PERMUTATION-TYPE FORMULAS OF FROBENIUS MAP AND THEIR APPLICATIONS *

Zhibo Chen
Department of Mathematics
Penn State University, McKeesport
PA 15132, U.S.A.

Abstract

Let $F_n = GF(q^n)$ denote the finite field of order q^n, and let $U_n = \cup_{i=1}^{n} F_i$. Explicit permutation-type formulas for the Frobenius map φ (defined by $\varphi(x) = x^q$) on F_n and on U_n are obtained by using the well-known number $\pi(i)$ (the number of monic irreducible polynomials of degree i in $F_1[x]$). Some results in [1] and [2] can be obtained from these formulas. Moreover, some other results are also given by using Pólya's counting theory.

1 Introduction.

Throughout this note, we let $F_n = GF(q^n)$ denote the finite field of order q^n, where n is a positive integer and q is a prime power. F_1 is usually written as F, and the set-theoretic union $\cup_{i=1}^{n} F_i$ is denoted by U_n (Note that $F_i \subseteq F_j$ if and only if i divides j). By using the Lagrange interpolation formula, every function $f : F_n \to F_n$ can be represented by a unique polynomial $f(x)$ of degree less than q^n in $F_n[x]$. It is also known ([1], Lemma 1) that every function $g : U_n \to U_n$ can be represented by a unique polynomial $g(x)$ of degree less than $|U_n|$ with coefficients in the extension field $E_n(= F_m)$ of $F_1, F_2, \cdots, F_n$ where $m = L.C.M.\{1, 2, \cdots, n\}$. Such polynomials $f(x) \in F_n[x]$ and $g(x) \in E_n[x]$ are called the representing polynomials of the functions $f : F_n \to F_n$ and $g : U_n \to U_n$, respectively. The function φ on F_n (U_n, respectively) with the representing polynomial $\varphi(x) = x^q$ is called the Frobenius map on F_n (U_n, respectively). It is

*This research is partially supported by the RDG grant of the Penn State University.

well-known (cf. [5, p. 351]) that φ is a permutation of F_n. Then it is easily seen that $\varphi(x)$ also represents a permutation of U_n. In this note we use the well-known number $\pi(i)$ (the number of monic irreducible polynomials of degree i in $F[x]$) to give explicit permutation-type formulas for the Frobenius map φ on F_n and on U_n. (A permutation σ on an m-set S is said to be of type $(n_1, n_2, \cdots, n_m)$ if the number of k-cycles in σ is n_k for $k = 1, 2, \cdots, m$. We also say that $(n_1, n_2, \cdots, n_m)$ is the permutation-type of σ on S.) As applications, some results of [1] and [2] follow as corollaries and other results are also given by using Pólya's counting theory.

2 Permutation-Type Formulas of φ.

Theorem 2.1 *The permutation φ on F_n defined by $\varphi(x) = x^q$ is of the type $(\lambda_1, \lambda_2, \cdots, \lambda_n, 0, \cdots, 0)$ where*

$$\lambda_i = \begin{cases} \pi(i), & if\ i|n, \\ 0, & otherwise. \end{cases}$$

The permutation of φ on $U_n = \cup_{i=1}^{n} F_i$ defined by $\varphi(x) = x^q$ is of the type $(\pi(1), \pi(2), \cdots, \pi(n), 0, \cdots, 0)$.

Proof. For any x in $U_n, x \in F_i$ for some $i \leq n$. So $x^{q^i} = x$, that is, $\varphi^i(x) = x$. Hence x is in a k-cycle of the permutation φ on U_n with $k \leq i \leq n$. Then there is no cycle of length greater than n in this permutation. Therefore, all the numbers after the first n entries in the permutation-type of φ on U_n must be equal to 0. It is easily seen that this conclusion also holds for the permutation-type of φ on F_n.

Let U_0 denote the empty set. Then U_n is the disjoint union of the non-empty sets $U_i \backslash U_{i-1}$ for $i = 1, 2, \cdots, n$. It is clear that for any i and n with $1 < i \leq n$, $x \in U_i \backslash U_{i-1}$ if and only if $x^{q^i} = x$ and $x^{q^j} \neq x$ for any j with $1 \leq j < i$. Thus, we see that $x \in U_i \backslash U_{i-1}$ if and only if x is in an i-cycle of the permutation φ on U_n. In fact, this conclusion also holds for $i = 1$, since $x \in U_1 \backslash U_0 = F$ if and only if $x^q = x$. From the above, the number of i-cycles of the permutation φ on U_n depends only on the action of φ on $U_i \backslash U_{i-1}$, and so only on i. Therefore, there is a fixed sequence $m_1, m_2, \cdots, m_k, \cdots$, such that $(m_1, m_2, \cdots, m_n, 0, \cdots, 0)$ is the type of φ on U_n. Now we consider the action of permutation φ on F_n. Let $(\lambda_1, \lambda_2, \cdots, \lambda_n, 0, \cdots, 0)$ be its type. Since $\varphi^n(x) = x^{q^n} = x$ for any

$x \in F_n$, the length of each cycle must divide n. Thus, $\lambda_i = 0$ if $i \nmid n$. For the case of $i|n$, since $U_i \backslash U_{i-1} \subseteq F_n \subseteq U_n$, x is in an i-cycle of φ on F_n if and only if x is in an i-cycle of φ on U_n. Thus we have $\lambda_i = m_i$ for $i|n$. Finally, we show that $m_i = \pi(i)$ for all i. Since $(\lambda_1, \lambda_2, \cdots, \lambda_n, 0, \cdots, 0)$ is the type of φ on F_n, $q^n = |F_n| = \sum_{i|n} i \cdot \lambda_i = \sum_{i|n} i \cdot m_i$. From the proved fact that $m_1, m_2, \cdots, m_k, \cdots$ is a fixed sequence, we see that m_i is a function of i defined for every integer i. Hence we may use the Möbius inversion formula to obtain

$$m_i = \frac{1}{i} \sum_{d|i} \mu(d) q^{\frac{i}{q}}$$

which is equal to $\pi(i)$ for all i.

This completes the proof for Theorem 2.1.

3 Applications

From the permutation-type of φ on U_n, we immediately have the following

Corollary 3.1 *[1, p. 149]* $|U_n| = \sum_{i=1}^{n} i\pi(i)$.

Let $A(q^n)$ denote the group of all permutations of F_n which commute with φ, and let $\mathcal{A}(q, n)$ denote the group of all permutations of U_n which commute with φ. The formulas for $|A(q^n)|$ and $|\mathcal{A}(q, n)|$ were obtained in [2] and [1], respectively. Now we can easily obtain these formulas in a unified way. Recall the following elementary result from permutation group theory: If σ belongs to the symmetric group S_n of degree n and σ is of the type $(r_1, r_2, \cdots, r_n)$, the centralizer of σ in S_n has the order $\prod_{i=1}^{n} i^{r_i} \cdot (r_i)!$. Then we immediately obtain the following corollaries 3.2 and 3.3 from Theorem 2.1.

Corollary 3.2 *[2, p. 134]* $|A(q^n)| = \prod_{d|n} (\pi(d))! \cdot d^{\pi(d)}$.

Corollary 3.3 *[1, p. 150]* $|\mathcal{A}(q, n)| = \prod_{d=1}^{n} (\pi(d))! \cdot d^{\pi(d)}$.

Corollary 3.4 *The number of functions $f : F_n \to F_n$ such that $f\varphi = \varphi f$ is given by $N = q^{q^n}$.*

Proof. By Theorem 2.1, φ has the type $(\lambda_1, \lambda_2, \cdots, \lambda_n, 0, \cdots, 0)$ where

$$\lambda_i = \begin{cases} \pi(i), & if\ i|n, \\ 0, & otherwise. \end{cases}$$

From [3, p. 172], we have

$$N = \prod_{i=1}^{n} \left(\sum_{k|i} k\lambda_k \right)^{\lambda_i} = \prod_{i|n} \left(\sum_{k|i} k\pi(k) \right)^{\pi(i)}.$$

Since

$$\pi(k) = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) q^d,$$

we have

$$N = \prod_{i|n} \left(\sum_{k|i} \sum_{d|k} \mu\left(\frac{k}{d}\right) q^d \right)^{\pi(i)}.$$

From [5, Lemma 3.23] we have

$$\sum_{k,d|k|i} \mu\left(\frac{i}{k}\right) = \begin{cases} 1, & if\ d = i, \\ 0, & if\ d|i\ and\ 1 \le d < i, \end{cases}$$

where the sum runs over k dividing i and divisible by d. It follows that

$$\sum_{k|i} \sum_{d|k} \mu\left(\frac{k}{d}\right) q^d = \sum_{d|i} \left[\sum_{k,d|k|i} \mu\left(\frac{k}{d}\right) \right] q^d = q^i.$$

Therefore,

$$N = \prod_{i|n} \left(q^i\right)^{\pi(i)} = q^{\sum_{i|n} i\pi(i)} = q^{q^n}.$$

Corollary 3.5 *Let $f : F_n \to F_n$ be a function with the representing polynomial $f \in F_n[x]$. Then $f\varphi = \varphi f$ on F_n if and only if $f \in F[x]$.*

Proof. The sufficiency is obvious, since for any $f \in F[x]$,

$$f\varphi(x) = f\left(x^q\right) = [f(x)]^q = \varphi f(x) \quad for\ all\ x \in F_n.$$

By Corollary 3.4, $N = q^{q^n}$, which is equal to the number of all polynomials in $F[x]$ with degree $< q^n$. Then the necessity follows immediately.

We note that Corollary 3.5 can also be proved in a way similar to [2, Lemma 1]. The Corollaries 3.4 and 3.5 are concerned with functions from F_n to F_n. Similarly we can obtain corresponding results for functions from U_n to U_n.

Corollary 3.6 *The number of functions $f : U_n \to U_n$ with $f\varphi = \varphi f$ is $q^{\sum_{i=1}^{n} i\pi(i)}$.*

Corollary 3.7 *Let $f : U_n \to U_n$ be a function with the representing polynomial $f \in F_m[x]$ where $m = L.C.M.\{1, 2, \cdots, n\}$. Then $f\varphi = \varphi f$ on U_n if and only if $f \in F[x]$.*

We note that Corollary 3.7 is already given as Lemma 2 in [1].

Now we turn to other applications of Theorem 2.1.

Let $G_n = Aut_F F_n$ be the Galois group of F_n over F. It is well-known (cf. [4, p. 282]) that G_n is a cyclic permutation group on F_n and that the Frobenius map φ is a generator of G_n, i.e., $G_n = \{\varphi, \varphi^2, \cdots, \varphi^n = 1\}$.

Corollary 3.8 *The cycle index of G_n is given by*

$$(*) \qquad P_{G_n} = \frac{1}{n} \sum_{k=1}^{n} \prod_{i|n} x_{\frac{i}{(i,k)}}^{(i,k)\pi(i)}$$

$$(**) \qquad = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \prod_{i|n} x_{\frac{i}{(i,d)}}^{(i,d)\pi(i)},$$

where ϕ is the Euler totient function.

Proof. Let φ be of the permutation type $(\lambda_1, \lambda_2, \cdots, \lambda_n, 0, \cdots, 0)$. For any positive integer k between 1 and n, φ^k splits each cycle of φ with length i into (i,k) cycles with length $\frac{i}{(i,k)}$. Then by the definition of cycle index, $P_{G_n} = \frac{1}{n} \sum_{k=1}^{n} \prod_{i=1}^{n} x_{\frac{i}{(i,k)}}^{(i,k)\lambda_i}$. By Theorem 2.1,

$$\lambda_i = \begin{cases} \pi(i), & if\ i|n \\ 0, & otherwise. \end{cases}$$

so we have

$$(*) \qquad P_{G_n} = \frac{1}{n}\sum_{k=1}^{n}\prod_{i|n} x_{\frac{i}{(i,k)}}^{(i,k)\pi(i)}.$$

To prove the second equality in Corollary 3.8, we use T_k to denote

$$\prod_{i|n} x_{\frac{i}{(i,k)}}^{(i,k)\pi(i)}.$$

Then (*) can be written as

$$(1) \qquad P_{G_n} = \frac{1}{n}\sum_{k=1}^{n} T_k$$

Note that for any i, n with $i|n, (n,k_1) = (n,k_2)$ implies $(i,k_1) = (i,k_2)$. It follows that $(n,k_1) = (n,k_2)$ implies $T_{k_1} = T_{k_2}$. For any $d|n$, let C_d = the number of integers k with $(n,k) = d$ and $1 \leq k \leq n$. Then (1) can be written as

$$(2) \qquad P_{G_n} = \frac{1}{n}\sum_{d|n} C_d T_d.$$

Since $(n,k) = d$ if and only if $\left(\frac{n}{d}, \frac{k}{d}\right) = 1$, we have $C_d = \phi\left(\frac{n}{d}\right)$. Then, from (2), we obtain

$$(**) \qquad P_{G_n} = \frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right)\prod_{i|n} x_{\frac{i}{(i,d)}}^{(i,d)\pi(i)}.$$

Define a relation $\sim$ on the set of all functions from F_n to F_n as follows: $f \sim g$ if and only if there is $\sigma \in G_n$ such that $f\sigma = g$. It is easily seen that $\sim$ is an equivalence relation. Let N_n be the number of the equivalence classes. We have

Corollary 3.9 $N_n = \frac{1}{n}\sum_{d|n} \varphi\left(\frac{n}{d}\right) q^{n\sum_{i|n}(i,d)\pi(i)}$.

Proof. By the well-known Pólya's Theorem (cf. [3, p.157]) $N_n = P_{G_n}(q^n, q^n, \cdots)$. Then the result immediately follows from Corollary 3.8.

It is easily seen that $N_1 = q^q = |F^F|$. So every function from F to F is only equivalent to itself.

Corollary 3.10 *Every function from F_n to F_n is only equivalent to itself if and only if $n = 1$.*

Proof. We only need to show the necessity. When $n > 1$,

$$\sum_{i|n}(i,d)\pi(i) \le \sum_{i|n} i\pi(i) = q^n \quad for\ any\ d,$$

and the inequality is restrict for the case $d = 1$ since

$$\sum_{i|n}(i,1)\pi(i) = \sum_{i|n}\pi(i) < \sum_{i|n} i\pi(i) = q^n.$$

Then it follows from Corollary 3.9 that

$$N_n < \frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)q^{nq^n} = q^{nq^n} \quad since \quad \sum_{d|n}\phi\left(\frac{n}{d}\right) = n.$$

That is, $N_n < (q^n)^{q^n} = |F_n^{F_n}|$. It proves the necessity.

Finally, we point out that we can also use Theorem 2.1 and the de Bruijn's counting theorems [3, Theorems 5.3 and 5.4] to obtain corresponding results.

Acknowledgment

The author would like to thank professors C.Y.Chao and G.L.Mullen for their helpful comments and suggestions.

References

[1] J.V. Brawley, *The number of polynomial functions which permute the matrices over a finite field*, J. Combinatorial Theory (A), 21 (1976), 147-154.

[2] L. Carlitz and D.R. *Hayes, Permutations with coefficients in a subfield*, Acta Arith. XXI (1972), 131-135.

[3] N.G. de Bruijn, *Pólya's theory of counting, in "Applied Combinatorial Mathematics"*, (E.F. Beckenback, Ed.) Wiley, New York (1964), 144-184.

[4] Thomas W. Hungerford, *Algebra*, Rinehart and Winston, New York (1974).

[5] R.Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, London (1983).