

Distance enumerators for permutation groups

Robert Bailey

Carleton University

robertb@math.carleton.ca

<http://www.math.carleton.ca/~robertb/>

1st Ottawa Mathematics Conference

1st May 2008

Joint work with Jonathan Dixon

(Queen Mary, University of London/Sydney, Australia)

ERROR-CORRECTING CODES

- We want to transmit a message *accurately* along a “noisy channel”, where there may be interference.
- If the received message contains errors, we want to *decode* it to receive the original transmitted message.
- If the possible messages are sufficiently “different”, then this will be possible.
- What do we mean by “different”?
If messages are strings of the same length, then the *Hamming distance* between two strings is the number of places in which they differ.
- For example, $d_H(001, 010) = 2$.
- Formally, a *code*, C , is a set of strings of symbols chosen from some alphabet.

DISTANCE ENUMERATORS

- To help us analyse C , we can define the following polynomial, for a fixed word $w \in C$:

$$\Delta_{C,w}(x) = \sum_{c \in C} x^{d_H(c,w)}$$

This is the *distance enumerator* of C (at w).

- Usual setting: a *linear code* is a k -dimensional subspace of \mathbb{F}_q^n .
- In this case, the vector space structure tells us that we'll get the same polynomial for any $w \in C$, so we might as well take $w = \mathbf{0}$.
- So we get the *weight enumerator* of C ,

$$W_C(x, y) = \sum_{c \in C} x^{\text{wt}(c)} y^{n - \text{wt}(c)}$$

where $\text{wt}(c) = d_H(c, \mathbf{0})$.

CODING WITH PERMUTATION GROUPS

- Let G be a permutation group acting on a set Ω , where $|\Omega| = n$.
- We can write elements of G as ordered n -tuples of distinct symbols from Ω ,

$$\text{e.g. } 231794685 \in S_9.$$

- Idea: use G as a code, with permutations in this form as codewords.
- Can define Hamming distance as before:
for example,

$$d(15432, 25413) = 3.$$

DISTANCE ENUMERATORS FOR PERMUTATION GROUPS

- We notice that

$$\begin{aligned}d_H(g, h) &= \#x \text{ where } x^g \neq x^h \\ &= n - \pi(gh^{-1}).\end{aligned}$$

- $\pi(g)$ is the number of fixed points of $g \in G$, which is the *permutation character* of G .
- The group structure tells us that we'll get the same distance enumerator for any $g \in G$, so we might as well take $g = 1$ (the identity element).
- So we have:

$$\Delta_G(y) = \sum_{g \in G} y^{n - \pi(g)}$$

(where n is the *degree* of G).

COMPUTING WITH CHARACTERS

- We can rewrite the distance enumerator of a group G as

$$\Delta_G(y) = \sum_{g \in R} |g^G| y^{n - \pi(g)}$$

where R is a set of conjugacy class representatives for G , and g^G denotes the conjugacy class containing g .

- Computer algebra systems often have built-in commands for computing the values of $|g^G|$ and $\pi(g)$ (in GAP, these are the `SizesConjugacyClasses` and `NaturalCharacter` commands.)
- So by using these commands it is straightforward to find the coefficients of Δ_G .
- However, this method is often computationally expensive, and is not always very efficient!

CYCLE INDEX

- In fact, the distance enumerator is related to a well-studied polynomial.
- The *cycle index* of G is the polynomial

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} \prod_{i \geq 1} s_i^{c_i(g)}$$

where $c_i(g)$ is the number of i -cycles of g , and the s_i are indeterminates.

- By substituting $s_1 \leftarrow x$, $s_i \leftarrow y^i$ for $i > 1$, we obtain

$$Q_G(x, y) = \frac{1}{|G|} \sum_{g \in G} x^{\pi(g)} y^{n - \pi(g)},$$

so $\Delta_G(y) = |G|Q_G(1, y)$.

- There are various identities for the cycle index, that we hope to specialise to our polynomial Q_G .

DIRECT PRODUCTS

- Suppose G acts on Ω (where $|\Omega| = n$) and H acts on Γ (where $|\Gamma| = m$), where the sets Ω and Γ are disjoint.
- Then the direct product, $G \times H$, acts on the disjoint union $\Omega \cup \Gamma$ in an obvious way.
- Clearly, the number of fixed points of an element $(g, h) \in G \times H$ is the sum of those numbers for g and h .
- Thus, for its action on $\Omega \cup \Gamma$, we have

$$Q_{G \times H}(x, y) = Q_G(x, y)Q_H(x, y).$$

PRODUCT ACTION

- The direct product also acts on the Cartesian product of Ω and Γ (also in a fairly obvious way).
- This time, however, a point $(\omega, \gamma) \in \Omega \times \Gamma$ is fixed by an element $(g, h) \in G \times H$ iff ω is fixed by g and γ is fixed by h .
- Define a product of monomials $x^a y^b \circ x^c y^d$ by the rule

$$x^a y^b \circ x^c y^d = x^{ac} y^{bc+ad+bd}$$

which is then extended linearly to a product of polynomials, $f(x, y) \circ g(x, y)$.

- Then it is possible to show that for its action on $\Omega \times \Gamma$,

$$Q_{G \times H}(x, y) = Q_G(x, y) \circ Q_H(x, y).$$

- These two identities for the direct product answered a question of Blake, Cohen and Deza from 1979.

WREATH PRODUCTS

- Again, suppose G acts on Ω (where $|\Omega| = n$) and H acts on Γ (where $|\Gamma| = m$).
- The *wreath product* of G and H , denoted $G \wr H$, is formed as follows:
 - Take the union of m disjoint copies of Ω , which are labelled by the elements of Γ .
 - Let the direct product $G^m = G \times G \times \cdots \times G$ act componentwise on the m copies of Ω , and then let H permute the copies according to how it acts on the labels.
 - The resulting group $G^m \rtimes H := G \wr H$ is the wreath product.
- We also have an identity for the distance enumerator of the wreath product.

WREATH PRODUCTS CONTINUED

- We also have an identity for the distance enumerator of the wreath product.
- For the wreath product $G \wr H$ acting on mn points, we have

$$Q_{G \wr H}(x, y) = Q_H(Q_G(x, y), y^n).$$

- This identity can be proved directly.....

EXAMPLE

- Consider the group $S_2 \wr S_2$, which is isomorphic to the dihedral group D_8 (the symmetry group of the square).

- It's easy to see that $Q_{S_2}(x, y) = \frac{1}{2}(x^2 + y^2)$.

- So our identity gives us

$$\begin{aligned} Q_{S_2 \wr S_2}(x, y) &= \frac{1}{2} \left(\left(\frac{1}{2}(x^2 + y^2) \right)^2 + y^4 \right) \\ &= \frac{1}{8} \left(x^4 + 2x^2y^2 + 5y^4 \right), \end{aligned}$$

which agrees with what we would expect for $Q_{D_8}(x, y)$.

- Therefore the distance enumerator is

$$\Delta_{D_8}(y) = 1 + 2y^2 + 5y^4.$$

GENERALISED HYPEROCTAHEDRAL GROUPS

- The *generalised hyperoctahedral group* is the wreath product $G = C_m \wr S_n$.
- We can also use our identity to obtain a formula for Q_G for this group:

$$Q_G(x, y) = \frac{1}{m^n n!} \sum_{i=0}^{mn} f(i) x^i y^{mn-i}$$

where

$$f(i) = \begin{cases} \sum_{k=0}^n m^{n-k} (m-1)^{k-\frac{i}{m}} \binom{n}{k} \binom{k}{i/m} d(n-k) & \text{if } m \mid i, \\ 0 & \text{if } m \nmid i. \end{cases}$$

- While this is a messy formula, it is easy to find (computationally) the polynomials for specific values of m and n .