Distance enumerators for permutation groups

Robert F. Bailey[*] and Jonathan P. Dixon
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road, London E1 4NS

November 14, 2006

Abstract

We consider the *distance enumerator* $\Delta_G(x)$ of a finite permutation group G, which is the polynomial $\sum_{g \in G} x^{n-\pi(g)}$, where n is the degree of G and $\pi(g)$ the number of fixed points of $g \in G$. In particular, we introduce a bivariate polynomial which is a special case of the cycle index of G, and from which $\Delta_G(x)$ can be obtained, and then use this new polynomial to prove some identities relating the distance enumerators of groups G and H with those of their direct and wreath products. In the case of the direct product, this answers a question of Blake, Cohen and Deza from 1979. We also use the identity for the wreath product to find an explicit combinatorial expression for the distance enumerators of the generalised hyperoctahedral groups $C_m \wr S_n$.

1 Introduction

For any code C (i.e. a set of words C where the Hamming distance d_H can be defined), and for a fixed codeword $w \in C$, one can define the following polynomial.

Definition 1. The *distance enumerator* of C at w is the polynomial

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

In the case where C is a *linear code* (i.e. a vector space over a finite field), the distance enumerator is independent of w, so it is conventional to take w to be the zero codeword, and thus the exponent in each term is $d_H(\mathbf{0}, c) = \mathrm{wt}(c)$, the *weight*

---

[*]Corresponding author. E-mail `r.f.bailey@qmul.ac.uk`

of c. Then the polynomial obtained is known as the *weight enumerator*, which is usually written as a two-variable, homogeneous polynomial as follows:

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

where n is the length of the codewords. While this is really just a one-variable polynomial 'in disguise', the two variables are of use, for instance in proving the *MacWilliams identities* which relate the weight enumerator of a linear code to that of its dual code; see Cameron and van Lint [7], chapter 9, for details.

In this article, we consider the distance enumerators of codes which are permutation groups. If one writes the elements of a permutation group G acting on $\Omega = \{1, \ldots, n\}$ in *list form* (i.e. as a list of the images of the points $1, \ldots, n$ in order), one can define the Hamming distance on these as usual. Now, for permutations $g, h \in G$, we have that $d_H(g,h) = n - \pi(gh^{-1})$, where $\pi(g)$ denotes the number of fixed points of G. Also, since G is a group, we have that for a fixed element g, the number of elements h such that $d_H(g,h) = i$ is the same as the number of elements at distance i from the identity. Hence the distance enumerator is independent of the choice of g, so we have

$$\Delta_G(x) = \sum_{g \in G} x^{d_H(1,g)} = \sum_{g \in G} x^{n - \pi(g)}.$$

We use the notation π as it is precisely the *permutation character* of the group G (see Cameron [5], chapter 2, for details). Now, as characters are constant on the conjugacy classes of G, we can rewrite the distance enumerator as follows:

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

where R is a set of conjugacy class representatives for G, and g^G denotes the conjugacy class containing g. This is a useful form for computing the distance enumerator, as computer algebra packages such as GAP [8] have inbuilt commands for computing the values of $|g^G|$ and $\pi(g)$ for a group G in a given action. (In GAP, these are the `SizesConjugacyClasses` and `NaturalCharacter` commands.) Thus, by using these commands, obtaining the coefficients of $\Delta_G(x)$ is a straightforward task, although (as we shall see in section 4) this method is not necessarily an efficient one.

2   The cycle index and related polynomials

In this section, we show how the distance enumerator $\Delta_G(x)$ is related to certain other polynomials, in particular the cycle index.

Definition 2. The *cycle index* of a group G acting on a finite set Ω is the polynomial

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

2

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

This is a well-studied polynomial; see Cameron [4], chapter 15, for a discussion of its properties. Now, the polynomial

$$P_G(x) = \frac{1}{|G|} \sum_{g \in G} x^{\pi(g)}$$

is clearly a special case of the cycle index, obtained by substituting x for s_1 and 1 for all other s_i, and by noting that $c_1(g) = \pi(g)$. ($P_G(x)$ is the probability generating function for the expected number of fixed points of a random element of G.) Obtaining this polynomial $P_G(x)$ is clearly equivalent to obtaining the distance enumerator, as (ignoring the scaling factor) the coefficients are exactly the same, but in the reverse order. So we have

$$\Delta_G(x) = |G| x^n P_G(\tfrac{1}{x}).$$

However, we will not use this identity when studying the distance enumerator. Instead, we introduce a new polynomial which encodes both $P_G(x)$ and $\Delta_G(x)$ simultaneously.

Definition 3. The *homogeneous support enumerator*, $Q_G(x,y)$, is defined as

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

where n is the degree of the group G.

This can obtained from the cycle index via the substitution

$$Q_G(x,y) = Z(G; s_1 \leftarrow x, s_i \leftarrow y^i \ \forall i > 1)$$

as $\sum_{i>1} i c_i(g) = n - \pi(g)$. Clearly, we have $P_G(x) = Q_G(x,1)$ and $\Delta_G(y) = |G| Q_G(1,y)$.
The name comes from the set of points moved by $g \in G$ being known as the *support* of G.

In the next section, we will see how this polynomial is the appropriate one to use when studying the distance enumerator.

3 Identities for direct and wreath products

There are known identities relating the cycle indices of G and H with those of the direct product $G \times H$, in both the usual (i.e. intransitive) and product actions. There is also an identity for the wreath product $G \wr H$ in the imprimitive action. For details these, we refer the reader to Cameron [4] and (for the direct product in the product action) to Cameron, Gewurz and Merola [6]. In this section, we derive similar identities for the homogeneous support enumerator, which then enable us

3

to compute the distance enumerator for these products. However, for each of the three identities, we will give direct proofs.

In each of the following, we suppose we have groups G and H acting on sets Ω and Γ respectively, where $|\Omega| = n$ and $|\Gamma| = m$.

Proposition 4. *For the direct product of G and H in the intransitive action on $\Omega \dot\cup \Gamma$, we have*
$$Q_{G \times H}(x,y) = Q_G(x,y)Q_H(x,y).$$

Proof. Suppose $g \in G$ fixes a set of a points A, and that $h \in H$ fixes a set of b points B. Then $(g,h) \in G \times H$ fixes the set $A \dot\cup B$ which has size $a + b$. So we have

$$
\begin{aligned}
Q_{G \times H}(x,y) &= \sum_{(g,h) \in G \times H} x^{a+b} y^{n+m-a-b} \\
&= \sum_{g \in G} x^a y^{n-a} \sum_{h \in H} x^b y^{m-b} \\
&= Q_G(x,y)Q_H(x,y).
\end{aligned}
$$

$\square$

In order to show how the homogeneous support enumerators of G and H are related to that of $G \times H$ in the product action, we 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, $f(x,y) \circ g(x,y)$. This is a specialisation of a corresponding product for the cycle index, as given by Cameron, Gewurz and Merola [6].

Proposition 5. *For the direct product $G \times H$ in the product action on $\Omega \times \Gamma$, we have*
$$Q_{G \times H}(x,y) = Q_G(x,y) \circ Q_H(x,y).$$

Proof. Again, we suppose $g \in G$ fixes a set of a points A, and that $h \in H$ fixes a set of b points B. This time $(g,h) \in G \times H$ fixes the set $A \times B$ which has size ab. Now, by definition, $x^a y^{n-a} \circ x^b y^{m-b} = x^{ab} y^{mn-ab}$, which is the monomial corresponding to (g,h). So we have

$$
\begin{aligned}
Q_{G \times H}(x,y) &= \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} x^{ab} y^{mn-ab} \\
&= \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} x^a y^{n-a} \circ x^b y^{m-b} \\
&= \left(\frac{1}{|G|} \sum_{g \in G} x^a y^{n-a} \right) \circ \left(\frac{1}{|H|} \sum_{h \in H} x^b y^{m-b} \right) \\
&= Q_G(x,y) \circ Q_H(x,y).
\end{aligned}
$$

$\square$

Determining these identities for the two actions of the direct product answers a question posed by Blake, Cohen and Deza [3], which asked how the distance enumerator of $G \times H$ is related to those of G and H.

Proposition 6. *For the wreath product in the imprimitive action, we have*

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

Proof. First, we set up our notation. Let π denote the permutation character of $G \wr H$ (so $\pi(a)$ is the number of fixed points of $a \in G \wr H$). Similarly, we let ψ denote the permutation character of G. For $h \in H$, $\mathrm{Fix}(h)$ denotes the set of points fixed by h, and $\mathrm{Supp}(h)$ denotes the set of points moved by h (i.e. the support of h).

Recall that $G \wr H$ (in the imprimitive action) acts on m blocks of size n; we label these blocks by the elements of $\Gamma = \{1, \ldots, m\}$. Also recall that an element $a \in G \wr H$ has the form $a = (g_1, \ldots, g_m; h)$. For such an element a we count the number of fixed points of a as follows.

Each block moved by h has all n points moved, while each block (say block i) fixed by h has $\psi(g_i)$ fixed points, and $n - \psi(g_i)$ moved points. So we can write $\pi(a) = \pi_1(a) + \cdots + \pi_m(a)$, where

$$\pi_i(a) = \begin{cases} \psi(g_i) & \text{if } i \in \mathrm{Fix}(h), \\ 0 & \text{if } i \in \mathrm{Supp}(h). \end{cases}$$

Thus we have

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

$\square$

Example 7. Consider the group $S_2 \wr S_2$, which is isomorphic to the dihedral group D_8. Now, $Q_{S_2}(x,y) = \frac{1}{2}(x^2 + y^2)$, so by Proposition 6 we have

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

5

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

4   Generalised hyperoctahedral groups

In this section we determine the distance enumerators of the groups $C_m \wr S_n$, in the imprimitive action on mn points. (Note that m and n have been reversed with respect to the previous section). As this family of groups contains the hyperoctahedral group $C_2 \wr S_n$, we use the name *generalised hyperoctahedral groups* for them. They are of interest in a coding theory setting; see the first author's papers [1, 2] for details of decoding algorithms for these groups when viewed as error-correcting codes.

The homogeneous support enumerators for C_m and S_n are both straightforward to calculate. In the cyclic group C_m, all $(m-1)$ non-identity elements move m points, so $Q_{C_m}(x,y) = \frac{1}{m}(x^m + (m-1)y^m)$. In the symmetric group S_n, the number of elements with k fixed points is precisely $\binom{n}{k}d(n-k)$ (where $d(i)$ is the number of derangements of a set of size i), for $0 \le k \le n$. Thus we have

$$Q_{S_n}(x,y) = \frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}d(n-k)x^k y^{n-k}.$$

So to calculate $Q_G(x,y)$ for $G = C_m \wr S_n$, we appeal to Proposition 6, giving the following result.

Proposition 8. *The homogeneous support enumerator of the generalised hyperoctahedral group $G = C_m \wr S_n$ is given by $Q_G(x,y) = \dfrac{1}{m^n n!}\displaystyle\sum_{i=0}^{mn} f(i)x^i y^{mn-i}$, where*

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

Proof. Using the substitution given in Proposition 6 (recalling that m and n have been interchanged from that proof), we obtain

$$
\begin{aligned}
Q_G(x,y) &= Q_{S_n}\big(\tfrac{1}{m}(x^m + (m-1)y^m), y^m\big) \\
&= \frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}d(n-k)\frac{1}{m^k}(x^m + (m-1)y^m)^k y^{m(n-k)} \\
&= \frac{1}{m^n n!}\sum_{k=0}^{n}m^{n-k}\binom{n}{k}d(n-k)\left(\sum_{j=0}^{k}\binom{k}{j}x^{mj}(m-1)^{k-j}y^{m(k-j)}\right)y^{m(n-k)} \quad (\star) \\
&= \frac{1}{m^n n!}\sum_{k=0}^{n}m^{n-k}\binom{n}{k}d(n-k)\sum_{j=0}^{n}\binom{k}{j}(m-1)^{k-j}x^{mj}y^{m(n-j)} \quad (\star\star) \\
&= \frac{1}{m^n n!}\sum_{j=0}^{n}\sum_{k=0}^{n}m^{n-k}(m-1)^{k-j}\binom{n}{k}\binom{k}{j}d(n-k)x^{mj}y^{m(n-j)}.
\end{aligned}
$$

($(\star)$ follows from the binomial theorem, while $(\star\star)$ follows from the observation that for $j > k$, $\binom{k}{j} = 0$.) The result can then be obtained from this, by noting that in the above expression, the powers of x and y occur only at multiples of m, thus any other powers will have coefficient 0. $\square$

We remark that this agrees with what we would expect, in that the number of fixed points of an element of $G = C_m \wr S_n$ clearly must be a multiple of m. Now, obtaining the distance enumerator of G is a matter of substituting $x = 1$ into $Q_G(x, y)$ and multiplying by $|G|$. That is, we have the following:

Corollary 9. *The distance enumerator of the generalised hyperoctahedral group $G = C_m \wr S_n$ is given by $\Delta_G(y) = \sum_{i=0}^{mn} g(i)y^i$, where $g(i) = f(mn - i)$ (and f is as in Proposition 8 above).*

We conclude with two remarks. First, we note that replacing a cyclic group of order m with a more general regular group of degree m does not alter the results of Proposition 8 and Corollary 9. Second, we remark that implementing the above formula in GAP to compute the coefficients of $\Delta_G(x)$ takes a considerably shorter amount of time than the method described in section 1. For instance, for $C_{10} \wr S_7$, it took 10 milliseconds compared with 33 minutes.

References

[1] R. F. Bailey, Uncoverings-by-bases for base-transitive permutation groups, *Des. Codes Cryptogr.* **41** (2006), 153–176.

[2] R. F. Bailey and T. Prellberg, Decoding generalised hyperoctahedral groups and asymptotic enumeration of error patterns, in preparation.

[3] I. F. Blake, G. Cohen and M. Deza, Coding with permutations, *Information and Control* **43** (1979), 1–19.

[4] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, 1994.

[5] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts (45), Cambridge University Press, Cambridge, 1999.

[6] P. J. Cameron, D. A. Gewurz and F. Merola, Product action, to appear in *Discrete Math.*

[7] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, London Mathematical Society Student Texts (22), Cambridge University Press, Cambridge, 1991.

[8] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2004, (http://www.gap-system.org).