

KATHOLIEKE
UNIVERSITEIT
LEUVEN

PERIODIC COARSE-GRAINING INVARIANT SEQUENCES

André Barbé Fritz von Haeseler

SCD/SISTA report nr. 04-224
December 2004

TOEGEPASTE WETENSCHAPPEN
Departement Elektrotechniek (ESAT-SCD)
Kasteelpark Arenberg, 10
B3001 Leuven /Heverlee - Belgium

Periodic coarse graining invariant sequences

A. Barbé, F. von Haeseler

K.U. Leuven, Department of Electrical Engineering
Kasteelpark Arenberg 10
B 3001 Leuven

Abstract

We introduce a general notion of coarse graining invariant sequences. Particular attention is payed to periodic coarse graining invariant sequences. We establish criteria for the existence of these sequences.

1 Introduction: Coarse graining invariant sequences

In the following $\mathbb{F}$ denotes a finite field of characteristic p. k denotes an integer with $|k| \geq 2$, and W denotes a complete residue set w.r.t. k, i.e., W is such that for every $x \in \mathbb{Z}$ there exist unique $\zeta(x) \in W$ and $\kappa(x) \in \mathbb{Z}$ such that

$$x = \zeta(x) + k\kappa(x).$$

The maps $\zeta : \mathbb{Z} \to W$ and $\kappa : \mathbb{Z} \to \mathbb{Z}$ are called *residue-map* and *image-part-map*, respectively. Note that $\kappa(kx + w) = x$ for all $x \in \mathbb{Z}$. The "natural" residue set w.r.t. k is $Z_k = \{0, 1, \ldots, |k| - 1\}$, and in general, any residue set W can be written as $W = \{i + k\nu_i \mid i \in Z_k\}$, with $\nu_i \in \mathbb{Z}$.

A sequence f is a map from $\mathbb{Z}$ to $\mathbb{F}$ and the set of sequences is denoted as $\mathbb{F}^{\mathbb{Z}}$.

Definition 1.1 *[cgi] Let $\Lambda \subset \mathbb{Z}$ be a finite set and $c : \Lambda \to \mathbb{F} \setminus \{0\}$. A sequence $f \in \mathbb{F}^{\mathbb{Z}}$ is called* coarse graining invariant *(CGI) w.r.t. the quadruplet (k, W, Λ, c) if*

$$[1]f(x) = \sum_{\lambda \in \Lambda} c(\lambda) f(H(x) + w + \lambda) \tag{1}$$

(arithmetic operations in $\mathbb{F}$) holds for all $x \in \mathbb{Z}$ and for all $w \in W$.

The collection of equations in the above definition is called CGI-equations. Using the image-part map, it can be shown that a sequence f is CGI if

$$[2]f(\kappa(x)) = \sum_{\lambda\in\Lambda} c(\lambda)f(x+\lambda) \tag{2}$$

holds for all $x \in \mathbb{Z}$.

Since the constant sequence $f(x) = 0$ $(x \in \mathbb{Z})$ is always a CGI-sequence, we will from now on only consider nontrivial CGI-sequences.

We present yet another description of CGI-sequences by using the notion of formal Laurent series.

To this end we consider the set $\mathbb{F}(X)$ with elements $f(X) = \sum_{j\in\mathbb{Z}} f_j X^j$. The support, $\mathrm{supp}(f)$, of f is the set $\mathrm{supp}(f) = \{j \mid f_j \neq 0\}$ and we say that f is a polynomial if $\mathrm{supp}(f)$ is a finite set.

For $v \in \mathbb{Z}$ we denote the decimation $\partial_w : \mathbb{F}(X) \to \mathbb{F}(X)$ w.r.t. H as the map

$$\partial_v(f)(X) = \sum_{j\in\mathbb{Z}} f_{H(j)+v} X^j.$$

In other words, if $f \in \mathbb{F}(X)$ is considered as a sequence $f : \mathbb{Z} \to S$, then $\partial_v(f)$ considered as a sequence is given as

$$\partial_v(f)(x) = f(H(x)+v)$$

with $x \in \mathbb{Z}$. Note that if W is a complete residue set for H, then every $f(X) \in \mathbb{F}(X)$ can be written as

$$f(X) = \sum_{w\in W} X^w \partial_w(f)(X^k).$$

The CGI-equations regarded as equations for Laurent series then can be written as

$$f(X) = \sum_{\lambda\in\Lambda} c(\lambda)\partial_{w+\lambda}(f)(X)$$

for all $w \in W$. If we write $w+\lambda = \zeta(w+\lambda)+H(\kappa(w+\lambda))$ then $\partial_{w+\lambda}(f)(X)$ can be written as

$$\partial_{w+\lambda}(f)(X) = \sum_{j\in\mathbb{Z}} f_{\zeta(w+\lambda)+H(j+\kappa(w+\lambda))} X^j$$

and changing the summation index one obtains

$$\partial_{w+\lambda}(f)(X) = X^{-\kappa(w+\lambda)} \sum_{j\in\mathbb{Z}} f_{H(j)+\zeta(w+\lambda)} X^j = X^{-\kappa(w+\lambda)} \partial_{\zeta(w+\lambda)}(f)(X).$$

Thus the CGI-equations in Laurent form become

$$f(X) = \sum_{\lambda \in \Lambda} c(\lambda) X^{-\kappa(w+\lambda)} \partial_{\zeta(w+\lambda)}(f)(X).$$

Theorem 1.2 *[Mahler] If $f : \mathbb{Z} \to \mathbb{F}$ is a CGI-sequence w.r.t. (c, H, W), then the formal Laurent series $f(X)$ satisfies the following equation $Q_W(X) f(X^k) = P_\Lambda(X) f(X)$, where*

$$Q_W(X) = \textstyle\sum_{w \in W} X^w \qquad P_\Lambda(X) = \textstyle\sum_{\lambda \in \Lambda} c(\lambda) X^{-\lambda}$$

Proof: If f is a CGI-sequence, then $f(X)$ satisfies

$$f(X) = \sum_{\lambda \in \Lambda} c(\lambda) X^{-\kappa(w+\lambda)} \partial_{\zeta(w+\lambda)}(f)(X)$$

for all $w \in W$. For $w \in W$, one considers

$$X^w f(X^k) = \sum_{\lambda \in \Lambda} c(\lambda) X^{w-k\kappa(w+\lambda)} \partial_{\zeta(w+\lambda)}(f)(X^k)$$

and observes that $w + \lambda = \zeta(w + \lambda) + k\kappa(w + \lambda)$ to obtain

$$X^w f(X^k) = \sum_{\lambda \in \Lambda} c(\lambda) X^{-\lambda+\zeta(w+\lambda)} \partial_{\zeta(w+\lambda)}(f)(X^k)$$

for $w \in W$. Therefore one has

$$\sum_{w \in W} X^w f(X^k) = \sum_{w \in W} \sum_{\lambda \in \Lambda} c(\lambda) X^{-\lambda+\zeta(w+\lambda)} \partial_{\zeta(w+\lambda)}(f)(X^k)$$

which is the same as

$$\sum_{w \in W} X^w f(X^k) = \sum_{\lambda \in \Lambda} c(\lambda) X^{-\lambda} \left(\sum_{w \in W} X^{\zeta(w+\lambda)} \partial_{\zeta(w+\lambda)}(f)(X^k) \right).$$

Since the sum over $w \in W$ gives $f(X)$, one obtains

$$\left(\sum_{w \in W} X^w \right) f(X^k) = \left(\sum_{\lambda \in \Lambda} c(\lambda) X^{-\lambda} \right) f(X),$$

the desired equation.

■

We thus see that a CGI-sequence satisfies a very special Mahler-equation, and we say that f is a CGI-sequence w.r.t. $(Q_W(X), P(X))$, if

$$Q_W(X)f(X^k) = P(X)f(X),$$

where $P(X)$ has finite support.

Lemma 1.3 *[prop] If f is a CGI-sequence w.r.t. $(Q_W(X), P(X))$, then*

1. *f is a CGI-sequence w.r.t. $(X^tQ_W(X), X^tP_\Lambda(X))$ and $t \in \mathbb{Z}$,*
2. *the sequence $g(X) = X^tf(X)$ is a CGI-sequence w.r.t. $(Q_W(X), X^{(k-1)t}P_\Lambda(X))$.*

The proofs are immediate. Using this lemma we can achieve a kind of normal form for CGI-equations. If F is a CGI-sequence w.r.t. $(Q_W(X), P(X))$ and $W = \{w_0 < w_1 < \ldots < w_{k-1}\}$ then 1. of Lemma 1.3 implies that f is a CGI-sequence w.r.t. $(Q(X), X^{-w_0}P(X))$, where

$$Q_{W'}(X) = X^0 + X^{w_1-w_0} + \ldots + X^{w_{k-1}-w_0}$$

and $W' = \{0, w_1 - w_0, \ldots, w_{k-1} - w_0\}$. Using 2. of Lemma 1.3 and setting $f(X) = X^sg(X)$, the CGI-equation for $g(X)$ becomes

$$Q_{W'}(X)g(X^k) = x^{-w_0}P(X)X^{s-ks}g(X),$$

and by a proper choice of $s \in \mathbb{Z}$ one can ensure that the support of $P'(X) = x^{-w_0}P(X)X^{s-ks}$ is in $\mathbb{N}$, where the power of first non zero coefficient of $P'(X)$ is as small as possible.

2 Periodic CGI-sequence

In this section we present necessary criteria for a CGI-sequence to be periodic.

A sequence $f \in \mathbb{F}^{\mathbb{Z}}$ is called periodic if there exists a $D \in \mathbb{N}$, $D \geq 1$, such that

$$f(x) = f(x + D)$$

for all $x \in \mathbb{Z}$. The smallest D with this property is called the *minimal* period of f. If f is a periodic sequence of period D, then f is given by a map $g : \mathbb{Z}_D \to \mathbb{F}$, where $\mathbb{Z}_D = \{0, 1, \ldots, D-1\}$ and $f(x) = g(i)$ if and only if $x \equiv i \bmod D$.

If f is a CGI-sequence w.r.t. (k, W, Λ, c) and if f has period D then f is given by a map $g : \mathbb{Z}_D \to \mathbb{F}$ and the CGI-equations for f transform into equations for g, namely, for all $s \in \mathbb{Z}_D$ one has

$$[3]g(s) = \sum_{[\lambda']\in\Lambda^*} d(\lambda')g(ks + w + \lambda')_D, \tag{3}$$

where $\Lambda^* = \Lambda/(D)$, i.e., the equivalence classes of Λ modulo D and

$$[4]d(\lambda') = \sum_{\lambda\in[\lambda']} c(\lambda), \tag{4}$$

and where the sum $(ks+w+\lambda')_D$ is considered modulo D, which is indicated by $(\ )_D$.

A first result concerns the possible period of a CGI-sequence. Since decimation invariant sequences, see [3, 4], are a special case of coarse graining invariant sequences, it is not surprising that the necessary conditions for the existence of periodic CGI-sequences are the same as for decimation invariant sequences.

Theorem 2.1 *[gcd=1] Let f be a CGI-sequence. If f has minimal period D, then* $\gcd(D, k) = 1$.

Proof: Since f is a periodic CGI-sequence the map $g : \mathbb{Z}_D \to \mathbb{F}$ associated with f satisfies equation (3), i.e.,

$$g(s) = \sum_{[\lambda']\in\Lambda^*} d(\lambda')g(ks + w + \lambda')_D$$

for all $s \in \mathbb{Z}_D$ and all $w \in W$. Now assume that $\gcd(D, k) = \delta > 1$. Then replacing s by $s + D/\delta$ this equation becomes

$$[4]g(s + D/\delta) = \sum_{[\lambda']\in\Lambda^*} d(\lambda')g(ks + D/\delta + w + \lambda')_D. \tag{5}$$

Since $k(s+D/\delta) = ks+rD$, where $r = k/\delta$ is an integer, and since $g(s+D) = g(s)$, (5) transforms into

$$g(s + D/\delta) = \sum d(\lambda')g(ks + w + \lambda')_D$$

and, by (3), the sum is equal to $g(s)$. This shows that $g(s + D/\delta) = g(s)$ for all $s \in \mathbb{Z}_D$. In other words, f has period $D/\delta < D$, which is a contradiction to the minimality of D. This proves that $\gcd(D, k) = 1$.

■

The next theorem provides an additional necessary condition for periodic CGI-sequences. With $W-W$ we denote the set $W-W = \{v-w \mid v, w \in W\}$.

Theorem 2.2 *[gcd2] Let f be a CGI-sequence with minimal period D. Then D is a divisor of* $\gcd(W-W)$.

Proof: As we have already seen (Theorem 2.1), the map $g : \mathbb{Z}_D \to \mathbb{F}$ associated with f satisfies equation (3)

$$g(s) = \sum_{[\lambda']\in\Lambda^*} d(\lambda')g(ks+w+\lambda')_D$$

for all $s \in \mathbb{Z}_D$ and all $w \in W$. This sum can also be written as

$$g(s) = \sum_{j\in\mathbb{Z}_D} d'(j)g(ks+w+j)_D,$$

where $d'(j) = 0$ if $[j] \notin \Lambda^*$ and $d'(j) = d(j)$ if $[j] \in \Lambda^*$. Changing the summation index, one obtains

$$[5]g(s) = \sum_{j\in\mathbb{Z}_D} d'(j-ks-w)_D g(j) \tag{6}$$

holds for all $s \in \mathbb{Z}_D$ and all $w \in W$. Due to the fact that $\gcd(D,k) = 1$, there exists $k^{-1} \in \mathbb{Z}_D$ such that $k^{-1}k \equiv 1 \bmod D$. For $v \in W$ the above sum can be rewritten as

$$g(s) = \sum_{j\in\mathbb{Z}_D} d'(j-k(s+k^{-1}(v-w))-w)_D g(j).$$

By equation (6), one sees that

$$g(s+k^{-1}(v-w))_D = \sum_{j\in\mathbb{Z}_D} d'(j-k(s+k^{-1}(v-w))-w)_D g(j).$$

This implies that $g(s) = g(s+k^{-1}(v-w))_D$. This means that g has period $(k^{-1}(v-w))_D$. Since D was supposed the minimal period, it follows that $k^{-1}(v-w) \equiv 0 \bmod D$ for $v, w \in W$ implying that D divides $\gcd(W-W)$.

■

Remark We remark in passing that the condition D divides $\gcd(W-W)$ in connection with the fact that W is a complete residue set for k implies that $\gcd(D,k)=1$. Indeed, the elements of W may be written as $w_i = k\nu_i + i$, where $i = 0,\ldots,k-1$. As D divides $\gcd(W-W)$, it follows that

$$k(\nu_i - \nu_j) + i - j \equiv 0 \bmod D$$

for all $i,j \in \{0,\ldots,k-1\}$. Assuming that $\gcd(D,k) = \delta > 1$would imply that

$$i - j \equiv 0 \bmod \delta$$

for all $i,j \in \{0,\ldots,k-1\}$. This is impossible if W is a complete residue set.

As $(j-ks-w_1)_D = (j-ks-w_2)_D$ for $w_1, w_2 \in W$ under the condition that D divides $\gcd(W_W)$, we obtain the following Corollary to Theorem 2.2

Corollary 2.3 *[tot] Let f be a CGI-sequence of period D. Then the map $g : \mathbb{Z}_D \to \mathbb{F}$ satisfies*

$$g(s) = \sum_{j\in\mathbb{Z}_D} d'(j-ks-w)_D g(j)$$

for all $s \in \mathbb{Z}_D$ and one $w \in W$.

Notice that, in terms of the original CGI-equations (1)

$$[6]d'(j-ks-w)_D = \sum_{\lambda\in[(j-ks-w)_D]} c(\lambda). \tag{7}$$

The corollary actually means that the vector $(g(s))_{s\in\mathbb{Z}_D}$ has to be a fixed point of the $\mathbb{F}$-linear map $A : \mathbb{F}^D \to \mathbb{F}^D$ where $A = (a_{s,i})_{s,i\in\mathbb{Z}_D}$ is given as

$$[gl3]a_{s,i} = d'(i-ks-w)_D = \sum_{\lambda\in[(j-ks-w)_D]} c(\lambda) \tag{8}$$

for s, $i \in \mathbb{Z}_D$ and some $w \in W$. As a consequence of this observation we note

Lemma 2.4 *[eigen] Let D divide $\gcd(W-W)$. If the matrix A as defined in equation (8) has 1 as eigenvalue, then the CGI-equations induced by (k,W,Λ,c) have a nontrivial periodic solution.*

Unfortunately, even if 1 is an eigenvalue of A, the above lemma does not guarantee that the minimal period of a periodic CGI-sequence is equal to D. In fact, it may be a divisor of D.

A closer look at the matrix A reveals that

$$a_{s,i} = a_{s-1,i-k}$$

holds for all s, $i \in \mathbb{Z}_D$, where the subscripts are reduced modulo D. This shows that A is a $(k)_D$-circulant matrix of size D, see [1, 10]. If $A \in \mathbb{F}^{D\times D}$ is a $(k)_D$-circulant matrix, then A is uniquely determined by its top row denoted as $(a_0, \ldots, a_{D-1})$. This implies that $\lambda = a_0 + \ldots + a_{D-1}$ is always a eigenvalue of A, with corresponding eigenvector the column vector consisting of D 1's. In view of Lemma 2.4, $\lambda = a_0 + \ldots + a_{D-1} = 1$ guarantees the existence of a periodic CGI-sequence which alas has period 1.

Due to the fact that A is circulant, one can under certain conditions compute the eigenvalues of the matrix A. However, since the results on eigenvalues of $(k)_D$-circulant matrices presented in [1] are valid for the field $\mathbb{C}$, certain restrictions apply in the case of a finite field.

We remind the reader of the notion of the cyclotomic field, see [13], p.63. The D-th cyclotomic field, denoted $\mathbb{F}^{(D)}$, is the splitting field of the polynomial $x^D - 1$ over the field $\mathbb{F}$. The roots of $x^D - 1$ in $\mathbb{F}^{(D)}$ are called the D-roots of unity over $\mathbb{F}$. Of particular interest is the case where the characteristic of $\mathbb{F}$ does not divide D. Then the roots of unity are given as ζ^j with $j = 0, \ldots, D-1$ (Theorem 2.42 in [13]).

To state the next theorem, we note that due to the fact that $\gcd(D, k) = 1$ the map $h : \mathbb{Z}_D \to \mathbb{Z}_D$, $h(s) = (ks)_D$ is a bijection. This means that h is an element of the symmetric group of the set $\mathbb{Z}_D$, i.e., h is a permutation. Therefore h can be written as a product of different disjoint cycles, i.e.,

$$h = (0)(s_1, h(s_1), \ldots, h^{l_1-1}(s_1)) \ldots (s_t, h(s_t), \ldots, h^{l_t-1}(s_t)) = (0)\pi_1\pi_2 \ldots \pi_t,$$

see e.g., [11].

Lemma 2.5 *[circ] Let* $\gcd(D, k) = 1$ *and let* D *be not be divisible by the characteristic of* $\mathbb{F}$. *If* $A \in \mathbb{F}^{D\times D}$ *is a* $(k)_D$*-circulant matrix with top row* $(a_0, \ldots, a_{D-1})$ *and let* $(0)\pi_1\pi_2 \ldots \pi_t$ *be the cycle representation of* $h : \mathbb{Z}_D \to \mathbb{Z}_D$. *The characteristic polynomial* $\chi_A(x)$ *of* A *is given by*

$$[7]\chi_A(X) = (x - \mu_0) \prod_{j=1}^{t} \left(x^{l_j} - \prod_{i=0}^{l_j-1} \mu_{h^i(s_j)} \right), \tag{9}$$

where

$$[8]\mu_m = \sum_{i=0}^{D-1} a_i \zeta^{im}. \tag{10}$$

The proof is basically a copy of the proof of Theorem 1 in [1] using the fact that the matrix $(\zeta^{ij})_{i,j\in\mathbb{Z}_D} \in (\mathbb{F}^{(D)})^{D\times D}$ is invertible. The following example provides an insight of the basic character of the proof.

Example Let the characteristic of $\mathbb{F}$ be 3, let $D = 5$ and let $k = 2$. A 2-circulant matrix A is given as

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_0 & a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 & a_0 & a_1 \end{pmatrix}.$$

The map h with $h(s) = 2s$ on $\mathbb{Z}_5$ has the cycle product $h = (0)(1,2,4,3)$. Now consider the column vectors $e_i = (\zeta^{ij})_{j=0,\ldots,4} \in (F^{(5)})^5$. Then one sees that (all operations in $\mathbb{F}^{(5)}$)

$$Ae_0 = \mu_0 e_0 \quad Ae_1 = \mu_1 e_2 \quad Ae_2 = \mu_2 e_4 \quad Ae_4 = \mu_4 e_3 \quad Ae_3 = \mu_3 e_1,$$

where the μ_j are defined by equation (10). This shows that A w.r.t. the base e_0, e_1, e_2, e_4, e_3 of $(\mathbb{F}^{(5)})^5$ is given as

$$A' = \begin{pmatrix} \mu_0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mu_1 & 0 & 0 \\ 0 & 0 & 0 & \mu_2 & 0 \\ 0 & 0 & 0 & 0 & \mu_4 \\ 0 & \mu_3 & 0 & 0 & 0 \end{pmatrix}.$$

This gives $\chi_A(x) = (x - \mu_0)(x^4 - \mu_1\mu_2\mu_3\mu_4)$. By Lemma 2.4 it follows that a non trivial periodic CGI-sequence exists if $\mu_0 = a_0 + \ldots + a_4 = 1$ or if $\mu_1\mu_2\mu_4\mu_3 = 1$. As we have already seen, the condition $\mu_0 = 1$ leads to the eigenvcetor $(1,1,1,1,1)^T$ and therefore induces a periodic CGI-sequence of period one, i.e., a constant sequence. If $\mu_1\mu_2\mu_4\mu_3 = 1$, then the column vector $(0, \mu_1\mu_2\mu_4\mu_3, \mu_2\mu_4\mu_3, \mu_4\mu_3, \mu_3)^T$ is an eigenvector of A' for the eigenvalue 1. If $B = [e_0 e_1 e_2 e_4 e_3]$ denotes the matrix with columns formed by e_i, then $g = B(0, \mu_1\mu_2\mu_4\mu_3, \mu_2\mu_4\mu_3, \mu_4\mu_3, \mu_3)^T$ satisfies $Ag = g$ and represents a periodic CGI-sequence. Since g and the vector $(1,1,1,1,1)^T$

are linearly independent fixed points of A, it follows that the CGI-sequence induced by g is not the constant sequence. Since 5 is a prime number the induced sequence has period 5.

The observation in the above example can be generalized.

Theorem 2.6 *[ex-per] Suppose the conditions of Lemma 2.5 are satisfied. If* $\prod_{i=0}^{l_j-1} \mu_{h^i(s_j)} = 1$ *for a* $j \in \{1,\ldots,t\}$*, then there exists a CGI-sequence such that its period* δ *is a divisor of* D *and* $\delta > 1$..

Proof: To the factor $x^{l_j} - \prod_{i=0}^{l_j-1} \mu_{h^i(s_j)}$ of the polynomial $\chi_A(x)$ corresponds an invariant subspace V_i of $(\mathbb{F}^{(D)})^D$ of dimension l_j, e.g., [12] Chap.7. If $\prod_{i=0}^{l_j-1} \mu_{h^i(s_j)} = 1$, then there exists a nontrivial eigenvector in V_i with eigenvalue 1. This nontrivial eigenvector is linearly independent of the eigenvector consisting of all ones. Therefore the period of the CGI-sequence corresponding to this eigenvector is greater than 1 and obviously a divisor of D.

■

If the period D in the above lemma is itself a prime number, then the existence of an additional eigenvalue 1 establishes the existence of a periodic CGI-sequence of period D.

Example Let $D = 3$, $k = 7$ and $\mathbb{F}_7$ is the field with seven elements, which are written as $\{0,1,\ldots,6\}$, and with arithmetic operations modulo 7. Then the 3-roots of unity are 2^j, $j = 0,1,2$, i.e., $\mathbb{F}$ is its own 3-rd cyclotomic field. Then A is $(7)_3 = 1$-circulant, i.e.,

$$A = \begin{pmatrix} a_0 & a_1 & a_2 \\ a_2 & a_0 & a_1 \\ a_1 & a_2 & a_0 \end{pmatrix}.$$

The cycle product of $h(s) = 7s$ on $\mathbb{Z}_3$ is given as $h = (0)(1)(2)$, which gives, according to Lemma 2.5, the characteristic polynomial

$$\chi_A(x) = (x - \mu_0)(x - \mu_1)(x - \mu_2)$$

with

$$[9]\mu_0 = a_0 + a_1 + a_2 \quad \mu_1 = a_0 + 2a_1 + 4a_2 \quad \mu_2 = a_0 + 4a_1 + 2a_2 \quad (11)$$

as eigenvalues. The corresponding eigenvectors are

$$(1,1,1)^T \quad (1,2,4)^T \quad (1,4,2)^T.$$

This shows that if $\mu_1 = 1$ or $\mu_2 = 1$, then there exists a CGI-sequence of period 3. The content of the period is determined by the eigenvectors. Consider for example, the CGI-equation

$$[10]f(x) = c(0)f(7s+w)+c(1)f(7s+w+1)+c(2)f(7s+w+2)+c(3)f(7s+w+3), \tag{12}$$

for all $w \in W = \{-9, -6, -3, 0, 3, 6, 9\}$, which indeed satisfies the necessary condition for 3-periodicity given by Theorem 2.2. Then use equation (8), with for example $w = 0$ (but any $w \in W$ will do), to find that

$$a(0) = c(0) + c(3) \quad a(1) = c(1) \quad a(2) = c(2).$$

With the choice $c(0) = c(1) = c(2) = c(3) = 1$ in (12), we see that the μ_j as given by (11) become

$$\mu(1) = 2 + 2.1 + 4.1 = 1 \quad \mu(2) = 2 + 4.2 + 2.1 = 1,$$

implying that the corresponding eigenvectors $(1, 2, 4)^T$ and $(1, 4, 2)^T$ define the nontrivial periodic solutions of the CGI-equation $f(x) = f(7s + w) + f(7s + w + 1) + f(7s + w + 2) + f(7s + w + 3)$. These solutions are

$$\cdots 1\ 2\ 4\ 1\ 2\ 4\ 1\ 2\ 4\ 1\ 2\ 4\ 1\ 2\ 4\ 1\ 2\ 4\cdots$$

and

$$\cdots 1\ 4\ 2\ 1\ 4\ 2\ 1\ 4\ 2\ 1\ 4\ 2\ 1\ 4\ 2\ 1\ 4\ 2\cdots$$

with in both cases a 1 at position $s = 0$.
If, on the other hand, we take $c(0) = 2, c(1) = 3, c(2) = 1, c(3) = 3$ in (12), yielding the CGI-equation $f(x) = 2f(7s + w) + 3f(7s + w + 1) + f(7s + w + 2) + 3f(7s + w + 3)$, then only $\mu(1) = 1$. The only periodic solution is then given by the first of the above sequences.

The above example has again a generalization.

Lemma 2.7 *[1-circ] Suppose the conditions of Lemma 2.5 are satisfied and additionally $k \equiv 1 \bmod D$. If $\mathbb{F}^{(D)}$ is the D-th cyclotomic field with units ζ^j, $j = 0, \ldots, D-1$, then the eigenvalues of A are given as*

$$\mu_j = \sum_{i=0}^{D-1} a_i \zeta^{ij},\ j = 0, \ldots, D-1$$

and the corresponding eigenvectors are given as

$$v_j = (1, \zeta^j, \zeta^{2j}, \ldots, \zeta^{(D-1)j})^T,\ j = 0, \ldots, D-1.$$

In particular, if $\mu_j = 1$ for $j \neq 0$, then there exists a periodic CGI-sequence of period D.

The proof is a direct consequence of Lemma 2.5 and the fact that the cycle representation of h is given as $(0)(1)(2)\cdots(D-1)$.

As the above reasoning indicates, if the characteristic of $\mathbb{F}$ does not divide D, one has a fairly good chance to 'create' CGI-equations which have a periodic solution. Unfortunately, this situation changes if the characteristic of $\mathbb{F}$ divides D. Of course Lemma 2.4 still applies, but there is no easy way to compute the eigenvalues directly from the matrix A.

If A is a 1-circulant matrix, then it is still possible to compute its eigenvalues. In order to formulate a result for this case we introduce some notation. With $P_N = (p_{ij})_{i,j=0,\ldots,N-1}$ we denote the 1-circulant matrix given by $p_{ij} = 1$ if and only if $j \equiv (i+1) \bmod N$, otherwise $p_{ij} = 0$. P_N is called the special 1-circulant matrix (of size N). If A is 1-circulant of size N with top row $(a_0, a_1, \ldots, a_{N-1}$ then A can be written as

$$A = \sum_{j=0}^{N-1} a_j P_N^j.$$

Lemma 2.8 *[help] Let $P_N \in \mathbb{F}^{N\times N}$ be the special 1-circulant matrix. If the characteristic p of $\mathbb{F}$ divides N, i.e., $N = p^\alpha N'$ with $\gcd(N', p) = 1$, then there exists a matrix $U \in (\mathbb{F}^{(N')})^{N\times N}$ such that $U^{-1}PU$ is a block diagonal matrix, i.e.,*

$$U^{-1}P_N U = (\Gamma(\zeta^0), \Gamma(\zeta), \ldots, \Gamma(\zeta^{N'-1})),$$

where $\Gamma(\xi)$ is a Jordan block of size $p^\alpha \times p^\alpha$, i.e., with ξ's on the diagonal and 1's on the superdiagonal.

Proof: The characteristic polynomial of P_N is given as $\chi_{P_N}(x) = x^N - 1$. Since $N = p^\alpha N'$ and since the charcteristic of $\mathbb{F}$ is p, it follows that

$$\chi_{P_N}(x) = (x^{N'} - 1)^{p^\alpha}.$$

This shows that the eigenvalues of P_N are given as the N'-roots ζ^j, $j = 0, \ldots, N'-1$, over $\mathbb{F}^{(N')}$. Now consider $Q_j = (P_N - \zeta^j \mathrm{Id}_N)^{p^\alpha}$ for a $j = 0, \ldots, N'-1$, and Id_N, the identity matrix of size $N \times N$. The matrix Q_j is a circulant block matrix of size $N \times N$, see [10], with top row

$$(-\zeta^{jp^\alpha}\mathrm{Id}_{p^\alpha}, \mathrm{Id}_{p^\alpha}, 0, \ldots, 0),$$

where 0 denotes the zero matrix of size $p^\alpha \times p^\alpha$. With V_j we denote the p^α-dimensional subvectorspace of $\mathbb{F}^{(N')}$ generated by the columns of the matrix

$$M_j = \begin{pmatrix} \mathrm{Id}_{p^\alpha} & \zeta^{jp^\alpha} Id_{p^\alpha} & \zeta^{2jp^\alpha}\mathrm{Id}_{p^\alpha} & \ldots & \zeta^{(N'-1)jp^\alpha}\mathrm{Id}_{p^\alpha} \end{pmatrix}^T.$$

Then one has that $Q_j V_j = \{0\}$. Moreover, one easily computes that $P_N(V_j) = V_j$ and that $(P_N - \zeta^j \mathrm{Id}_n)^{p^\alpha - 1} M_j$ is not a zero matrix. This shows that there exists an element $v \in V_j$, e.g., the first colum of M_j, such that the vectors $(P_N - \zeta^j \mathrm{Id}_n)^s(v)$, $s = 0, \ldots, p^\alpha - 1$ are linearly independent and $P_N : V_j \to V_j$ has a Jordan block with ζ^j on the diagonal as matrix representation. Since $\mathbb{F}^{(N')}$ is the direct sum of V_j, $j = 0, \ldots, N' - 1$, it follows that P_N has the desired matrix representation.

■

Using the above lemma we can compute the eigenvalues of a 1-circulant matrix of size D.

Lemma 2.9 *[1st] Let the characteristic p of $\mathbb{F}$ be a divisor of D, i.e., $D = p^\alpha D'$, $\gcd(p, D') = 1$, and let $k \equiv 1 \bmod D$. If A is a 1-circulant matrix of size D with top row $(a_0, \ldots, a_{D-1})$, then the eigenvalues of A are given as*

$$\mu_j = \sum_{s=0}^{D-1} a_s \zeta^{js},$$

where ζ^j, $j = 0, \ldots, D'$ are the D'-th roots of unity over $\mathbb{F}^{(D')}$.

Proof: Since A is 1-circulant one has that

$$A = \sum_{s=0}^{D-1} a_s P_D^s$$

and according to Lemma 2.8, there exists an $U \in (\mathbb{F}^{(D')})^{D \times D}$ such that

$$U^{-1} P_N^s U = (\Gamma(\zeta^0)^s, \Gamma(\zeta)^s, \ldots, \Gamma(\zeta^{D'-1})^s)$$

for $s = 0, \ldots, D - 1$. Combining these two equations yields the desired result.

■

Example Let $\mathbb{F}$ be a field of characteristic 2 and let $D = 6 = 2 \cdot 3$. Then there exists $U \in (\mathbb{F}^{(3)})^{6 \times 6}$ such that

$$U^{-1} P_6 U = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta & 1 & 0 & 0 \\ 0 & 0 & 0 & \zeta & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta^2 & 1 \\ 0 & 0 & 0 & 0 & 0 & \zeta^2 \end{pmatrix}$$

where $1, \zeta, \zeta^2$ are the roots of unity over $\mathbb{F}^{(3)}$. If A is a 1-circulant matrix with top row $(a_0, \ldots, a_5)$, then the eigenvalues of A are given as

$$\mu_0 = a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = (a_0 + a_3) + (a_1 + a_4) + (a_2 + a_5)$$
$$\mu_1 = a_0 + a_1\zeta + a_2\zeta^2 + a_3 + a_4\zeta + a_5\zeta^2 = (a_0 + a_3) + (a_1 + a_4)\zeta + (a_2 + a_5)\zeta^2$$
$$\mu_2 = a_0 + a_1\zeta^2 + a_2\zeta + a_3 + a_4\zeta^2 + a_5\zeta = (a_0 + a_3) + (a_1 + a_4)\zeta^2 + (a_2 + a_5)\zeta.$$

Applied to the question on the existence of periodic CGI-sequences, we can say that a nontrivial periodic CGI-sequence exists if there is a j such that $\mu_j = 1$. Note that if μ_0, μ_1, and μ_2 are given, then there exist $a_0, \ldots, a_5$ such that A has the given eigenvalues.

We conclude with a special result for k-circulant matrices of size $D = p^\alpha D'$ and $\gcd(k, D) = 1$.

Lemma 2.10 *[special] Let $A \in \mathbb{F}^{D \times D}$ be a k-circulant matrix, and let $\gcd(k, D) = 1$, $D = p^\alpha D'$. If the order of $k \in \mathbb{Z}_D^*$, i.e., the smallest positive number δ with $k^\delta \equiv 1 \bmod D$, is a power of p, then the eigenvalues of A are the same as the eigenvalues of A^δ.*

Proof: The proof is straightforward. Since δ is a power of p, one has

$$\chi_{A^\delta}(x^\delta) = \det\left(A^\delta - x^\delta \mathrm{Id}_D\right) = (\det(A - x\mathrm{Id}_D))^\delta = \chi_A(x)^\delta = \chi_A(x^\delta).$$

This shows that $\chi_{A^\delta}(x) = \chi_A(x)$.

■

Since the l-th power of a k-circulant matrix A of size D is a k^l-circulant matrix, one can apply Lemma 2.9 to compute the eigenvalus of a matrix which satisfies the conditions Lemma 2.10.

Example Let $\mathbb{F}$ be of characteristic 2, let $D = 24$ and let $k = 5$. Then the eigenvalues of a 5-circulant matrix of size 24 are equal to the eigenvalues of the 1-circulant matrix A^2. If one of these eigenvalues equals 1, then there exist CGI-sequences w.r.t. $(5, W, \Lambda, c)$ for some W, Λ, c with period 24.

Acknowledgement This research was supported by the Concerted Action Project GOA-Mefisto of the Flemisch Community, by the FWO (Fund for Scientific Research Flanders) projects G.0080.01, G.0121.03, and by the Belgian Program on Interuniversity Attraction Poles of the Belgian Prime Minister's Office for Science Technology and Culture (IAP V-22)

References

[1] [*Ablow*] C.M. Ablow, J.L. Brenner, Roots and canonical forms for circulant matrices, Trans. Amer. Math. Soc. bf 107, 1963, 360–376.

[2] [*Barbe1*] A. Barbé, F.v. Haeseler, Generalized decimation invariant sequences in dimension N. Internat. J. Bifur. Chaos Appl. Sci. Engrg. 12 (2002), no. 4, 709–737.

[3] [*Barbe8*] A. Barbé, F.v. Haeseler, Symmetries of decimation invariant sequences and digit sets. Theoret. Comput. Sci. 289 (2002), no. 1, 105–136.

[4] [*Barbe2*]A. Barbé, G. Skordev, Decimation-invariant sequences and their automaticity. Theoret. Comput. Sci. 259 (2001), no. 1-2, 379–403

[5] [*Barbe3*]A. Barbé, Multiscale coarse-graining invariant sequences. Sequences and their applications (Singapore, 1998), 146–160, Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London, 1999.

[6] [*Barbe4*]A. Barbé, H.-O. Peitgen, G. Skordev, Automaticity of coarse-graining invariant orbits of one-dimensional linear cellular automata. Internat. J. Bifur. Chaos Appl. Sci. Engrg. 9 (1999), no. 1, 67–95

[7] [*Barbe5*]A. Barbé, Complex order from disorder and from simple order in coarse-graining invariant orbits of certain two-dimensional linear cellular automata. Internat. J. Bifur. Chaos Appl. Sci. Engrg. 7 (1997), no. 7, 1451–1496.

[8] [*Barbe6*]A. Barbé, Coarse-graining invariant orbits of one-dimensional $\mathbb{Z}_p$-linear cellular automata. Internat. J. Bifur. Chaos Appl. Sci. Engrg. 6 (1996), no. 12A, 2237–2297.

[9] [*Barbe7*]A. Barbé, F.v. Haeseler, H.-O. Peitgen, G. Skordev, Coarse-graining invariant patterns of one-dimensional two-state linear cellular automata. Internat. J. Bifur. Chaos Appl. Sci. Engrg. 5 (1995), no. 6, 1611–1631.

[10] [*Davis*] Davis, Philip J., *Circulant Matrices.* A Wiley-Interscience Publication. Pure and Applied Mathematics. John Wiley & Sons, New York-Chichester-Brisbane, 1979.

[11] [*Gallian*] J.A. Gallian, *Contemporary Abstract Algebra*, D.C. Heath and Company, Lexington, MA, 1990.

[12] [*Lang*] S. Lang, *Linear Algebra*, Addison-Wesley Publishing Company, New York, 1972.

[13] [*Lidl*] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20, Addison-Wesley Publishing Company, Reading, MA, 1983.