FPSAC 2013 Paris, France DMTCS proc. **AS**, 2013, 897–908

Counting Strings over $\mathbb{Z}2^d$ with Given Elementary Symmetric Function Evaluations

Charles Robert Miers[1†] and Frank Ruskey[2‡]

[1]*Dept. of Mathematics, University of Victoria, Canada*
[2]*Dept. of Computer Science, University of Victoria, Canada*

Abstract. Let α be a string over $\mathbb{Z}_q$, where $q = 2^d$. The j-th elementary symmetric function evaluated at α is denoted $e_j(\alpha)$. We study the cardinalities $S_q(m; \tau_1, \tau_2, \ldots, \tau_t)$ of the set of length m strings for which $e_i(\alpha) = \tau_i$. The *profile* $\mathbf{k}(\alpha) = \langle k_1, k_2, \ldots, k_{q-1}\rangle$ of a string α is the sequence of frequencies with which each letter occurs. The profile of α determines $e_j(\alpha)$, and hence S_q. Let $h_n : \mathbb{Z}_{2^{n+d-1}}^{(q-1)} \mapsto \mathbb{Z}_{2^d}[z] \bmod z^{2^n}$ be the map that takes $\mathbf{k}(\alpha) \bmod 2^{n+d-1}$ to the polynomial $1 + e_1(\alpha)z + e_2(\alpha)z^2 + \cdots + e_{2^n-1}(\alpha)z^{2^n-1}$. We show that h_n is a group homomorphism and establish necessary conditions for membership in the kernel for fixed d. The kernel is determined for $d = 2, 3$. The range of h_n is described for $d = 2$. These results are used to efficiently compute $S_4(m; \tau_1, \tau_2, \ldots, \tau_t)$ for $d = 2$ and the number of complete factorizations of certain polynomials.

Résumé. Soit α un mot sur $\mathbb{Z}_q$, où $q = 2^d$. La $j-$ième fonction symmétrique élémentaire évaluée à α est dénotée $e_j(\alpha)$. Nous étudions les cardinalités $S_q(m; \tau_1, \tau_2, \ldots, \tau_t)$ de l'ensemble des mots de longueur m pour lesquels $e_i(\alpha) = \tau_i$. Le *profil* $\mathbf{k}(\alpha) = \langle k_1, k_2, \ldots, k_{q-1}\rangle$ d'un mot α est la suite de fréquences d'apparition de chaque lettre. Le profil de α détermine $e_j(\alpha)$ et donc S_q. Soit $h_n : \mathbb{Z}_{2^{n+d-1}}^{(q-1)} \mapsto \mathbb{Z}_{2^d}[z] \bmod z^{2^n}$ la fonction qui associe à $\mathbf{k}(\alpha) \bmod 2^{n+d-1}$ le polynôme $1 + e_1(\alpha)z + e_2(\alpha)z^2 + \cdots + e_{2^n-1}(\alpha)z^{2^n-1}$. Nous démontrons que h_n est un homomorphisme de groupe et nous établissons des conditions nécessaires à l'appartenance au noyau pour un d fixé. Le noyau est déterminé pour $d = 2, 3$. L'image de h_n est décrite pour $d = 2$. Ces résultats sont utilisés pour calculer de manière efficace $S_4(m; \tau_1, \tau_2, \ldots, \tau_t)$ pour $d = 2$ ainsi que le nombre de factorisations complètes de certains polynômes.

Keywords: elementary symmetric function, monomial factorization, integers mod 2^d, group homomorphism, kernel.

1 Introduction and motivation

Before getting too deeply into the abstract and technical details let us illustrate the types of computations that we will be able to easily carry out after proving our results. Let $[\![P]\!]$ be 1 or 0 depending of whether the proposition P is true or false, respectively. Consider the problem below.

†Partially supported by a UVic Faculty Research Grant
‡Partially supported by NSERC

EXAMPLE 1 *How many strings are there of length* 100 *over the alphabet* $0, 1, 2, 3$ *that satisfy the following six conditions, with arithmetic done mod 4? Conditions: (a) The sum of the characters is 0 and, (b) the sum of the products of all pairs of characters is 3 and, (c) the sum of the products of all 4-tuples of characters is 3, (d) the sum of the products of all 8-tuples of characters is 2, (e) the sum of the products of all 16-tuples of characters is 3, (f) the sum of the products of all 32-tuples of characters is 3. The answer is approximately* 2.33×10^{58}*, or exactly*

$$23283888738988446954113680611180557044216386182393836339200, \tag{1}$$

which is the value of the sum

$$\sum_{k_0+k_1+k_2+k_3=100} \binom{100}{k_0, k_1, k_2, k_3} [\![k_1, k_3 \text{ even}, k_2 \text{ odd}, k_1 + k_3 \equiv 54 \bmod 64]\!].$$

That is, the answer is the sum of 667 multinomial coefficients. Furthermore, the sum above applies for strings of length m*; one need only replace the* 100 *by* m*.*

There are several natural questions that should occur to the reader at this point. Firstly, why are the "tuples" involved all powers of two? The reason is that, for example, the sum of products of all 3-tuples is determined already by the value of the sum of products of 1-tuples and 2-tuples. Secondly, why do the mysterious parity and modular conditions arise; in particular why is it some condition mod 64 and not just mod 4? We will answer all these questions in due course, generalizing from arithmetic done mod 4 to arithmetic done mod 2^d.

EXAMPLE 2 *In this example all computations are done mod 8. The following equation illustrates the non-unique factorization of a polynomial into monomials.*

$$(1 + z)^3(1 + 5z)^5 = (1 + 3z)^9(1 + 7z)^1 \tag{2}$$

Given a polynomial factored into monomials, we do not know a nice or efficient way to express the number of its other such factorizations, but we can count them mod z^{2^n} *(simply meaning that we ignore all terms involving* z^{2^n} *for* $k \geq 2^n$*). For example,*

$$(1 + z)^6(1 + 2z)^1(1 + 4z)^1(1 + 6z)^3 = (1 + 3z)^{20}(1 + 5z)^{14}(1 + 7z)^4 \bmod z^8 \tag{3}$$

and we will show that the total number of possible distinct right hand sides in (3) is 2^{22} *if the exponents on the monomials* $(1 + jz)^k$ *(*$j = 1, 2, \ldots, 7$*) are restricted so that* $0 \leq k < 32$*; here 32 is the minimum value required to ensure "periodicity."*

One aim of this paper is to explain this example and to generalize it to other powers of 2. We hope that these examples entice the reader to keep reading.

The theory of symmetric functions has long been a basic tool of combinatorial enumeration. In some combinatorial settings it is useful to enumerate the number of variable substitutions to symmetric functions so that the functions achieve given values. Stanley discusses some of these issues in Section 7.8 of [6]. Our initial interest in the elementary symmetric functions stems from the counting of degree n monic irreducible polynomials over finite fields with prescribed coefficients for x^{n-1} and x^{n-2}. 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 (circular) string of coefficients occurring in the factorization.

If a string α has its alphabet in a finite commutative ring R, we can evaluate the j-th elementary symmetric function e_j at α. This evaluation depends on the profile $\mathbf{k} = \langle k_1, k_2, \ldots \rangle$ of α where k_i is the frequency with which the ring element x_i occurs in α. The relationship between strings, polynomials, an elementary symmetric functions is contained in the map $E_{\mathbf{k}}(z) := \prod(1+jz)^{k_j}$ since $e_j(\alpha) = [z^j]E_{\mathbf{k}}(z)$. This relationship can be refined to give a sequence of mappings $h_n : \mathbb{Z}_m^{(|R|-1)} \to G$, where G is an appropriate multiplicative subgroup of $\mathbb{Z}_\ell[[z]]$ where m and ℓ depend on n.

In [3] we studied the the case $R = \mathbb{Z}_p$, where p is prime. These results were then used in [4] in order to enumerate certain circular strings. Here we choose the substitutions to come from the ring of integers mod 2^d. A fundamental difference between the case considered in [3] is that in the $\mathbb{Z}_p$ case the h_n are one-to-one, whereas in the $\mathbb{Z}_{2^d}$ case, they are not. However, there is an underlying group homomorphism and a periodic repetition which will allow us to provide much structural information and a complete characterization for specific small values of d. As a byproduct, we are able to enumerate the number of non-unique factorizations of certain types of polynomials in $\mathbb{Z}_{2^d}[z]$.

A primary aim in this extended abstract is to state/prove some basic facts about h_n, particularly about its kernel; most proofs have been omitted, although a few proof sketches are given. In doing so we will make use of some binomial coefficient congruences and manipulations of formal power series. Interestingly, it will prove useful to allow the profiles contain negative integers and to use the infinite version of the homomorphism which we call h_∞. In the final part of the paper we apply the necessary conditions established earlier to determine the kernel for $d = 2$ and $d = 3$ and give the range for $d = 2$. In principle, the same approach would work for higher values of d, but the computations required become prohibitive.

2 Notation and Preliminaries

In this section we carefully define the problem and introduce some of the basic tools. All computations are done mod q. We set $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ to denote the ring of integers mod q.

2.1 Strings

Consider a string $\alpha = a_1 a_2 \cdots a_m$ where each $a_i \in \mathbb{Z}_q$. The j-th elementary symmetric function evaluated at α, denoted $e_j(\alpha)$, is the sum

$$e_j(\alpha) := \sum_{1 \le i_1 < i_2 < \cdots < i_j \le m} a_{i_1} a_{i_2} \cdots a_{i_j} \pmod{q}.$$

Clearly, $(-1)^j e_j(\alpha)$ is the coefficient of z^{n-j} in the polynomial $(z - a_1)(z - a_2) \cdots (z - a_m)$.

By $S_q(m; \tau_1, \tau_2, \ldots, \tau_t)$ we denote the number of strings α over $\mathbb{Z}_q$ of length m for which $e_i(\alpha) = \tau_i$ for $i = 1, 2, \ldots, t$. Obviously if $t = 0$, then $S_q(m) = q^m$. It is also true that $S_q(m; s) = q^{m-1}$ for any $s \in \mathbb{Z}_q$, since $e_1(\alpha x)$ takes on distinct values for each $x \in \mathbb{Z}_q$. The numbers $S_q(m; \tau_1, \tau_2, \ldots, \tau_t)$ satisfy the following recurrence relation. If $n = 1$, then $S_q(m; \tau_1, \tau_2, \ldots, \tau_t) = [\![\tau_2 = \cdots = \tau_t = 0]\!]$, and for $m > 0$,

$$S_q(m; \tau_1, \tau_2, \ldots, \tau_t) = \sum_{x \in \mathbb{Z}_q} S_q(m-1; \rho_1, \rho_2, \ldots, \rho_t), \tag{4}$$

where $\rho_0 = 1$, and $\rho_i = \tau_i - \rho_{i-1}x$ for $i = 1, 2, \ldots, t$.

Recurrence relation (4) implies that the power series $\sum_{m\geq 0} S_q(m;\tau_1,\tau_2,\ldots,\tau_t)z^m$ is rational. We can evaluate $S_q(m;\tau_1,\tau_2,\ldots,\tau_t)$ by creating a table of size mq^t consisting of S_q for all strings of length at most m and over the first t elementary symmetric functions. Each table entry requires $\Theta(qt)$ ring operations and $\Theta(q)$ arithmetic operations, for a total of $\Theta(mtq^{t+1})$ ring operations and $\Theta(mq^{t+1})$ arithmetic operations. An aim of this paper is to reduce the number of ring and arithmetic operations required to evaluate S_q.

2.2 Profiles

Suppose that the string α has k_x occurrences of the symbol x for $x \in \mathbb{Z}_q$. We refer to the $(q-1)$-tuple of natural numbers $\mathbf{k} = \langle k_1, k_2, \ldots, k_{q-1}\rangle$ as the *profile* of the string. The elementary symmetric function $e_j()$ depends only on the profile. Note that k_0 is omitted since it does not affect $e_j()$. It will prove useful to have profiles consisting of integers, positive or negative; and to have profiles consisting of integers mod a natural number. Which case is in effect will usually be obvious from context. From now on, a bold letter will only denote a profile. We add profiles componentwise and define $x\mathbf{k} = \langle xk_1, xk_2, \ldots, xk_{q-1}\rangle$.

For $\mathbf{k} = \langle k_1, k_2, \ldots, k_{q-1}\rangle \in \mathbb{Z}^{q-1}$, define in $\mathbb{Z}_q[[z]]$ the formal power series

$$E_{\mathbf{k}}(z) := \prod_{j=1}^{q-1}(1+jz)^{k_j} \tag{5}$$

We make no assumption here that the k_i are positive.

Observe that $e_j(\alpha) = [z^j]E_{\mathbf{k}}(z)$, where the notation $[z^j]A(z)$ means the coefficient of z^j in the generating function $A(z)$. Clearly,

$$E_{\mathbf{a}+\mathbf{b}}(z) = E_{\mathbf{a}}(z)E_{\mathbf{b}}(z) \tag{6}$$

We also denote the $e_j(\alpha)$ by $e_j(\mathbf{k})$ or $e_j(\langle k_1, k_2, \ldots, k_{q-1}\rangle)$ when we wish to emphasize the role of profiles.

The evaluation of S_q in terms of profiles is given by

$$S_q(m;\tau_1,\tau_2,\ldots,\tau_t) = \sum_{\substack{k_0+k_1+\cdots+k_{q-1}=m \\ \mathbf{k}:=\langle k_1,\ldots,k_{q-1}\rangle}} \binom{m}{k_0, k_1, \ldots, k_{q-1}} \prod_{i=1}^{t} [\![e_i(\mathbf{k}) = \tau_i]\!]. \tag{7}$$

In order to evaluate (7) efficiently we need to be able to determine efficiently those profiles $\mathbf{k}$ for which $e_i(\mathbf{k}) = \tau_i$ for $i = 1, 2, \ldots, t$. We do this by recasting the conditional as

$$\prod_{i=1}^{t} [\![e_i(\mathbf{k}) = \tau_i]\!] = [\![E_{\mathbf{k}}(z) \bmod z^{t+1} = \sum_{i=0}^{t} \tau_i z^i]\!],$$

where τ_0 is defined to be 1.

This approach to the problem was established in [3] in the case where $p = q$ is prime. There it is proven that there is a bijection between the set of all polynomials $\sum_{0\leq i<p} \tau_i z^i$ in $\mathbb{Z}_p[z]$ and $E_{\mathbf{k}}(z) \bmod z^p$ where $\mathbf{k} \in \mathbb{Z}_p^{(p-1)}$. This bijection is then extended to a bijection between polynomials

$$\sum_{j=0}^{m-1}\sum_{i=0}^{p-1} \tau_{ip^j} z^{ip^j} \text{ where } \tau_{ip^j} \in \mathbb{Z}_p$$

and $E_{\mathbf{k}}(z) \bmod z^{p^m}$ where $\mathbf{k} \in \mathbb{Z}_{p^m}^{(p-1)}$. For $q = 2^d$ the situation is considerably more complicated. Our first goal is to determine the algebraic structure of those $\mathbf{k}$ for which $E_{\mathbf{k}}(z) = 1$.

3 General Results

3.1 Periodicity and group structure

Our initial aim is to establish the periodic nature of the profiles $\mathbf{k}$ when used to determine $E_{\mathbf{k}}(z)$. In this section all computation is done mod 2^d unless noted otherwise.

THEOREM 1 *If* $0 \le s \le d-1$, *then as polynomials in two variables* y *and* z,

$$(1 + (y + 2^{d-s})z)^{2^s} = (1 + yz)^{2^s} \bmod 2^d.$$

LEMMA 1 *With arithmetic mod* 2^d *and* $0 < t \le d$, *where* b, t, d, m *are integers,*

$$(1 + 2^t bz)^m = (1 + 2^t bz)^{m \bmod 2^{d-t}}.$$

THEOREM 2 *With arithmetic mod* 2^d, *for any* $n \ge 1$, *we have* $E_{2^{d+n-1}\mathbf{k}}(z) = E_{2^{d-1}\mathbf{k}}(z^{2^n})$.

Proof: Our proof is by induction on n; details omitted. □

COROLLARY 1 (PERIODICITY) *In* $\mathbb{Z}_{2^d}[[z]] \bmod z^{2^n}$,

$$E_{\mathbf{a}+2^{d+n-1}\mathbf{b}}(z) = E_{\mathbf{a}}(z).$$

Proof: Follows from (6) and Theorem 2. □

This last corollary implies that if we are only considering $e_j()$ with $j < 2^n$, then we need only consider values of the profile taken mod 2^{d+n-1}.

THEOREM 3 *The set* $M_n = \{E_{\mathbf{a}}(z) \bmod z^{2^n} \mid \mathbf{a} \in \mathbb{Z}_{2^{d+n-1}}^{(2^d-1)}\}$ *is a multiplicative group in* $\mathbb{Z}_{2^d}[[z]] \bmod z^{2^n}$, *where the multiplication operation is polynomial multiplication mod* z^{2^n}.

For each $n \in \mathbb{Z}^+$, define the map $h_n : \mathbb{Z}_{2^{d+n-1}}^{(2^d-1)} \mapsto M_n$ that takes $\mathbf{a}$ to $E_{\mathbf{a}}(z) \pmod{z^{2^n}}$. We also define the set $M_\infty = \{E_{\mathbf{a}}(z) \subseteq \mathbb{Z}_{2^d}[[z]] \mid \mathbf{a} \in \mathbb{Z}^{(2^d-1)}\}$ and the map $h_\infty : \mathbb{Z}^{(2^d-1)} \mapsto M_\infty$ that takes $\mathbf{a}$ to $E_{\mathbf{a}}(z)$ (no mod-ing by z^{2^n}). Clearly M_∞ is also a group, where the operation is multiplication of power series in $\mathbb{Z}_{2^d}[[z]]$.

THEOREM 4 *For each* $n > 0$, *the map* h_n *is a group homomorphism. The map* h_∞ *is also a group homomorphism.*

The fact that h_n is a homomorphism can be used to garner information about certain polynomials. In general the *kernel*, Ker h of a homomorphism h is the set of elements in the domain that are mapped to the identity element in the range. In our case Ker $h_n = \{\mathbf{a} \in \mathbb{Z}_{2^{d+n-1}}^{(2^d-1)} \mid 1 = E_{\mathbf{a}}(z)\}$. Since there are $2^{(2^d-1)(d+n-1)}$ elements in the domain of h_n, the number of distinct polynomials of the form $E_{\mathbf{a}}(z)$ in the range of h_n is

$$\frac{2^{(2^d-1)(d+n-1)}}{|\text{Ker } h_n|}. \tag{8}$$

Note also that $|\text{Ker } h_n|$ is the number of distinct complete factorizations of any polynomial $E_{\mathbf{k}}(z)$ in $\mathbb{Z}_{2^d}[[z]] \bmod z^{2^n}$. The value of $|\text{Ker } h_n|$ is computed for $d = 2, 3$ later in the paper.

Since Ker h_∞ is closed under component-wise addition and scalar multiplication by integers, Ker h_∞ is a $\mathbb{Z}$-module. Similarly, Ker h_n is a $\mathbb{Z}_{2^{d+n-1}}$-module. We will show below that Ker h_∞ has a basis but Ker h_n does not, and determine the rank of Ker h_∞ for $d = 2, 3$ in later sections of the paper.

THEOREM 5 *A profile $\mathbf{k} \in$ Ker h_∞ if and only if $\mathbf{k} \bmod 2^{d+n-1} \in$ Ker h_n for all $n \geq 0$.*

For example, with $d = 2$, the identity $1 = (1+z)^{-2}(1+3z)^2$ holds and thus $\langle -2, 0, 2\rangle \in$ Ker h_∞. Hence, with $n = 3$ we have $\langle 14, 0, 2\rangle \in$ Ker h_3 and so $1 = (1+z)^{14}(1+3z)^2 \bmod z^8$.

We will need a variant of Theorem 5 which says that if $\mathbf{k}$ is in the kernel of h_n and n is large enough, then $\mathbf{k}$, appropriately normalized, is also in the kernel of h_∞. Before stating that result we need to define some notation and prove a small technical lemma. Let $\mathbf{u}_j$ denote the unit profile whose i-th entry is equal to $[\![i = j]\!]$. For $0 \leq s \leq d-1$ and $x, y \in \mathbb{Z}_{2^d}$ we define the profile

$$\mathbf{u}(s; x, y) := 2^s \mathbf{u}_x - 2^s \mathbf{u}_{x+y2^{d-s}},$$

and the set of profiles

$$U_s := \{\mathbf{u}(s; x, y) \mid x, y \in \mathbb{Z}_{2^d}\}.$$

By Theorem 1 $U_s \subseteq$ Ker h_∞ for each s. For example, with $d = 3$ we have $\mathbf{u}(2; 1, 3) = \langle 4, 0, 0, 0, 0, 0, -4\rangle \in$ Ker h_∞ since $(1+z)^4 = (1+3z)^4 = (1+5z)^4 = (1+7z)^4$ by Theorem 1.

LEMMA 2 *For all $n, d \geq 1$, if $2^{n-1} \leq k < 2^{d+n-1}$, then $\binom{k}{2^{n-1}} \not\equiv 0 \bmod 2^d$.*

THEOREM 6 *There is a smallest value $N(d)$, dependent only on d, with the following property: If $n \geq N(d)$ and $\mathbf{k} \in$ Ker h_n, then there is a $\mathbf{k}' \equiv \mathbf{k} \bmod 2^{d+n-1}$ such that $\mathbf{k}' \in$ Ker h_∞.*

Proof: (sketch) Assume that $1 = E_{\mathbf{k}}(z) \bmod z^{2^n}$ for some n. The main idea of the proof is to apply an "exponent reduction" of the k_i with $i > 1$ using the sets U_s for $s = d-1, d-2, \ldots, 2, 1$ for the odd i and Lemma 1 for the even i. At the end of the reduction process, we can express $\mathbf{k} = \mathbf{a} + \mathbf{v}$ where $\mathbf{v} \in$ Ker h_∞ is a linear combination of the $\mathbf{u}(s; x, y)$ and the $\mathbf{u}_i$. In addition $\sum_{i=2}^{2^d-1} a_i \leq D_d$, where

$$D_d := (2^d + 2^{d-1} - 2d - 1) + (d-1) = 2^d + 2^{d-1} - d - 2.$$

We can thus write

$$(1+z)^{a_1 \bmod 2^{d+n-1}} = P(z) + O(z^{2^n}) \tag{9}$$

where $P(z)$ is a polynomial of degree at most D_d.

Below is a table of the values of D_d. Note that $1 + \lceil \lg(D_d+1) \rceil = d + 2$ for $d \geq 4$.

d	2	3	4	5	6	7	8	9	10	11	12
D_d	2	7	18	41	88	183	374	757	1524	3059	6130
$1 + \lceil \lg(D_d{+}1) \rceil$	3	4	6	7	8	9	10	11	12	13	14

We now want to show that $(a_1 \bmod 2^{d+n-1}) \leq 2^n$ for large enough n. It then follows that $(1+z)^a = P(z)$ where $a = a_1 \bmod 2^{d+n-1}$, which will prove the theorem. Let n be such that $\deg(P(z)) \leq D_d < 2^{n-1}$. By Lemma 2, $[z^{2^{n-1}}](1+z)^a \neq 0$ for any a in the range $2^{n-1} \leq a < 2^{d+n-1}$. Thus $a < 2^{n-1}$ and so

$$(1+z)^a = P(z) \text{ in } \mathbb{Z}_d[[z]].$$

Taking $n = 1 + \lceil \lg(D_d{+}1) \rceil$ the theorem is proven, $1 + \lceil \lg(D_d{+}1) \rceil$ is an upper bound on $N(d)$. □

EXAMPLE 3 *We illustrate the proof technique of the preceding theorem. In this example we take $d = 3$ (so arithmetic is mod 8). Consider the profile $\mathbf{k} = \langle 63, 67, 3, 1, 61, 5, 65 \rangle$. A Maple calculation reveals that*

$$(1{+}z)^{63}(1{+}2z)^{67}(1{+}3z)^{3}(1{+}4z)^{1}(1{+}5z)^{61}(1{+}6z)^{5}(1{+}7z)^{65} = 1 + O(z^{16})$$

Thus we want $n = 4$, and so $d + n - 1 = 6$. The even indexed factors give

$$(1+2z)^{67}(1+4z)^{1}(1+6z)^{5} = (1+2z)^{3}(1+4z)^{1}(1+6z)^{1} = 1.$$

We can write the linear combination

$$\begin{aligned} \mathbf{k} &= 16 \cdot \langle 4,0,0,0,0,0,-4 \rangle + 30 \cdot \langle 2,0,0,0,-2,0,0 \rangle + \langle 187,3,3,1,1,1,1 \rangle \\ &= 16 \cdot \mathbf{u}(2;1,3) + 30 \cdot \mathbf{u}(1;1,1) + 4 \cdot \mathbf{u}_6 + \langle 187,3,3,1,1,1,1 \rangle \end{aligned}$$

Thus

$$(1+z)^{-187} = (1+3z)^{3}(1+5z)^{1}(1+7z)^{1} \bmod z^{16},$$

from which it follows that $(1+z)^{-5}(1+3z)^3(1+5z)(1+7z) = 1$ and so $\langle -5,3,3,1,1,1,1 \rangle \in$ Ker h_∞ and $\mathbf{k}' = \langle -129, 3, 3, 1, 61, 5, 65 \rangle \in$ Ker h_∞, where $\mathbf{k}' \equiv \mathbf{k} \bmod 2^{d+n-1}$.

3.2 An even-odd decomposition of the kernel

Define

$$E_n := \{(k_2, k_4, \ldots, k_{2^d-2}) \mid 1 = \prod_{j=1}^{2^d-1} (1+jz)^{k_j [\![j \text{ even}]\!]} \text{ in } \mathbb{Z}_{2^d}[[z]] \bmod z^{2^n}\},$$

$$O_n := \{(k_1, k_3, \ldots, k_{2^d-1}) \mid 1 = \prod_{j=1}^{2^d-1} (1+jz)^{k_j [\![j \text{ odd}]\!]} \text{ in } \mathbb{Z}_{2^d}[[z]] \bmod z^{2^n}\}.$$

The sets E_∞ and O_∞ are defined analogously by removing the $\bmod z^{2^n}$.

THEOREM 7 *The kernels can be decomposed into the following cartesian products*

$$\textit{Ker } h_\infty = E_\infty \times O_\infty, \text{ and}$$

$$\textit{Ker } h_n = E_n \times O_n, \text{ if } n \geq N(d),$$

subject to a shuffling of the indices.

Proof: (Sketch.) We first treat h_∞. By Lemma 1 we may assume that all the even indexed profile numbers k_{2i} are non-negative. Re-arranging the equation $E_{\mathbf{k}}(z) = 1$, we have the following equality of *polynomials*

$$\prod_{j=1}^{2^d-1} (1+jz)^{k_j [\![j \text{ even}]\!]} \prod_{j=1}^{2^d-1} (1+jz)^{k_j [\![k_j>0]\!][\![j \text{ odd}]\!]} = \prod_{j=1}^{2^d-1} (1+jz)^{-k_j [\![k_j<0]\!][\![j \text{ odd}]\!]}.$$

The leading coefficient, $\prod_{j \text{ odd}} j^{-k_j}$, of the polynomial on the right must be odd. The leading coefficient of the polynomial on the left will be even unless $1 = \prod_{j=1}^{2^d-1}(1+jz)^{k_j[\![j \text{ even}]\!]}$. Thus $(k_2, k_4, \ldots, k_{2^d-2}) \in E_\infty$ and hence $(k_1, k_3, \ldots, k_{2^d-1}) \in O_\infty$.

If $\mathbf{k} \in$ Ker h_n, then by Theorem 6 there is a $\mathbf{k}' \in$ Ker h_∞ such that $\mathbf{k}' \equiv \mathbf{k} \bmod 2^{d+n-1}$. By our previous discussion $\mathbf{k}' = \mathbf{e}' \times \mathbf{o}'$ where $\mathbf{e}' \in E_\infty$ and $\mathbf{o}' \in O_\infty$. By Theorem 5, it follows that $\mathbf{e} \in E_n$ and $\mathbf{o} \in O_n$, where $\mathbf{e}$ and $\mathbf{o}$ are defined as expected.

The h_n case follows from Theorem 6. □

LEMMA 3 *The following two conditions are necessary for membership in the respective kernels.*

- *If $\mathbf{k} \in$ Ker h_∞, then $\sum_{j=1}^{2^d-1} k_j [\![j \textit{ odd}]\!] = 0$. This is an integer sum.*
- *If $\mathbf{k} \in$ Ker h_n and $n \geq N(d)$, then $\sum_{j=1}^{2^d-1} k_j [\![j \textit{ odd}]\!] = 0$ mod 2^{d+n-1}.*

COROLLARY 2 *The $\mathbb{Z}$-module Ker h_∞ has a basis.*

Proof: (Sketch.) Show that Ker h_∞ is finitely-generated and torsion-free. Any finitely-generated torsion-free module has a basis. □

The rank of Ker h_∞ is at most $2^d - 1$ since it is a sub-module of $\mathbb{Z}^{(2^d-1)}$. After proving the following technical lemma, we will establish a useful necessary condition for membership in Ker h.

LEMMA 4 *For all $j \in \mathbb{Z}_{2^d}$, where $d \geq 4$,*

$$j^{2^{d-2}} \equiv [\![j odd]\!] \pmod{2^d}$$

If $d = 2$ exceptions occur for $j = 2, 3$, since $2^{2^0} \equiv 2$ and $3^{2^0} \equiv 3$ mod 4. If $d = 3$ exceptions occur for $j = 2, 6$, since $2^{2^1} \equiv 6^{2^1} \equiv 4 \bmod 8$.

LEMMA 5 *The logarithmic derivative of $E_{\mathbf{k}}(z)$ can be written as*

$$\frac{d}{dz} \log E_{\mathbf{k}}(z) = \sum_{k=0}^{d-2} (-z)^k \sum_{j=1}^{2^d-1} k_j j^{k+1} [\![j \textit{ even}]\!] + \sum_{k \geq 0} (-z)^k \sum_{j=1}^{2^d-1} k_j j^{(k+1) \bmod P} [\![j \textit{ odd}]\!],$$

where $P = 2^{d-2}$ if $d \geq 3$ and $P = 2$ if $d = 2$.

Proof: (Sketch.) Expand. The left part of the sum is a polynomial since if j is even and $k + 1 \geq d$, then $j^{k+1} = 0 \bmod 2^d$. The right part of the sum has periodic coefficients by Lemma 4. □

LEMMA 6 *The conditions listed below are necessary for a profile* $\mathbf{k}$ *to be in Ker* h_∞ *or in Ker* h_n *if* $n \geq N(d)$.

$$0 = \sum_{j=1}^{2^d-1} k_j j^{k+1} [\![j \text{ even}]\!] \bmod 2^d, \text{ for } k = 0, 1, \ldots, d-2 \tag{10}$$

$$0 = \sum_{j=1}^{2^d-1} k_j j^{k+1} [\![j \text{ odd}]\!] \bmod 2^d \text{ for } k = 0, 1, \ldots, P-1, \tag{11}$$

where $P = 2^{d-2}$ *if* $d \geq 3$ *and* $P = 2$ *if* $d = 2$.

Proof: Omitted. □

The $k = d-2$ condition in (10) is implied by the $k = d-3$ condition. In a similar vein, when $k = 2^{d-2} - 1$ condition (11) becomes $0 = \sum_{j=1}^{2^d-1} k_j [\![j \text{ odd}]\!]$.

To finish this section we will determine the cardinality of Ker h_1. In the case where $n = 1$ the condition $0 = [z]E_{\mathbf{k}}(z) = \sum_j jk_j$ is both necessary and sufficient since $\bmod 2^{d+n-1} = 2^d$. Since we can solve for k_1 for any values of $k_2, k_3, \ldots, k_{2^d-1}$,

$$|\text{Ker } h_1| = 2^{d(2^d-2)}. \tag{12}$$

4 The kernel for small values of d

In this section we determine the kernels of h_∞ and h_n for $d = 2$ and $d = 3$.

4.1 The kernel when $d = 2$

THEOREM 8 *Ker* $h_\infty = \{\mathbf{k} \mid k_1 \equiv k_2 \equiv k_3 \equiv 0 \bmod 2$ *and* $k_1 + k_3 = 0\}$.

COROLLARY 3 *For the* $\mathbb{Z}$*-module Ker* h_∞, $\{\langle -2, 0, 2\rangle, \langle 0, 2, 0\rangle\}$ *is a basis.*

THEOREM 9 *If* $n = 1$, *then*

$$\begin{aligned} \text{Ker } h_1 \quad = \quad & \{\langle 0,0,0\rangle, \langle 0,2,0\rangle, \langle 2,0,2\rangle, \langle 2,2,2\rangle, \langle 1,1,3\rangle, \langle 3,1,1\rangle, \langle 1,3,3\rangle, \langle 3,3,1\rangle, \\ & \langle 0,0,2\rangle, \langle 0,2,2\rangle, \langle 2,0,0\rangle, \langle 2,2,0\rangle, \langle 1,0,1\rangle, \langle 3,0,3\rangle, \langle 1,2,1\rangle, \langle 3,2,3\rangle\}. \end{aligned}$$

If $n > 1$, *then*

$$\text{Ker } h_n = \{\mathbf{a} \mid a_1 = a_2 = a_3 = 0 \bmod 2 \text{ and } a_1 + a_3 = 0 \bmod 2^{n+1}\}$$

Proof: An exhaustive computation can be used to verify the result for $n = 1$ and $n = 2$. Assume that $n > 2$. The result follows from applying Theorem 6 to the kernel of h_∞ as expressed in Theorem 8. Theorem 6 can be used for any $n \geq N(2) = 3$. □

LEMMA 7

$$|Ker\ h_n| = \begin{cases} 16 & \text{if } n = 1 \\ 2^{2n} & \text{if } n > 1 \end{cases}$$

Proof: The $n = 1$ result is clear from the previous theorem. Use Theorem 9. Mod 2^{n+1} the value of k_3 is determined by the value of k_1. There are 2^n even elements in $\mathbb{Z}_{2^{n+1}}$. Thus there are 2^n choices for k_1 and 2^n choices for k_2, for a total of 2^{2n} choices. □

Since there are 2^{2n} elements in the kernel of h_n, by the properties of homomorphisms, the number of distinct polynomials in the range of h_n is $2^{3n+3}/2^{2n} = 2^{n+3}$ if $n > 1$. Another consequence is that the number of distinct factorizations of $E_{\mathbf{k}}(z) \bmod z^{2^n}$ in $\mathbb{Z}_4[z]$ is 2^{2n} if $n > 1$.

4.2 The kernel when $d = 3$

The necessary conditions from Lemma 6 imply the following for the even indexed profile numbers:

$$k_2 + 2k_4 + 3k_6 \equiv 0 \bmod 4. \tag{13}$$

For the odd indexed profile numbers we have

$$\begin{aligned} k_1 + k_3 + k_5 + k_7 &= 0 \\ k_1 + 3k_3 + 5k_5 + 7k_7 &\equiv 0 \bmod 8 \\ k_1 + k_3 + k_5 + k_7 &\equiv 0 \bmod 8 \end{aligned}$$

These conditions are not sufficient, but the changes required to make them sufficient are small.

THEOREM 10 *The set E_∞, is a $\mathbb{Z}$-module with basis $B = \{(4,0,0),(2,0,2),(3,1,1)\}$.*

Proof: By Lemma 1, we have with arithmetic mod 8, $(1+2z)^k = (1+2z)^{k \bmod 4}$, $(1+6z)^k = (1+6z)^{k \bmod 4}$, and $(1+4z)^k = (1+4z)^{k \bmod 2}$.

The profiles that satisfy the necessary condition (13) can therefore be classified as $(k_2 \bmod 4, k_4 \bmod 2, k_6 \bmod 4)$, where an exhaustive listing gives

$$\{(0,0,0),(2,0,2),(1,1,3),(3,1,1)\} \cup \{(1,0,1),(3,0,3),(0,1,2),(2,1,0)\}.$$

A routine calculation shows that the left set is in the kernel, but the right set is not. To show that B is a basis, we first note that it is linearly independent, since the system of equations (14) has only the solution $n_1 = n_2 = n_3 = 0$.

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} n_1 \\ n_2 \\ n_3 \end{bmatrix} \tag{14}$$

To show that B spans E_∞ note that $(0,2,0) = 2\cdot(3,1,1) - (4,0,0) - (2,0,2)$, $(0,0,4) = 2\cdot(2,0,2) - (4,0,0)$, and $(1,1,3) = (3,1,1) + (2,0,2) - (4,0,0)$. □

COROLLARY 4 *A profile $\mathbf{k} = \langle k_2, k_4, k_6 \rangle$ is in E_∞ if and only if $k_2 \equiv k_4 \equiv k_6 \bmod 2$ and $k_2 + 2k_4 + 3k_6 \equiv 0 \bmod 4$.*

We now turn our attention to the odd indexed profile numbers.

THEOREM 11 *The set* O_∞ *is a* $\mathbb{Z}$*-module with basis* $B = \{(1,1,-1,-1), (-1,1,1,-1), (4,-4,0,0)\}$.

By Theorems 10 and 11, the rank of Ker h_∞ is 6.

LEMMA 8 *The value of* $|E_n| \cdot |O_n|$ *over* $\mathbb{Z}_8$ *is*

$$2^{3n+3} \cdot \begin{cases} 512 & \text{if } n = 1, \\ 1024 & \text{if } n = 2, \\ 2^{3n+3} & \text{if } n \geq 3. \end{cases}$$

Proof: The number of kernel elements in E_n is 2^{3n+3}.

In the case where operations are done mod $2^{d+n-1} = 2^{n+2}$, a certain linear system, used in the proof of the previous theorem, has 8 distinct solutions, namely

$$n_1 = n_2 \in \{0, 2^{n+1}\} \text{ and } n_3 \in \{0, 2^n, 2^{n+1}, 3 \cdot 2^n\}.$$

Note that these solutions are the submodule with basis $\{\langle 2^{n+1}, 2^{n+1}, 0\rangle, \langle 0, 0, 2^n\rangle\}$. The number of kernel elements in O_n is therefore $2^{3(n+2)}/8 = 2^{3n+3}$, since there are three basis elements and any kernel element can be written in exactly 8 distinct ways as linear combination of basis elements, where the coefficients of the combination come from $\mathbb{Z}_{2^{d+n-1}} = \mathbb{Z}_{2^{n+2}}$. □

LEMMA 9 *The value of* $|$*Ker* $h_n|$ *over* $\mathbb{Z}_8$ *is*

$$\begin{cases} 2^{18} = 262144 & \text{if } n = 1, \\ 2^{19} = 524288 & \text{if } n = 2, \\ 2^{22} = 4194304 & \text{if } n = 3, \\ 2^{6n+6} & \text{if } n \geq 4. \end{cases}$$

Proof: The value for $|$Ker $h_1|$ is from (12). The value for $|$Ker $h_2|$ and $|$Ker $h_3|$ is from an exhaustive computer listing [5]. Since $N(3) \leq 4$, the value for $n \geq 4$ follows from Lemma 8. Note that $N(3) = 4$ since $22 \neq 24 = 6 \cdot 3 + 6$. □

4.3 The range of the kernel when $d = 2$

In this subsection all computation is done mod 4. We will show that the indices of certain "critical" elementary symmetric functions determine the remaining elementary symmetric function values. These critical indices occur at the powers of two. We can use this information to get fast algorithms for converting between a profile and elementary symmetric function evaluations.

LEMMA 10 *Let* $k' = 2^n + k$. *Then*

$$[z^{2^{n-1}}]E_{k',x,y}(z) = 2 + [z^{2^{n-1}}]E_{k,x,y}(z).$$

It is easy to see, for example, by an exhaustive listing, that there is a bijection between profiles in $\mathbb{Z}_{16} \times \mathbb{Z}_2^{(2)}$ and triples $(e_1, e_2, e_4) \in \mathbb{Z}_4^{(3)}$.

EXAMPLE 4 *This is an explanation of Example 2 from the Introduction. What is the profile, if any, that corresponds to the sequence of six elementary symmetric function values* $e_1, e_2, e_4, e_8, e_{16}, e_{32} = 0, 3, 3, 2, 3, 3$*? Consider first* $e_1, e_2, e_4 = 0, 3, 3$ *which corresponds to profile* $6, 1, 0 \bmod 16$*. Here* $e_8(6, 1, 0) = 0$*, so Lemma 10 tells us to add 16 to* k_1 *to get* $e_8(22, 1, 0) = 2$*, while preserving the values of* e_1, e_2, e_4*. In a similar manner, since* $e_{16}(22, 1, 0) = 1$*, we add 32 to* k_1 *to get* $e_{16}(54, 1, 0) = 3$*. Now* $e_{32}(54, 1, 0) = 3$*, so we are done. Any profile that has* k_1 *and* k_3 *even,* k_2 *odd, and* $k_1 + k_3 \equiv 54$ *mod 64 has the required trace values. Furthermore, these determine all traces* e_j *where* $j = 1, 2, \ldots, 63$ *as per the theorem stated below.*

We can extrapolate this example to an algorithm whose running time is $O(n)$. The running time of this algorithm is clearly $O(n)$ so long as the values of $e_{2^j}(\mathbf{k})$ can be computed in constant time. We show how to do this, essentially by a table lookup, in the full paper.

THEOREM 12 *The values of* e_{2^i} *for* $i = 0, 1, \ldots, n-1$ *determine the values of* e_j *for* $j = 1, 2, \ldots, 2^n - 1$.

Acknowledgements

We thank Herb Wilf and Robert Israel for helpful discussion.

References

[1] H. Cheng and G. Lebahn, *Computing all Factorizations in* $\mathbb{Z}_N[x]$ ISAAC '01, Proceedings of the 2001 international symposium on symbolic and algebraic computation, pages 64–71.

[2] C. Frei and S. Frisch, *Non-unique factorizations of polynomials over residue class rings of the integers*, Communications in Algebra, 39 (2011) 1482–1490.

[3] 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 on Discrete Mathematics, 17 (2004) 675–685.

[4] C.R. Miers and F. Ruskey, *Counting Strings with Given Elementary Symmetric Function Evaluations II: Circular Strings*, SIAM Journal on Discrete Mathematics, 18 (2004) 71–82.

[5] C.R. Miers and F. Ruskey, Tables, `http://www.cs.uvic.ca/~ruskey/Publications/Symmetric/SymmetricZ2d.html`.

[6] R.P. Stanley, *Enumerative Combinatorics, Volume 2*, Cambridge University Press, 1999.