THE NUMBER OF IRREDUCIBLE POLYNOMIALS AND LYNDON WORDS WITH GIVEN TRACE

F. RUSKEY*, C.R. MIERS†, AND J. SAWADA‡

Abstract. The *trace* of a degree n polynomial $f(x)$ over $GF(q)$ is the coefficient of x^{n-1}. Carlitz [Proc. AMS, 3 (1952) 693-700] obtained an expression $I_q(n,t)$, for the number of monic irreducible polynomials over $GF(q)$ of degree n and trace t. Using a different approach, we derive a simple explicit expression for $I_q(n,t)$. If $t > 0$, $I_q(n,t) = (\sum \mu(d) q^{n/d})/(qn)$, where the sum is over all divisors d of n which are relatively prime to q. This same approach is used to count $L_q(n,t)$, the number of q-ary Lyndon words whose characters sum to t mod q. This number is given by $L_q(n,t) = (\sum \gcd(d,q)\mu(d)q^{n/d})/(qn)$, where the sum is over all divisors d of n for which $\gcd(d,q)|t$. Both results rely on a new form of Möbius inversion.

Key words. Irreducible polynomial, trace, finite field, Lyndon word, Möbius inversion

AMS subject classifications. 05T06, 11T06

1. Introduction. The *trace* of a degree n polynomial $f(x)$ over $GF(q)$ is the coefficient of x^{n-1}. It is well known that the number of degree n irreducible polynomials over $GF(q)$ is given by

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}, \tag{1.1}$$

where $\mu(d)$ is the Möbius function. Less well-known is the formula

$$I_2(n,1) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{n/d}, \tag{1.2}$$

which is the number of degree n irreducible polynomials over $GF(2)$ with trace 1 (this can be inferred from results in Jungnickel [3], Section 2.7). One purpose of this paper is to refine (1.1) and (1.2) by enumerating the irreducible degree n polynomials over $GF(q)$ with a given trace. Carlitz [1] also solved this problem, arriving via a different technique at an expression that is different, but equivalent to the one given below. Our version of the result is stated in Theorem 1.1.

THEOREM 1.1. *Let q be a power of prime p. The number of irreducible polynomials of degree $n > 0$ over $GF(q)$ with a given non-zero trace t is*

$$I_q(n,t) = \frac{1}{qn} \sum_{\substack{d|n \\ p\nmid d}} \mu(d) q^{n/d}. \tag{1.3}$$

Note that the expression on the right hand side of (1.3) is independent of t and that $I_q(n,0)$ can be obtained by subtracting

$$I_q(n,0) = I_q(n) - (q-1) I_q(n,1).$$

*Dept. of Computer Science, University of Victoria, research supported in part by NSERC. e-mail: fruskey@csr.uvic.ca

†Dept. of Mathematics and Statistics, University of Victoria. e-mail: crmiers@math.uvic.ca

‡Dept. of Computer Science, University of Victoria, research supported in part by a NSERC. e-mail: jsawada@csr.uvic.ca

A Lyndon word is the lexicographically smallest rotation of an aperiodic string. If $L_q(n)$ denotes the number of q-ary Lyndon words of length n, then it is well known that $L_q(n) = I_q(n)$. The *trace* of a Lyndon word is the sum of its characters mod q. Let $L_q(n,t)$ denote the number of Lyndon words of trace t. The second purpose of this paper is to obtain an explicit formula for $L_q(n,t)$. This result is stated in Theorem 1.2.

THEOREM 1.2. *For all integers $n > 0$, $q > 1$, and $t \in \{0, 1, \ldots, q-1\}$,*

$$L_q(n,t) = \frac{1}{qn} \sum_{\substack{d|n \\ \gcd(d,q)|t}} \gcd(d,q)\mu(d)q^{n/d}.$$

Note that $I_q(n,t) = L_q(n,s)$ whenever $t \neq 0$ and $\gcd(n,s) = 1$.

In order to prove Theorems 1.1 and 1.2 we need a new form of Möbius inversion. This is presented in the next section.

2. A generalized Möbius inversion formula. The defining property of the Möbius functions is

$$\sum_{d|n} \mu(d) \; = \; [\![n = 1]\!], \tag{2.1}$$

where $[\![P]\!]$ for proposition P represents the "Iversonian convention": $[\![P]\!]$ has value 1 if P is true and value 0 if P is false (see [4], pg. 24).

DEFINITION 2.1. *Let $\mathcal{R}$ be a set, $\mathbb{N} = \{1, 2, 3, \ldots\}$, and let $\{X(d,t)\}_{t\in\mathcal{R},d\in\mathbb{N}}$ be a family of subsets of $\mathcal{R}$. We say that $\{X(d,t)\}_{t\in\mathcal{R},d\in\mathbb{N}}$ is* recombinant *if*

(i) $X(1,t) = \{t\}$ *for all* $t \in \mathcal{R}$, *and*

(ii) $\{e' \in X(d', e) : e \in X(d,t)\} = \{e \in X(dd', t)\}$ *for all* $d, d' \in \mathbb{N}, t \in \mathcal{R}$.

THEOREM 2.2. *Let $\{X(d,t)\}_{t\in\mathcal{R},d\in\mathbb{N}}$ be a recombinant family of subsets of $\mathcal{R}$. Let $A : \mathbb{N} \times \mathcal{R} \to \mathcal{C}$ and $B : \mathbb{N} \times \mathcal{R} \to \mathcal{C}$ be functions, where $\mathcal{C}$ is a commutative ring with identity. Then*

$$A(n,t) = \sum_{d|n} \sum_{e\in X(d,t)} B(\frac{n}{d}, e)$$

for all $n \in \mathbb{N}$ and $t \in \mathcal{R}$ if and only if

$$B(n,t) = \sum_{d|n} \mu(d) \sum_{e\in X(d,t)} A(\frac{n}{d}, e)$$

for all $n \in \mathbb{N}$ and $t \in \mathcal{R}$.

Proof. Consider the sum, call it S, on the right-hand side of the first equation

$$\begin{aligned}
S &= \sum_{d|n} \sum_{e\in X(d,t)} B(\frac{n}{d}, e) \\
&= \sum_{d|n} \sum_{e\in X(d,t)} \sum_{d'|(n/d)} \sum_{e'\in X(d',e)} \mu(d')A(\frac{n}{dd'}, e') \\
&= \sum_{d|n} \sum_{dd'|n} \mu(d') \sum_{e\in X(d,t)} \sum_{e'\in X(d',e)} A(\frac{n}{dd'}, e').
\end{aligned}$$

Now substitute $f = dd'$ and use recombination to get

$$\begin{aligned}
S &= \sum_{d|n}\sum_{f|n} [\![f = dd']\!] \mu(\frac{f}{d}) \sum_{e\in X(d,t)} \sum_{e'\in X(d',e)} A(\frac{n}{f}, e') \\
&= \sum_{f|n}\sum_{d|f} \mu(\frac{f}{d}) \sum_{e\in X(f,t)} A(\frac{n}{f}, e) \\
&= \sum_{f|n}\sum_{e\in X(f,t)} A(\frac{n}{f}, e) \sum_{d|f} \mu(\frac{f}{d}) \\
&= \sum_{f|n}\sum_{e\in X(f,t)} A(\frac{n}{f}, e) [\![f = 1]\!] \\
&= A(n,t)
\end{aligned}$$

Verification in the other direction is similar and is omitted. □

LEMMA 2.3. *Let $d \in \mathbb{N}$ and e, t members of an additive monoid $\mathcal{R}$. The sets $\{e : de = t\}$ form a recombinant family.*

Proof. Here de means $e + e + \cdots + e$ (d terms). Suppose that $de = t$ and $d'e' = e$. Clearly, $dd'e' = t$. Conversely, if $dd'e' = t$ then $d'e'$ is equal to some element of $\mathcal{R}$, call it e. Then $d'e' = e$ and $de = t$. □

COROLLARY 2.4. *For a fixed prime power q, the sets $X_q(d,t) = \{e \in GF(q) : de = t\}$ form a recombinant family of subsets of $GF(q)$.*

COROLLARY 2.5. *For a fixed integer q, the sets $X_q(d,t) = \{e \in \mathbb{Z}_q : de \equiv t(q)\}$ form a recombinant family of subsets of $\mathbb{Z}_q$, where $\mathbb{Z}_q$ are the integers mod q.*

3. Irreducible polynomials with given trace. In this section, the irreducible polynomials with a given trace are counted. We begin by introducing some notation that will be used in the remainder of the paper. We use Jungnickel [3] as a reference for terminology and basic results from finite field theory.

The trace of an element $\beta \in GF(q^n)$ over $GF(q)$ is denoted $Tr(\beta)$, and is given by

$$Tr(\beta) = \beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{n-1}}.$$

If $\beta \in GF(q^n)$ and d is the smallest positive integer for which $\beta^{q^d} = 1$, then $f(x)$ is the minimal polynomial of β, denoted $Min(\beta)$, where

$$f(x) = (x - \beta)(x - \beta^q) \cdots (x - \beta^{q^{d-1}}).$$

The value of d must be a divisor of n.

Let $\mathbf{Irr}_q(n,t)$ denote the set of all monic irreducible polynomials over $GF(q)$ of degree n and trace t. By $a \cdot \mathbf{Irr}_q(n,t)$ we denote the multiset consisting of a copies of $\mathbf{Irr}_q(n,t)$. Classic results of finite field theory imply the following equality of multisets

$$\bigcup_{\beta\in \mathrm{GF}(q^n)} \{Min(\beta)\} \;=\; \bigcup_{d|n} d \cdot \mathbf{Irr}_q(d) \;=\; \bigcup_{d|n} \frac{n}{d} \cdot \mathbf{Irr}_q(\frac{n}{d}), \tag{3.1}$$

where $\mathbf{Irr}_q(d)$ is the set of monic irreducible polynomials of degree d over $GF(q)$. From (3.1) it is easy to derive (1.1) via a standard application of Möbius inversion.

Now we restrict the equality (3.1) to trace t field elements to obtain

$$\begin{aligned}
\bigcup_{\substack{\beta \in \mathrm{GF}(q^n) \\ Tr(\beta)=t}} \{Min(\beta)\} &= \bigcup_{d|n} \frac{n}{d} \cdot \{f \in \mathbf{Irr}_q(\frac{n}{d}) \ : \ Tr(f^d) = t\} \\
&= \bigcup_{d|n} \frac{n}{d} \cdot \{f \in \mathbf{Irr}_q(\frac{n}{d}) \ : \ d \cdot Tr(f) = t\} \\
&= \bigcup_{d|n} \bigcup_{de=t} \frac{n}{d} \cdot \{f \in \mathbf{Irr}_q(\frac{n}{d}) \ : \ Tr(f) = e\} \\
&= \bigcup_{d|n} \bigcup_{de=t} \frac{n}{d} \cdot \{f \in \mathbf{Irr}_q(\frac{n}{d}, e)\} \qquad (3.2)
\end{aligned}$$

Note that the equation $de = t$ is asking whether the d-fold sum of $e \in GF(q)$ is equal to $t \in GF(q)$. We use the notation $GF(q^n, t)$ for the set of elements in $GF(q^n)$ with trace t, for $t = 0, 1, \ldots, q-1$, where $q = p^m$ and p is prime. Consider the map ρ that sends α to $\alpha + \gamma$, where $\gamma \in GF(q^n)$ has trace 1. We claim that $\rho(GF(q^n, t)) = GF(q^n, t+1)$, and so the number of elements is the same for each trace value. Thus

$$|GF(q^n, t)| = q^{n-1}.$$

Taking cardinalities in (3.2) gives

$$q^{n-1} = \sum_{d|n} \sum_{de=t} \frac{n}{d} I_q(\frac{n}{d}, e).$$

From Theorem 2.2 and Corollary 2.4, we obtain

$$I_q(n, t) = \frac{1}{qn} \sum_{d|n} \sum_{de=t} \mu(d) q^{n/d}.$$

The equation $de = t$ where d is an integer and $e, t \in GF(q)$ has a unique solution e if $t \neq 0$ and $p \nmid d$. If $t = 0$, then there is one solution $e = 0$ if $p \nmid d$ and there are q solutions if $p \mid d$. Thus, if $t \neq 0$ then

$$I_q(n, t) = \frac{q-1}{qn} \sum_{\substack{d|n \\ p \nmid d}} \mu(d) q^{n/d},$$

thereby proving Theorem 1.1. Otherwise, if $t = 0$, then

$$I_q(n, 0) = I_q(n, 1) + \frac{q-1}{qn} \sum_{\substack{d|n \\ p|d}} \mu(d) q^{n/d}.$$

4. Lyndon words with given trace. If $\mathbf{a} = a_1 a_2 \cdots a_n$ is a word, then we define its trace mod q, $Tr_q(\mathbf{a})$, to be $\sum a_i \bmod q$. Let $L_q(n, t)$ denote the number of q-ary Lyndon words of length n and trace t mod q. Note that any q-ary string of length n can be expressed as the concatenation of d copies of the rotation of some Lyndon word of length n/d, for some $d \mid n$. Note further that there are precisely q^{n-1}

words of length n with trace t, because any word of length $n-1$ can have a final n-th character appended in only one way to have trace t. It therefore follows that

$$q^{n-1} = \sum_{d|n} \sum_{de \equiv t(q)} \frac{n}{d} L_q(\frac{n}{d}, e). \tag{4.1}$$

This can be solved using Theorem 2.2 and Corollary 2.5 to yield

$$nL_q(n,t) = \sum_{d|n} \mu(d) \sum_{de \equiv t(q)} q^{n/d-1}.$$

Hence

$$L_q(n,t) = \frac{1}{qn} \sum_{\substack{d|n \\ \gcd(q,d)|t}} \gcd(q,d)\mu(d) q^{n/d}. \tag{4.2}$$

Equation (4.2) is true because $de \equiv t(q)$ has a solution if and only if $\gcd(d,q) \mid t$. If a solution exists, then it has precisely $\gcd(d,q)$ solutions (e.g., [2], Corollary 33.22, pg. 821). This proves Theorem 1.2.

We could also consider the more general question of computing $L_{q,r}(n,t)$, the number of q-ary Lyndon words with trace mod r, and derive similar but more complicated formulae. If $M_q(n,t)$ is the number of q-ary length n strings whose characters sum to t, then clearly $M_q(1,t) = [\![0 \le t < q]\!]$, and for $n > 1$

$$M_q(n,t) = \sum_{i=0}^{q} M_q(n-1, t-i).$$

If $T_{q,r}(n,t)$ denotes the number of q-ary length n strings with trace mod r equal to t, then

$$T_{q,r}(n,t) = \sum_{s \equiv t(r)} M_q(n,s).$$

Using the same approach as before

$$L_{q,r}(n,t) = \frac{1}{n} \sum_{d|n} \mu(d) \sum_{de \equiv t(r)} T_{q,r}(\frac{n}{d}, e).$$

The equation for $L_{q,r}(n,t)$ seems to produce no particularly nice formulae, except in the case seen previously where $q = r$, or if $q = 2$. When $q = 2$, $M_2(n,t) = \binom{n}{t}$ and

$$T_{2,r}(n,t) = \sum_{s \equiv t(r)} \binom{n}{s}.$$

However, in this case there is already a well-known formula for the number of Lyndon words with k 1's, namely

$$P_2(n,k) = \frac{1}{n} \sum_{d|\gcd(n,k)} \mu(d) \binom{n/d}{k/d},$$

from which we obtain $L_{2,r}(n,t) = \sum_{s \equiv t(2)} P_2(n,s)$.

5. Final Remarks. Our generalized Möbius inversion theorem can be extended to a Möbius inversion theorem on posets. Background material on Möbius inversion on posets may be found in Stanley [5]. We state here the modified definition of recombinant and the inversion theorem, but omit the proof.

DEFINITION 5.1. *Let $\mathcal{P}$ be a poset, let $\mathcal{R}$ be a set, and let $\{X(y,x,t)\}_{x,y\in\mathcal{P},y\preceq x,t\in\mathcal{R}}$ be a family of subsets of $\mathcal{R}$. The family $\{X(y,x,t)\}_{x,y\in\mathcal{P},y\preceq x,t\in\mathcal{R}}$ is* recombinant *if*

(i) *$X(x,x,t)=\{t\}$ for all $t\in\mathcal{R}$, and*

(ii) *$\{e'\in X(z,y,e) : e\in X(y,x,t)\} = \{e\in X(z,x,t)\}$ for all $z\preceq y\preceq x\in\mathcal{P}, t\in\mathcal{R}$.*

We note that if $\mathcal{P}$, is the divisor lattice, and $\mathcal{R}$ is an additive monoid, then the collection $\{X(x,y,t)\}_{x,y\in\mathcal{P},x\leq y,t\in\mathcal{R}}$ where $X(x,y,t)=\{e\in\mathcal{R} : (y/x)e=t\}$ is recombinant, as per Lemma 1.

THEOREM 5.2. *Let $\mathcal{P}$ be a poset, $\mathcal{R}$ be a set, and $\{X(y,x,t)\}_{x,y\in\mathcal{P},y\preceq x,t\in\mathcal{R}}$ be a recombinant family. Let $A:\mathcal{P}\times\mathcal{R}\to\mathcal{C}$, and $B:\mathcal{P}\times\mathcal{R}\to\mathcal{C}$, be functions where $\mathcal{C}$ is a commutative ring with identity. Then*

$$A(x,t)=\sum_{y\preceq x}\sum_{e\in X(y,x,t)} B(y,e)$$

for all $x\in\mathcal{P}$ and $t\in\mathcal{R}$ if and only if

$$B(x,t)=\sum_{y\preceq x}\mu(y,x)\sum_{e\in X(y,x,t)} A(y,e)$$

for all $x\in\mathcal{P}$ and $t\in\mathcal{R}$. (Here $\mu(y,x)$ is the Möbius function of the poset $\mathcal{P}$.)

Tables of the numbers $I_q(n,t)$ and $L_q(n,t)$ for small values of q and n may be found on Frank Ruskey's Combinatorial Object Server (COS) at `www.theory.csc.uvic.ca/~cos/inf/{lyndon.html,irreducible.html}`. They also appear in Neil Sloane's On-line Encyclopedia of Integer Sequences (at `http://www.research.att.com/~njas/sequences/`) as $I_2(n,0)=L_2(n,0)=$ A051841, $I_2(n,1)=L_2(n,1)=$ A000048, $I_3(n,0)=L_3(n,0)=$ A046209, $I_3(n,1)=L_3(n,1)=$ A046211, $L_4(n,0)=$ A054664, $I_4(n,1)=L_4(n,1)=$ A054660, $L_5(n,0)=$ A054661, $I_5(n,1)=L_5(n,1)=$ A054662, $L_6(n,0)=$ A054665, $L_6(n,1)=$ A054666, $L_6(n,2)=$ A054667, $L_6(n,3)=$ A054700.

The authors wish to thank Aaron Gulliver for helpful discussions regarding this paper.

REFERENCES

[1] L. Carlitz, *A theorem of Dickson on irreducible polynomials*, Proc. AMS, 3 (1952) 693-700.
[2] T.H. Cormen, C.E. Leiserson, and R.L. Rivest, *Introduction to Algorithms*, McGraw-Hill, 1990.
[3] Dieter Jungnickel, *Finite Fields: structure and arithmetics*, B.I. Wissenschaftsverlag, 1993.
[4] D.E. Knuth, R.L. Graham, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.
[5] Richard P. Stanley, *Enumerative Combinatorics, Vol. I*, Cambridge University Press, 1997.