^\perp) - A_{w_i}(D^\perp)$
0	1	$4(2w_1 - w_2)$
1	2	$-4w_2$
2	4	0

- Between the two examples, can show that dual codes have different w-weight enumerators, except for the case of the Hamming weight.

Many* w-weight enumerators? Which ones?

- Recall that $\mathring{w} = \min\{w_0, w_1, \ldots, w_{m-1}\}$.
- Assumptions on weight w so that MacWilliams identities fail for wwe over a finite chain ring, except Hamming weight and homogeneous weight ($|R| = 4$ only):
  1. $\mathring{w} < w_0$;
  2. $\mathring{w} = w_0 < \min\{w_1, \ldots, w_{m-1}\}$;
  3. $\mathring{w} = w_0 \leq w_1 \leq \cdots \leq w_{m-1}$.

One slide about case $R = M_{k\times k}(\mathbb{F}_q)$

- Use message module $M = M_{k\times(k+1)}(\mathbb{F}_q)$.
- Functionals $\lambda \in \mathrm{Hom}_R(M, R) = M_{(k+1)\times k}(\mathbb{F}_q)$.
- For C, use all λ with $\mathrm{rk}\,\lambda = 1$, same multiplicity.
- Weights $w(xG_C)$ depend only on $\mathrm{rk}\,x$.
- To get D, swap weight values on one orbit of rank 2 in M with $q^k - q$ orbits of rank 1.
- For the homogeneous weight on R, all w_i satisfy $\mathring{w} \le w_i < 2\mathring{w}$ (except when $k = q = 2$, where $\mathring{w} = w_2 < w_1 = 2w_2$).

Thank you

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