JOURNAL OF COMBINATORIAL THEORY, Series A 56, 75–83 (1991)

Circular Codes, Loop Counting, and Zeta-Functions

GERHARD KELLER

Mathematisches Institut, Universität Erlangen-Nürnberg, Bismarckstrasse $1\frac{1}{2}$, D-8520 Erlangen, West Germany

Communicated by Andrew Odlyzko

Received August 10, 1989

We prove a simple formula for the zeta-function of coded systems generated by circular codes (and more generally by circular Markov codes). We apply this to the loop counting method for determining the topological entropy of a subshift of finite type, to the zeta-function of the Dyck-shift over $2N$ symbols, and to the zeta-function of a subshift of finite ype which is obtained from a full shift by deleting one block of arbitrary length. © 1991 Academic Press, Inc.

1. INTRODUCTION

Let C be a set of words over a finite alphabet Σ, and suppose that each two-sided infinite periodic sequence of letters from Σ has at most one decomposition into words from C. (Such sets C are called circular codes in [1].) The following identity is proved in Proposition 4.7.11 of [7]:

$$\zeta(z) = (1 - f(z))^{-1}, \tag{1}$$

where $f(z)$ is the generating function of the code C and $\zeta(z)$ is the zeta-function for the (not necessarily closed) subshift $C^\infty \subseteq \Sigma^{\mathbb{Z}}$.

Another well known formula from symbolic dynamics is the Bowen–Lanford formula for the zeta-function of a topological Markov chain:

$$\zeta(z) = \det(Id - zA)^{-1},$$

where A is the 0–1-transition matrix defining the chain.

In Section 2 we prove a generalization of these two formulas to circular Markov codes (defined in that section). Some examples are presented in Section 3, and in Section 4 formula (1) is applied to two problems on subshifts of finite type: First we give a short justification of the loop counting method for determining the entropy of an irreducible topological Markov chain (cf. [4]), and then we derive a simple expression for the zeta-function of a subshift of finite type which is obtained from a full shift by deleting one block of arbitrary size.

0097-3165/91 $3.00

2. The Zeta-Function

Fix the following notation: Σ is a finite set (alphabet), $\Sigma^+ = \{a_1 \cdots a_n : n \in \mathbb{N},\ a_i \in \Sigma\}$ is the set of nonempty finite words over Σ, and $\Sigma^{\mathbb{Z}}$ is the space of two-sided infinite sequences of symbols from Σ endowed with the (compact!) product topology arising from the discrete topology on Σ. The shift-transformation $\sigma: \Sigma \to \Sigma$ defined by $\sigma((\omega_i)_{i \in \mathbb{Z}}) = (\omega_{i+1})_{i \in \mathbb{Z}}$ is a homeomorphism of $\Sigma^{\mathbb{Z}}$ (cf. [3]). For $\omega \in \Sigma^{\mathbb{Z}}$ and $i < j$ in $\mathbb{Z}$ let $\omega_{[i,j)} = \omega_i \omega_{i+1} \cdots \omega_{j-1}$ in Σ^+.

With a quadrupel $\mathscr{C} = (C, I, A, r)$, where $C \subseteq \Sigma^+$, I a finite index set, A a $\{0, 1\}$-valued $I \times I$-matrix, and r a function from $C \to I$, we associate the following shift-invariant subset of $\Sigma^{\mathbb{Z}}$:

$$\Omega_{\mathscr{C}} = \{\omega \in \Sigma^{\mathbb{Z}} : \text{there are} \ldots k_{-1} < k_0 \leqslant 0 < k_1 < \ldots \text{ in } \mathbb{Z} \text{ such that}$$
$$\omega_{[k_i, k_{i+1})} \in C \text{ and } a_{r(\omega_{[k_{i-1}, k_i)}),\, r(\omega_{[k_i, k_{i+1})})} = 1 \ (i \in \mathbb{Z})\}.$$

By $\bar{\Omega}_{\mathscr{C}}$ we denote the topological closure of $\Omega_{\mathscr{C}}$ in $\Sigma^{\mathbb{Z}}$.

For $n \geqslant 1$ define $I \times I$-diagonal matrices $D(\mathscr{C}, n)$ by

$$d_{i,i}(\mathscr{C}, n) = \operatorname{card}\{w \in C : \operatorname{length}(w) = n,\ r(w) = i\}$$

and a matrix-valued generating function by

$$F(\mathscr{C}, z) = \sum_{n=1}^{\infty} D(\mathscr{C}, n)\, A z^n.$$

For a shift-invariant subset Y of $\Sigma^{\mathbb{Z}}$ (not necessarily closed) let

$$\pi(Y, n) = \operatorname{card}\{\omega \in Y : \sigma^n \omega = \omega\}$$

and

$$\zeta(Y, z) = \exp \sum_{n=1}^{\infty} \frac{z^n}{n} \pi(Y, n).$$

Observe that all these power series converge for $|z| < \operatorname{card}(\Sigma)^{-1}$.

Finally we call $\mathscr{C} = (C, I, A, r)$ a *circular Markov code* if each periodic sequence $\omega \in \Omega_{\mathscr{C}}$ has a unique decomposition into words from C which respects the transition rules imposed by A and r.

If I is a one-point set, we recover the circular codes from [1], called very pure monoids in [7]. In this case we simply write C instead of $\mathscr{C}$ and call C a circular code.

Theorem 1. *If $\mathscr{C}$ is a circular Markov code, then*

$$\zeta(\Omega_{\mathscr{C}}, z) = \det(Id - F(\mathscr{C}, z))^{-1}.$$

Proof. We use the following notation: If $g(z)=\sum_{n=0}^{\infty} a_n z^n$ is a (formal) power series, then $c_k(g)=a_k$. The following relation defines the (formal) derivative of g:

$$c_{k-1}(g')=k\cdot c_k(g) \qquad (k\geqslant 1).$$

Hence, if we write F for $F(\mathscr{C}, z)$,

$$\begin{aligned}
-\log \operatorname{trace}(Id-F) &= \sum_{m=1}^{\infty} \operatorname{trace} c_m(-\log (Id-F))\, z^m \\
&= \sum_{m=1}^{\infty} \frac{1}{m} \operatorname{trace} c_{m-1}(F'(Id-F)^{-1})\, z^m \\
&= \sum_{m=1}^{\infty} \frac{z^m}{m} \sum_{j=0}^{m-1} \operatorname{trace}(c_j(F')\, c_{m-1-j}((Id-F)^{-1})) \\
&= \sum_{m=1}^{\infty} \frac{z^m}{m} \sum_{j=0}^{m-1} (j+1) \operatorname{trace}(c_{j+1}(F)\, c_{m-1-j}((Id-F)^{-1})) \\
&= \sum_{m=1}^{\infty} \frac{z^m}{m} \sum_{j=1}^{m} j\cdot \operatorname{trace}(c_j(F)\, c_{m-j}((Id-F)^{-1})) \qquad (2)
\end{aligned}$$

and we obtain

$$\begin{aligned}
&-\log \det(Id-F) \\
&\quad = -\operatorname{trace} \log(Id-F) \\
&\quad = \sum_{m=1}^{\infty} \frac{z^m}{m} \sum_{j=1}^{m} j \operatorname{trace}(c_j(F)\, c_{m-j}((Id-F)^{-1})) \\
&\quad = \sum_{m=1}^{\infty} \frac{z^m}{m} \sum_{j=1}^{m} j \operatorname{card}\{w=w_1\cdots w_k : k\geqslant 1, w_i\in C, \text{length }(w_1)=j, \\
&\qquad\qquad \text{length }(w)=m, a_{r(w_i), r(w_{i+1})}=1\ (i=1, ..., k-1), a_{r(w_k), r(w_1)}=1\} \\
&\quad = \sum_{m=1}^{\infty} \frac{z^m}{m} \pi(\Omega_{\mathscr{C}}, m) \\
&\quad = \log \zeta(\Omega_{\mathscr{C}}, z).
\end{aligned}$$

The first identity is well known for finite matrices, the second one follows from (2) and from the linearity and continuity of the trace, and the third one is just an interpretation of the fact that $(Id-F)^{-1}=\sum_{k=0}^{\infty} F^k$. We comment on the fourth equality: For $\omega\in\Omega_{\mathscr{C}}$ and $m\geqslant 1$, one has $\sigma^m\omega=\omega$ if and only if ω is a two-sided infinite concatenation of a word $w=w_1\cdots w_k$ of length m with $w_i\in C$ and $a_{r(w_i), r(w_{i+1})}=1$ $(i=1, ..., k)$, $w_{k+1} := w_1$. In this case w is uniquely determined up to a cyclic permutation of the subwords $w_1, ..., w_k$. This is all due to the fact that $\mathscr{C}$ is a circular Markov code. If we fix the zeroeth coordinate of ω and choose $w = w_1 \cdots w_k$ such that ω_0 is covered by a copy of w_1, then we see that each $\omega \in \mathrm{Fix}(\sigma^m)$ determines exactly one word w as above, and the same word w is determined by exactly length (w_1) different $\omega \in \mathrm{Fix}\ (\sigma^m)$. ∎

The following lemma is useful for relating $\zeta(\Omega_{\mathscr{C}}, z)$ and $\zeta(\bar{\Omega}_{\mathscr{C}}, z)$:

LEMMA 1. *Let $\omega \in \bar{\Omega}_{\mathscr{C}}$, where $\mathscr{C}$ is a circular Markov code, and suppose that $\sigma^n \omega = \omega$. Denote $w = \omega_{[0, n)}$. Then either $\omega \in \Omega_{\mathscr{C}}$ or for any $k \in \mathbb{N}$ there is $v \in C$ such that w^k is a subword of v.*

Proof. As $\omega \in \bar{\Omega}_{\mathscr{C}}$, there are, for any $k \in \mathbb{N}$, words $v_{k,1}, ..., v_{k,r(k)} \in C$ with $a_{r(v_{k,i}), r(v_{k,i+1})} = 1$ such that w^k is a subword of $v_{k,1} \cdots v_{k,r(k)}$. Let

$$S = \sup\{\text{length } (v_{k,i}) \colon k \in \mathbb{N}, 1 \leqslant i \leqslant r(k)\}.$$

If $S < \infty$ there are only finitely many, say N, different words among all $v_{k,i}$, such that for $k > NS$ there are $0 \leqslant i < j < k$ for which $\omega_{in} = (w^k)_{in}$ and $\omega_{jn} = (w^k)_{jn}$ match with the same position of the same word from this finite collection. This implies $\omega \in \Omega_{\mathscr{C}}$. If $S = \infty$, but for some $m \in \mathbb{N}$ there is no $v \in C$ for which w^m is a subword of v, then

$$S_0 = \sup\{\text{length}(v_{k,i}) \colon k \in \mathbb{N}, 1 < i < r(k)\} < \infty$$

but

$$L = \sup\{\text{length } (v_{k,2} \cdots v_{k,r(k)-1}) \colon k \in \mathbb{N}\} = \infty,$$

and the same argument as in the case $S < \infty$ shows that $\omega \in \Omega_{\mathscr{C}}$. ∎

3. EXAMPLES

We use the notation $P_n(\mathscr{C}) = \{\omega \in \bar{\Omega}_{\mathscr{C}} \backslash \Omega_{\mathscr{C}} \colon \sigma^n \omega = \omega \text{ but } \sigma^k \omega \neq \omega \text{ for all } 0 < k < n\}$.

EXAMPLE 1. Let I be a one-point set and $C = \{0^n 1^n \colon n \in \mathbb{N}\}$. By Lemma 1, $P_1(\mathscr{C}) = \{0^\infty, 1^\infty\}$ and $P_n(\mathscr{C}) = \varnothing$ for $n \geqslant 2$. Hence

$$\begin{aligned} \zeta(\bar{\Omega}_{\mathscr{C}}, z) &= \zeta(\Omega_{\mathscr{C}}, z)(1-z)^{-2} \\ &= \left(\left(1 - \sum_{n=1}^{\infty} z^{2n}\right)(1-z)^2\right)^{-1} \\ &= \frac{1+z}{(1-2z^2)(1-z)}. \end{aligned}$$

EXAMPLE 2. Let $I=\{0,1,2\}$, $C_i=\{0^n1 : 0\leqslant n=i \bmod 3\}$ $(i\in I)$, $C=C_0\cup C_1\cup C_2$, $r(w)=i$ if $w\in C_i$, and $A=(a_{i,j})$, where $a_{i,j}=1$ if and only if $i\neq j$. By Lemma 1 we have $P_1(\mathscr{C})=\{0^\infty\}$, $P_n(\mathscr{C})=\varnothing$ $(n\geqslant 2)$. Hence $\zeta(\bar{\Omega}_{\mathscr{C}},z)=\zeta(\Omega_{\mathscr{C}},z)/(1-z)$ and

$$\zeta(\Omega_{\mathscr{C}},z)=1/\det\begin{pmatrix} 1 & -z/(1-z^3) & -z/(1-z^3) \\ -z^2/(1-z^3) & 1 & -z^2/(1-z^3) \\ -z^3/(1-z^3) & -z^3/(1-z^3) & 1 \end{pmatrix}$$
$$=1/(1-(z^3+z^4+z^5+z^6-z^7-z^8)(1-z^3)^{-3}).$$

EXAMPLE 3. We apply Theorem 1 to calculate the zeta-function for the Dyck-shift over $2N$ symbols. This result is due to W. Krieger.

Notation. $C^\infty=\Omega_{\mathscr{C}}$ if $\mathscr{C}=(C,I,A,r)$ is a circular code, i.e., $\operatorname{card}(I)=1$.

Let $N\geqslant 1$. The Dyck-language D over $2N$ symbols is the set of all properly nested sequences of brackets of N different types (cf. [5], Sect. 4). More exactly, let $L=\{a_1,\dots,a_N\}$, $R=\{\bar{a}_1,\dots,\bar{a}_N\}$, and $\Sigma=L\cup R$. D is defined as the smallest subset of Σ^+ containing the words $a_k\bar{a}_k$ $(k=1,\dots,N)$ and satisfying $DD\subseteq D$, $a_k D\bar{a}_k\subseteq D$ $(k=1,\dots,N)$. Denote by E the set of all elementary words from D, i.e., $w\in E$ if $w\in D$ and there is no decomposition $w=uv$ with $u,v\in D$. Let

$$E_+=\{wu\in\Sigma^+ : w\in E, u\in R^*\},\qquad E_-=\{uw\in\Sigma^+ : w\in E, u\in L^*\},$$

where $R^*=R^+\cup\{\text{empty word}\}$, $L^*=L^+\cup\{\text{empty word}\}$. It is known (cf. [1]) that

$$f(E,z)=\tfrac{1}{2}(1-\sqrt{1-4Nz^2}). \tag{3}$$

(Observe that $1-\sqrt{1-z^2}$ is the generating function of the first return time to 0 of a symmetric random walk with increments ± 1.) From (3) one obtains the generating functions for E_+ and E_- as

$$f(E_+,z)=f(E_-,z)=f(E,z)\cdot\sum_{k=0}^{\infty}N^kz^k=f(E,z)/(1-Nz). \tag{4}$$

The Dyck-shift over $2N$ symbols is defined as $\bar{\Omega}_D$.

Suppose now that $\omega\in\bar{\Omega}_D$ is periodic, say $\sigma^m\omega=\omega$. Define $h:\mathbb{N}\to\mathbb{Z}$ by

$$h(n)=\sum_{k=0}^{n-1}(\chi_L(\omega_k)-\chi_R(\omega_k)).$$

As $\sigma^m\omega=\omega$ we have $h(n+m)-h(n)=h(m)$ for all $n\in\mathbb{N}$. Suppose first that $h(m)\leqslant 0$. Let H be the set of all $j\in\{m+1,\dots,2m\}$ for which $h(j)<h(j+1)$

and $h(j) \leqslant h(i)$ for all $0 \leqslant i \leqslant j$. H is finite, say $H = \{j_1, ..., j_r\}$ with $j_i < j_{i+1}$. We also set $j_{r+1} = j_1 + m$. If $H \neq \varnothing$, then each $\omega_{[j_i, j_{i+1})}$ belongs to E_+ and hence $\omega \in E_+^\infty$, If $H = \varnothing$, then $\omega_{[j, j+m)} \in R^m$. Similarly one shows: $\omega \in E_-^\infty$ or $\omega_{[j, j+m)} \in L^m$ if $h(m) \geqslant 0$, and $\omega \in E^\infty$ if $h(m) = 0$. Hence

$$\zeta(\bar{\Omega}_D, z) = \frac{\zeta(E_+^\infty, z) \cdot \zeta(E_-^\infty, z)}{\zeta(E^\infty, z) \cdot (1 - Nz)^2}. \tag{5}$$

Next we show that E, E_+, and E_- are circular codes. Suppose f.e. that $\omega \in E_+^\infty$ and $\sigma^m \omega = \omega$ (the proofs for E and E_- are similar). Then there is $j \in \{m+1, ..., 2m\}$ such that $\omega_{[j, j+m)} = w_1 \cdots w_r$ with $w_1, ..., w_r \in E_+$ and $j + \text{length}\,(w_1 \cdots w_{r-1}) < 2m$. If h and H are defined as above, it is obvious that $H = \{j + \sum_{i=1}^{k-1} \text{length}\,(w_i) \colon k = 1, ..., r\}$, and as H is defined independently of $w_1, ... w_r$, the above decompsition is unique. Combining (3), (4), (5), and Lemma 1 we thus obtain

$$\zeta(\bar{\Omega}_D, z) = \frac{2(1 + \sqrt{1 - 4Nz^2})}{(1 - 2Nz + \sqrt{1 - 4Nz^2})^2}.$$

4. Applications to Subshifts of Finite Type

Loop Counting

In [6] Petersen has reexamined the loop counting method for computing the topological entropy $h(\Omega)$ of an irreducible subshift of finite type Ω over a finite alphabet Σ (for definitions see, e.g., [3]). This method says that $\exp(-h(\Omega))$ is the (unique!) positive root of the equation

$$p_b(z) := \sum_{n=1}^{\infty} N_n z^n = 1, \tag{6}$$

where b is an arbitrary but fixed symbol in Σ, and N_n is the number of blocks bwb of length $(n+1)$ which are allowed in Ω, where the word w contains no b. We show how this result follows from Theorem 1: Let

$$C(b) = \{bw \colon bwb \text{ is an allowed block in } \Omega \text{ and } w \text{ contains no } b\}$$

and

$$\Omega_b = \{\omega \in \Omega \colon \omega \text{ contains no } b\}.$$

Ω_b is again a subshift of finite type, and $C(b)$ is a circular code with

$$N_n = \text{card}\{bw \in C(b) \colon \text{length}(bw) = n\}.$$

Hence $f(C(b), z) = p_b(z)$ from Eq. (6).

As each periodic point in Ω is either in $C(b)^\infty$ or in Ω_b, we obtain

$$\zeta(\Omega, z) = \zeta(\Omega_b, z) \cdot \zeta(C(b)^\infty, z) = \zeta(\Omega_b, z) \cdot \frac{1}{1 - p_b(z)}. \tag{7}$$

Observe that we did not use the irreducibility of Ω to derive (7). If Ω is irreducible, the topological entropy of Ω_b is strictly smaller than that of Ω, such that in this case $\exp(-h(\Omega))$, the smallest positive pole of $\zeta(\Omega, z)$, must coincide with the positive root of $p_b(z) = 1$.

If $\Sigma = \{b_1, ..., b_N\}$ and $C_j = \{b_j w : b_j w b_j$ is an allowed block in Ω and w contains no b_i $(1 \leqslant i \leqslant j)\}$, then a repeated application of (7) yields

$$\zeta(\Omega, z) = \prod_{j=1}^{N} \zeta(C_j^\infty, z) = \prod_{j=1}^{N} \frac{1}{1 - f(C_j, z)}.$$

Deleting Long Blocks from Full Shifts

Let $B = b_1, ..., b_l$ be a word of length $l \geqslant 1$ over the alphabet $\Sigma = \{1, ..., d\}$, and let

$$\Omega_B = \{\omega \in \Sigma^{\mathbb{Z}} : \omega \text{ does not contain } B \text{ as a subword}\}.$$

We give a formula for the zeta-function $\zeta(\Omega_B, z)$ of Ω_B in terms of the autocorrelation ψ_B of B, i.e., of the polynomial

$$\psi_B(z) = \sum_{i=0}^{l-1} a_i z^i, \qquad \text{where } a_i = 1 \text{ if } b_j = b_{j+i}\ (j = 1, ..., l-i) \text{ and } a_i = 0 \text{ otherwise.}$$

PROPOSITION 1. $\zeta(\Omega_B, z) = (z^l + (1 - dz)\,\psi_B(z))^{-1}$.

The proof relies on three combinatorial indentities from string enumeration theory:

Proof. Let f_n $(n \geqslant 0)$ be the number of words of length n which do not contain B as a subword, let g_n $(n \geqslant 1)$ be the number of words of length n ending with the string B but with no further occurrence of B as a subword, and let h_n $(n \geqslant l+1)$ be the number of words of length n starting and ending with (possibly overlapping) copies of B but with no further occurrence of B as a subword. The corresponding generating functions are

$$F(z) = 1 + \sum_{n=1}^{\infty} f_n z^n$$

$$G(z) = \sum_{n=l}^{\infty} g_n z^n$$

$$H(z) = \sum_{n=l+1}^{\infty} h_n z^n.$$

Obviously

$$d \cdot f_n = f_{n+1} + g_{n+1} \qquad (n \geqslant 0)$$

and

$$d \cdot g_n = g_{n+1} + h_{n+1} \qquad (n \geqslant l)$$

and hence

$$d \cdot F(z) = z^{-1}(F(z) - 1 + G(z)) \tag{8}$$

and

$$d \cdot G(z) = z^{-1}(G(z) - z^l + H(z)). \tag{9}$$

These are Eqs. (2.5) and (2.6) from [4] with z replaced by z^{-1}.

Also the relation

$$f_n = \sum_{i=0}^{l-1} a_i g_{n+l-i}$$

is easy to prove, and it implies that

$$z^l F(z) = \psi_B(z)\, G(z) \tag{10}$$

(see Eq. (2.7) in [4]). Now (8), (9), and (10) yield

$$1 - z^{-l}H(z) = (1 - dz)(z^l + (1 - dz)\, \psi_B(z))^{-1}. \tag{11}$$

(The route to Eq. (11) is also outlined in Exercise VII.3.2 of [1].) Next let for $n \geqslant 1$

$$C_n = \{w \in \Sigma^n \colon Bw \text{ starts and ends with (possibly overlapping) copies of } B \text{ but has no further occurrence of } B \text{ as a subword}\}.$$

It is not hard to see that $C = \bigcup_{n=1}^{\infty} C_n$ is a circular code and card $(C_n) = h_{n+l}$. Hence, by Theorem 1,

$$\zeta(\Omega_C, z) = (1 - z^{-l}H(z))^{-1}. \tag{12}$$

But $\zeta(\Omega_C, z) \cdot \zeta(\Omega_B, z) = \zeta(\Sigma^{\mathbb{Z}}, z) = (1 - dz)^{-1}$, such that

$$\zeta(\Omega_B, z) = (z^l + (1 - dz)\, \psi_B(z))^{-1}. \quad \blacksquare$$

I would like to mention that I heard about the identities from string enumeration theory in a talk given by D. Lind at the "Workshop on

Topological Markov Shifts and Related Systems," Heidelberg, 1987. He used the equation

$$F(z) = \psi_B(z)(z^l + (1 - dz)\,\psi_B(z))^{-1}$$

(which follows from (8) and (10)) to show that if $\lambda = \exp(h(\Omega_B))$, then $d - \lambda$ is of order d^{-l}.

Acknowledgment

I thank the referee for some helpful remarks, in particular for the reference to [7].

References

1. J. Berstel and D. Perrin, "Theory of Codes," Academic Press, London, 1985.
2. F. Blanchard and G. Hansel, Systèmes codés, *Theoret. Comput. Sci.* **44** (1986), 17–49.
3. M. Denker, C. Grillenberger, and K. Sigmund, Ergodic theory on compact spaces, "Lecture Notes in Mathematics," Vol. 527, Springer-Verlag, Berlin/Heidelberg/New York, 1976.
4. L. J. Guibas and A. M. Odlyzko, Maximal prefix-synchronized codes, *SIAM J. Appl. Math.* **35** (1978), 401–418.
5. W. Krieger, On the uniqueness of the equilibrium state, *Math. Systems Theory* **8** (1974), 97–104.
6. K. Peterson, Chains, entropy, coding. *Ergodic Theory Dynamical Systems* **6** (1986), 415–448.
7. R. P. Stanley, "Enumerative Combinatorics," Vol. I, Brooks–Cole, Monterey, CA, 1986.