COUNTING THE CYCLES OF THE FROBENIUS AUTOMORPHISM

GARETH JONES, DARRYL MCCULLOUGH, AND MARCUS WANDERLEY

It is a useful basic fact from algebra that the group of automorphisms of the finite field $\mathbb{F}_q$, where q is the prime power p^s, is a cyclic group generated by the Frobenius automorphism Φ that sends each x to x^p. Since Φ has order s, the integer $\lceil \frac{q}{s} \rceil$ is trivially a lower bound for the number Orb_q of orbits of $\mathrm{Aut}(\mathbb{F}_q)$, and since Φ fixes each element of the subfield $\mathbb{F}_p$, $\lceil \frac{q-p}{s} \rceil + p$ is an obvious lower bound. In fact, the exact number of orbits of $\mathrm{Aut}(\mathbb{F}_q)$ is given by a simple closed formula:

$$\mathrm{Orb}_q = \frac{1}{s} \sum_{r|s} \varphi(s/r)\, p^r \ ,$$

where φ is the Euler totient function.

This formula for Orb_q is surely well-known, although we have not found an explicit statement in the literature. Experts in finite fields (we thank, in particular, H. Niederreiter) observe that the number of orbits is the same as the number of monic irreducible polynomials over $\mathbb{F}_p$ of degree dividing s, each orbit being the set of roots of one such polynomial. Consequently, the number $e(r)$ of orbits with r elements (which equals the number of monic irreducible polynomials of degree r) satisfies $q = \sum_{r|s} re(r)$, and a formula for $e(s)$ can be obtained using Möbius inversion (see for example [3, Ch. III.2]). In fact the formula for $e(s)$ is the same as our formula for Orb_q but with φ replaced by the Möbius function μ. Summing these for r dividing s and then manipulating using the fact (also a consequence of Möbius inversion) that $\frac{\varphi(s)}{s} = \sum_{r|s} \frac{\mu(r)}{r}$ gives our formula for Orb_q. The purpose of this note is to show how to establish this formula for Orb_q in a few lines using Burnside's Lemma and a few of the most elementary properties of $\mathbb{F}_q$.

Burnside's Lemma says that the number of orbits of a finite group acting on a finite set equals the average number of fixed points of the elements of the group:

Date: February 7, 2005.

The second author was supported in part by NSF grant DMS-0102463.

Lemma 1 (Burnside's Lemma)**.** *If a finite group G acts on a finite set Ω, then the number of orbits is given by*

$$\frac{1}{|G|}\sum_{g\in G}\pi(g)$$

where $\pi(g)$ is the number of points fixed by g.

Burnside's Lemma can be proven by elementary counting arguments (see for example [1]), and a better name for it is the Burnside-Cauchy-Frobenius formula (see [4]).

To obtain the formula for Orb_q, we will apply Burnside's Lemma with $\Omega = \mathbb{F}_{p^s}$ and $G = \mathrm{Aut}(\mathbb{F}_{p^s})$. Recall that $\mathbb{F}_{p^r}$ occurs as a subfield of $\mathbb{F}_{p^s}$ if and only if $r|s$, and that it is the unique subfield of this order. Each element Φ^m of G has order s/r, where $r = \gcd(m, s)$, and there are $\varphi(s/r)$ elements of this order for each divisor r of s. Such an element has the same fixed points as Φ^r, since each is a power of the other, and the fixed points of Φ^r are the roots of the polynomial $x^{p^r} - x$. These roots form the subfield F_{p^r}, so $\pi(\Phi^m) = p^r$. Burnside's Lemma now implies that the number of orbits is

$$\frac{1}{s}\sum_{r|s}\varphi(s/r)\,p^r\ .$$

The same argument, with q in the role of p, shows that for any prime power q, the number of orbits of the action of the Galois group $\mathrm{Aut}_{\mathbb{F}_q}\mathbb{F}_{q^s}$ on $\mathbb{F}_{q^s}$ is $\displaystyle\frac{1}{s}\sum_{r|s}\varphi(s/r)\,q^r$.

The obvious lower bound $\lceil \frac{q-p}{s}\rceil + p$ gives the exact count whenever s is prime (or $s = 1$), since then all orbits contain s elements except those in the subfield $\mathbb{F}_p$. But even for composite s this bound is very accurate, apart from a few small values of q, because the vast majority of elements of $\mathbb{F}_q$ do not lie in any proper subfield and consequently almost all orbits have s elements. For example, using GAP [2] we find that for $\mathrm{Orb}_{2^{30}} = 35,792,568$, the bound of $35,791,397$ is approximately 99.9967% of the exact value, while the bound of $29,484,565,267,122,446$ is approximately 99.99999984% of $\mathrm{Orb}_{29^{16}} = 29,484,565,316,813,125$.

References

1. Kenneth P. Bogart, An obvious proof of Burnside's lemma, *Amer. Math. Monthly* 98 (1991), 927–928.
2. GAP: Groups, Algorithms, and Programming, available at the St. Andrews GAP website `http://turnbull.mcs.st-and.ac.uk/~gap/` .
3. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Revision of the 1986 first edition, Cambridge Univ. Press, Cambridge, 1994.
4. P. M. Neumann, A lemma which is not Burnside's, *Math. Sci.* 4 (1979), 133–141

School of Mathematics, University of Southampton, Southampton SO17 1BJ, Great Britain
E-mail address: `G.A.Jones@maths.soton.ac.uk`

Department of Mathematics, University of Oklahoma, Norman, Oklahoma 73019, USA
E-mail address: `dmccullough@math.ou.edu`
URL: `www.math.ou.edu/~dmccullough/`

Departmento de Matematica, Universidade Federal de Pernambuco, Av. Prof. Luiz Freire, s/n, Cid. Universitaria-Recife-PE, CEP 50.740-540, Brazil
E-mail address: `mvw@dmat.ufpe.br`