ON FEEDFORWARD TRANSFORMS AND p-FOLD PERIODIC p-ARRAYS

Dong-sheng Chen
Graduate School
Academia Sinica
Beijing China

Zong-duo Dai
Institute of Math.
Academia Sinica
Beijing, China

Abstract

In this paper we discuss non-linear feedforward transforms of arbitrary non-singular linear shift register sequences. The approach is to give an algebraic representation of p-array modules together with description of the structure of such modules. On the basis of this, an algebraic description of the non-linear transform is given.

I. Introduction

Let

$$u_i = (u_i(0), u_i(1), \dots, u_i(j), \dots) \quad 1 \leq i \leq p \quad (1)$$

be binary periodic sequences with periods T_i , and n_i be the degrees of the minimal generating polynomials $f_i(x)$ of u_i . Consider an arbitrary Boolean function

$$\phi(x_1, \dots, x_{n_1}, \dots, x_{p_1}, \dots, x_{p_{n_p}}) = \sum_{0 \leq s \leq n} a_{s_1, \dots, s_p} x_{1s_1} \dots x_{ps_p} \quad (2)$$

put

$$u(j) = \sum_{0 \leq s_1 \leq n_1} a_{s_1, \dots, s_p} u_1(j-s_1) \dots u_p(j-s_p) \\ u = (u(0), u(1), \dots, u(j), \dots) \quad (3)$$

then u is called feedforward sequence of u_i ($1 \leq i \leq p$) defined by the feedforward transform ϕ .

The problem we enface is of a twofold character, namely, to analyse the structure of the sequence u given the transform ϕ and to determine the transform ϕ given the sequence u .

A p-array u is defined to be a mapping from I^p to the binary field F_2 where I is the set of nonnegative integers, $I^p = \{(i_1, \dots, i_p) \mid i_j \in I\}$.

A p-fold p-array (i.e. p.p-array) is defined to be a p-array u

with $T_i \in I$ ($1 \leq i \leq p$), such that $u(T_i e_i + \bar{j}) = u(\bar{j})$, $\forall \bar{j} \in I^p$, where $e_i = (0 \dots 0 \underset{i}{1} 0 \dots 0) \in I^p$.

Set

$$\mathcal{M}_p = \{v \mid v \text{ is a p.p-array}\}, \quad R = F_2[x_1, \dots, x_p]$$

For any $v, v_i \in \mathcal{M}_p$, $f \in R$, $f = \sum a_s \bar{s}$, the operations

$$(v_1 + v_2)(\bar{j}) = v_1(\bar{j}) + v_2(\bar{j}), \quad (fv)(\bar{j}) = \sum a_s v(\bar{j} - \bar{s})$$

introduce in $\mathcal{M}_p$ a structure of an R -module.

A product p-array $w = u_1 x_1 \dots x_p$ ($u_i \in \mathcal{M}_1$) is defined to be a p-array such that $w(j_1, \dots, j_p) = \prod_{i=1}^p u_i(j_i)$, $\forall (j_1, \dots, j_p) \in I^p$. It is obvious that $w \in \mathcal{M}_p$.

Operator π is defined to be a mapping from $\mathcal{M}_p$ to $\mathcal{M}_1$ such that $(\pi v)(j) = v(\bar{j})$, $\forall v \in \mathcal{M}_p$, $\bar{j} = (j, \dots, j) \in I^p$.

Let u_i be as in (1), $w = u_1 x_1 \dots x_p$, $a_s \dots a_p$ be as in (2), $f = \sum a_{s_1 \dots s_p} x_1^{s_1} \dots x_p^{s_p}$ and u be as in (3). It is easy to see $\pi fw = u$. So the problem of determining ϕ and u from each other is thus reduced to the problem of solving the equation $\pi fw = u$ for u or f .

The approach is to analyse the structure of the module $\langle w \rangle$ (the R -module generated by w). In [1], using languages of algebraic geometry, A.A. Grigoriev discussed the equation $\pi fw = u$ for the case where the minimal generating polynomial of u_i have no multiple factors. In this paper, relying on an algebraic representation of R -module $\mathcal{M}_p$, we'll discuss the equation $\pi fw = u$ without any restriction on u_i .

For the limitation of space, in this paper we omit proofs of Theorems.

II. Algebraic representations of the modules

If $u = (u(0), u(1), \dots, u(j), \dots) \in \mathcal{M}_p$ with period T , then its generating function is

$$A(u) = \sum_{i=0}^{\infty} u(i) x^i = \frac{A_0(x)}{1-x^T} = \frac{h(x)}{f(x)}, \quad (4)$$

where $A_0(x) = \sum_{0 \leq i < T} u(i) x^i$, $(h, f) = 1$, $\deg(h) \leq \deg(f)$, $f(0) = 1$. $f(x)$ is called the minimal generating polynomial of u . Similarly, if $u \in \mathcal{M}_p$, its generating function is

$$A(x) = \sum_{0 \leq j_k < \infty} u(j_1 \dots j_p) x_1^{j_1} \dots x_p^{j_p} = \frac{A_0(x)}{(1-x_1^{T_1}) \dots (1-x_p^{T_p})}$$

where $A_0(x) = \sum_{0 \leq j_k < T_k} u(j_1 \dots j_p) x_1^{j_1} \dots x_p^{j_p}$. In particular, for product p.p-array $w = u_1 x_1 \dots x_p$ its generating function is

$$A(w) = \prod_{i=1}^p \frac{h_i(x_i)}{f_i(x_i)} \quad (5)$$

where $A(u_i) = \frac{h_i(x)}{f_i(x)}$ as in (4).

Set

$$\mathcal{A}_p = \{ \frac{G}{F} \mid G, F \in R, F = \prod_{i=1}^p f_i(x_i), f_i(0)=1, \deg_i[G] \leq \deg_i[F] \} \quad (6)$$

Let $\frac{G}{F}$ be as in (6), write

$$I_F = (f_1(x_1), \dots, f_p(x_p)) \quad (7)$$

(the ideal generated by $f(x)$). $\mathcal{A}_p$ is an additive subgroup of $F_1(x_1, \dots, x_p)$. For any $f \in R$, $\frac{G}{F} \in \mathcal{A}_p$, the operation

$$f \frac{G}{F} = \frac{G_i}{F_i} \quad (8)$$

where $G_i \equiv fG \pmod{I_F}$, $\deg_i[G_i] < \deg_i[F]$, $\forall i$, introduce in additive group $\mathcal{A}_p$ a structure of an R -module.

Theorem 1 The mapping $u \mapsto A(u)$ is a module isomorphism from $\mathcal{M}_p$ onto $\mathcal{A}_p$.

By Thm.1, we can identify u with $A(u)$.

III. Structure of p.p-array modules.

For $v \in \mathcal{M}_p$, let $\text{Ann}_R \langle v \rangle = \{ f \mid fv=0, f \in R \}$. Let $\frac{G}{F}$ as in (6), I_F as in (7). It is easy to see that 1) $\text{Ann}_R \langle \frac{G}{F} \rangle = (I_F : G)$, 2) if $(G, I_F) = R$, then $\langle \frac{G}{F} \rangle = \langle \frac{1}{F} \rangle$, 3) $\dim_{F_1} \langle \frac{1}{F} \rangle = \sum_{i=1}^p \deg[f_i(x_i)]$.

If $w = u_1 \times \dots \times u_p$, and u_i have powers of irreducible polynomials as their minimal generating polynomials, we call w as a standard product p.p-array. Let w be an arbitrary product p.p-array, it is easy to see that $w = \sum_{j=1}^m w_j$, $w = \oplus \langle w_j \rangle$, where w_j are standard product p.p-arrays, and can calculate $\mathcal{M}_j(x) \in R$, such that $w_j = \mathcal{M}_j(\bar{x})w$.

By the above, w.l.g., we only consider standard product p.p-arrays w as in (5), and

$$f_i(x) = p_i(x)^{1+t_i}, \quad \frac{h_i(x)}{p_i(x)} = \sum_{j=1}^p \frac{\lambda_i^j}{(1-\theta_i^j x)^{1+t_i}} \quad (9)$$

where $p_i(x)$ are irreducible, $p_i(0)=1$, $t_i \geq 0$, θ_i is one of the roots of $p_i(x)$, $n_i = \deg[p_i]$, $\lambda_i \in F_1(\theta_i)$.

Before stating Theorem 2, we make some preparations. Let $N = [n_1, \dots, n_p]$, then $F_2^N = F_2(\theta_1, \dots, \theta_p)$. Let $V = \{ (\theta_1^{j_1} \dots \theta_p^{j_p}) \mid 0 \leq j_i < n_i \}$. For any $\bar{\theta}$, $\bar{\theta}' \in V$, we say $\bar{\theta} = (\theta_1^{j_1}, \dots, \theta_p^{j_p})$ is conjugate to $\bar{\theta}'$, if $\exists$

$\sigma \in \text{Gal } F_2^N / F_2$, such that $(\sigma \theta_1^{j_1}, \dots, \sigma \theta_p^{j_p}) = \bar{\theta}'$. Let $r_i = 1$,

$r_i = (n_i, \dots, n_{i-1}, n_i)$, $2 \leq i \leq p$. For any $\bar{j} = (j_1, \dots, j_p)$, $\{\bar{\theta}_{\bar{j}+k\bar{1}} \mid 0 \leq k < N\}$, $\bar{\theta}_{\bar{j}+k\bar{1}} = (\theta_1^{i_1+k}, \dots, \theta_p^{i_p+k})$ is a complete conjugate class in V . Write

$Z_{r_1, \dots, r_p} = \{\bar{j} \mid \bar{j} = (j_1, \dots, j_p), 0 \leq j_i < r_i\}$. It is known that V is the union of $\{\bar{\theta}_{\bar{j}+k\bar{1}} \mid 0 \leq k < N\}$, $\bar{j} \in Z_{r_1, \dots, r_p}$. Let $f(\bar{x}) = \sum a_{\bar{s}} \bar{x}^{\bar{s}} \in R$, define $f^{\bar{k}}(\bar{x}) = \sum a_{\bar{s}} (\bar{s}/\bar{k}) \bar{x}^{\bar{s}}$, where $\bar{s} = (s_1, \dots, s_p)$, $\bar{x}^{\bar{s}} = x_1^{s_1} \dots x_p^{s_p}$, $\bar{k} = (k_1, \dots, k_p)$, $(\bar{s}/\bar{k}) = \prod_{i=1}^p \binom{s_i}{k_i}$. For any i , let $\{e_j(i) \mid 0 \leq j < r_i\}$ be the dual base of $\{\theta_i^j \mid 0 \leq j < r_i\}$.

Theorem 2 Let w be as in (5) and (9), I_F as in (7). Then

$$1. \quad w = \sum_{\bar{j} \in Z_{r_1, \dots, r_p}} u(\bar{\theta}_{\bar{j}}, \bar{t}, \lambda_{\bar{j}}), \text{ where } u(\bar{\theta}_{\bar{j}}, \bar{t}, \lambda_{\bar{j}}) = \sum_{0 \leq k < N} \frac{\lambda_{\bar{j}}^{2^k}}{\prod_{i=1}^p (1 - \theta_i^{2^{i+k}} x_i)^{1+t_i}},$$

$$\bar{j} = (j_1, \dots, j_p), \quad \lambda_{\bar{j}} = \prod_{i=1}^p \lambda_i^{2^{j_i}}, \quad \bar{t} = (t_1, \dots, t_p).$$

2. Let n be any integer with $2^n \geq 1 + \sum t_i$. Take

$$e_{\bar{j}}(\bar{x}) = \sum_{0 \leq i_k < n_i} \text{Tr}_{F_{2^N}/F_2} (e_{i_1}(1) e_{i_2}(2) \dots e_{i_p}(p)) x_1^{i_1} x_2^{i_2} \dots x_p^{i_p}$$

$$e_{\bar{j}}(\bar{x}) = e_{\bar{j}}(\bar{x})^{2^n} \pmod{I_F}.$$

Then $u(\bar{\theta}_{\bar{j}}, \bar{t}, \lambda_{\bar{j}}) = e_{\bar{j}}(\bar{x}) w$.

$$3. \quad \langle w \rangle = \bigoplus_{\bar{j} \in Z_{r_1, \dots, r_p}} \langle u(\bar{\theta}_{\bar{j}}, \bar{t}, \lambda_{\bar{j}}) \rangle.$$

$$4. \quad f \cdot u(\bar{\theta}_{\bar{j}}, \bar{t}, \lambda) = \sum_{0 \leq k \leq \bar{t}} u(\bar{\theta}_{\bar{j}}, \bar{t} - \bar{k}, \lambda f^{\bar{k}}(\bar{\theta}_{\bar{j}}^{-1})), \text{ where } \bar{\theta}_{\bar{j}}^{-1} = (\theta_1^{-2^{j_1}}, \dots, \theta_p^{-2^{j_p}}).$$

$$5. \quad \langle u(\bar{\theta}, \bar{t}, \lambda) \rangle = \langle u(\bar{\theta}, \bar{t}, 1) \rangle = \left\{ \sum_{0 \leq \bar{k} \leq \bar{t}} u(\bar{\theta}, \bar{k}, \alpha_{\bar{k}}) \mid \alpha_{\bar{k}} \in F_{2^N} \right\}$$

where $\lambda \neq 0 \in F_{2^N}$ and $\sum_{0 \leq \bar{k} \leq \bar{t}} u(\bar{\theta}, \bar{k}, \alpha_{\bar{k}}) = 0$ iff. $\alpha = 0, \forall \bar{k}$.

$$6. \quad \text{Ann}_R \langle u(\bar{\theta}_{\bar{j}}, \bar{t}, 1) \rangle = (I_F, 1 - e_{\bar{j}}(\bar{x})).$$

IV The operator π

First we make some conventions. Let $S = \{\rho_{\bar{j}} \mid \rho_{\bar{j}} = \prod_{i=1}^p \theta_i^{2^{j_i}}, \bar{j} \in Z_{r_1, \dots, r_p}\}$. Let $Z'_{r_1, \dots, r_p} \subset Z_{r_1, \dots, r_p}$, and $\{\rho_{\bar{j}} \mid \bar{j} \in Z'_{r_1, \dots, r_p}\}$ be a complete set of representatives of the conjugate classes over F_2 in S . Let $q_{\bar{j}}(x)$ be an irreducible polynomial with $\rho_{\bar{j}}$ being a root. If $k = \sum k_i 2^{i_j}$, $j = \sum j_i 2^{i_j}$, $k_i, j_i = 0$ or 1 , define $k \vee j = \sum (k_i \vee j_i) 2^{i_j}$, $k \vee j \vee m = (k \vee j) \vee m$ and so on.

Let $V_{\bar{t}} = t_1 \vee t_2 \vee \dots \vee t_p$, $L_{\bar{t}} = \max_{0 \leq k \leq \bar{t}} V_k$. It is known that $L_{\bar{t}} = -1 + 2^{\bar{j}} + \sum_{j \geq j_0} (\sum_{i=1}^p t_{ij}) 2^j$,

where $t_i = \sum_{j=1}^p t_{ij} 2^j$, $t = 0$ or 1 , j_0 is the smallest integer such that $\sum_{i=1}^p t_{ij} < 2$, $\forall j \geq j_0$.

Theorem 4. (The notations being as above)

1. $\pi u(\bar{\theta}_j, \bar{t}, \lambda) = u(\rho_j, V_{\bar{t}}, \text{Tr}_{F_{2^N}/F_2}(\rho_j)^{(\lambda)})$
2. $\pi(u(\bar{\theta}_j, \bar{t}, \lambda)) = \langle u(\rho_j, L_{\bar{t}}, 1) \rangle$
3. $\pi(w) = \pi(\bigoplus_{j \in Z_{r_1}, \dots, r_p} \langle u(\bar{\theta}_j, \bar{t}, \lambda_j) \rangle) = \bigoplus_{j \in Z_{r_1}, \dots, r_p} \langle u(\rho_j, L_{\bar{t}}, 1) \rangle =$
 $= \langle \frac{1}{H(x)} \rangle$, where $H(x) = \prod_{j \in Z_{r_1}, \dots, r_p} q_j(x)$

V. The equation $\pi fw = u$.

From the above, it is not difficult to see that the equation $\pi fw = u$ could be reduced to the two kinds of algebraic equations:

1. For any $\alpha \in F(\rho)$, $\rho \in F_{2^N}$, to find y such that

$$\text{Tr}_{F_{2^N}/F_2}(\rho)(y) = \alpha$$

2. For $\beta_{\bar{k}} \in F_{2^N}$, $0 \leq \bar{k} \leq \bar{t}$, to find $f(\bar{x}) \in R$, such that

$$f^{-\bar{k}}(\theta_1^{-1}, \dots, \theta_p^{-1}) = \beta_{\bar{k}} \quad 0 \leq \bar{k} \leq \bar{t}, \forall \bar{k} \quad (10)$$

By the Theorem 2, there exists unique $f(x) \bmod \langle \text{Ann}_R(u(\theta, t, 1)) \rangle$ satisfying (10).

References

1. A.A.Grigoriev, Problems of Control and Information Theory Vol. 9(4) (1980).
2. Neal Zieve and W.H.Mills, J.Algebra, 27.(1973).
3. 陶仁骥, 有限自动机的可逆性, 科学出版社.