COUNTING STRINGS WITH GIVEN ELEMENTARY SYMMETRIC FUNCTION EVALUATIONS II: CIRCULAR STRINGS

C.R. MIERS* AND F. RUSKEY†

Abstract. Let α be a string over an alphabet that is a finite ring, R. The k-th elementary symmetric function evaluated at α is denoted $T_k(\alpha)$. In a companion paper we studied the properties of $\mathbf{S}_R(n;\tau_1,\tau_2,\ldots,\tau_k)$, the set of of length n strings for which $T_i(\alpha)=\tau_i$. Here we consider the set, $\mathbf{L}_R(n;\tau_1,\tau_2,\ldots,\tau_k)$, of equivalence classes under rotation of aperiodic strings in $\mathbf{S}_R(n;\tau_1,\tau_2,\ldots,\tau_k)$, sometimes called Lyndon words. General formulae are established, and then refined for the cases where R is the ring of integers $\mathbb{Z}_q$ or the finite field $\mathbb{F}_q$.

Key words. elementary symmetric function, combinatorial enumeration, integers mod q, Lyndon word, Möbius inversion, multinomial coefficient, finite field.

AMS subject classifications. 05A15, 05E05, 05A19.

1. Introduction. The main purpose of this paper is to count certain equivalence classes of strings over $\mathbb{Z}_q$ the ring of integers mod q, and over the finite field $\mathbb{F}_q$. The equivalence classes contain all strings that are rotationally equivalent (sometimes called *conjugate*, [7]), and that achieve specified values when regarded as the parameters of elementary symmetric functions. Aside from the intrinsic interest of the enumerative formulae and the techniques used to derive them, this paper can be viewed as part of a program to enumerate certain classes of polynomials with coefficients in a finite ring and whose coefficients are prescribed. In [2], degree n monic irreducible polynomials over $\mathbb{F}_2$ with prescribed coefficients for x^{n-1} and x^{n-2} were enumerated. If such a polynomial is factored in a splitting field, these coefficients can be interpreted as the first and second elementary symmetric functions evaluated at the string of coefficients in the factorization. The techniques in [2] (and in [11]) rely on the relationship between Lyndon words and irreducible polynomials. The relationship between strings, polynomials and elementary symmetric functions generalizes. If a string α has its alphabet in a finite commutative ring R, we can evaluate the k-th elementary symmetric function T_k at α. This evaluation depends on the *profile* $\mathbf{k}=\langle k_1,k_2,\ldots,k_{|R|-1}\rangle$ where k_i is the frequency with which ring element x_i occurs in α. The relationship between strings, polynomials, and elementary symmetric functions is contained in the map $\alpha\mapsto A_{\mathbf{k}}(z)=\prod_{j=1}^{|R|-1}(1+x_jz)^{k_j}$, since $T_m(\alpha)=[z^m]A_{\mathbf{k}}(z)$. In [8] we exploit this relationship to compute $S_{\mathbb{Z}_p}(n;\tau_1,\tau_2,\ldots,\tau_t)$, the number of strings over $\mathbb{Z}_p$ of length n for which $T_m(\alpha)=\tau_m$. Related results can be found in [5], [9], [11].

2. Notation and Preliminaries. In what follows we will assume R is a finite commutative ring with identity, denoted $\mathbf{1}$. In this case R has a characteristic c which is the least positive integer such that the c-fold sum $\mathbf{1}+\mathbf{1}+\cdots+\mathbf{1}=0$. If $d\in\mathbb{Z}^+$, then $d\in R$ where d is the d-fold sum $\mathbf{1}+\mathbf{1}+\cdots+\mathbf{1}$ mod (c).

We consider strings $\alpha=a_1a_2\cdots a_n$ where each $a_i\in R$, and define the k-*trace* of α, denoted $T_k(\alpha)$, as the sum

$$T_k(\alpha)=\sum_{1\le i_1<i_2<\cdots<i_k\le n} a_{i_1}a_{i_2}\cdots a_{i_k}.$$

*Dept. of Mathematics, University of Victoria, research supported in part by UVic faculty research grant. e-mail: crmiers@math.uvic.ca

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

These are the elementary symmetric functions of $a_1, a_2, \ldots, a_n$. Occasionally we will call T_1 the *trace*, T_2 the *subtrace*, and T_3 the *subsubtrace*. The trace terminology is used, in analogy with the theory of finite fields, since $(-1)^k T_k(\alpha)$ is the coefficient of z^{n-k} in the polynomial $(z-a_1)(z-a_2)\cdots(z-a_n)$ (see [10]).

By $S_R(n;\tau_1,\tau_2,\ldots,\tau_k)$ we denote the number of strings α over R of length n for which $T_i(\alpha)=\tau_i$ for $i=1,2,\ldots,k$. Obviously if $k=0$, then $S_R(n)=q^n$, where q is the number of elements in R. It is also true that $S_R(n;t)=q^{n-1}$ for any $t\in R$, since $T_1(\alpha x)$ takes on distinct values for each $x\in R$; we use here only the fact that R is an additive group.

The notation $[\![P]\!]$ for a proposition P has the value 1 if P is true and the value 0 if P is false. This is "Iverson's convention," as used in [6].

The numbers $S_R(n;\tau_1,\tau_2,\ldots,\tau_k)$ satisfy the following recurrence relation. If $n=1$, then $S_R(n;\tau_1,\tau_2,\ldots,\tau_k)=[\![\tau_2=\cdots=\tau_k=0]\!]$, and for $n>0$,

$$S_R(n;\tau_1,\tau_2,\ldots,\tau_k)=\sum_{x\in R} S_R(n-1;\rho_1,\rho_2,\ldots,\rho_k), \tag{2.1}$$

where $\rho_0=1$, and $\rho_j=\tau_j-\rho_{j-1}x$ for $j=1,2,\ldots,k$. This recurrence relation holds even if R is not commutative. It allows us to evaluate $S_R(n;\tau_1,\tau_2,\ldots,\tau_k)$ in $O(nr^k)$ ring and integer operations (by, in effect, creating a size nr^k table of S_R evaluated on all strings of length at most n on all possible values of the first k k-traces). The properties of $S_{\mathbb{Z}_p}$ for p prime are studied in [8].

A *rotation* of a string α is any string β that can be written as $\beta=\gamma\delta$, where $\alpha=\delta\gamma$. A string α is *aperiodic* if there are no non-empty strings γ and δ such that $\alpha=\gamma\delta=\delta\gamma$. Let $A_R(n;\tau_1,\tau_2,\ldots,\tau_k)$ denote the number of aperiodic strings α over R of length n for which $T_i(\alpha)=\tau_i$ for $i=1,2,\ldots,k$. Since every rotation of an aperiodic string is distinct, $A_R(n;\tau_1,\tau_2,\ldots,\tau_k)$ is divisible by n. The number $L_R(n;\tau_1,\tau_2,\ldots,\tau_k)=(1/n)A_R(n;\tau_1,\tau_2,\ldots,\tau_k)$ is the number of equivalence classes of aperiodic strings under rotation. The lexicographically least representatives of these equivalence classes are often called *Lyndon words* [7].

LEMMA 2.1. *For all $k\ge 1$ and $d\ge 1$,*

$$T_k(\alpha^d)=\sum_{\nu_1+2\nu_2+\cdots+k\nu_k=k}\binom{d}{\nu_1,\ldots,\nu_k,d-(\nu_1+\cdots+\nu_k)}T_1(\alpha)^{\nu_1}T_2(\alpha)^{\nu_2}\cdots T_k(\alpha)^{\nu_k}.$$

Proof. From the string $\alpha^d=\alpha_1\alpha_2\cdots\alpha_d$, where $\alpha_i=\alpha$ for all i, we need to select k positions in all possible ways. We classify those ways according to the distribution $(\nu_1,\nu_2,\ldots,\nu_k)$ where ν_j is the number of α_i's containing j of the selected positions. Such an α_i will contribute a multiplicative factor of $T_j(\alpha)$ to the sum, with $T_1(\alpha)^{\nu_1}T_2(\alpha)^{\nu_2}\cdots T_k(\alpha)^{\nu_k}$ being the total contribution for a given distribution and selection of the α_i's. There are $\binom{d}{\nu_1,\ldots,\nu_k,d-(\nu_1+\cdots+\nu_k)}$ ways to associate a distribution with particular α_i's. Finally, a distribution is valid if and only if $\nu_1+2\nu_2+\cdots+k\nu_k=k$. □

Note that the multinomial coefficient can be written as

$$\binom{d}{\nu_1,\ldots,\nu_k,d-V_k}=\binom{d}{\nu_1}\binom{d-V_1}{\nu_2}\cdots\binom{d-V_{k-1}}{\nu_k}, \tag{2.2}$$

where $V_j=\nu_1+\nu_2+\cdots+\nu_j$.

If $\mathbf{t} = (t_1, t_2, \ldots, t_k) \in R^k = R \times R \times \cdots \times R$ and d is a natural number, define the map $\theta_d : R^k \to R^k$ as $\theta_d(\mathbf{t}) = \mathbf{u}$, where $\mathbf{u} = (u_1, u_2, \ldots, u_k)$ has the value, mod c,

$$u_j = \sum_{\nu_1+2\nu_2+\cdots+j\nu_j=j} \binom{d}{\nu_1, \ldots, \nu_j, d-(\nu_1+\cdots+\nu_j)} t_1^{\nu_1} t_2^{\nu_2} \cdots t_j^{\nu_j} \tag{2.3}$$

$$= \sum_{\nu_1+2\nu_2+\cdots+j\nu_j=j} d^{(\nu_1+\nu_2+\cdots+\nu_j)} \frac{t_1^{\nu_1}}{\nu_1!} \frac{t_2^{\nu_2}}{\nu_2!} \cdots \frac{t_j^{\nu_j}}{\nu_j!} \tag{2.4}$$

We use in (2.4) the notation $d^{(m)} = d(d-1)\cdots(d-m+1)$ for the falling factorial. In light of Lemma 2.1, since every periodic string is the repeated concatenation of an aperiodic string,

$$S_R(n; \mathbf{u}) = \sum_{d|n} \sum_{\mathbf{t} \in R^k} [\![\theta_d(\mathbf{t}) = \mathbf{u}]\!] \; A_R(\frac{n}{d}; \mathbf{t}). \tag{2.5}$$

In principle (2.5) may be inverted recursively as long as all the solutions $\mathbf{t}$ to the equations $\mathbf{u} = \theta_d(\mathbf{t})$ can be determined. That is, when $d = 1$, the only solution is $t_j = u_j$ for $j = 1, 2, \ldots, k$, giving the term $A_R(n; t_1, t_2, \ldots, t_k)$ All other terms have first parameter smaller than n. However, our aim is to invert (2.5) explicitly whenever possible.

In the sequel it often happens that the equation $\mathbf{u} = \theta_d(\mathbf{t})$ has has at most one solution for particular values of n and $\mathbf{u}$; i.e., if it has a solution then $\mathbf{t} = \theta_d^{-1}(\mathbf{u})$. Then (2.5) becomes

$$S_R(n; \mathbf{u}) = \sum_{d|n} [\![\theta_d^{-1}(\mathbf{u}) \text{ exists}]\!] A_R(\frac{n}{d}; \theta_d^{-1}(\mathbf{u})). \tag{2.6}$$

Let us explicitly write out (2.4) for $k = 1, 2, 3, 4$ as a preparation for some examples to follow and to better understand the nature of the equation.

$$u_1 = dt_1 \tag{2.7}$$

$$u_2 = dt_2 + \binom{d}{2} t_1^2 \tag{2.8}$$

$$u_3 = dt_3 + d(d-1)t_1 t_2 + \binom{d}{3} t_1^3 \tag{2.9}$$

$$u_4 = dt_4 + d(d-1)t_1 t_3 + \binom{d}{2} t_2^2 + (d-2)\binom{d}{2} t_1^2 t_2 + \binom{d}{4} t_1^4 \tag{2.10}$$

Next we state a fundamental multiplicative property of the mapping θ.

Lemma 2.2. *For all natural numbers a and b,*

$$\theta_a(\theta_b(\mathbf{t})) \;=\; \theta_{ab}(\mathbf{t}).$$

Proof. Let $h_d(z) = \sum_{n\geq 1} u_n z^n = \sum_{n\geq 1}(n!u_n)z^n/n!$. Then $h_d(z) = f_d(g(z))$, where

$$f_d(z) = \sum_{n\geq 1} d^{\underline{n}}\frac{z^n}{n!} = \sum_{n\geq 1}\binom{d}{n}z^n \quad \text{and} \quad g(z) = \sum_{n\geq 1} n!t_n\frac{z^n}{n!} = \sum_{n\geq 1} t_n z^n,$$

by the Faà di Bruno formula (see Comtet [3], pp. 137–138). Our lemma then reduces to the statement that $f_a(f_b(g(z))) = f_{ab}(g(z))$, which we can prove by showing that $f_a(f_b(z)) = f_{ab}(z)$. But this is a trivial substitution since $f_a(z) = (1+z)^a - 1$. $\square$

Note that the lemma holds where a and b are formal variables; but we will use it only when they are members of $\mathbb{Z}_q$.

For fixed k and q, we will be interested in the period of the sequence $\binom{n}{k}$ mod q, for $n = 0, 1, 2, \ldots$. The value of this period has been determined by Zabek [12], and we state this result below.

Theorem 2.3 (Zabek). *Let the prime factorization of q be*

$$q = p_1^{n_1}p_2^{n_2}\cdots p_e^{n_e}$$

where the p_i's are distinct primes and the n_i's are positive integers. The period of the sequence $(\binom{0}{j}, \binom{1}{j}, \binom{2}{j}, \ldots)$ mod q is denoted q'_j and is equal to

$$q'_j = \prod_{i=1}^{e} p_i^{n_i+d_i}, \quad \text{where } d_i = \lfloor \log_{p_i} j \rfloor.$$

Corollary 2.4. *If p is prime then the period of the sequence $(\binom{0}{j}, \binom{1}{j}, \binom{2}{j}, \ldots)$ mod p is $p^{1+\lfloor \log_p j\rfloor}$.*

We note that Zabek's Theorem (together with (2.2)) implies that $\theta_a(\mathbf{t}) : R^k \to R^k$ is periodic in the sense that

$$\theta_{a+q'_k}(\mathbf{t}) = \theta_a(\mathbf{t}). \tag{2.11}$$

Hence we will consider the integer subscripts of θ_a as integers mod q'_k; i.e., $a \in \mathbb{Z}_{q'_k}$. By $\mathbb{Z}_q^*$ we denote the group of units (invertible elements) of $\mathbb{Z}_q$.

Corollary 2.5. *If $a \in \mathbb{Z}^*_{q'_k}$ then θ_a is invertible and $\theta_a^{-1} = \theta_{a^{-1}}$.*

Proof. This follows from fact that $\theta_{\mathbf{1}}$ is the identity mapping and Lemma 2.2. $\square$

3. A Generalized Möbius Inversion. In this section we prove a generalized Möbius inversion that is very useful in obtaining expressions for $A_R(n;\tau_1,\tau_2,\ldots,\tau_k)$ and $L_R(n;\tau_1,\tau_2,\ldots,\tau_k)$, when $R = \mathbb{Z}_q$ or $R = \mathbb{F}_q$. In this section q can be any positive integer. In the expressions below the reader should be careful about the context in which d is used. We use, here and throughout the remainder of the paper, the notation $d \equiv x(q)$ to mean $d \equiv x \bmod q$.

Lemma 3.1. *If n mod $q \in \mathbb{Z}_q^*$, then*

$$\sum_{x\in\mathbb{Z}_q^*}\sum_{\substack{d|n\\ d\equiv x(q)}} \mu(\frac{n}{d}) = [\![n=1]\!].$$

Proof. The defining recurrence relation for the Möbius function is $\sum_{d|n}\mu(d) = [\![n=1]\!]$ (e.g., [6]). The lemma follows from this and the observation that if n mod $q \in \mathbb{Z}_q^*$ and $d|n$, then d mod $q \in \mathbb{Z}_q^*$. $\square$

The following theorem was proven for $q = 2$ in [4] and for $q = 4$ in [2].

THEOREM 3.2. *Let f_x and g_x be sets of functions indexed by $x \in \mathbb{Z}_q^*$. The following two statements are equivalent. For all $x \in \mathbb{Z}_q^*$,*

$$f_x(n) = \sum_{a \in \mathbb{Z}_q^*} \sum_{\substack{d|n \\ d \equiv a(q)}} g_{ax}(\frac{n}{d}). \tag{3.1}$$

For all $x \in \mathbb{Z}_q^*$,

$$g_x(n) = \sum_{a \in \mathbb{Z}_q^*} \sum_{\substack{d|n \\ d \equiv a(q)}} \mu(d) f_{ax}(\frac{n}{d}). \tag{3.2}$$

Proof. Let X be the right-hand side of (3.1) and assume that (3.2) is true. Then

$$\begin{aligned} X &= \sum_{a \in \mathbb{Z}_q^*} \sum_{\substack{d|n \\ d \equiv a(q)}} g_{ax}(\frac{n}{d}) \\ &= \sum_{a \in \mathbb{Z}_q^*} \sum_{\substack{d|n \\ d \equiv a(q)}} \sum_{b \in \mathbb{Z}_q^*} \sum_{\substack{d'|(n/d) \\ d' \equiv b(q)}} \mu(d') f_{abx}(\frac{n/d}{d'}). \end{aligned}$$

We now make the substitutions $dd' = m$ and $ab = c$ and interchange the order of summation to obtain

$$\begin{aligned} X &= \sum_{c \in \mathbb{Z}_q^*} \sum_{b \in \mathbb{Z}_q^*} \sum_{\substack{m|n \\ m \equiv c(q)}} \sum_{\substack{d|m \\ d \equiv cb^{-1}(q)}} \mu(\frac{m}{d}) f_{cx}(\frac{n}{m}) \\ &= \sum_{c \in \mathbb{Z}_q^*} \sum_{\substack{m|n \\ m \equiv c(q)}} f_{cx}(\frac{n}{m}) \sum_{b \in \mathbb{Z}_q^*} \sum_{\substack{d|m \\ d \equiv cb^{-1}(q)}} \mu(\frac{m}{d}) \\ &= \sum_{c \in \mathbb{Z}_q^*} \sum_{\substack{m|n \\ m \equiv c(q)}} f_{cx}(\frac{n}{m}) [\![m = 1]\!] \\ &= f_x(n). \end{aligned}$$

The second equality above uses Lemma 3.1, noting that the condition $m \equiv c(q)$ on the second summation implies that $m \bmod q \in \mathbb{Z}_q^*$.

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

4. General Results. In this section we present some results that apply over various finite commutative rings. We assume throughout that R has r elements and prime characteristic p.

The following formula for $A_R(n)$ is well known and depends only on the number of elements in the ring and not its algebraic structure.

$$A_R(n) = \sum_{d|n} \mu(\frac{n}{d}) r^d = \sum_{d|n} \mu(d) r^{n/d}. \tag{4.1}$$

The following two lemmas will be useful in simplifying certain later sums.

LEMMA 4.1. *Let a be a natural number, b and j be a positive integers, and f a function from the positive integers to a commutative ring with identity. Then*

$$\sum_{\substack{d|n\\ d\equiv ja(jb)}} f(d) \;=\; [\![j|n]\!] \sum_{\substack{d|\frac{n}{j}\\ d\equiv a(b)}} f(jd). \tag{4.2}$$

Proof. The condition $d \equiv ja(jb)$ implies that $j \mid d$. Let $d = jd'$. Observe that

$$[\![d \mid n]\!][\![d \equiv ja(jb)]\!] \;=\; [\![jd'|n]\!][\![jd' \equiv ja(jb)]\!] \;=\; [\![j|n]\!][\![d'|\frac{n}{j}]\!][\![d' \equiv a(b)]\!].$$

Summation index d is used on the left-hand side of (4.2) and d' is used on the right-hand side. ∎

In the arguments to follow, we will use Lemma 4.1 with two sets of values for j, a, b. First, in the next lemma we use $j = q$, $a = 0$, and $b = 1$. In this case the congruence in the right-hand sum becomes $d \equiv 0(1)$ which is vacuously satisfied and can be omitted. Later, we will use $j = 2$, $a = 1$, and $b = 2$.

LEMMA 4.2. *Let n and q be positive integers. Then*

$$\sum_{\substack{d|n\\ d\equiv 0(q)}} A_R(\frac{n}{d}) = [\![q|n]\!] \sum_{d|\frac{n}{q}} A_R(\frac{n/q}{d}) = [\![q|n]\!] r^{n/q}.$$

Proof. The first equality follows from Lemma 4.1, the second from the fact that every string is the repeated concatenation of some aperiodic string. ∎

LEMMA 4.3. *Let R have prime characteristic p. If $k < p$ (and $\mathbf{0}$ is the k-tuple $(0, 0, \ldots, 0)$), then*

$$S_R(n; \mathbf{0}) \;=\; \sum_{\substack{d|n\\ d\equiv 0(p)}} A_R(\frac{n}{d}) + \sum_{\substack{d|n\\ d\not\equiv 0(p)}} A_R(\frac{n}{d}; \mathbf{0}) \;=\; [\![p|n]\!] r^{n/p} + \sum_{\substack{d|n\\ d\not\equiv 0(p)}} A_R(\frac{n}{d}; \mathbf{0}).$$

Proof. The second equality follows from Lemma 4.2. To prove the first equality, take equation (2.5) and break the sum into two parts depending on whether $d \equiv 0(p)$ or not. Recall (2.4).

Consider first the case where $d \equiv 0(p)$. From $p|d$ and $j \geq 1$ it follows that $p|d^{(\nu_1+\nu_2+\cdots+\nu_j)}$. Since $\nu_i \leq k < p$, we have $p \nmid \nu_1!\nu_2!\cdots\nu_j!$. Thus p divides $d^{(\nu_1+\nu_2+\cdots+\nu_j)}/(\nu_1!\nu_2!\cdots\nu_j!)$ from which it follows that $u_j = 0$ irrespective of the values of $\mathbf{t}$. Thus

$$\sum_{\mathbf{t}\in R^k} [\![\theta_d(\mathbf{t}) = \mathbf{0}]\!] \; A_R(\frac{n}{d}; \mathbf{t}) = \sum_{\mathbf{t}\in R^k} A_R(\frac{n}{d}; \mathbf{t}) = A_R(\frac{n}{d}).$$

Now consider the case where $d \not\equiv 0(p)$. In the notation of Theorem 2.3, $q'_k = p$ since $k < p$. Since $d \in \mathbb{Z}_p^*$, by Corollary 2.5 the function θ_d is invertible, and $\theta_d^{-1} = \theta_{d^{-1}}$. Thus $\mathbf{t} = \theta_{d^{-1}}(\mathbf{0}) = \mathbf{0}$ and hence

$$\sum_{\mathbf{t}\in R^k} [\![\theta_d(\mathbf{t}) = \mathbf{0}]\!] \; A_R(\frac{n}{d}; \mathbf{t}) = \sum_{\mathbf{t}\in R^k} [\![\mathbf{t} = \mathbf{0}]\!] \; A_R(\frac{n}{d}; \mathbf{t}) = A_R(\frac{n}{d}; \mathbf{0}).$$

∎

Corollary 4.4. *If R is a ring of prime characteristic p with $k < p$, then*

$$L_R(n;\mathbf{0}) = \frac{1}{n}\sum_{\substack{d|n\\ d\not\equiv 0(p)}} \mu(d)\left(S_R(\frac{n}{d};\mathbf{0}) - [\![pd|n]\!] r^{n/(pd)}\right),$$

where R contains r elements and $\mathbf{0}$ is the k-tuple $(0,0,\ldots,0)$.

Proof. Note that the sum in Lemma 4.3 is over $\{1,2,\ldots,p-1\} = \mathbb{Z}_p^*$ for prime p. Apply Theorem 3.2 with $f_x(n) = S_R(n;\mathbf{0})$ and $g_x(n) = A_R(n;\mathbf{0})$ for all x. □

5. Strings over the ring $\mathbb{Z}_q$. In [9] we showed that

$$L_{\mathbb{Z}_q}(n;t) = \frac{1}{qn}\sum_{\substack{d|n\\ \gcd(d,q)|t}} \mu(d)\gcd(d,q)q^{n/d}. \tag{5.1}$$

From this the next lemma follows.

Lemma 5.1. *If $\gcd(q,t) = \gcd(q,t')$ then $L_{\mathbb{Z}_q}(n;t) = L_{\mathbb{Z}_q}(n;t')$.*

Note that $x \in \mathbb{Z}_q^*$ if and only if $x \in \mathbb{Z}_{q'_k}^*$ since $\gcd(x,q) = 1$ if and only if $\gcd(x,q'_k) = 1$.

Lemma 5.2. *For all $n \geq 1$ and primes p*

$$\sum_{\substack{d|n\\ d\not\equiv 0(p)}} A_{\mathbb{Z}_p}(\frac{n}{d};1) = p^{n-1}. \tag{5.2}$$

Proof. This follows from the equation

$$p^{n-1} = S(n;1) = \sum_{d|n}\sum_{de=1} A_R(\frac{n}{d};e) = \sum_{e\in\mathbb{Z}_p^*}\sum_{d|n} A_R(\frac{n}{d};e^{-1}).$$

□

Let us say that a parameter pair $(n;\mathbf{t})$ is *unit invertible* if the equation $\mathbf{u} = \theta_d(\mathbf{t})$ has a unique solution for all $d \in \mathbb{Z}_{q'_k}^*$, and has no solution if $d \notin \mathbb{Z}_{q'_k}^*$. For example, $(n;\mathbf{t})$ is unit invertible if $t_1 \in \mathbb{Z}_q^*$ or if $n \in \mathbb{Z}_q^*$.

Theorem 5.3. *If $(n;\mathbf{t})$ is unit invertible, then*

$$L_{\mathbb{Z}_q}(n;\mathbf{t}) = \frac{1}{n}\sum_{r\in\mathbb{Z}_{q'_k}^*}\sum_{\substack{d|n\\ d\equiv r^{-1}(q'_k)}} \mu(d)S_{\mathbb{Z}_q}(\frac{n}{d};\theta_{r^{-1}}(\mathbf{t})). \tag{5.3}$$

Proof. Under the stated hypotheses we can write equation (2.6) as

$$S(n;\mathbf{t}) = \sum_{a\in\mathbb{Z}_{q'_k}^*}\sum_{\substack{d|n\\ d\equiv a(q'_k)}} A(\frac{n}{d};\theta_a^{-1}(\mathbf{t})). \tag{5.4}$$

By Corollary 2.5, we have $\theta_a^{-1}(\mathbf{u}) = \theta_{a^{-1}}(\mathbf{u})$. Substitute $\mathbf{t} = \theta_x(\mathbf{u})$ in (5.4) and use the multiplicative property $\theta_{a^{-1}}(\theta_x(\mathbf{u})) = \theta_{a^{-1}x}(\mathbf{u})$ to obtain

$$S(n;\theta_x(\mathbf{u})) = \sum_{a\in\mathbb{Z}_{q'_k}^*}\sum_{\substack{d|n\\ d\equiv a(q'_k)}} A(\frac{n}{d};\theta_{a^{-1}x}(\mathbf{u})). \tag{5.5}$$

Written in this form we can apply Theorem 3.2 with $f_x(n) = S(n; \theta_x(\mathbf{u}))$ and $g_x(n) = A(n; \theta_{x^{-1}}(\mathbf{u}))$ to obtain equation (5.3) □

Example: If $q = k = 3$ then $q'_k = 9$ and $\theta_{d^{-1}}(1,0,0)$ takes on the values

$$\{(1,0,0),(2,1,0),(1,0,1),(2,1,1),(1,0,2),(2,1,2)\}$$

for $d = 1,2,4,5,7,8$. The number, $L_{\mathbb{Z}_3}(n;1,0,0)$, of length n Lyndon words over $\mathbb{Z}_3$ with $(t_1,t_2,t_3) = (1,0,0)$ is therefore equal to

$$\frac{1}{n}\sum_{j\in\mathbb{Z}_3}\left(\sum_{\substack{d|n\\ d\equiv(3j+1)^{-1}(9)}}\mu(d)S_{\mathbb{Z}_3}(\frac{n}{d};1,0,j)+\sum_{\substack{d|n\\ d\equiv(3j+2)^{-1}(9)}}\mu(d)S_{\mathbb{Z}_3}(\frac{n}{d};2,1,j)\right),$$

giving rise to the sequence of numbers 1, 1, 1, 1, 1, 1, 6, 36, 141, 422, 1062, 2371, 4995, 11082, 29230, 90735, for $n = 1, 2, \ldots, 16$.

According to the results of [8], over $\mathbb{Z}_3$ the traces (t_1,t_2,t_3) determine the traces t_4 and t_5, so that $L_{\mathbb{Z}_3}(n;1,0,0) = L_{\mathbb{Z}_3}(n;1,0,0,0,0)$. Furthermore, the $S_{\mathbb{Z}_3}$ numbers can be expressed as sums of multinomial coefficients; e.g., for $S_{\mathbb{Z}_3}(n;1,0,0)$ we have

$$S_{\mathbb{Z}_3}(n;1,0,0) = \sum_{\substack{k_0+k_1+k_2=n\\ k_2\equiv 0(3)\\ k_1-k_2\equiv 1(9)}}\binom{n}{k_0,k_1,k_3}.$$

6. Strings over the ring $\mathbb{F}_q$.

6.1. The field $\mathbb{F}_q$ for q odd. In this section we consider the computation of the number of strings in the various classes over $\mathbb{F}_q$, where $q = p^m$, with p an odd prime.

In [9] we reproved a result of Carlitz [1] that, if $t \neq 0$, then

$$L_{\mathbb{F}_q}(n;t) = \frac{1}{qn}\sum_{\substack{d|n\\ p\nmid d}}\mu(d)q^{n/d}.$$

Here we generalize this to the first $p-1$ traces.

Theorem 6.1. *If $q = p^m$, where p is an odd prime and $k < p$, then*

$$L_{\mathbb{F}_q}(n;\mathbf{t}) = \begin{cases} \dfrac{1}{n}\displaystyle\sum_{\substack{d|n\\ p\nmid d}}\mu(d)\left(S_{\mathbb{F}_q}(\frac{n}{d};\mathbf{0}) - [\![pd|n]\!]q^{n/(pd)}\right) & \text{if } \mathbf{t} = \mathbf{0}\\ \dfrac{1}{n}\displaystyle\sum_{\substack{d|n\\ p\nmid d}}\mu(d)S_{\mathbb{F}_q}(\frac{n}{d};\theta_{d^{-1}}(\mathbf{t})) & \text{otherwise.}\end{cases}$$

Proof: The $\mathbf{t} = \mathbf{0}$ case follows from Corollary 4.4. In the other case there is some index $j \leq k$ such that $t_1 = \cdots = t_{j-1} = 0$ and $t_j \neq 0$. Consider the equation $\mathbf{t} = \theta_d(\mathbf{u})$ in (2.5). If $d \equiv 0(p)$ then we must have $\mathbf{t} = \mathbf{0}$. Thus $d \not\equiv 0(p)$. Hence $u_1 = u_2 = \cdots = u_{j-1} = 0$ and $t_j = du_j$ so that $u_j = d^{-1}t_j$. Repeated substitution will give unique values for $u_j, u_{j+1}, \ldots, u_k$. We can therefore use (2.6) and write

$$\begin{aligned} S_{\mathbb{F}_q}(n;\mathbf{t}) &= \sum_{\substack{d|n\\ d\not\equiv 0(p)}} A_{\mathbb{F}_q}(\frac{n}{d};\theta_{d^{-1}}(\mathbf{t}))\\ &= \sum_{x\in\mathbb{Z}_p^*}\sum_{\substack{d|n\\ d\equiv x^{-1}(p)}} A_{\mathbb{F}_q}(\frac{n}{d};\theta_{x^{-1}}(\mathbf{t})), \end{aligned}$$

which can then be inverted by Theorem 3.2 to obtain the stated result. □

The case where $p = 2$ will be handled in the next section.

6.2. The field $\mathbb{F}_{2^m}$. In this section $p = 2$. Since $p = 2$, if $k < p$ then $k = 0$ or $k = 1$. However, the value of $L_{\mathbb{Z}_{2^m}}(n; \mathbf{t})$ is known for $k = 0, 1$ (equations (4.1) and (6.1)), so unlike the previous subsection here we have $k \geq p$. In this section we will consider in detail the $k = 3$ case, which is the largest value for which $p'_k = 2^2 = 4$. In other words, we derive a formula for $L_{\mathbb{F}_{2^m}}(n; t_1, t_2, t_3)$. We also state without proof the result for $L_{\mathbb{F}_{2^m}}(n; t_1, t_2)$.

Here the values of $\binom{d}{2}$ mod 2 follow the pattern 0,0,1,1 mod 4 and the values of $\binom{d}{3}$ mod 2 follow the pattern 0,0,0,1, so we consider the value of d mod 4 in the equations (2.7),(2.8),(2.9) taken mod 2 (but with the roles of u and t reversed). If $d \equiv 0(4)$, then $t_1 = t_2 = t_3 = 0$, but u_1, u_2 and u_3 are unrestricted. If $d \equiv 1(4)$, then $u_1 = t_1$, $u_2 = t_2$ and $u_3 = t_3$. If $d \equiv 2(4)$, $t_1 = 0$, $u_1^2 = t_2$, and $t_3 = 0$. Fortunately, in a field of characteristic 2, square roots always exist and are unique, so we can set $u_1 = \sqrt{t_2}$. Finally, if $d \equiv 3(4)$, then $u_1 = t_1$, $u_2 = t_2 + t_1^2$, and $t_3 = u_3 + t_1^3$. Thus,

$$\begin{aligned}
S_{\mathbb{F}_{2^m}}(n; t_1, t_2, t_3) = [\![t_1 = 0]\!][\![t_2 = 0]\!][\![t_3 = 0]\!] &\sum_{\substack{d|n \\ d\equiv 0(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}) \\
&+ \sum_{\substack{d|n \\ d\equiv 1(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; t_1, t_2, t_3) \\
&+ [\![t_1 = 0]\!][\![t_2 = 0]\!] \sum_{\substack{d|n \\ d\equiv 2(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; \sqrt{t_2}) \\
&+ \sum_{\substack{d|n \\ d\equiv 3(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; t_1, t_2 + t_1^2, t_3 + t_1^3).
\end{aligned}$$

We now consider the different values of the trace, subtrace and sub-subtrace. If $t_1 = t_2 = t_3 = 0$, then

$$S_{\mathbb{F}_{2^m}}(n; 0, 0, 0) = \sum_{\substack{d|n \\ d\equiv 0(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}) + \sum_{\substack{d|n \\ d\equiv 2(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}, 0) + \sum_{\substack{d|n \\ d \text{ odd}}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}, 0, 0, 0). \tag{6.1}$$

If $s \neq 0$ but $t_1 = t_3 = 0$, then

$$S_{\mathbb{F}_{2^m}}(n; 0, t_2, 0) = \sum_{\substack{d|n \\ d\equiv 2(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; \sqrt{t_2}) + \sum_{\substack{d|n \\ d \text{ odd}}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; 0, t_2, 0). \tag{6.2}$$

If $t_1 = 0$ but $t_3 \neq 0$, then

$$S_{\mathbb{F}_{2^m}}(n; 0, s, r) = \sum_{\substack{d|n \\ d \text{ odd}}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; 0, t_2, t_3). \tag{6.3}$$

The equations where $t_1 \neq 0$ come in parameter pairs, (t_1, t_2, t_3) and $(t_1, t_2 + t_1^2, t_3 + t_1^3)$. The quantity $S_{\mathbb{F}_{2^m}}(n; t_1, t_2, t_3)$ is equal to

$$\sum_{\substack{d|n \\ d\equiv 1(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; t_1, t_2, t_3) + \sum_{\substack{d|n \\ d\equiv 3(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; t_1, t_2 + t_1^2, t_3 + t_1^3). \tag{6.4}$$

We can use Theorem 3.2 to invert the pairs (6.4) to obtain

$$L_{\mathbb{F}_{2^m}}(n;t_1,t_2,t_3) = \frac{1}{n}\sum_{\substack{d\mid n\\ d\equiv 1(4)}} \mu(d) S_{\mathbb{F}_{2^m}}(\frac{n}{d};t_1,t_2,t_3) + \frac{1}{n}\sum_{\substack{d\mid n\\ d\equiv 3(4)}} \mu(d) S_{\mathbb{F}_{2^m}}(\frac{n}{d};t_1,t_2+t_1^2,t_3+t_1^3).$$

To invert (6.2) we will need the following lemma and corollary. The lemma holds over general finite fields.

Lemma 6.2. *Let $q = p^m$ with p prime. For all $n \geq 1$,*

$$\sum_{\substack{d\mid n\\ d\not\equiv 0(p)}} A_{\mathbb{F}_q}(\frac{n}{d};1) = q^{n-1}, \quad \textit{and} \tag{6.5}$$

$$\sum_{\substack{d\mid n\\ d\not\equiv 0(p)}} A_{\mathbb{F}_q}(\frac{n}{d};0) = q^{n-1} - [\![p|n]\!] q^{n/p} \tag{6.6}$$

Proof. To prove (6.5) consider the equation below, where $y \in \mathbb{Z}_p^*$.

$$q^{n-1} = S_{\mathbb{F}_q}(n;y) = \sum_{d\mid n}\sum_{dx\equiv y} A_{\mathbb{F}_q}(\frac{n}{d};x) = \sum_{\substack{d\mid n\\ d\in\mathbb{Z}_p^*}} A_{\mathbb{F}_q}(\frac{n}{d};d^{-1}y) = \sum_{\substack{d\mid n\\ d\in\mathbb{Z}_p^*}} A_{\mathbb{F}_q}(\frac{n}{d};1)$$

The second equality is a restatement of (2.5). The equation $dx = y$ has a solution only if $d \in \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$, namely $x = d^{-1}y \bmod p$, giving the third equality. The equalities $S_{\mathbb{F}_q}(n;y) = \sum_{\substack{d\mid n\\ d\in\mathbb{Z}_p^*}} A_{\mathbb{F}_q}(\frac{n}{d};d^{-1}y)$ can be inverted by Theorem 3.2 to obtain

$$A_{\mathbb{F}_q}(n;y) = \sum_{\substack{d\mid n\\ d\in\mathbb{Z}_p^*}} \mu(d) S_{\mathbb{F}_q}(\frac{n}{d};d^{-1}y), \tag{6.7}$$

thereby implying that $A_{\mathbb{F}_q}(n;y) = A_{\mathbb{F}_q}(n;1)$ for all $y \in \mathbb{Z}_p^*$ and justifying the last equality. □

The following corollary generalizes Lemma 5 from [2].

Corollary 6.3. *Let m be a positive integer. Then*

$$\sum_{\substack{d\mid n\\ d\equiv 2(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d},1) = [\![n \textit{ even}]\!](2^m)^{n/2-1}, \tag{6.8}$$

$$\sum_{\substack{d\mid n\\ d\equiv 0(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}) + \sum_{\substack{d\mid n\\ d\equiv 2(4)}} A_{\mathbb{F}_{2^m}}(\frac{n}{d},0) = [\![n \textit{ even}]\!](2^m)^{n/2-1}. \tag{6.9}$$

Proof. To prove (6.8) we first use Lemma 4.1 with $j = b = 2$ and $a = 1$. This produces a sum of the form of (6.5), except with $n/2$ substituted for n, and 2^m substituted for q.

To prove (6.9), note that the first term of the left-hand side is $[\![4|n]\!](2^m)^{n/4}$ by Lemma 4.2 with $q = 4$. By Lemma 4.2 the second term of the left-hand side is equal to $[\![n \text{ even}]\!] \sum_{d|(n/2),d\not\equiv 0(2)} A(n/(2d), 0)$. By Lemma 6.3 this is in turn equal to $[\![n \text{ even}]\!]((2^m)^{n/2-1} - [\![2|(n/2)]\!](2^m)^{n/4})$. Adding the two terms together we get $[\![n \text{ even}]\!](2^m)^{n/2-1}$. □

Note from (6.1) that $A_{\mathbb{F}_{2^m}}(n; 1) = A_{\mathbb{F}_{2^m}}(n; \sqrt{t_2})$ for any $t_2 \neq 0$. In view of Lemma 6.3, for any t_2, we can write

$$S_{\mathbb{F}_{2^m}}(n; 0, t_2, 0) = [\![n \text{ even}]\!](2^m)^{n/2-1} + \sum_{\substack{d|n \\ d \text{ odd}}} A_{\mathbb{F}_{2^m}}(\frac{n}{d}; 0, t_2, 0).$$

This equation can be inverted using the Möbius inversion of Theorem 3.2 to obtain

$$L_{\mathbb{F}_{2^m}}(n; 0, t_2, 0) = \frac{1}{n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)(S_{\mathbb{F}_{2^m}}(\frac{n}{d}; 0, t_2, 0) - [\![n/d \text{ even}]\!](2^m)^{n/(2d)-1}).$$

The various cases are summarized in the following theorem.

Theorem 6.4. *If $q = 2^m$, then the value of $L_{\mathbb{F}_q}(n; t_1, t_2, t_3)$ is*

$$\begin{cases} \frac{1}{n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) \left(S_{\mathbb{F}_q}(\frac{n}{d}; 0, t_2, 0) - [\![r = 0]\!][\![2|\frac{n}{d}]\!] q^{n/(2d)-1} \right) & \text{if } t_1 = 0 \\ \frac{1}{n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)\ S_{\mathbb{F}_q}(\frac{n}{d}; t_1, t_2 + \frac{d-1}{2} t_1^2, t_3 + \frac{d-1}{2} t_1^3) & \text{if } t_1 \neq 0. \end{cases}$$

By similar arguments, or by summing over t_3 in the preceding theorem we obtain the theorem below.

Theorem 6.5. *If $q = 2^m$, then*

$$L_{\mathbb{F}_q}(n; t_1, s_1) = \begin{cases} \frac{1}{n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) \left(S_{\mathbb{F}_q}(\frac{n}{d}; 0, t_2) - [\![\frac{n}{d} \text{ even}]\!] q^{n/(2d)-1} \right) & \text{if } t_1 = 0 \\ \frac{1}{n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)\ S_{\mathbb{F}_q}(\frac{n}{d}; t_1, t_2 + \frac{d-1}{2} t_1^2) & \text{if } t_1 \neq 0. \end{cases}$$

7. Acknowledgement. We wish to thank the referee and editor for helpful comments.

8. Final Remarks. Tables of some of the numbers discussed in this paper for $k = 1, 2$ may be accessed from the page `www.theory.cs.uvic.ca/~cos/inf/trs/`. There are many relevant sequence numbers in Neil J. Sloane's online encylopedia of integer sequences. For example, over $\mathbb{Z}_3$ it contains: $L_{\mathbb{Z}_3}(n; 0, 0) =$ A053548, $L_{\mathbb{Z}_3}(n; 0, 1) =$ A053560, $L_{\mathbb{Z}_3}(n; 0, 2) =$ A053561, $L_{\mathbb{Z}_3}(n; 1, 0) = L_{\mathbb{Z}_3}(n; 2, 0) =$ A053562, $L_{\mathbb{Z}_3}(n; 1, 1) = L_{\mathbb{Z}_3}(n; 2, 1) =$ A053563, $L_{\mathbb{Z}_3}(n; 1, 2) = L_{\mathbb{Z}_3}(n; 2, 2) =$ A053564.

REFERENCES

[1] L. Carlitz, *A theorem of Dickson on irreducible polynomials*, Proc. AMS, 3 (1952) 693–700.

[2] K. Cattell, F. Ruskey, C.R. Miers, J. Sawada, and M. Serra, *The Number of Irreducible Polynomials over GF(2) with Given Trace and Subtrace*, Journal of Combinatorial Mathematics and Combinatorial Computing, 47 (2003) 31–64.

[3] Louis Comtet, *Advanced Combinatorics*, 1974, D. Reidel, Dordrecht, Holland.
[4] Dieter Jungnickel, *Finite Fields: structure and arithmetics*, B.I. Wissenschaftsverlag, 1993.
[5] E.N. Kuz'min, *On a class of irreducible polynomials over a finite field*, (Russian) Dokl. Akad. Nauk SSSR 313 (1990), No. 3, 552-555; translation in Soviet Math. Dokl. 42 (1991) No. 1, 45–48.
[6] D.E. Knuth, R.L. Graham, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.
[7] M. Lothaire, *Combinatorics on Words*, Addison-Wesley, Reading, MA, 1983.
[8] C.R. Miers and F. Ruskey, *Counting Strings with Given Elementary Symmetric Function Evaluations I: Strings over $\mathbb{Z}_p$ with p prime*, SIAM Journal Discrete Mathematics, to appear, 2004.
[9] F. Ruskey, C.R. Miers, and J. Sawada, *The Number of Irreducible Polynomials and Lyndon Words with a Given Trace*, SIAM J. Discrete Mathematics, 14 (2001) 240–245.
[10] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1994.
[11] J.L. Yucas and G.L. Mullen, *Irreducible Polynomials over GF(2) with Prescribed Coefficients*, Discrete Mathematics, 274 (2004) 265–279.
[12] S. Zabek, *Sur la periodicite modulo m des suits de nombres* $\binom{n}{k}$, Ann. Univ. Mariae Curie-Sklodowska Sect. A, 10 (1956), 37–47.