Hokkaido Mathematical Journal Vol. 19 (1990) p. 385-401

On the number of solutions of certain linear diophantine equations

Andreas W. M. DRESS and Christian SIEBENEICHER
(Received December 28, 1988)

Abstract: In this note various old and new combinatorial facts related to the so called *cyclotomic identity* are presented and discussed.

Introduction

Around 1800 C. F. Gauss considered the problem to compute the number $M(q, n)$ of irreducible polynomials of degree n over the finite field $\boldsymbol{F}_q$ with q elements and solved it in the following way (cf. [G]): Combining the two facts that there are precisely q^n polynomials of degree n with leading coefficient 1 and that every such polynomial decomposes uniquely into a product of irreducibles he derived the so called *cyclotomic identity*

$$\frac{1}{1-qt}=\prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{M(q,n)} \tag{1}$$

which in turn allowed him to determine the numbers $M(q, n)$ by considering its logarithmic derivative. Thereby he obtained (in modern notation and with μ denoting the Moebius function)

$$n\cdot M(q, n)=\sum_{d|n}\mu(d)q^{n/d}.$$

In 1872 M. C. Moreau discussed in [M] necklaces with n beads which are coloured with q colours and obtained for the number $M'(q, n)$ of *primitive* or *aperiodic* necklaces the same formula:

$$n\cdot M'(q, n)=\sum_{d|n}\mu(d)q^{n/d}.$$

In a paper of E. Witt from 1937 (cf. [W1]) the same number occurs as the dimension of the submodule of homogeneous elements of degree n in the free Lie algebra with q generators. Witt wondered why his number coincides with the number of irreducible polynomials, determined by Gauss.

Today, there are well understood explanations for these coincidences. Consider for a (finite) set A the set $P(A)$ of periodic functions on the integers $\boldsymbol{Z}$ with values in the set A together with the *shift map*

$$\begin{aligned} \alpha &: P(A) \longrightarrow P(A) \\ g &\mapsto (\alpha g : \boldsymbol{Z} \to A : \alpha g(i) := g(i+1)). \end{aligned} \tag{2}$$

If the set A has q elements, then for each positive integer n the set of elements of $P(A)$, invariant under the iterate α^n of α, contains precisely q^n elements. If q is a prime power, $\hat{\boldsymbol{F}}_q$ denotes the algebraic closure of the field $\boldsymbol{F}_q$, and $\alpha : \hat{\boldsymbol{F}}_q \to \hat{\boldsymbol{F}}_q$ is the Frobenius automorphism $x \mapsto x^q$, then the elements of $\hat{\boldsymbol{F}}_q$, invariant under α^n, are precisely the elements of the extension field $\boldsymbol{F}_{q^n}$ of $\boldsymbol{F}_q$ of degree n and therefore their number equals q^n. An argument of Burnside (cf. [DS2]) then shows that $P(A)$ and $\hat{\boldsymbol{F}}_q$ are isomorphic as *cyclic sets*, i. e. as sets on which the infinite cyclic group $\boldsymbol{Z}$ acts by permutations. In particular, it follows that both sets contain the same number $M(q, n)$ of $\boldsymbol{Z}$-orbits of length n for every positive integer n.

It is clear that an orbit of length n in the cyclic set $\hat{\boldsymbol{F}}_q$ consists of the set of roots of an irreducible polynomial of degree n over $\boldsymbol{F}_q$ and that there are as many such orbits as there are irreducible polynomials.

On the other hand, the orbits of length n in the cyclic set $P(A)$ are precisely the primitive necklaces of length n. Hence the number of irreducible polynomials of degree n coincides with the number of primitive necklaces of length n.

The relation between Witt's number and the number of primitive necklaces becomes apparent if one considers so called Lyndon words over the somehow linearily ordered alphabet A. Lyndon words are the minimal elements in the set of cyclic permutations of primitive words with respect to the lexicographic order on the set of words. Since primitive words correspond in a one to one manner to periodic functions on $\boldsymbol{Z}$ (repeat the primitive word indefinitely to the left and to the right), to each orbit of $P(A)$ there corresponds precisely one Lyndon word, i. e. the number of orbits of length n equals the number of Lyndon words of that length. In [V] and [L] it is shown that the Lyndon words of length n provide a basis of the module of homogeneous elements of degree n in the free Lie algebra generated by A. Hence the dimension of this module equals $M(q, n)$.

Amazingly enough, the identity (1) plays a key rôle in the quite different context of Witt vectors, which have been invented by E. Witt in 1937, too (cf. [W2]). Universal Witt vectors over the ring R are infinite sequences $\boldsymbol{q} = (q_1, q_2, \ldots)$ of elemets of R together with an addition and a multiplication which are defined by universal polynomials. It is well known (cf. [C]) that the map

$$W(R)\to\Lambda(R)$$
$$\boldsymbol{q}=(q_1, q_2, \ldots)\mapsto\prod_{i=1}^{\infty}\frac{1}{1-q_it^i}$$

of the ring of Witt vectors over R onto the set $\Lambda(R)$ of formal power series with constant term 1 and coefficents in R provides an isomorphism from the additive group of $\boldsymbol{W}(R)$ onto the multiplicative group $\Lambda(R)$. It becomes even an isomorphism of rings, if $\Lambda(R)$ is equipped with Grothendieck's multiplication, which is also defined by universal polynomials. Using this isomorphism and (1) one has for the image of $\boldsymbol{q}=(q_1, q_2, \ldots)\in\boldsymbol{W}(\boldsymbol{Z})$ in $\Lambda(\boldsymbol{Z})$ with $M(\boldsymbol{q}, n):=\sum_{d|n}M(q_d, n/d)$ the relation

$$\prod_{i=1}^{\infty}\frac{1}{1-q_it^i}=\prod_{i=1}^{\infty}\prod_{d=1}^{\infty}\left(\frac{1}{1-t^{di}}\right)^{M(q_i,d)}=\prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{M(\boldsymbol{q},n)}$$

and by additivity $M(\boldsymbol{q}+\boldsymbol{q}', n)=M(\boldsymbol{q}, n)$. This relation allows to calculate the components of the Witt vector $\boldsymbol{q}+\boldsymbol{q}'$ recursively:

$$(\boldsymbol{q}+\boldsymbol{q}')_1=M(\boldsymbol{q}+\boldsymbol{q}', 1)=M(\boldsymbol{q}, 1)+M(\boldsymbol{q}', 1)=q_1+q_1'$$
$$\vdots\qquad\qquad\vdots$$
$$(\boldsymbol{q}+\boldsymbol{q}')_n=M(\boldsymbol{q}, n)+M(\boldsymbol{q}', n)-\sum_{d\|n}M((\boldsymbol{q}+\boldsymbol{q}')_d, n/d).$$

Recently there has been interest in a direct combinatorial interpretation of (1): if we denote by $s(P(A))$ the set of all maps $u: P(A)\to\boldsymbol{N}_0$ which have finite support and are shift invariant (i.e. $u(ag)=u(g)$ for all $g\in P(A)$) and if for any such $u\in s(P(A))$ we denote by $|u|\in\boldsymbol{N}_0$ the sum $|u|=\sum_{g\in P(A)}u(g)$, then the more or less obvious identities

$$\begin{aligned}\prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{M(q,n)}&=\prod_{n=1}^{\infty}(1+t^n+t^{2n}+\ldots)^{M(q,n)}\\&=\prod_{<a>g\in<a>\backslash P(A)}(1+t^{\#(<a>g)}+t^{2\cdot\#(<a>g)}+\ldots)\\&=\sum_{u\in s(P(A))}t^{|u|}\\&=\sum_{0}^{\infty}\#\{u\in s(P(A))\,|\,|u|=n\}\cdot t^n\end{aligned}$$

imply that (1) is equivalent with the assertion that the set

$$s^n(P(A)):=\{u\in s(P(A))\,|\sum_{g\in P(A)}u(g)=n\}$$

has the same cardinality as the set A^n. So it seemed natural to ask for a "canonical" bijection between these two sets. In [MR1, MR2]

N. Metropolis and G.-C. Rota raised this problem and established a certain bijection which implies that $\#s^n(P(A))=\#A^n=q^n$.

Their work stimulated further research (cf. [DS2] and [VW]) trying to develop additional insight into the combinatorial structures underlying these relationships. In addition, N. G. de Bruijn and D. A. Klarner established a bijection between $s^n(P(A))$ and A^n already in 1982 (cf [dBK]), using Lyndon words, though without realizing neither the relationship with the use of Lyndon words in the combinatorial theory of words as developed by the french school around Schützenberger (cf. [V] and [L]) nor the relationship with the cyclotomic identity (1).

In this note it is our purpose to show at first that a thorough analysis of the facts mentioned above can be used to establish a certain refinement of the result $\#s^n(P(A))=q^n$, which allows to compute the exact number of solutions of certain linear diophantine equations. Secondly we will use our approach in the last section to analyze the relationship between the various contributions towards a combinatorial interpretation of the cyclotomic identity mentioned above.

Acknowledgment: We are greatful to D. Foata, G.-C. Rota and V. Strehl for several helpful comments concerning this paper.

The main theorem

To state our result on the number of solutions of a certain linear diophantine equation we collect some definitions. Given a set A, we define a map $g: \boldsymbol{Z}\to A$ to be periodic if there exists some positive integer $n \in \boldsymbol{N}:=\{1, 2, 3, ...\}$ with $g(i+n)=g(i)$ for all $i\in\boldsymbol{Z}$. Examples of periodic maps are provided in the following way: If $\sigma: E\to E$ is a permutation of the finite set E, $f: E\to A$ an arbitrary map and ϵ an element of E then the map

$$f_\sigma^\epsilon: \boldsymbol{Z}\to A$$
$$i\mapsto f(\sigma^i\epsilon)$$

is a periodic map. Indeed, any periodic map $g: \boldsymbol{Z}\to A$ can be constructed in this way. Let $P(A)$ denote the set of all periodic maps from $\boldsymbol{Z}$ to A. The *shift map* α (cf. (2)) induces on $P(A)$ an equivalence relation, two periodic functions g and g' being equivalent if and only if g and g' are in the same α-orbit, i. e. $\alpha^k g=g'$ for some $k\in N$. Note that, with the above notations, the equivalence class $\overline{f_\sigma^\epsilon}$ of f_σ^ϵ consists of all $f_\sigma^{\sigma^i\epsilon}(i\in\boldsymbol{Z})$. Let $\overline{P(A)}$ denote the set of equivalence classes of $P(A)$ with respect to this equivalence relation — i. e. the set of α-orbits of $P(A)$. Obviously, each equivalence class in $\overline{P(A)}$ is finite. Hence, for any $T\in\overline{P(A)}$ the num-

bers

$$\Delta(a, T) := \#\{g \in T \mid g(0) = a\} \quad (a \in A)$$

are necessarily finite, too. With these definitions one has

THEOREM 1. *If A is a finite set and $s : A \to \boldsymbol{N}_0 := \boldsymbol{N} \cup \{0\}$ an arbitrary map, then the set*

$$U(s) := \{u \in \boldsymbol{N}_0^{\overline{P(A)}} \mid \sum_{T \in \overline{P(A)}} \Delta(a, T) \cdot u(T) = s(a) \text{ for all } a \in A\}$$

of non negative integral solutions of the linear equation $\Delta \cdot u = s$ has cardinality

$$((s)) := \frac{\left(\sum_{a \in A} s(a)\right)!}{\prod_{a \in A} s(a)!}.$$

From Theorem 1 one may derive immediately the following corollary which provides the possibility of a recursive calculation of the numbers

$$\chi(s) := \#\{T \in \overline{P(A)} \mid \Delta(\cdot, T) = s\}$$

COROLLARY 1.

$$((s)) = \sum_{k=1}^{|s|} \sum_{\substack{s_1, \cdots, s_k \\ n_1, \cdots, n_k}} \prod_{i=1}^{k} \binom{\chi(s_i) + n_i - 1}{n_i}$$

$$= \chi(s) + \sum_{k=2}^{|s|} \sum_{\substack{s_1, \cdots, s_k \\ n_1, \cdots, n_k}} \prod_{i=1}^{k} \binom{\chi(s_i) + n_i - 1}{n_i}$$

where for all $k \in \boldsymbol{N}$ the sum is taken over all subsets $\{s_1, \ldots, s_k\} \subset \boldsymbol{N}_0^A$ of cardinality k and all $n_1, \ldots, n_k \in \boldsymbol{N}$ for which $s = n_1 s_1 + \ldots + n_k s_k$.

Before proving Theorem 1 let us illustrate its content by discussing a particular example. Take $A = \{0, 1\}$ and the functions $s_{2,2}$, $s_{3,1}$ and $s_{3,2}$, where $s_{a,b}$ denotes that function from A to $\boldsymbol{N}_0$ which takes the walue a on the element 0 of A and the value b on 1. Note first that for $u \in U(s)$ one has necessarily

$$|u| := \sum_{T \in \overline{P(A)}} u(T) \cdot \#T = \sum_{T \in \overline{P(A)},\, a \in A} u(T) \cdot \Delta(T, a)$$

$$= \sum_{a \in A} s(a) =: |s|, \tag{3}$$

in particular $u(T) \neq 0$ only if $\#T \leq |s|$. Let us denote by $\epsilon_1 \epsilon_2 \ldots \epsilon_n$ the function $\boldsymbol{Z} \longrightarrow A$ mapping i to $\epsilon_{i \bmod n}$ and by $\overline{\epsilon_1 \epsilon_2 \ldots \epsilon_n}$ its equivalence class.

By inspection of the following scheme, in which the front part dis-

plays that part of the matrix Δ which results from the elements $T \in \overline{P(A)}$ with $\#T \leq \max(|s_{2,2}|, |s_{3,1}|, |s_{3,2}|) = 5$, we see immediately that the subsequent columns — in which only the nonzero entries have been displayed — provide the non negative integral solutions u of the system $\Delta \cdot u = s$ of linear equations.

	Δ		$U(s_{3,2})$		
	0 1	$U(s_{2,2})$	$U_0(s_{3,2})$	$U(s_{3,2}) \setminus U_0(s_{3,2})$	U($s_{3,1}$)
$\bar{1}$	0 1	2 1 1	2 1 1	1	1
$\bar{0}$	1 0	2 1 1	3 2 1 2 1 1		3 1 1
$\overline{10}$	1 1	1 2	1 2	1	1
$\overline{110}$	1 2	1	1		
$\overline{100}$	2 1	1	1	1	1
$\overline{1110}$	1 3				
$\overline{1100}$	2 2	1	1		
$\overline{1000}$	3 1			1	1
$\overline{11110}$	1 4				
$\overline{11100}$	2 3				
$\overline{11010}$	2 3				
$\overline{11000}$	3 2			1	
$\overline{101000}$	3 2			1	

Counting the respective numbers of solutions shows that in these cases the theorem provides the correct numbers.

Consider now more generally for an arbitrary function $s = s_{a,b}$ together with the set $U(s)$ the sets

$$U_0(s) = \{u \in U(s) | u(\bar{0}) > 0\}$$

and

$$U_1(s) = \{u \in U(s) | u(\bar{1}) > 0\}.$$

It is clear that for every element $u \in U_0(s)$ (resp. $u \in U_1(s)$) the corresponding element $u_0 \in \boldsymbol{N}_0^{\overline{P(A)}}$ (resp. $u_1 \in \boldsymbol{N}_0^{\overline{P(A)}}$) defined by

$$u_0(\overline{\epsilon_1 \epsilon_2 \ldots \epsilon_n}) = \begin{cases} u(\bar{0}) - 1 & \text{if} \quad \overline{\epsilon_1 \epsilon_2 \ldots \epsilon_n} = \bar{0} \\ u(\overline{\epsilon_1 \epsilon_2 \ldots \epsilon_n}) & \text{otherwise} \end{cases}$$

respectively by

$$u_1(\overline{\epsilon_1\epsilon_2\ldots\epsilon_n})=\begin{cases}u(\bar{1})-1 & \text{if} \quad \overline{\epsilon_1\epsilon_2\ldots\epsilon_n}=\bar{1}\\ u(\overline{\epsilon_1\epsilon_2\ldots\epsilon_n}) & \text{otherwise}\end{cases}$$

is contained in $U(s_{a-1,b})$(resp. $U(s_{a,b-1})$) and that the mapping $u\mapsto u_0$ (resp. $u\mapsto u_1$) provides a bijection from $U_0(s_{a,b})$ to $U(s_{a-1,b})$(resp. from $U_1(s_{a,b})$ to $U(s_{a,b-1})$). Hence

$$\#U(s_{a,b})=\binom{a+b}{a}$$
$$\#U_0(s_{a,b})=\binom{a+b-1}{a-1}$$
$$\#U_1(s_{a,b})=\binom{a+b-1}{b-1}$$

by Theorem 1. Using the recursion formula for the binomial coefficients (Pascal's triangle) it follows that

$$\begin{aligned}\#\{u\in U(s_{a,b})\mid u(\bar{0})=0\}&=\binom{a+b}{a}-\binom{a+b-1}{a-1}\\&=\binom{a+b-1}{a}\\&=\#U(s_{a,b-1})\end{aligned}$$

as well as

$$\begin{aligned}\#\{u\in U(s_{a,b})\mid u(\bar{0})=u(\bar{1})=0\}&=\binom{a+b-2}{a-1}\\&=\#U(s_{a-1,b-1})\end{aligned}$$

in case $a\cdot b>0$. But inspection of the above examples for $s=s_{3,2}$ does not supply in an obvious fashion a $1-1$ correspondence between

$$U(s_{3,2})\setminus U_0(s_{3,2}) \text{ and } U(s_{3,1})$$

or between

$$U(s_{3,2})\setminus(U_0(s_{3,2})\cup U_1(s_{3,2})) \text{ and } U(s_{(2,1)}).$$

Hence it is probably a bit complicated to prove the above theorem by simple recursion.

The key lemma

Instead for any $u\in N_0^{\overline{P(A)}}$ we will consider

- the set

$$[u] := \{(g, \gamma) | g \in P(A) \text{ and } 1 \leq \gamma \leq u(\bar{g})\},$$

where $\bar{g} \in \overline{P(A)}$ denotes the equivalence class of $g \in P(A)$ (note that $\#[u] = \sum_{T \in \overline{P(A)}} u(T) \cdot \#T = |u|$)

- the evaluation map

$$ev_u : [u] \longrightarrow A$$

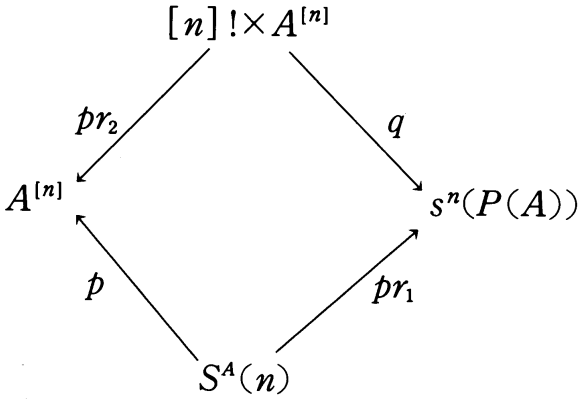
which associates to an element $(g, \gamma) \in [u]$ the value $g(0)$ (note that $\#ev_u^{-1}(a) = \sum_{T \in \overline{P(A)}} \Delta(a, T) \cdot u(T)$)

- the sets:
  - $s^n(P(A)) := \{u : \overline{P(A)} \longrightarrow \boldsymbol{N}_0 | \, |u| = n\}$

and

- $S^A(n) := \{(u, \Phi) | u \in s^n(P(A)), \ \Phi : [n] \longrightarrow [u] \text{ bijective}\}$ where $[n] := \{1, 2, \ldots, n\}$

- and the diagram



in which

- $[n]!$ denotes the group of all permutations of the set $[n]$
- the maps pr_1 and pr_2 are the canonical projection maps onto the first resp. the second factor
- the maps p and q are defined as follows:
  - $p : S^A(n) \longrightarrow A^{[n]} : (u, \Phi) \mapsto ev_u \circ \Phi$
  - $q : [n]! \times A^{[n]} \longrightarrow s^n(P(A)) : (\sigma, f) \mapsto u_{\sigma, f}$ where

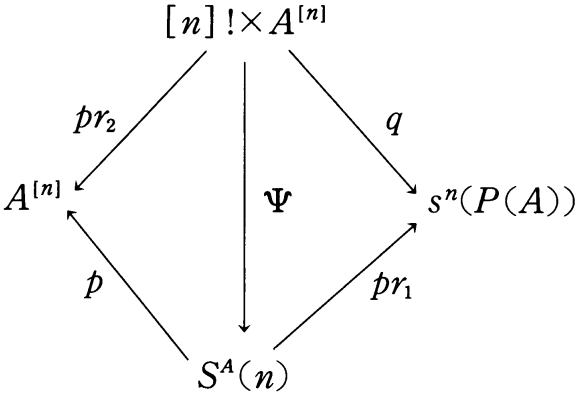
$$u_{\sigma, f} : \overline{P(A)} \longrightarrow N_0$$

is defined by choosing for any $T \in \overline{P(A)}$ some $g \in T$ and associating to T the number $\#\{\nu \in [n] | f_\sigma^\nu = g\}$ which is in

dependent of the choice of g.
(Note, that $[n]!\times A^{[n]}$ is, in terms of [MR2], the set of *placements of necklaces* with *colours* in A and *places* in $[n]$.)

Obviously, the fibres of the projection maps pr_1 and pr_2 have cardinality $n!$. Moreover, we know (but will not need) from [DS2] that all fibres of q have also cardinality $n!$. In addition, for any $f\in A^{[n]}$ consider the mapping $s_f : A\longrightarrow N_0$ which maps an element a in A to $\#f^{-1}(a)$. Obviously $|s_f|=\sum_{a\in A} s_f(a)=n$. Hence $U(s_f)\subset s^n(P(A))$ by (3). More precisely, if $u\in s^n(P(A))$, then $u\in U(s_f)$ if and only if there exists some bijection $\Phi : [n]\longrightarrow[u]$ with $f=ev_u\circ\Phi$ in which case there exist precisely $\prod_{a\in A} s_f(a)!$ such Φ. Hence the theorem will follow once we know that any fibre of p has cardinality $n!$. This in turn follows from the above analysis of the diagram in conjunction with the following

LEMMA 1. *There exists a bijection* $\Psi : [n]!\times A^{[n]}\longrightarrow S^A(n)$ *which one may insert into the above diagram to obtain the following commutative diagram* :



PROOF: We have to define a bijection Ψ such that $p\circ\Psi=pr_2$ and $pr_1\circ\Psi=q$. To this end consider for an element (σ,f) in $[n]!\times A^{[n]}$ the map

$$\gamma_{\sigma,f} : [n]\longrightarrow N_0$$
$$\nu\mapsto\gamma_{\sigma,f}(\nu) :=\#\{\mu\in[n] \mid \mu\leq\nu \text{ and } f_\sigma^\mu=f_\sigma^\nu\}.$$

Note that

$$\gamma_{\sigma,f}(\nu)\leq u_{\sigma,f}(\overline{f_\sigma^\nu})=\#\{\mu\in[n] \mid f_\sigma^\mu=f_\sigma^\nu\}.$$

With this definition in mind we may associate to the element (σ,f) in $[n]!\times A^{[n]}$ the map

$$\Phi_{\sigma,f} : [n] \longrightarrow [u_{\sigma,f}]$$
$$\nu \mapsto (f_\sigma^\nu, \gamma_{\sigma,f}(\sigma\nu)).$$

This map is well defined in view of $\overline{f_\sigma^{\sigma\nu}} = \overline{f_\sigma^\nu}$ and therefore

$$\gamma_{\sigma,f}(\sigma\nu) \leq u_{\sigma,f}(\overline{f_\sigma^{\sigma\nu}}) = u_{\sigma,f}(\overline{f_\sigma^\nu})$$

and is easily seen to be a bijection. Define

$$\Psi : [n]\,! \times A^{[n]} \longrightarrow S^A(n)$$

by

$$(\sigma, f) \mapsto (u_{\sigma,f}, \Phi_{\sigma,f}).$$

With these definitions one has indeed

$$pr_1 \circ \Psi(\sigma, f) = u_{\sigma,f} = q(\sigma, f)$$

and for any $\nu \in [n]$ one has

$$\begin{aligned} p \circ \Psi(\sigma, f)(\nu) &= ev_{u_{\sigma,f}}(\Phi_{\sigma,f}(\nu)) = ev_{u_{\sigma,f}}(f_\sigma^\nu, \ldots) \\ &= f_\sigma^\nu(0) = f(\sigma^0\nu) \\ &= f(\nu), \end{aligned}$$

i. e. $p \circ \Psi = pr_2$, showing that the map Ψ renders the diagram commutative.

Next we show that Ψ is injective. It is clear that for given $(\sigma, f) \in [n]\,! \times A^{[n]}$ one can reconstruct f from $\Psi(\sigma, f)$ in view of $pr_2 = p \circ \Psi$, i. e. $f = p \circ \Psi(\sigma, f)$. Now put $u := u_{\sigma,f}$ and $\Phi := \Phi_{\sigma,f}$ so that $\Psi(\sigma, f) = (u, \Phi)$ and for $\nu \in [n]$ put $\Phi(\nu) := (g_\nu, \gamma_\nu)$.

To reconstruct σ from u and Φ note that for $\nu \in [n]$ one has

$$\sigma\nu \in \{\mu \in [n] \mid g_\mu(i) = \alpha g_\nu(i) = g_\nu(i+1) \text{ for all } i \in \boldsymbol{Z}\}$$

since

$$(g_{\sigma\nu}, \gamma_{\sigma\nu}) = \Phi_{\sigma,f}(\sigma\nu) = (f_\sigma^{\sigma\nu}, \gamma_{\sigma,f}(\sigma(\sigma\nu)))$$

and therefore

$$\begin{aligned} g_{\sigma\nu}(i) = f_\sigma^{\sigma\nu}(i) &= f(\sigma^i(\sigma\nu)) = f(\sigma^{i+1}\nu) = f_\sigma^\nu(i+1) \\ &= g_\nu(i+1) = \alpha g_\nu(i). \end{aligned}$$

Hence if

$$\{\mu \in [n] \mid g_\mu = \alpha g_\nu\} = \{\mu_1, \mu_2, \ldots, \mu_k\}$$

with $k := u(\bar{g}_\nu)$ and $\mu_1 < \mu_2 < \ldots < \mu_k$, then $\sigma\nu = \mu_{\gamma_\nu}$ by the definition of the map $\gamma_{\sigma,f} \circ \sigma$, used in the definition of the map Ψ. Hence the value of the

permutation σ on an element $\nu\in[n]$ is uniquely determined by the element $\Phi(\nu)=(g_\nu, \gamma_\nu)$ in $[n]$. This proves the injectivity of the map Ψ and also indicates how to prove its surjectivity. □

From our basic observation that Ψ is a bijection one can deduce as well as an immediate corollary that for any given $f:[n]\longrightarrow A$ and $u\in U(s_f)$ the set $\sum(u, f)$ of all permutations $\sigma\in[n]!$ with $u=u_{\sigma,f}$ has cardinality $\prod_{a\in A} s_f(a)!$:

$$\#\sum(u, f)=\prod_{a\in A} s_f(a)!. \tag{4}$$

Obviously, this result in turn is strong enough to yield the above theorem as one of its immediate consequences. Hence the following direct characterization of $\sum(u, f)$ might be of some interest in our context as well:

LEMMA 2. *For any $f\in A^{[n]}$, $u\in U(s_f)$ and $\sigma\in[n]!$ one has $u=u_{\sigma,f}$ if and only if for any $g\in T\in\overline{P(A)}$ there exists a subset $K(g)\subset[n]$ of cardinality $u(T)$, uniquely determined by g and σ, such that*

$$K(g)\subset f^{-1}(g(0))$$

and

$$\sigma K(g)=K(ag),$$

where ag is the shift of g.

The proof of Lemma 2 whose details are left to the reader is based on the fact that for $\sigma\in\sum(u, f)$ and $g\in T\in\overline{P(A)}$ the set $K(g)$ coincides with the set of all $\nu\in[n]$ for which $f_\sigma^\nu=g$.

Obviously, Lemma 2 implies (4) (and, therefore, it provides a slightly different proof of the above Theorem as well), since it allows to construct $\sum(u, f)$ as follows: for any $a\in A$ and any $g\in T\in\overline{P(A)}$ with $g(0)=a$ choose a subset $K(g)\subset f^{-1}(g(0))$ of cardinality $u(T)$ such that all these subsets are disjoint. For any $a\in A$ this can be done in

$$\frac{s_f(a)!}{\prod_{\substack{g\in P(A)\\ g(0)=a}} u(\bar{g})!}$$

different ways. Next, for any $a\in A$ and $g\in T\in\overline{P(A)}$ as above choose a bijection $\sigma_g: K(g)\longrightarrow K(ag)$ which can be done in $u(T)!$ different ways. Finally define σ as the union of the σ_g:

$$\coprod_g \sigma_g : [n]=\coprod_g K(g)\longrightarrow \coprod_g K(ag)=[n]$$

Hence indeed

$$\#\Sigma(u,f)=\prod_{a\in A}\frac{s_f(a)!}{\prod\limits_{\substack{g\in P(A)\\ g(0)=a}}u(\bar{g})!}\cdot\prod_{a\in A}\Big(\prod_{\substack{g\in P(A)\\ g(0)=a}}u(\bar{g})!\Big)=\prod_{a\in A}s_f(a)!.$$

We can draw some additional consequences from this analysis. To this end let us define a pair $(\sigma,f)\in[n]!\times A^{[n]}$ to be *trimmed* if for $i,\ j\in[n]$ with $i<j$ and $f_\sigma^i=f_\sigma^j$ one has $\sigma i<\sigma j$, that is, if σ is monotonically increasing on the fibres $K(g)$ $(g\in P(A))$ of the map

$$[n]\longrightarrow P(A)\quad i\mapsto f_\sigma^i$$

in which case σ is completely determined by the various sets $K(g)$ $(g\in P(A))$. Hence for any $f\in A^{[n]}$ and any $u\in U(s_f)$ there exist precisely

$$\prod_{a\in A}\frac{s_f(a)!}{\prod\limits_{\substack{g\in P(A)\\ g(0)=a}}u(\bar{g})!}$$

permutations $\sigma\in[n]!$ with $u=u_{\sigma,f}$ such that (σ,f) is trimmed and, so, for any $u\in s^n(P(A))$ there exist precisely

$$\frac{n!}{\prod\limits_{g\in P(A)}u(\bar{g})!}$$

trimmed pairs $(\sigma,f)\in[n]!\times A^{[n]}$ with $u=u_{\sigma,f}$.

If, in addition, A is linearily ordered, we may define a pair $(\sigma,f)\in[n]!\times A^{[n]}$ to be *well trimmed*, if f is monotonically increasing on all of $[n]$ and σ is monotonically increasing on the fibres $f^{-1}(a)$ $(a\in A)$ of $f:[n]\longrightarrow A$, which by definition contain the subsets $K(g)$ for all $g\in P(A)$ with $g(0)=a$ and obviously form intervals in $[n]$ if f is monotonically increasing. Note that for any $s:A\longrightarrow\boldsymbol{N}_0$ with $|s|=n$ there exists precisely one monotonically increasing $f=f_s\in A^{[n]}$ with $s=s_f$. It follows immediately from Lemma 2 that a trimmed pair (σ,f) is well trimmed if and only if also all the subsets $K(g)$ $(g\in P(A))$ are intervals, ordered in such a way that $K(g)$ comes before $K(g')$ if and only if there exists some $i\in\boldsymbol{N}_0$ with

$$g(0)=g'(0),\ g(1)=g'(1),\ \dots,\ g(i-1)=g'(i-1)\ \text{and}\ g(i)<g'(i),$$

(that is, if and only if $g<g'$ with respect to the canonical lexicographic ordering of $P(A)$, induced by the linear order of A) since otherwise our σ would not be monotonically increasing on $K(a^{i-1}g)\cup K(a^{i-1}g')\subset$

$f^{-1}(g(i-1))$. Hence for any given $u\in s^n(P(A))$ there exists precisely one well trimmed pair (σ, f) with $u=u_{\sigma,f}$. In other words, we get a *section*

$$s^n(P(A))\xrightarrow{G}[n]!\times A^{[n]}$$

by associating to each $u\in s^n(P(A))$ the unique well trimmed pair $(\sigma, f)\in[n]!\times A^{[n]}$ with $u=u_{\sigma,f}$.

A more direct construction of G runs as follows: At first let us order the set $[u]$ lexicographically by $(g, i)<(g', i')$ if and only if $g<g'$ or $g=g'$ and $i<i'$. Then consider the resulting (order) isomorphism

$$\xi=\xi_u : [n]\longrightarrow[u]$$

of ordered sets and observe that the shift map α induces a permutation

$$\alpha=\alpha_u : [u]\longrightarrow[u] \qquad (g, i)\mapsto(\alpha g, i)$$

in $[u]!$. Finally put

$$\sigma_u := \xi^{-1}\circ\alpha\circ\xi\in[n]!$$

and

$$f_u := ev\circ\xi : [n]\longrightarrow[u]\longrightarrow A.$$

Then one verifies easily tht $G(u)=(\sigma_u, f_u)$. In other words, the section G results naturally from the observation that a linear order on A induces a linear order on $[u]$ and therefore a natural section of the projectiou $pr_1 : S^A(n)\longrightarrow s^n(P(A))$ given by

$$u\mapsto(u, \xi_u)$$

which transforms into G by composing it with Ψ^{-1}. Altogether we recover an unpublished observation of I. Gessel, which has been communicated to us by Jaques Désarménien (cf. [DW]).

COROLLARY 2. *There exist precisely q^n pairs $(\sigma, f)\in[n]!\times A^{[n]}$ for which f is monotonically increasing and σ is monotonically increasing on all intervalls $f^{-1}(a)$ $(a\in A)$, that is,*

$$\sigma(i)>\sigma(i+1) \text{ implies } f(i)<f(i+1).$$

In addition, if E is a set of cardinality n and τ a permutation of E then the number of pairs (σ, f) as above with $([n], \sigma)\cong(E, \tau)$ coincides with the number of $u\in s^n(P(A))$ with $([u], \alpha_u)\cong(E, \tau)$, that is, if τ has n_i cycles of length i on E, then there exist precisely

$$\prod_{i=1}^{n}\binom{n_i+M(q,\,i)-1}{n_i}$$

of such pairs.

Discussion

As we have pointed out already, Lemma 1 implies in particular an (almost) "bijective" proof of the relation $\#s^n(P(A))=\#A^{[n]}$ which is the essential combinatorial content of the cyclotomic identity. Moreover, it clarifies the relationship between different observations and results in this context:

- The proof of the cyclotomic identity, suggested in [DS2, 6.3.3.], consists of an analysis of the map $q:[n]!\times A^{[n]}\longrightarrow s^n(P(A))$ (though in the terminology of [DS2] $s^n(P(A))$ was denoted by $S^n(A^{(C)})^C$).
- The bijection G between $s^n(P(A))$ and the set of well trimmed pairs $(\sigma,f)\in[n]!\times A^{[n]}$ which results quite naturally from our basic diagram coincides (up to terminology and at least for the example given there) with *Gessel's* bijection "entre l'ensemble des parures et l'ensemble des couples (σ, s) constitués d'une permutation $\sigma\in S_n$ et d'une suite s compatible avec descentes(σ)" explained in [DW].
- The construction of a bijection $s^n(P(A))\to A^{[n]}$ given in [dBK] via Lyndon words (assuming the set A to be linearily ordered) can be viewed as a construction of another appropiate section of the map q composed with pr_2(cf. [DS3]).
- The proof of the cyclotomic identity, given in [MR1, MR2] and reinterpreted in terms of *species* (cf. [J]) in [VW], can be viewed as an analysis of the restriction of the map

  $$\Psi:[n]!\times A^{[n]}\longrightarrow S^A(n)$$

  onto the fibres of the map $q:[n]!\times A^{[n]}\longrightarrow s^n(P(A))$ over those elements $u\in s^n(P(A))$ having as support precisely one orbit.

Lemma 1 shows that all these approaches deal with special aspects of just one and the same more basic phenomenon.

In addition, there is a more general and fundamental relationship between cyclic sets (as considered in [DS1, DS2]) and species.

Let X denote a cyclic set, i. e. a set X together with an action of the additive group $\boldsymbol{Z}$ on X. Let $S(X)$ denote its symmetric algebra, i. e.

$$S(X) := \{u : X \longrightarrow N_0 \mid \sum_{x \in X} u(x) < \infty\}.$$

For any $u \in S(X)$ define

$$[u] := \{(x, \alpha) \mid x \in X \text{ and } 1 \leq \alpha \leq u(g)\}$$

Note that this set has n elements if $\sum_{x \in X} u(x) = n$, i. e. if $u \in S^n(X)$, the *n-th symmetric power* of X.

Define now for the cyclic set X the associated species $S(X)$ (same notation as for its symmetric algebra !) by assigning to a finite set E the set

$$S(X)(E) := \{(u, \Phi) \mid u \in S(X),\ u\ \boldsymbol{Z}\text{-invariant, and } \Phi : E \to [u] \text{ bijective}\}.$$

This provides a functor from cyclic sets to species which transforms sums (of cyclic sets) into products (of species). Moreover, the generating function (or *cardinality*) $S(X)(t)$ of $S(X)$ coincides with $s_t(X)$, the *ζ-function* of the cyclic set X defined in terms of its symmetric powers which has been studied in [DS1, DS2]. In particular, any formal power series with constant term 1 and integer coefficients is of the form $S(X)(t) \cdot S(Y)(t)^{-1}$ for some appropriate *almost finite* cyclic sets X and Y. We believe that this observation may help to make understandable, why formal power series appear to be so closely related to both concepts, cyclic sets as well as species.

In the particular case, considered above, the two relevant species are

$$S_A : E \mapsto E! \times A^E,$$

the species of *placements of nceklaces* and $S(P(A))$, where $\boldsymbol{Z}$ acts on $P(A)$ via the shift map. Note that $S(P(A))([n]) = S^A(n)$. Hence Lemma 1 can be interpreted as providing a " bijective " proof that $S(P(A))$ and S_A are *equipotent* species, i. e. they satisfy $\#S(P(A))(E) = \#S_A(E)$ for every finite set E.

Added in proof

As outlined in [DS4], the functor $S(X)$ is also equivalent to the functor

$$S_X : E \mapsto \{(\sigma, f) \in E! \times X^E \mid f(\sigma e) = \alpha f(e)\}$$

with $\alpha = \alpha_1 : X \longrightarrow X$ the shift-map, associated with the generator $1 \in \boldsymbol{Z}$. In this form our construction can be generalized considerably, see[N] for the discussion of some rather interesting specific cases, derived by replacing the additive group $\boldsymbol{Z}$ by other groups, and [DM, sec. 4] for a discus-

sion of a rather general setting in terms of forgetful functors, defined on topos-like categories, which still preserve all the combinatorial features needed for our most basic results.

References

[dBK] N. G. de BRUIJN and D. A. KLARNER: *Multisets of aperiodic cycles*, SIAM J. Alg. Disc. Meth., vol. **3** (1982), 359-368.

[C] P. CARTIER: *Groupes formels associées aux anneaux de Witt généralisées*, C. R. Acad. Sc. Paris, vol. **265** (1967), 49-52.

[DS1] A. W. M. DRESS and Ch. SIEBENEICHER: *Symmetric Powers of Cyclic Sets and the Definition of A. Weil's Zeta-Functions*, Proceedings of Symposia in Pure Mathematics, vol. **47** (1987), 407-411.

[DS2] A. W. M. DRESS and Ch. SIEBENEICHER: *The Burnside Ring of the Infinite Cyclic Group and its Relations to the Necklace Algebra, λ-Rings and the Universal Ring of Witt Vectors* (1987), Advances in Mathematics, vol. **78** (1989), 1-41.

[DS3] A. W. M. DRESS und Ch. SIEBENEICHER: *Ein Lemma über Perlenketten*, Séminaire Lotharingien de Combinatoire, vol. **20** (1988), 47-55.

[DW] J. DÉSARMÉNIEN et M. WACHS: *Descente des Dérangements et Mots circulaires*, Séminaire Lotharingien de Combinatoire, vol. **20** (1988), 13-21.

[G] C. F. GAUSS: *Werke Band II*, Königliche Gesellschaft der Wissenschaften, Göttingen (1863), 219-222.

[J] A. JOYAL: *Une Théorie combinatoire des séries formelles*, Advances in Mathematics, vol. **42** (1981), 1-82.

[L] M. LOTHAIRE: *Combinatorics on Words*, Encyclopedia of Mathematics and its Applications, Addison-Wesley Publishing Company (1983).

[MR1] N. METROPOLIS and G.-C. ROTA: *Witt Vectors and the Algebra of Necklaces*, Advances in Mathematics, vol. **50** (1983), 95-125.

[MR2] N. METROPOLIS and G.-C. ROTA: *The cyclotomic Identity*, in Contemporary Mathematics vol. **34** AMS (1984), 19-24.

[M] C. MOREAU: *Sur les permutation circulaires distinct*, Nouv. Ann. de Math., vol. **11** (1872), 309-314.

[V] G. VIENNOT: . *Algébre de Lie Libres et Monoides Libres*, Lecture Notes in Mathematics **691**, Springer (1978).

[VW] K. VARADARAJAN and K. WEHRHAHN: *Aperiodic Rings, Necklace Rings and Witt Vectors*, to appear in: Advances in Mathematics.

[W1] E. WITT: *Treue Darstellungen Liescher Ringe*, J. Reine Angew. Math., vol. **177** (1937), 152-161.

[W2] E. WITT: *Zyklische Körper und Algebren der Charakteristik p vom Grade p^n*, J. Reine Angew. Math. (Crelle), vol. **176** (1937), 126-140.

References added in proof

[DS4] DRESS (A. W. M.) und SIEBENEICHER (Ch.)—*Zur Abzählung periodischer Worte*, Séminaire Lotharingien de Combinatoire, 21^e session, Publ. I. R. M. A. Strasbourg, (1989).

[DM] DRESS (A. W. M.) und MÜLLER (T.)—*Logarithm of generating functions and combinatorial decomposition of functors*, Preprint Bielefeld (1990).

[N] NELSON (A. M.)—*A Generalized Cyclotomic Identity,* The University of Sydney, Pure Mathematics Research Reports, 89-7, (1989).

Universität Bielefeld, Fakultät für Mathematik
Postfach 8640
D4800 Bielefeld 1, FRG
e-mail: sieben @mathb. uni-bielefild. de