On the Character of S_n acting on Subspaces of $\mathbb{F}_q^n$

R. F. Lax

September 4, 2003

A binary code of length n is a subspace of the vector space $\mathbb{F}_2^n$. Two such codes are equivalent if one can be obtained from the other by permuting coordinates. Thus, one can consider the action of S_n on the set of all subspaces of $\mathbb{F}_2^n$ defined by permuting coordinates, and the equivalence classes of binary codes of length n are exactly the orbits of this action.

More generally, one can consider the action of S_n on all subspaces of $\mathbb{F}_q^n$, but two q-ary codes of length n are equivalent if one can be obtained from the other by permuting coordinates and/or multiplying some coordinates by nonzero elements of $\mathbb{F}_q$. This leads one to consider the action of the wreath product of $\mathbb{F}_q^\times$ and S_n on the subspaces of $\mathbb{F}_q^n$, and the equivalence classes of q-ary codes of length n are the orbits of this action.

Let $G_{n,q}$ denote the number of subspaces of the vector space $\mathbb{F}_q^n$. This number was called a Galois number by J. Goldman and G.-C. Rota [4], and they showed that

$$G_{n,q} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q ,$$

where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the q-binomial coefficient.

If $f, g : \mathbb{N} \to \mathbb{R}^+$, then we write $f \sim g$ if $f(n)/g(n) \to 1$ as $n \to \infty$. We write $f(n) = O(g(n))$ if there exists a constant C and an integer n_0 such that $f(n) \leq Cg(n)$ for all $n \geq n_0$. Let $b(n)$ denote the number of distinct equivalence classes of binary codes of length n. M. Wild [8] claimed that, asymptotically, $b(n) \sim G_{n,2}/n!$. However, there is a mistake in the proof of (24) in [8]. In that argument, if $\sigma \in S_n$ and σ is the product of disjoint cycles $C_1, \ldots, C_r$, then $\rho(\sigma)$ denotes the number of the cycles C_j that have length equal to a power of 2 (including 2^0). If the length of C_j is l_j and one writes $l_j = 2^{\alpha_j} u_j$, with u_j odd and $\alpha_j \geq 0$, for $j = 1, \ldots, r$, then $\mu_1 = \max\{2^{\alpha_j} | 1 \leq j \leq r\}$. Wild puts $\tau = \sigma^{\mu_1}$ and claims in the proof of (24) that $\rho(\tau) = \rho(\sigma)$. However, this is false. For example, if n is even and σ is a product of $n/2$ disjoint transpositions, then τ is the identity, so $\rho(\tau) = n$ while $\rho(\sigma) = n/2$. In a private communication, Wild suggested that the definition of ρ could be changed to equal the sum of the lengths of those C_j that have length equal to a power of 2. This would allow the proof of his (24) to go through, but it creates a problem in the proof of his (25). There does not appear to be an easy way to fix this gap in Wild's arguments. Let $\mathcal{G}_{n,q}$ denote the set of all subspaces of the vector space $\mathbb{F}_q^n$. Then S_n acts on $\mathcal{G}_{n,q}$ by permuting the coordinates of $\mathbb{F}_q^n$, and we let χ_n denote the character of the associated permutation representation. Thus, if $\sigma \in S_n$, then

$$\chi_n(\sigma) = \#\{W \in \mathcal{G}_{n,q} | \sigma \cdot W = W\}.$$

Our main result is that, for all q, the normalized character $\chi_n / G_{n,q}$ asymptotically approaches the trivial character (which takes the value 1 on the identity and 0 on all other permutations). In order to prove Wild's result, one needs that

$$\sum_{\sigma \neq (1)} \chi_n(\sigma)/G_{n,2} \to 0 \text{ as } n \to \infty,$$

where (1) denotes the identity permutation, so our result when $q = 2$ is weaker. Our results are not surprising in light of the work of A. M. Vershik and S. V. Kerov [7] and P. Biane [1, 2], who have shown that the normalized characters of irreducible representations of S_n corrresponding to "balanced" Young diagrams approach the trivial character asymptotically.

We thank W. A. Adkins and James Oxley for very helpful conversations and suggestions.

1 Preliminaries

Let q be a power of a prime p. We define an action of S_n on $\mathbb{F}_q^n$ as follows. If we think of an element $(x_1, x_2, \ldots, x_n)$ of $\mathbb{F}_q^n$ as being the mapping $\phi : \{1, 2, \ldots, n\} \to \mathbb{F}_q$ that takes i to x_i, then, given $\sigma \in S_n$, we define $\sigma\phi$ to be the mapping $\phi \circ \sigma^{-1}$. So, if $\sigma \in S_n$, then let

$$T_\sigma : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

denote the linear map that sends $(x_1, x_2, \ldots, x_n)$ to

$$(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)}).$$

The matrix of T_σ relative to the canonical basis of $\mathbb{F}_q^n$ is just the permutation matrix obtained by applying the permutation σ to the rows of the $n \times n$ identity matrix.

We then have an action of S_n on $\mathcal{G}_{n,q}$ given by

$$\begin{array}{ccccc} S_n & \times & \mathcal{G}_{n,q} & \to & \mathcal{G}_{n,q} \\ & (\sigma, W) & & \mapsto & T_\sigma(W) \end{array}$$

This differs from the action defined in [8], but agrees with the action defined in [6]. Let χ_n denote the character of the associated permutation representation of S_n.

Let T be a linear transformation on a finite-dimensional vector space V. The lattice $\mathcal{L}(T)$ of T-invariant subspaces consists of all subspaces W of V such that $T(W) \subseteq W$. Then, with notation as above, we have $\chi_n(\sigma) = \#\mathcal{L}(T_\sigma)$. Let $g_1^{n_1}(X) g_2^{n_2}(X) \cdots g_s^{n_s}(X)$ be the factorization of the minimal polynomial of T into a product of powers of irreducible polynomials over $\mathbb{F}_q$. Put

$$V_i = \ker g_i(T)^{n_i} \text{ and } T_i = T|_{V_i}$$

for $i = 1, 2, \ldots, s$. The Primary Decomposition Theorem [5] says that $V = \oplus_{i=1}^s V_i$, each V_i is invariant under T, and the minimal polynomial of T_i is $g_i^{n_i}(X)$. Also, from [3], we have that

$$\mathcal{L}(T) = \oplus_{i=1}^s \mathcal{L}(T_i).$$

The dimension of the subspace of vectors left fixed by T_σ is well-known. Write σ as the product of disjoint cycles, including cycles of length 1. Let $c(\sigma)$ denote the number of cycles in this decomposition.

Lemma 1.1. *The dimension of* $\ker(T_\sigma - I)$ *is* $c(\sigma)$.

Proof. Let $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$. Write σ as a product of disjoint cycles. Then T_σ leaves $\vec{x}$ fixed precisely when, for each cycle $(i_1, i_2, \ldots, i_m)$ in this product, we have $x_{i_1} = x_{i_2} = \cdots = x_{i_m}$. Therefore, σ leaves $q^{c(\sigma)}$ vectors fixed. □

Lemma 1.2. *Suppose $\sigma = C_1C_2\cdots C_r$ is the product of disjoint cycles of lengths $l_1, l_2, \ldots, l_r$, respectively. If p_1 is a prime divisor of l_j for some $j = 1, 2, \ldots, r$, then there exists N such that σ^N is a product of disjoint cycles of length p_1.*

Proof. Let N' denote the least common multiple of $l_1, l_2, \ldots, l_r$. Then N' is the order of σ in the symmetric group. Put $N = N'/p_1$. Then the order of σ^N is p_1, which implies that σ^N is a product of disjoint cycles of length p_1. □

Lemma 1.3. *Let σ be a product of disjoint cycles of lengths $m^{r_1}, \ldots, m^{r_s}$, where $r_1 \geq r_2 \geq \cdots \geq r_s \geq 0$. Then the minimal polynomial of T_σ is $X^{m^{r_1}} - 1$.*

Proof. Clearly, $(T_\sigma)^{m^{r_1}}$ is the identity map. Now let $f(X)$ be a polynomial with leading term a_dX^d, where $d < m^{r_1}$. Without loss of generality, we may assume that the decomposition of σ as a product of disjoint cycles contains the cycle $(1, 2, \ldots, m^{r_1})$. Then the image of the n-tuple $(1, 0, 0, \ldots, 0)$ under the map $f(T_\sigma)$ is the n-tuple with a_d in the $(d+1)$st coordinate, hence $f(T_\sigma)$ is nonzero. □

In the special case when σ is the product of disjoint transpositions and $p \neq 2$, we can give the value of $\chi_n(\sigma)$ exactly.

Proposition 1.4. *Suppose $p \neq 2$. Let σ be the product of t disjoint transpositions. Then*

$$\chi_n(\sigma) = G_{n-t,q} \cdot G_{t,q}.$$

Proof. The minimal polynomial of T_σ is $(X-1)(X+1)$. The dimension of $V_1 = \ker(T_\sigma - I)$ is $c(\sigma) = t + n - 2t = n - t$, and the dimension of $V_2 = \ker(T_\sigma + I)$ is then t. It is clear that each subspace of V_1 and V_2 is left fixed by the restriction of T_σ, so $\#\mathcal{L}(T_1) = G_{n-t,q}$ and $\#\mathcal{L}(T_2) = G_{t,q}$. □

Since $G_{n,q} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q$, and since $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is a polynomial in q of degree $k(n-k)$, one expects that $G_{n,q}$ behaves asymptotically like $q^{n^2/4}$ (coming from the q-binomial coefficient with $k = n/2$) . Indeed, Wild [8] showed the following result.

Lemma 1.5. *For each fixed prime power q, there are nonzero constants a_1, a_2 (dependent on q) such that*

$$G_{2m+1,q} \sim a_1 q^{(2m+1)^2/4} \text{ and } G_{2m,q} \sim a_2 q^{(2m)^2/4}.$$

2 Main theorem

Theorem 2.1. *Put*

$$\tilde{\chi}(n) = \max_{\sigma \neq (1)} \chi_n(\sigma)/G_{n,q}.$$

Then

$$\tilde{\chi}(n) = O(q^{-n/2}).$$

Proof. We split up the permutations into two classes. First, suppose there exists a prime $p_1 \neq p$ such that p_1 divides the length of some cycle in the decomposition of σ into a product of disjoint cycles. Then by Lemma 1.2, there exists N such that σ^N is a product of disjoint cycles of length p_1. Note that $\chi_n(\sigma) \leq \chi_n(\sigma^N)$. By Lemma 1.3, the minimal polynomial of σ^N is $X^{p_1} - 1$.

Let

$$X^{p_1} - 1 = (X-1)g_2(X)g_3(X)\cdots g_r(X)$$

be the factorization of $X^{p_1} - 1$ into the product of irreducible polynomials over $\mathbb{F}_q$. Put $V_i = \ker(g_i(T_{\sigma^N}))$ and $V' = \oplus_{i=2}^r V_i$.

From Lemma 1.1, the dimension of V_1 is $c(\sigma^N)$, and from the Primary Decomposition Theorem, the dimension of V' is $n - c(\sigma^N)$. It follows that $\chi_n(\sigma) \leq \chi_n(\sigma^N) \leq G_{c(\sigma^N),q} G_{n-c(\sigma^N),q}$. Now,

$$G_{c(\sigma^N),q} G_{n-c(\sigma^N),q} = O(q^{[c(\sigma^N)^2 + (n-c(\sigma^N))^2]/4}) = O(q^M),$$

where

$$\begin{aligned} M &= \tfrac{c(\sigma^N)^2 + (n-c(\sigma^N))^2}{4} \\ &= \tfrac{n^2 - 2c(\sigma^N)[n-c(\sigma^N)]}{4}. \end{aligned}$$

It is easy to see that the minimum of $c(\mu)[n - c(\mu)]$ over all nontrivial permutations $\mu \in S_n$ is $n-1$. (We remark that $n - c(\mu)$ is frequently denoted $|\mu|$ and equals the minimum number of transpositions needed to write μ as a product of transpositions.) Hence, if n is sufficiently large, we have that $\chi_n(\sigma)$ will be bounded by a constant (not dependent on σ) times

$$q^{\frac{n^2}{4}-\frac{n}{2}}.$$

Using Lemma 1.5, it follows that $\chi_n(\sigma)/G_{n,q}$ is bounded by a constant times $q^{-\frac{n}{2}}$ if n is sufficiently large.

Our second class of permutations consists of those permutations that are the disjoint product of cycles each having length equal to a power of p. If σ is such a nontrivial permutation, then it follows from Lemma 1.3 that the minimal polynomial of T_σ is of the form $X^{p^m}-1=(X-1)^{p^m}$ for some $m>0$. Now we argue as in [8], pp. 199-200. Since a subspace of V is T_σ-invariant if and only if it is $(T_\sigma-I)$-invariant, we have $\mathcal{L}(T_\sigma)=\mathcal{L}(T_\sigma-I)$. Since $T_\sigma-I$ is nilpotent, we may apply the following result due to Brickman and Fillmore:

Lemma 2.2. *([3], Theorem 7). If Q is nilpotent on V, then*

$$\mathcal{L}(Q)=\cup_{W\in\mathcal{L}(Q|_{Q(V)})}[W,Q^{-1}(W)],$$

where $[W,Q^{-1}(W)]$ is an interval in the lattice of all subspaces of V. Each interval satisfies the equation

$$\dim Q^{-1}(W)-\dim W=\dim\ker Q.$$

In our setting, if we put $Q=T_\sigma-I$, then $\dim\ker Q=c(\sigma)$, and $\dim Q(V)=n-c(\sigma)$. Then the number of subspaces in each interval $[W,Q^{-1}(W)]$ is bounded by $G_{c(\sigma),q}$ and $\#\mathcal{L}(Q|_{Q(V)})\le G_{n-c(\sigma),q}$, so we have

$$\chi_n(\sigma)=\#\mathcal{L}(T_\sigma-I)\le G_{n-c(\sigma),q}G_{c(\sigma),q}.$$

As in the argument above,

$$G_{n-c(\sigma),q}G_{c(\sigma),q}=O(q^{M'}),$$

where $M'=\frac{n^2-2c(\sigma)[n-c(\sigma)]}{4}$. Hence, as above, we get that $\chi_n(\sigma)/G_{n,q}$ is bounded by a constant times $q^{-\frac{n}{2}}$ if n is sufficiently large.

□

3 Remarks on the action of the wreath product

Let $\mathbb{F}_q^\times$ wr S_n denote the wreath product of the multiplicative group of $\mathbb{F}_q$ and the symmetric group S_n. (This is also sometimes called the complete monomial group on $\mathbb{F}_q^\times$, or a generalized symmetric group, since $\mathbb{F}_q^\times$ is the cyclic group of order $q-1$.) We recall (cf.[6]) that the elements of this wreath product look like

$$(\vec{\alpha};\sigma) = (\alpha_1, \alpha_2, \ldots, \alpha_n; \sigma),$$

where $\alpha_i \in \mathbb{F}_q^\times$ for $i = 1, 2, \ldots, n$ and $\sigma \in S_n$. The operation in the wreath product is defined by

$$(\vec{\alpha};\sigma)(\vec{\beta};\tau) = (\alpha_1\beta_{\sigma^{-1}(1)}, \ldots, \alpha_n\beta_{\sigma^{-1}(n)}; \sigma\tau).$$

We have an action of $\mathbb{F}_q^\times$ wr S_n on $\mathbb{F}_q^n$ given by

$$(\vec{\alpha};\sigma)\cdot(x_1, x_2, \ldots, x_n) = (\alpha_1 x_{\sigma^{-1}(1)}, \ldots, \alpha_n x_{\sigma^{-1}(n)}).$$

Thus, this action permutes the coordinates according to the permutation σ and then multiplies the (new) ith coordinate by α_i for $i = 1, 2, \ldots, n$. This gives a linear mapping $T_{(\vec{\alpha};\sigma)}$ on $\mathbb{F}_q^n$ for each element of $\mathbb{F}_q^\times$ wr S_n and the matrix of this linear mapping with respect to the canonical basis is the generalized permutation matrix obtained by permuting the rows of the $n \times n$ identity matrix according to σ and then multiplying the ith row by α_i for $i = 1, 2, \ldots, n$. We then have an action of $\mathbb{F}_q^\times$ wr S_n on $\mathcal{G}_{n,q}$ given by

$$\begin{array}{ccccc} \mathbb{F}_q^\times \text{ wr } S_n & \times & \mathcal{G}_{n,q} & \to & \mathcal{G}_{n,q} \\ & ((\vec{\alpha};\sigma), W) & & \mapsto & T_{(\vec{\alpha};\sigma)}(W) \end{array}$$

Let χ_n' denote the character of the associated permutation representation of $\mathbb{F}_q^\times$ wr S_n.

It will not be true here that $\chi_n'((\vec{\alpha};\sigma))$ will equal $G_{n,q}$ only for the identity element. The diagonal subgroup Δ of $\mathbb{F}_q^\times$ wr S_n is defined by

$$\Delta = \{(\alpha, \alpha, \ldots, \alpha; (1)) \,|\alpha \in \mathbb{F}_q^\times\}.$$

It is clear that every element in Δ will leave fixed every subspace in $\mathcal{G}_{n,q}$. But, we make the following conjectures.

Conjecture 3.1. *Put*

$$\tilde{\chi}'(n) = \max_{(\vec{\alpha};\sigma)\notin\Delta} \chi_n'((\vec{\alpha};\sigma))/G_{n,q}.$$

Then $\tilde{\chi}'(n) \to 0$ *as* $n \to \infty$.

Conjecture 3.2.

$$\sum_{(\vec{\alpha};\sigma)\notin\Delta} \chi_n'((\vec{\alpha};\sigma))/G_{n,q} \to 0 \text{ as } n \to \infty.$$

Of course, the second conjecture is stronger than the first. Assuming the second conjecture is true, one can give, asymptotically, the number of inequivalent codes. Let $C_{n,q}$ denote the number of distinct equivalence classes of q-ary linear codes of length n. Then $C_{n,q}$ is the number of orbits of the action of $\mathbb{F}_q^\times$ wr S_n on $\mathcal{G}_{n,q}$. By the Cauchy-Frobenius (or Burnside) Lemma, this number is

$$\frac{1}{(q-1)^n n!} \sum_{(\vec{\alpha};\sigma)\in\mathbb{F}_q^\times \text{ wr } S_n} \chi_n'((\vec{\alpha};\sigma)).$$

Assuming the truth of Conjecture (3.2), then we have

$$C_{n,q} \sim \frac{G_{n,q}}{(q-1)^{n-1} n!}.$$

References

[1] P. Biane, Representations of symmetric groups and free probability, Adv. Math. 138 (1998), 126–181.

[2] P. Biane, Free cumulants and representations of large symmetric groups, XIIIth International congress on mathematical physics, (London, 2000), 321-326, Int. Press, Boston, MA, 2001

[3] L. Brickman and P. A. Fillmore, The invariant subspace lattice of a linear transformation, Canad. J. Math. 19 (1967), 810-822.

[4] J. Goldman and G.-C. Rota, The number of subspaces of a vector space, in "Recent progress in combinatorics" (W. Tutte, Ed.), pp. 75–83. Academic Press, San Diego, CA, 1969.

[5] K. Hoffman and R. Kunze, Linear algebra, 2nd edition, Prentice-Hall, Englewood Cliffs, NJ, 1971.

[6] A. Kerber, Applied group actions, 2nd edition, Springer, Berlin-Heidelberg-New York, 1999.

[7] A. M. Vershik and S. V. Kerov, Asymptotic theory of characters of the symmetric group, Funct. Anal. and its Appl. 15 (1981), 246–255.

[8] M. Wild, The asymptotic number of inequivalent binary codes and non-isomorphic binary matriods, Finite Fields Appl. 6 (2000), 192–202.