Annales Univ. Sci. Budapest., Sect. Comp. 40 (2013) 363–377

CIRCULANTS, LINEAR RECURRENCES AND CODES

L. Jiang (Dalian, China)

S. Kanemitsu (Iizuka, Japan)

H. Kitajima (Saga, Japan)

To Professors Zoltán Daróczy and Imre Kátai, with great respect and friendship

Communicated by Bui Minh Phong

(Received March 21, 2013; accepted April 07, 2013)

Abstract. We shall give some intriguing applications of the theory of circulants—the circulant matrices—and that of linear recurrence sequences (LRS). The applications of the former in §2 ranges from a simple derivation of the Blahut theorem to the energy levels of hydrogen atoms in circular hydrocarbons, where the Blahut theorem is to the effect that the Hamming weight of a code is equal to the rank of the associated Fourier matrix. The latter in §3 is connected to the understanding of an LFSR (linear feedback shift register) as an LRS, and culminates to a corollary asserting that the linear complexity of the periodically repeated sequence is equal to the rank of the DFT matrix, revealing the relationship between Blahut's and Massey's formulations. At the end of §3 we give a proof of Blahut's theorem by Massey's theorem. We also mention other relevance of circulants to the hydrocarbons and class numbers of cyclotomic fields in §4. This constitutes a companion paper to [8] and deals with more concrete cases.

1. Introduction and statement of results

Let F be a field of $\operatorname{char} F = p$ such that its extension field E contains an N-th root $\zeta = \zeta_N$ of 1, where $p \nmid N$. This is the case because for $p = 0$, $E = \mathbb{C}$

Key words and phrases: Circulant matrices, linear recurrence sequence,linear feedback shift register,Blahut's and Massey's formulation.
2010 Mathematics Subject Classification: Primary 11B37, 11H71. Secondary 94H15.
https://doi.org/10.71352/ac.40.363

and $\zeta = e^{2\pi i \frac{1}{N}}$, and for $p > 0$, by the theory of finite fields, there exists an extension E containing ζ.

In this paper we confine either to finite fields $\mathbf{F} = \mathbf{F}_q = \mathrm{GF}(q)$ with $q = p^m$ elements, with p a prime and m a positive integer, or to commutative rings $\mathcal{R}$ (not necessarily integral domains as furnished by the example of the residue class ring modulo a composite) and assume that their extension field (or ring) E contains a primitive root of unity. By abuse of language we refer to them as a field F whose extension E contains a primitive N-th root ζ of unity.

Let $\mathbf{a} = (a_0, \cdots, a_{N-1}) \in F^N$ be a sequence of N terms (or a periodic sequence of period N). Then the *discrete Fourier transform* (sometimes Finite Fourier Transform) $\mathrm{DFT}(\mathbf{a})$ is given by $\hat{\mathbf{a}} = \mathrm{DFT}(\mathbf{a}) = (\hat{a}_0, \cdots, \hat{a}_{N-1}) \in E^N$, where $\hat{a}_j$ is defined by

$$\hat{a}_j = \sum_{k=0}^{N-1} a_k \zeta^{-jk}, \quad 0 \le j \le N-1, \tag{1.1}$$

where we mean by ζ^{-1} the conjugate of ζ i.e. ζ^{N-1}.

The inverse transform is

$$a_k = \frac{1}{N} \sum_{j=0}^{N-1} \hat{a}_j \zeta^{kj}, \quad 0 \le k \le N-1. \tag{1.2}$$

We say that ζ generates a $\mathrm{DFT}(\mathbf{a})$ of length N. For DFT, cf. e.g. [2], [4], [9], [13], etc. and references therein.

The *circulant matrix* formed from $\mathrm{DFT}(\mathbf{a})$ is called the DFT matrix $M(\hat{\mathbf{a}})$ of $\mathbf{a}$:

$$M(\hat{\mathbf{a}}) = \begin{pmatrix} \hat{a}_0 & \hat{a}_1 & \cdots & \hat{a}_{N-1} \\ \hat{a}_1 & \hat{a}_2 & \cdots & \hat{a}_0 \\ & \cdots & & \\ \hat{a}_{N-1} & \hat{a}_0 & \cdots & \hat{a}_{N-2} \end{pmatrix}. \tag{1.3}$$

In §2 we shall derive the following Blahut theorem as an immediate consequence of the fundamental theorem in the theory of circulants (cf. [5]). Let $w(\mathbf{a})$ denote the number of non-zero terms of the code-word $\mathbf{a}$, which is an important quantity in error-correcting codes and is referred to as the *Hamming weight*.

Theorem 1.1. (Blahut) *The Hamming weight of* $\mathbf{a}$ *is the rank of the DFT matrix* $M(\mathbf{a})$.

Further in §3, we shall elucidate hitherto somewhat ambiguous treatment of LFSR from the point of view of linear recurrence sequences and deduce

Massey's version (Theorem 3.1) of the Blahut theorem in a lucid way. As a bonus, we obtain a new result, Corollary 3.1 as a combination of Blahut's and Massey's theorems.

Toward the end, we shall also mention codes arising from topological matrices associated with hydrocarbons and a relation of circulants to the class number problem.

2. Circulant matrices and the Blahut theorem

In [3, Chapter 1] we applied the theory of circulant matrices to calculating the energy levels of molecular orbitals of cyclo-polyenes (cyclic hydrocarbons) e.g. the benzene. The following is an extract from [5].

Definition 2.1. For $\gamma = (c_1, \ldots, c_N) \in \mathbb{C}^N$, we call

$$C = \operatorname{circ}\gamma = \operatorname{circ}(c_1, \ldots, c_N) = \begin{pmatrix} c_1 & c_2 & \cdots & c_N \\ c_N & c_1 & \cdots & c_{N-1} \\ \cdots & \cdots & \cdots & \cdots \\ c_2 & c_3 & \cdots & c_1 \end{pmatrix}$$

a *circulant matrix* (or a circulant). Also, putting

$$\pi = \begin{pmatrix} \mathbf{e}_2' \\ \mathbf{e}_3' \\ \vdots \\ \mathbf{e}_1' \end{pmatrix}$$

we call it the *shift forward matrix* (which plays a fundamental role in the theory of circulant matrices), where $\mathbf{e}_k' = (\delta_{k,1}, \cdots, \delta_{k,n})$ with $\delta_{k,\ell}$ denoting the Kronekcer symbol, are fundamental unit vectors (π is for push). Using this, we conclude that $C = c_1 + c_2\pi + \cdots + c_N\pi^{N-1}$. Viewing this as a polynomial, we call

$$p_\gamma(z) = c_1 + c_2 z + \cdots + c_N z^{N-1} \tag{2.1}$$

a *representor* of C.

Note that $n \times n$ circulant matrices are matrix representations of the group ring over $\mathbb{C}$ or $\mathrm{GF}(q)$ as the case may be, of the underlying cyclic group ([14]). E.g., $\{\pi, \pi^2, I\}$ is the matrix representation of the group ring $\mathbb{C}[<r>]$, where

$$\pi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{2.2}$$

and $r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ is the rotation by $\frac{\pi}{3}$.

Letting $\zeta = \zeta_N$ be a primitive N-th root of 1, we define the *Fourier matrix* F by means of its conjugate transpose F^*:

$$F^* = \frac{1}{\sqrt{N}} \left(\zeta^{(i-1)(j-1)} \right) = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \zeta & \cdots & \zeta^{N-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \zeta^{N-1} & \cdots & \zeta^{(N-1)(N-1)} \end{pmatrix}. \tag{2.3}$$

Theorem 2.1. ([5, Theorem 3.2.2, p. 72]) *Any circulant matrix C can be diagonalized as*

$$C = F^* \Lambda F \tag{2.4}$$

by the Fourier matrix F, where

$$\Lambda = \Lambda_C = \begin{pmatrix} p_\gamma(1) & 0 & \cdots & 0 \\ 0 & p_\gamma(\zeta) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & p_\gamma\left(\zeta^{N-1}\right) \end{pmatrix}. \tag{2.5}$$

Thus, in particular, the eigenvalues of C are $p_\gamma(1)$, $p_\gamma(\zeta)$, …, $p_\gamma(\zeta^{n-1})$.

Corollary 2.1. ([5, (3.2.14), p. 75])

$$\det C = \det(\operatorname{circ} \gamma) = \prod_{j=0}^{N-1} p_\gamma(\zeta^j), \tag{2.6}$$

where $p_\gamma(z)$ is the representor of $\operatorname{circ} \gamma$ *defined by* (2.1).

Proof of Theorem 2.1 follows verbatim to that of Theorem 3.2.2 in [5] since it is a consequence of Theorem 3.2.1 asserting the diagonalization of π:

$$\pi = F^* \Omega F, \tag{2.7}$$

where

$$\Omega = \Omega_C = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \zeta & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \zeta^{N-1} \end{pmatrix}. \tag{2.8}$$

From (2.8), (2.4) follows as in [5, (3.2.2)]:

$$C = \operatorname{circ}\gamma = p_\gamma(\pi) = p_\gamma(F^* \Omega F) = F^* p_\gamma(\Omega) F = F^* \Lambda F, \tag{2.9}$$

where we note a typo in [5] in which Ω is written as π.

Proof of Theorem 1.1. We apply Theorem 2.1 with $c_j = \hat{a}_{j-1}$. Then the representor in (2.1) is

$$p_\gamma(\zeta^{j-1}) = \hat{a}_1 + \hat{a}_2\zeta^{j-1} + \cdots + \hat{a}_N\zeta^{(j-1)(N-1)}, \tag{2.10}$$

which is a_{j-1} by (1.2). Hence the rank of $M(\mathbf{a})$ is the number of non-zero components in $\mathbf{a}$, i.e. $w(\mathbf{a})$, completing the proof. ■

Cf. another proof using results of Massey in §3.

Corollary 2.1 has been extensively used. E.g. in [12], the determinant $\det((a, a+h, \cdots, a+(N-1)h)$ has been evaluated, which turns out to be [5, Exercise 4, p. 80]. Another example appears with regard to the determinant expression for the class number of imaginary quadratic fields (cf. §5 below).

3. Shift-register synthesis

In [11], the Blahut theorem over a commutative ring (with a primitive root of 1) is stated in terms of the length of shortest linear feedback shift register (LFSR), which in turn is the linear complexity of the relevant sequence. In that paper, the Fourier matrix (2.3) appears as the Vandermonde matrix M_ζ ([11, (5)]).

An LFSR R of length L (an L-stage LFSR) is a cascade of L unit delay cells–stages–whose contents are to combine linearly to form the input into the first stage. The output of the LFSR is to be taken from the last stage and the initial contents $s_0, s_1, \cdots, s_{L-1}$ of the L stages are to coincide with the first L output digits and the remaining output digits are uniquely assigned by the recurrence

$$s_j + \sum_{i=1}^{L} c_i s_{j-i} = 0, \quad j = L, L+1, \cdots, \tag{3.1}$$

where c_j's are feedback coefficients which lie in a fixed field as with the outputs s_j's. With these coefficients, we form the *connection polynomial* $C(X)$ in the indeterminate X of the LFSR by

$$C(X) = \sum_{j=0}^{L} c_j X^j. \tag{3.2}$$

An LFSR R is said to *generate* a finite sequence $\mathbf{s} = \{s_0, s_1, \cdots, s_{N-1}\}$ if the first N output digits of R for some initial loading coincides with $\mathbf{s}$. If

$L \geq N$, then R generates $\mathbf{s}$, while if $L < N$, then R generates $\mathbf{s}$ if and only (3.1) holds for $j = L, L+1, \cdots, N-1$. Let $S(X)$ be the Huffman X-transform ([11, (16)])

$$S(X) = \sum_{j=0}^{\infty} s_j X^j, \tag{3.3}$$

which is therefore a *generating power series* of the periodically repeated sequence $\mathbf{s}^\infty = \mathbf{s}, \mathbf{s}, \cdots$.

Let $\mathbf{s} = (s_0, \cdots, s_{N-1}) \in F^N$. We recall the definition of the *linear complexity* of $\mathbf{s}^\infty$ (cf. [16]). It is the smallest non-negative integer L such that (3.1) holds true, whence in the terminology of LFRS, it is the length of the shortest LFSR ([10]). For this notion, cf. e.g. [16], [17].

A fundamental result is the following ([10, Corollary to Theorem 4]). Let $\mathcal{R}$ denote a commutative ring in which there is a primitive N-th root of 1.

Lemma 3.1. *If the Huffman transform of the sequence* $\mathbf{s}$ *is of the form* $S(X) = \frac{P(X)}{C(X)}$, *where* $P, C \in \mathcal{R}$ *are relatively prime polynomials with* $C(0) = 1$, *then* $C(X)$ *is the connection polynomial of the shortest LFRS that generates* $\mathbf{s}$ *and its length is* $\max\{\deg C(X), \deg P(X) + 1\}$.

Theorem 3.1. (Massey's version of the Blahut theorem) *If* ζ *generates a DFT* ($\mathbf{s} = \mathrm{DFT}(\mathbf{a})$) *of length* N *in* $\mathcal{R}$, *then the linear complexity of the periodically repeated sequence* $\mathbf{s}^\infty$ *is equal to the Hamming weight* $w(\mathbf{a})$ *of* $\mathbf{a}$.

Corollary 3.1. *If* ζ *generates a DFT* ($\mathbf{s} = \mathrm{DFT}(\mathbf{a})$) *of length* N *in* $\mathcal{R}$, *then the linear complexity of the periodically repeated sequence* $\mathbf{s}^\infty$ *is equal to the rank of the DFT matrix* $M(\mathbf{a})$ *of* $\mathbf{a}$ *defined by* (1.3).

In the sequel we shall introduce some basics of linear recurrence sequences whose main result is the expression of the solutions according to Theorem 3.2 below.

A sequence $\mathbf{s} = \{s_n\}$ is said to be a linear recurrence sequence of order L if it satisfies the recurrence (3.1), where c_j's are coefficients. Therefore the sequence is uniquely determined by the initial terms $\{s_0, \cdots, s_{L-1}\}$. We suppose that $c_0 = 1$ and $c_L \neq 0$. The former is a normalization while the latter is a natural restriction not incorporated in [11]. For otherwise, in (3.1) the highest term would be c_{L-1}, which could be named by c_L. This restriction removes the maximum condition in Massey's version of the linear complexity since the $\deg P < L$. Let $S(X)$ denote the generating power series (3.3) for $\mathbf{s}$.

Theorem 3.2. *Suppose the connection polynomial* (3.2) *decomposes as*

$$C(X) = \sum_{j=0}^{L} c_j X^j = \prod_{i=1}^{q} (1 - \omega_i X)^{\sigma_i}, \tag{3.4}$$

where ω_i*'s are distinct and* $\sum_{i=1}^{q} \sigma_i = L$*. Then*

1. *All the solutions to the recurrence equation* (3.1) *form an* s*-dimensional subspace* $\mathcal{V}$ *of the vector space* $\mathbb{C}^L$ *and its basis* $\{\omega_i\}$*'s can be extended to a basis of* $\mathbb{C}^L$ *and the elements of* $\mathcal{V}$ *are given as in* (3.5)*.*

2. $\mathbf{s} = \{s_n\}$ *is a linear recurrence sequence if and only if its generating power series is a rational function:* $S(X) = \frac{P(X)}{C(X)}$*, where* $P(X)$ *is a polynomial of degree* $< L$*.*

3. *There exist unique polynomials* $f_i(z) \in \mathbb{C}(s_i, c_i, \omega_i)[z]$ *of degree* $< \sigma_i$ $(1 \leq \leq i \leq s)$ *such that*

$$s_j = \sum_{j=1}^{q} f_i(j)\omega_i^j \quad (j = 0, 1, \cdots). \tag{3.5}$$

Proof. We shall prove 2 and 3. Suppose (3.1) holds. Then

$$C(z)S(z) = \sum_{j=0}^{L-1} \left(\sum_{i=0}^{j} c_i s_{j-i} \right) z^j + \sum_{j=L}^{\infty} \left(s_j + \sum_{i=0}^{L-1} c_i s_{j-i} \right) z^j, \tag{3.6}$$

so that the only first summand remains, which is a polynomial, say $P(z)$, whose degree $< L$. Hence the assertion follows.
Conversely, if $C(z)S(z) = P(z)$ holds for a polynomial whose degree $< L$, then in the expansion of $C(z)S(z)$, all the terms with z^m, $m \geq L$ must vanish, which means we have (3.1), and the converse is also true.

Regarding the expression, we appeal to the partial fraction expansion (3.13) in the form

$$S(z) = \sum_{i=1}^{q} \sum_{j=1}^{\sigma_i} b_{i,j} \frac{1}{(1 - \beta_i z)^j}. \tag{3.7}$$

Then by the binomial expansion,

$$S(z) = \sum_{i=1}^{q} \sum_{j=1}^{\sigma_i} b_{i,j} \sum_{m=0}^{\infty} \binom{-j}{m} (\beta_i z)^m. \tag{3.8}$$

Then applying the identity $\binom{-j}{m} = \binom{m+j-1}{m}$ and changing the order of summation, we transform (3.8) into

$$S(z) = \sum_{m=0}^{\infty} \sum_{i=1}^{q} \sum_{j=1}^{\sigma_i} b_{i,j} \binom{m+j-1}{m} {\beta_i}^m z^m. \tag{3.9}$$

Comparing the coefficients, we immediately deduce (3.5), completing the proof. ■

Another proof of Theorem 3.2, 1. Assuming the existence of the inverse operator as in the case of Laplace transforms, we may argue as follows, in which we omit the identity operator symbol. We think of the solutions of (3.10) as the result operated the inverse operator on 0, i.e. we find $\{y_n\}$ such that

$$0 = (E-\alpha)y_n = y_{n+1} - \alpha y_n. \tag{3.10}$$

This gives rise to $y_n = a_0\alpha^n$, a geometric sequence.

In the case of a double root, we make a small trick: We express the 2nd order linear recurrence

$$0 = (E-\alpha)^2 y_n = y_{n+1} - y_n = y_{n+2} - 2\alpha y_{n+1} + \alpha^2 y_n \tag{3.11}$$

as $(z_n = y_{n+1} - y_n)$

$$z_{n+1} = \alpha z_n,$$

whence $z_n = a_0\alpha^n$. Hence $y_{n+1} = \alpha y_n + a_o\alpha^n$ and inductively, we deduce that

$$y_n = y_0\alpha^n + a_0 n\alpha^n. \tag{3.12}$$

Hence we find a basis $\{\alpha^n, n\alpha^n\}$.

We may now go on inductively until we reach the algebraic multiplicity of the root α. This complete the proof. ■

The following theorem provides us with the partial fraction expansion.

Theorem 3.3. *If the denominator $C(z)$ of the rational function $S(z) = \frac{P(z)}{C(z)}$ is given by* (3.4)*, then*

$$S(z) = \sum_{i=1}^{q} \sum_{j=0}^{\sigma_i - j} a_{k,\sigma_k - j} \frac{1}{(z-\beta_i)^{\sigma_i - j}}, \tag{3.13}$$

where the coefficients are given by

$$a_{i,\sigma_i - j} = \frac{1}{j!} \lim_{z\to\beta_i} \frac{\mathrm{d}^j}{\mathrm{d}z^j} \left((z-\beta_i)^{\sigma_i} R(z) \right). \tag{3.14}$$

Thus it follows that the shortest LFSR synthesis problem amounts to finding the partial fraction expansion of the generating power series.

To illustrate this principle, we prove Theorem 3.1 by Theorem 3.3. To this end, we need the following

Lemma 3.2. *Let ξ denote a primitive N-th root of 1. Then for each fixed i, $0 \le i \le N-1$*

$$\prod_{\substack{j=0 \\ j\neq i}}^{N-1} (\xi^i - \xi^j) = N\xi^{i(N-1)} = N\xi^{-i} \tag{3.15}$$

and as a consequence, we have

$$\prod_{\substack{0\le i,j\le N-1 \\ j\neq i}} (\xi^i - \xi^j) = (-1)^{N-1} N^N. \tag{3.16}$$

Proof. It is known that all the N-th roots of 1 are powers of ξ, so that

$$X^N - 1 = \prod_{j=0}^{N-1} (X - \xi^i). \tag{3.17}$$

Differentiating (3.17), we obtain

$$NX^{N-1} = \sum_{i=0}^{N-1} \prod_{\substack{j=0 \\ j\neq i}}^{N-1} (X - \xi^j). \tag{3.18}$$

Substituting $X = \xi^i$ with fixed i gives (3.15).

To prove (3.16), we multiply (3.15) to obtain

$$\prod_{\substack{0\le i,j\le N-1 \\ j\neq i}} (\xi^i - \xi^j) = N^N \left(\prod_{j=0}^{N-1} \xi^j \right)^N. \tag{3.19}$$

By comparing the constant term of (3.17), we obtain

$$\prod_{j=0}^{N-1} \xi^j = (-1)^{N-1}. \tag{3.20}$$

Substituting (3.20) in (3.19) completes the proof of (3.16), completing the proof. ■

Proof of Theorem 3.1. We use the notation of Massey so that the typos can be noticed easily. For $\mathbf{s} = \mathrm{DFT}(\mathbf{a})$ we write $\mathbf{B} = \mathrm{DFT}(\mathbf{b})$, where $\mathbf{B} = (B[0], \cdots, B[N-1])$ and $\mathbf{b} = (b[0], \cdots, b[N-1])$. It suffices to verify the partial fraction expansion

$$\left(\sum_{n=0}^{N-1} B[n]z^n\right)\frac{1}{1-z^N} = \sum_{n=0}^{N-1}\frac{b[n]}{1-\xi^n z}, \tag{3.21}$$

which is [11, (8)] (Cf. the passage following this proof).

For as given toward the end of the paper [11], writing the right-hand side of (3.21) as $\sum_{\substack{n=0\\ b[n]\neq 0}}^{N-1}\frac{b(n)}{1-\xi^n z} = \frac{P(z)}{C(z)}$, then the polynomial $C(z) = \prod_{\substack{n=0\\ b[n]\neq 0}}^{N-1}\frac{b(n)}{1-\xi^n z}$ is the connection polynomial of the shortest LFSR that generates the periodically repeated sequence $\mathbf{B}^\infty$. By Lemma 3.1, the linear complexity of this sequence is equal to the degree of the connection polynomial $C(z)$, which is the number of non-zero elements $b[n]$, which in turn is the Hamming weight of $\mathbf{b}$, proving Theorem 3.1.

We now turn to the proof of (3.21). First note that (3.17) may be written as

$$z^N - 1 = \prod_{j=0}^{N-1}(z-\xi^{-j}). \tag{3.22}$$

Writing

$$-\left(\sum_{n=0}^{N-1} B[n]z^n\right)\frac{1}{1-z^N} = \sum_{i=0}^{N-1} a_i\frac{1}{z-\xi^{-i}}, \tag{3.23}$$

we obtain by Theorem 3.3

$$a_i = \lim_{z\to\xi^{-i}}\frac{\sum_{n=0}^{N-1}B[n]z^n}{\prod_{j\neq i}(z-\xi^{-j})} = \frac{\sum_{n=0}^{N-1}B[n]\xi^{-in}}{\prod_{j\neq i}(\xi^{-j}-\xi^{-j})}. \tag{3.24}$$

Now the denominator is $N\xi^i$ by Lemma 3.2. Hence (3.23) reads

$$a_i = \xi^{-i}b(i), \tag{3.25}$$

whence (3.23) leads to (3.21), completing the proof. ■

In the proof of [11, Theorem 4] (which is Theorem 3.1), there are some typos, which we point out here. [11, Eq. (10)] should read

$$\frac{P(D)}{C(D)} = \sum_{\substack{n=0\\ b(n)\neq 0}}^{N-1} b[n]\frac{1}{1-\xi^n D} \tag{10}$$

and [11, Eqn. (12)] should read

$$S(D) = \left(B[0] + B[1]D + \cdots + B[N-1]D^{N-1}\right) \frac{1}{1 - D^N}. \tag{12}$$

I.e. [11, Eqn.(8)] should be given as (3.21) with $z = D$.

Proof of Blahut's theorem, Theorem 1.1*, a là Massey's results*

Note that (1.1) reads

$$\hat{\mathbf{a}} = \mathrm{DFT}(\mathbf{a}) = F\mathbf{a} \tag{3.26}$$

while (1.2)

$$\mathbf{a} = \frac{1}{N} F^* \hat{\mathbf{a}}, \tag{3.27}$$

where we view the row vectors as column vectors. Hence we have the following equality for the representor

$$\begin{aligned} p_{\hat{\mathbf{a}}}(z) = \hat{a}_0 + \hat{a}_1 z + \cdots + \hat{a}_{N-1} z^{N-1} &= \sum_{\ell=0}^{N-1} \hat{a}_\ell z^\ell = \sum_{\ell=0}^{N-1} z^\ell \sum_{k=0}^{N-1} a_k \zeta^{-k\ell} \\ &= \sum_{k=0}^{N-1} a_k \sum_{\ell=0}^{N-1} \left(z\zeta^{-k}\right)^\ell = \sum_{k=0}^{N-1} a_k \frac{1 - z^N}{1 - z\zeta^{-k}}, \end{aligned} \tag{3.28}$$

which is [11, (8)]=(3.21) on which the proof hinges. For each fixed $j, 0 \le j \le$ $\le N-1$, we now put $z = \zeta^j$ in the formula above to deduce that

$$p_{\hat{\mathbf{a}}}(\zeta^j) = \hat{a}_0 + \hat{a}_1 \zeta^j + \cdots + \hat{a}_{N-1} \zeta^{(j)(N-1)} = a_j. \tag{3.29}$$

Cf. Theorem 2.1. By the result of Massey, we conclude that $p_{\hat{\mathbf{a}}}(z) = C(z)$, the connection polynomial, whence that the eigen-values of $M(\mathbf{a})$ are $p_{\hat{\mathbf{a}}}(\zeta^j)$, $0 \le j \le N-1$. Hence it follows that the number of non-zero eigen-values is the same as that of non-zero elements in $\mathbf{a}$.

4. Topological matrices of cyclic orbitals

In this section we consider the topological matrix associated to a ring-shaped polyene (cyclo-polyene, typically, hydrocarbons). Letting $H_n(\lambda)$ be the matrix of degree n whose first row, second row, ... are

$$\begin{aligned} &(-\lambda, 1, 0, \ldots, 0, 1), (1, -\lambda, 1, 0, \ldots, 0), \\ &(0, 1, -\lambda, 1, 0, \ldots, 0), \ldots, (1, 0, \ldots, 0, 1, -\lambda), \end{aligned}$$

respectively. Then $H_n(\lambda)$ is the (π-electron) Hückel matrix for a cyclo-polyene by viewing $-\lambda, 1$ as α (Coulomb integral), β (overlapping integral), resp. It may be decomposed as $-\lambda E + T$, where T is the *topological matrix* of the cyclo-polyene consisting of entries

$$(0,1,0,\ldots,0,1)\,,(1,0,1,0,\ldots,0)\,,$$
$$(0,1,0,1,0,\ldots,0)\,,\ldots,(1,0,\ldots,0,1,0)\,,$$

which is a circulant matrix with $\gamma = (0,1,0,\ldots,0,1)$, so that $p_\gamma(z) = z + z^{n-1}$. Cf. [1, Chapter 5, pp. 56-70].

Let $g_n(\lambda) = \det H_n(\lambda)$. Then the solutions of $g_n(\lambda) = 0$ are the eigenvalues of the matrix $\pi + \pi^{-1} (= 2M_1)$, say. Since $p_\gamma(\zeta^j) = \zeta^j + \zeta^{j(n-1)} = \zeta^j + \zeta^{-j} = 2\,\mathrm{Re}\,\zeta^j$, it follows that the eigenvalues are $2\,\mathrm{Re}\,1$, $2\,\mathrm{Re}\,\zeta$, …, $2\,\mathrm{Re}\,\zeta^{n-1} = 2$, $2\cos\frac{2\pi}{n}$, …, $2\cos\frac{2(n-1)\pi}{n}$.

For $n = 4$, the energy levels of the π electrons of 1,3-cyclobutadiene are

$$2, 2\cos\frac{2\pi}{4}, 2\cos\pi, 2\cos\frac{6\pi}{4} = 2, 0, -2, 0,$$

while those for benzene are

$$2, 2\cos\frac{2\pi}{6}, 2\cos\frac{4\pi}{6}, 2\cos\pi, 2\cos\frac{8\pi}{6}, 2\cos\frac{10\pi}{6} = 2, 1, -1, -2, -1, 1.$$

An (n,k)-*code* C *over* $GF(q)$ is a k-dimensional subspace of $GF(q)^n$. A matrix G is called a **generating matrix** of C if it contains k linearly independent row vectors, which are called **information sets**. Hence, to give an (n,k)-code it suffices to assign a generating matrix. In the case of $GF(2)$, we have the following theorem

Theorem 4.1. *A cyclo-polyene with n hydrogen atoms generates an $(n, n-2)$ linear code with n alphabets and $(n-2)$-dimensional subspace, the number of codewords being 2^{n-2}.*

Subsequently we illustrate Theorem 4.1.

- Cyclo-propenyl radical (cf. e.g. [15, p.153]) has the topological matrix

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \pi + \pi^2, \tag{4.1}$$

with π in (2.2). (4.1) gives rise to the ((3,2)-linear) cyclic code over GF(2):

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

- 1,3-cyclobutadiene gives rise to a $(4,2)$-linear code over GF(2):

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

- Similarly, cyclopentadienylanion and benzene give rise to a $(5,3)$-linear code and ($(6,4)$-linear) code, resp.

For our curiosity, we record the following from [5, Exercises 4,5 p.30], which is to be compared with the case of the Cebyshëv polynomials of the second kind ([3, Chapter 1]).

For a positive integer p, put $2M_p = \pi^p + \pi^{-p}$. Then

$$M_p = M_{n-p},\ M_0 = M_n = E\,(\text{unit matrix}),\ 2M_pM_q = M_{p+q} + M_{p-q}.$$

In particular,

$$M_{p+1} = 2M_1M_p - M_{p-1}, \tag{4.2}$$

whence comparing this with the recurrence satisfied by the Cebyshëv polynomials T_p of the first kind, we deduce that

$$M_p = T_p\,(M_1)\,. \tag{4.3}$$

5. Relation to the class number

With respect to the notion of Maillet determinant, the circulant matrices appeared, cf. e.g. [6, pp.14-15]. We confine to the specific example. Let p be an odd prime and let $r = \frac{p-1}{2}$. Let $R'(a)$ denote the absolutely smallest residue of a mod p, i.e. $R'(a) \equiv a\,(\mathrm{mod}\,p)$, $-r \le R'(a) \le r$. For a prime to p let $S(a) = (-1)^{R'(a)}$ and let $S_p = (S(ab'))_{1\le a,b\le r}$, where b' is the inverse of b mod p which exists because a, b are relatively prime to p.

Now let g be a primitive root modulo p and for $j \ge 0$ let g_j be denote an integer such that $1 \le g_j \le p-1$, $g_j \equiv g^j\,(\mathrm{mod}\,p)$. Further let

$$a_j = \begin{cases} \frac{1}{2}g_j & g_j \equiv 0\,(\mathrm{mod}\,2) \\ \frac{1}{2}(g_j - p) & g_j \equiv 1\,(\mathrm{mod}\,2) \end{cases}$$

and $s_j = (-1)^{a_j}$. Then (s_{i+j}), where $1 \le i, j \le r$ is a circulant matrix and its determinant can be expressed as (2.6), which is stated as Eq. (5) in [6, p.17]. It is proved ([6, (2), p.15]) that

$$|S_p| = |\det(s_{i+j})|.$$

Then by [6, (5), p.17], for $11 < p \equiv 3\,(\mathrm{mod}\,4)$, the equivalence of $S_p \equiv 0\,(\mathrm{mod}\,p)$ and $\sum_{a=1}^{\frac{p-3}{4}} a^{2j} \equiv 0\,(\mathrm{mod}\,2)$ for some $5 \le j \le \frac{p-3}{2}$, which is known to be equivalent to χ-irregularity.

This reminds us of one of equivalent formulations of Chowla's problem of giving an elementary proof of the non-vanishingness of $L(1,\chi)$, with $L(s,\chi)$ being the Dirichlet L-function with the Dirichlet character χ. We hope to return to the study of this problem at another occasion.

References

[1] **Andrews, J.G. and R.R. McLone,** *Mathematical Modelling*, Butterworths, Londodn 1976.

[2] **Auslander, L., R. Tolimieri, and S. Winograd,** Hecke's theorem in quadratic reciprocity, finite nilpotent groups and the Cooley-Tuckey algorithm, *Adv. Math.*, **42** (1982), 123–172.

[3] **Chakraborty, K., S. Kanemitsu and H. Tsukada,** *Vistas of Special Functions II*, World Sci., New Jersey-London-Singapore etc. 2009.

[4] **Cooley, J.W. and J.W. Tuckey,** An algorith for machine calculation of complex Fourier series, *Math. Comp.*, **19** (1965), 297–301.

[5] **Davis, Ph.J.,** *Circulant Matrices,* Wiley New York etc. 1979.

[6] **Endô, A.,** The relative class numbers of certain imaginary abelian number fields and determinants, *J. Number Theory*, **34** (1990), 13–20.

[7] **Kanemitsu, S. and H. Tsukada,** *Vistas of Special Functions,* World Sci.. New Jersey-London-Singapore etc. 2007.

[8] **Kanemitsu, S. and M. Waldschmidt,** Matrices for finite Abelian groups, finite Fourier transforms and codes, in: *Arithmetic in ShangriLa*, Proc. 6th China-Japan Sem. Number Theory, World Sci., London etc. 2012, 90–106.

[9] **Kutzuko, Ph.C.,** The cyclotomy on finite commutative P.I.R's, Ill., *J. Math.*, **19** (1976), 1–17.

[10] **Massey, J.L.,** Shift-register systhesis and BCH decoding, *IEEE Trans. on Info. Th. IT-15* (1969), 122–127.

[11] **Massey, J.L.,** The discrete Fourier transform in coding and cryptography, IEEE Inform. *Theory Workshop ITW 98, San Diego* (1998), 9–11.

[12] **Waldschmidt, M.,** Proof of a conjecuture of Alladi Ramakrishnan, in: *The legacy of Alladi Ramakrishnan in the mathematical sciences*, ed. by K. Alladi, J. Klauder, C. R. Rao, Springer, Berlin-Heidelberg-New York 2010, 329–334.

[13] **Weaver, H.J.,** *Applications of Discrete and Continuous Fourier Transforms, Wiley,* New York etc. 1983.

[14] **Wilde, A.C.,** Algebras of operators isomorphic to the circulant algebra, *Proc. Amer. Math. Soc.*, **105** (1989), 808–818.

[15] **Yoshida, M.,** *How to Utilize the Molecular Orbital Method, 2nd ed.*, Tokyo Kagaku-dohjin, Tokyo 1986.

[16] **Zheng, J.-R. and T. Kaida,** On linear complexity and Schaub bound for cyclic codes by defining sequence with unknown coefficients, *IEICE Trans.*, (Fund. E89A), No. **9** (2006), 2337–2340.

[17] **Zheng, J.-R. and T. Kaida,** A note on the shift bound for cyclic codes by the DFT, *IEICE Trans.* (Fund. E93A), No. **11** (2010), 1918–1922.

L. Jiang
Director
Dalian Power Tech Co. Ltd
1-4-1, Liang Hua Shan Lu 37,Dalian,116021, Liaoning
China
jiiangli168@hotmail.com

S. Kanemitsu
Graduate School of Advanced Technology
Kinki University
Iizuka, Fukuoka 820-8555
Japan
kanemitu@fuk.kindai.ac.jp

H. Kitajima
Dept. of Intelligence Information Systems
Saga University
Honjo-cho 1, Saga 840-8502
Japan
hitomik1200@yahoo.co.jp