

# Distance enumerators for permutation groups

Robert Bailey

*Joint work with Jonathan Dixon*

Canadian Mathematical Society

Winter Meeting 2008

# Distance enumerators

- ▶ Suppose we have an error-correcting code  $C$ , with the usual Hamming distance  $d_H$ .

# Distance enumerators

- ▶ Suppose we have an error-correcting code  $C$ , with the usual Hamming distance  $d_H$ .
- ▶ To help us analyse  $C$ , we can define the following polynomial, for a fixed word  $w \in C$ :

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

# Distance enumerators

- ▶ Suppose we have an error-correcting code  $C$ , with the usual Hamming distance  $d_H$ .
- ▶ 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  $w$ ).

## Distance enumerators, continued

- ▶ Usual setting: a *linear code* is a  $k$ -dimensional subspace of  $\mathbb{F}_q^n$ .

## Distance enumerators, continued

- ▶ 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  $w = \mathbf{0}$ .

## Distance enumerators, continued

- ▶ 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  $\Omega$ , where  $|\Omega| = n$ .

# Coding with permutation groups

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

e.g.  $231794685 \in S_9$ .

# Coding with permutation groups

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

e.g.  $231794685 \in S_9$ .

- ▶ Idea: use  $G$  as a code, with permutations in this form as codewords.

# Coding with permutation groups

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

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,

$$d_H(1\ 5\ 4\ 3\ 2, 2\ 5\ 4\ 1\ 3) = 3.$$

# Distance enumerators for permutation groups

- ▶ We notice that

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

# 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  $G$ .

# 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).

# 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  $g$ .

# 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.)

# 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  $\Delta_G$ .

# 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  $\Delta_G$ .
- ▶ 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.

# 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.

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

## 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  $\Omega$  (where  $|\Omega| = n$ ) and  $H$  acts on  $\Gamma$  (where  $|\Gamma| = m$ ), where the sets  $\Omega$  and  $\Gamma$  are disjoint.

## Direct products

- ▶ Suppose  $G$  acts on  $\Omega$  (where  $|\Omega| = n$ ) and  $H$  acts on  $\Gamma$  (where  $|\Gamma| = m$ ), where the sets  $\Omega$  and  $\Gamma$  are disjoint.
- ▶ Then the direct product,  $G \times H$ , acts on the disjoint union  $\Omega \cup \Gamma$  in an obvious way.

## Direct products

- ▶ Suppose  $G$  acts on  $\Omega$  (where  $|\Omega| = n$ ) and  $H$  acts on  $\Gamma$  (where  $|\Gamma| = m$ ), where the sets  $\Omega$  and  $\Gamma$  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  $h$ .

## Direct products

- ▶ Suppose  $G$  acts on  $\Omega$  (where  $|\Omega| = n$ ) and  $H$  acts on  $\Gamma$  (where  $|\Gamma| = m$ ), where the sets  $\Omega$  and  $\Gamma$  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

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

## Direct product: product action

- ▶ The direct product also acts on the Cartesian product of  $\Omega$  and  $\Gamma$  (also in a fairly obvious way).

## Direct product: product action

- ▶ The direct product also acts on the Cartesian product of  $\Omega$  and  $\Gamma$  (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  $\omega$  is fixed by  $g$  and  $\gamma$  is fixed by  $h$ .

## Direct product: product action

- ▶ The direct product also acts on the Cartesian product of  $\Omega$  and  $\Gamma$  (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  $\omega$  is fixed by  $g$  and  $\gamma$  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,  $f(x, y) \circ g(x, y)$ .

## Direct product: product action

- ▶ The direct product also acts on the Cartesian product of  $\Omega$  and  $\Gamma$  (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  $\omega$  is fixed by  $g$  and  $\gamma$  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  $\Omega \times \Gamma$ ,

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

## Direct product: product action

- ▶ The direct product also acts on the Cartesian product of  $\Omega$  and  $\Gamma$  (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  $\omega$  is fixed by  $g$  and  $\gamma$  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  $\Omega$  (where  $|\Omega| = n$ ) and  $H$  acts on  $\Gamma$  (where  $|\Gamma| = m$ ).

# Wreath products

- ▶ Again, suppose  $G$  acts on  $\Omega$  (where  $|\Omega| = n$ ) and  $H$  acts on  $\Gamma$  (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  $\Omega$ , which are labelled by the elements of  $\Gamma$ .
  - ▶ Let the direct product  $G^m = G \times G \times \cdots \times G$  act componentwise on the  $m$  copies of  $\Omega$ , 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.

## Wreath products, continued

- ▶ 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

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

## 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.....

Ouch!

$$\begin{aligned} Q_{G \wr H}(x, y) &= \frac{1}{|G \wr H|} \sum_{a \in G \wr H} x^{\pi(a)} y^{nm - \pi(a)} \\ &= \frac{1}{|G|^m |H|} \sum_{a \in G \wr H} \prod_{i=1}^m x^{\pi_i(a)} y^{n - \pi_i(a)} \\ &= \frac{1}{|G|^m |H|} \sum_{h \in H} \sum_{(g_1, \dots, g_m) \in G^m} \prod_{i \in \text{Fix}(h)} x^{\psi(g_i)} y^{n - \psi(g_i)} \prod_{i \in \text{Supp}(h)} y^n \\ &= \frac{1}{|H|} \sum_{h \in H} \left( \prod_{i \in \text{Fix}(h)} \frac{1}{|G|} \sum_{g_i \in G} x^{\psi(g_i)} y^{n - \psi(g_i)} \right) \left( \prod_{i \in \text{Supp}(h)} \frac{1}{|G|} \sum_{g_i \in G} y^n \right) \\ &= \frac{1}{|H|} \sum_{h \in H} \left( \prod_{i \in \text{Fix}(h)} Q_G(x, y) \right) \left( \prod_{i \in \text{Supp}(h)} y^n \right) \\ &= Q_H(Q_G(x, y), y^n). \end{aligned}$$

## Example

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

## 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  $Q_{S_2}(x, y) = \frac{1}{2}(x^2 + y^2)$ .

## 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

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

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

## 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

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

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  $G = C_m \wr S_n$ .

# 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

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

# 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, for specific values of  $m$  and  $n$  one can compute these polynomials near-instantaneously.

THE END

# THE END

► Reference:

R. F. Bailey and J. P. Dixon, Distance enumerators for permutation groups, *Comm. Algebra* **35** (2007), 3045–3051.