NECKLACES AND THE POLYNOMIALS OF C. MOREAU

THOMAS WEIGEL

Necklaces. We think of a *necklace* as a finite number of perls - say $n \in \mathbb{N}$ - we put on a string. After we have put n perls on the string, we knot the ends together magically, so that we do not see the knot. The perls are colored by a finite set of colors X of cardinality $r \in \mathbb{N}$. Arranging the necklace in the Gaussian plane $\mathbb{C}$ of complex numbers we may think that we have put a perl precisely on the elements of the group

$$C_n = \{\, z \in \mathbb{C} \mid z^n = 1 \,\} = \left\{ \exp\left(\frac{2\pi i}{n} \cdot k\right) \;\middle|\; 0 \leq k \leq n-1 \right\} \tag{1}$$

of n^{th}-roots of unity. This defines a function $f \in \mathfrak{F} = \mathfrak{F}(C_n, X)$, where $f(\omega)$ is

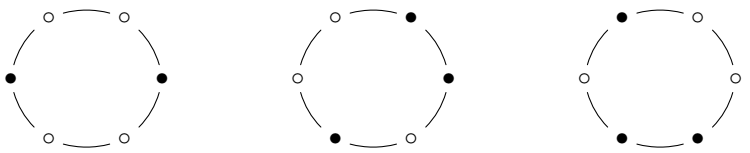

FIGURE 1. Necklaces of length 6 with $X = \{\circ, \bullet\}$.

the color of the perl we have put in the place ω. However, the set $\mathfrak{F}$ describes the arrangements of all necklaces rather than the set of all necklaces. Indeed, we would say that the function f and its translate $z \cdot f$, $z \in C_n$, describe the same necklace. Here, $z \cdot f$ denotes the function given by

$$(z \cdot f)(\omega) = f(z^{-1} \cdot \omega), \qquad \omega \in C_n. \tag{2}$$

E.g., if $f_2, f_3 \in \mathfrak{F}(C_6, \{\circ, \bullet\})$ denote the functions associated to the second and third necklace arrangement of Figure 1, one has $z \cdot f_3 = f_2$ for $z = \exp(2\pi i/3)$.

Therefore, a necklace corresponds to an *orbit* $C_n \cdot f$ of the left C_n-action on the finite set $\mathfrak{F}$. Again a significant difference arises. While $C_6 \cdot f_2$ has 6-elements, the C_6-orbit $C_6 \cdot f_1$ has only 3. Here $f_1 \in \mathfrak{F}(C_6, \{\circ, \bullet\})$ corresponds to the first necklace arrangement in Figure 1. One says that a necklace is *primitive*, if the C_n-orbit $C_n \cdot f$ has precisely n elements. The necklace $C_n \cdot f$ is a non-primitive if, and only if, $\mathrm{stab}_{C_n}(f) \neq \{1\}$. In this case f induces a function

$$\bar{f} \in \mathfrak{F}(C_n/\mathrm{stab}_{C_n}(f), X), \tag{3}$$

and the $C_n/\mathrm{stab}_{C_n}(f)$-orbit $(C_n/\mathrm{stab}_{C_n}(f)) \cdot \bar{f}$ has precisely $|C_n/\mathrm{stab}_{C_n}(f)|$ elements. Thus, a non-primitive necklace $C_n \cdot f$ defines a unique primitive necklace of length $|C_n/\mathrm{stab}_{C_n}(f)|$. E.g., the necklace $C_6 \cdot f_1$ corresponds to the primitive necklace $(C_6/\mathrm{stab}_{C_6}(f_1)) \cdot \bar{f}_1$ of length 3, where $\bar{f}_1$ is described as in Figure 2. Let $m_d(r)$ denote the number of primitive necklaces of length d which are made of perls

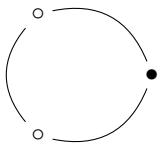

FIGURE 2. $\bar{f}_1$

of r different colors. Then $m_d(r)$ is the number of C_n-orbits on $\mathfrak{F} = \mathfrak{F}(C_n, X)$ of length d. In particular, the orbit formula implies that

$$r^n = |\mathfrak{F}| = \sum_{d|n} d \cdot m_d(r). \tag{4}$$

So, although our approach produces a formula involving the quantities $m_d(r)$ we are interested in, it does not give us a satisfactory answer yet.

The Möbius function. The problem arising from (4) can be formulated in a general context.

Problem. Let $\mathbf{a},\ \mathbf{b} \in \mathfrak{F}(\mathbb{N}, \mathbb{C})$ be two series satisfying

$$\mathbf{b}(n) = \sum_{d|n} \mathbf{a}(d). \tag{5}$$

How can we compute the series $\mathbf{a}$ from the knowledge of the series $\mathbf{b}$?

In order to give a satisfactory answer we consider the *convolution product* on $\mathfrak{F}(\mathbb{N}, \mathbb{C})$. In more detail, for $\mathbf{a}, \mathbf{b} \in \mathfrak{F}(\mathbb{N}, \mathbb{C})$ we define $\mathbf{a} * \mathbf{b} \in \mathfrak{F}(\mathbb{N}, \mathbb{C})$ by

$$(\mathbf{a} * \mathbf{b})(n) = \sum_{d|n} \mathbf{a}(d) \cdot \mathbf{b}(n/d). \tag{6}$$

Some straightforward calculations show that "$*$" is commutative, associative, and that $\delta \in \mathfrak{F}(\mathbb{N}, \mathbb{C})$, $\delta(1) = 1$, $\delta(k) = 0$ for $k \neq 1$, is a neutral element for "$*$", i.e.,

$$\delta * \mathbf{a} = \mathbf{a} * \delta = \mathbf{a} \qquad \text{for all } \mathbf{a} \in \mathfrak{F}(\mathbb{N}, \mathbb{C}). \tag{7}$$

This gives $(\mathfrak{F}(\mathbb{N}, \mathbb{C}), +, *)$ a ring structure. Let $\mathbf{1} \in \mathfrak{F}(\mathbb{N}, \mathbb{C})$ be the constant 1 function, i.e., $\mathbf{1}(n) = 1$ for all $n \in \mathbb{N}$. Then (5) is equivalent to

$$\mathbf{b} = \mathbf{1} * \mathbf{a}. \tag{8}$$

A function $\mathbf{a} \in \mathfrak{F}(\mathbb{N}, \mathbb{C})$ is said to be *arithmetic*, if $\mathbf{a}(1) = 1$, and if for all $m, n \in \mathbb{N}$, $\gcd(m, n) = 1$, one has

$$\mathbf{a}(m \cdot n) = \mathbf{a}(m) \cdot \mathbf{a}(n). \tag{9}$$

E.g., δ and $\mathbf{1}$ are arithmetic. Let $\mathfrak{Ar}(\mathbb{N}, \mathbb{C}) \subseteq \mathfrak{F}(\mathbb{N}, \mathbb{C})$ denote the set of all arithmetic functions. Then $(\mathfrak{Ar}(\mathbb{N}, \mathbb{C}), *)$ is a group. Indeed, the convolution inverse $\mu = \mathbf{1}^{-1}$ - also called the *Möbius function* - can be calculated explicitly. Obviously, $\mu(1) = 1$, and property (9) implies that it suffices to know μ on the set of prime powers p^k, p prime, $k \in \mathbb{N}$. Thus putting $\mu(p^k) = 0$ for $k \geq 2$ and $\mu(p) = -1$, one obtains for $k \geq 1$ that

$$(\mu * \mathbf{1})(p^k) = \sum_{0 \leq j \leq k} \mu(p^j) \cdot \mathbf{1}(p^{k-j}) = 1 \cdot 1 + (-1) \cdot 1 = 0 = \delta(p^k). \tag{10}$$

Thus $\mu(n) = 0$ if for some prime number p one has $p^2|n$, and $\mu(p_1 \cdots p_r) = (-1)^r$ if p_i are pairwise distinct prime numbers. So, if (5) holds for two functions $\mathbf{a}, \mathbf{b} \in \mathfrak{F}(\mathbb{N}, \mathbb{C})$, one concludes that

$$\mathbf{a} = \mu * \mathbf{b} = \mathbf{b} * \mu. \tag{11}$$

The Necklace polynomials. Applying (11) to (4) yields that

$$m_n(r) = \frac{1}{n} \cdot \sum_{d|n} \mu(n/d) \cdot r^d. \tag{12}$$

The polynomial

$$M_n(T) = \frac{1}{n} \cdot \sum_{d|n} \mu(n/d) \cdot T^d \in \mathbb{Q}[T] \tag{13}$$

is called the n^{th}*-necklace polynomial*. Usually one uses the letter M_n for the notation of these polynomials in order to give credit to C. Moreau who studied the number of necklaces already around 1872. One has

$$\begin{aligned}
M_1(T) &= T \\
M_2(T) &= \frac{1}{2}(T^2 - T) \\
M_3(T) &= \frac{1}{3}(T^3 - T) \\
M_4(T) &= \frac{1}{4}(T^4 - T^2) \\
M_5(T) &= \frac{1}{5}(T^5 - T) \\
M_6(T) &= \frac{1}{6}(T^6 - T^3 - T^2 + T) \\
&\vdots \\
M_{p^k}(T) &= \frac{1}{p^k}(T^{p^k} - T^{p^{k-1}}).
\end{aligned}$$

Necklace polynomials arise naturally in many quite different contexts.

(a) Counting primitive elements in a finite extension of finite fields;
(b) in the Euler product formula of the Dedekind ζ-function of the polynomial ring over a finite field;
(c) in the dimension formula for the homogeneous components of a free Lie algebra (Hall-Witt formula) (cf. [1]);
(d) in the dimension formula for the homogeneous components of a graded Lie algebra of type FP (cf. [2]).

References

[1] N. Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation. MR 1728312

[2] Th. Weigel, *Graded Lie algebras of type FP*, Israel J. Math. **205** (2015), no. 1, 185–209. MR 3314587