THE LAPLACE-GALOIS TRANSFORM IN THE THEORY OF SEQUENTIAL MACHINES

Ya. Z. Tsypkin, R. G. Faradzhev

1966

SovietRxiv

Abstract

Full Text

UDC 519.95

CYBERNETICS AND CONTROL THEORY

Ya. Z. Tsypkin, R. G. Faradzhev

THE LAPLACE-GALOIS TRANSFORM IN THE THEORY OF SEQUENTIAL MACHINES

(Presented by Academician B. N. Petrov on May 6, 1965)

In recent years, for the analysis and synthesis of sequential machines (switching circuits, multicycle coding circuits), methods analogous to the methods of field theory have begun to be used. The beginning of this direction was laid by the works of D. Huffman ([1,2]); it was further developed in papers ([3–6]), where varieties of discrete functional transformations were widely used.

In the present paper the concepts are introduced of sampled Boolean functions taking values in a finite Galois field, and of their discrete Laplace transform, called, for brevity, the Laplace-Galois transform. These concepts make it possible to construct a theory of sequential machines analogous to the well-known theory of impulse systems ([7]).

Let $GF(2^k)$ be a finite field and let ε be its generating element; then $0, \varepsilon^0, \varepsilon^1, \ldots, \varepsilon^N, \varepsilon^{-N}, \ldots, \varepsilon^{-2}, \varepsilon^{-1}$, where $N = 2^{k-1} - 1$, are all possible elements of this field ([8,9]). A function

$$y[n] = f(x_1[n], x_2[n], \ldots, x_r[n]), \tag{1}$$

where $y[n]$, $x_1[n]$, $x_2[n], \ldots, x_r[n]$ belong to $GF(2^k)$ for all $n = 0, 1, 2, \ldots$, will be called a **sampled Boolean function**. Sampled Boolean functions are very convenient in considering "dynamic" problems in the theory of sequential machines. They allow all logical operations to be represented through the operations of addition $\oplus$ and multiplication $\cdot$ over the elements of the field.

We define the Laplace-Galois transform of a sampled Boolean function by the relation

$$F^*(q) = \sum_{n=0}^{\infty} \varepsilon^{qn} \cdot f[n], \quad GF(2^k). \tag{2}$$

Here q is the transform parameter, and summation and multiplication are performed over the elements of the field $GF(2^k)$. By analogy with the discrete

Laplace transform ([7]), the correspondence between the "original" $f[n]$ and the "image" $F^*(q)$, i.e., the direct Laplace-Galois transform, is written in the form

$$F^*(q) = D\{f[n]\} \div f[n], \quad GF(2^k). \tag{3}$$

A sampled Boolean function is called **transformable** if (2) has meaning. It is easy to show that sampled Boolean functions corresponding to any finite sequence, periodic sequence, and sequence tending to a periodic one are transformable. Their corresponding images are a polynomial, a proper and improper fraction in ε^{-q} (or, for all cases, a rational fractional function in ε^q).

Transformable lattice Boolean functions include, for example, $f[n] = \varepsilon^{a\bar{\omega}n}$, where $0 \leq a < 2^k - 1$, a is an integer, and $\bar{\omega}$ is one of the divisors of the number $2^k - 1$,

$$D\{\varepsilon^{a\bar{\omega}n}\} = \frac{\varepsilon^q}{\varepsilon^q \oplus \varepsilon^{a\bar{\omega}}}, \quad GF(2^k). \tag{4}$$

As nontransformable lattice Boolean functions one may cite $f[n] = \varepsilon^{\alpha_1}$ for $n = \varphi[m]$, where $m = 0, 1, 2, ...$, $\varphi[m] \neq m$, and $f[n] = \varepsilon^{\alpha_2}$ for the remaining n, where ε^{α_1} and ε^{α_2} are elements of the field $GF(2^k)$. It is interesting to note that nontransformable lattice Boolean functions constitute events that are irregular in the sense of Kleene ([10]).

The inverse Laplace-Galois transform

$$f[n] = D^{-1}\{F^*(q)\}, \quad GF(2^k) \tag{5}$$

can be represented in various forms. Thus, directly from (3) it follows that

$$f[n] = \frac{1}{n!}\frac{d^n}{d\varepsilon q^n}[F^*(q)]_{\varepsilon^{-q}=0}, \quad GF(2^k), \quad n = 0, 1, 2, \dots, \tag{6}$$

However, it is often considerably more convenient for determining $f(n)$ to use the inversion formula

$$f[n] = \sum_{q=-N}^{N} F^*(q)\varepsilon^{qn}, \quad GF(2^k). \tag{7}$$

where q is an integer and the sum on the right-hand side is understood in the improper sense. To compute $f[n]$ one may use a kind of residue theory, and then

$$f[n] = \sum_{q=-N}^{N} F^*(q)\varepsilon^{qn} = \sum_{\nu} \mathrm{Res}_{\varepsilon q_\nu}\,[F^*(q)\varepsilon^{q(n-1)}], \tag{8}$$

where the residue corresponding to εq_ν of multiplicity r_ν is

$$\mathrm{Res}_{\varepsilon q_\nu}\left[F^*(q)\varepsilon^{q(n-1)}\right] =$$

$$= \frac{1}{(r_\nu - 1)!}\left\{\frac{d^{r_\nu - 1}}{d\varepsilon^{q(r_\nu - 1)}}\left[F^*(q)(\varepsilon^q \oplus \varepsilon^{q_\nu})^{r_\nu}\varepsilon^{q(n-1)}\right]\right\}_{\varepsilon^q = \varepsilon^{q_\nu}} GF(2^k). \quad (9)$$

In particular, for $r_\nu = 1$

$$\mathrm{Res}_{\varepsilon q_\nu}\left[F^*(q)\varepsilon^{q(n-1)}\right] = \left[F^*(q)(\varepsilon^q \oplus \varepsilon^{q_\nu})\varepsilon^{q(n-1)}\right]_{\varepsilon^q = \varepsilon^{q_\nu}}. \quad (10)$$

From the definitions of the direct and inverse Laplace–Galois transforms there follow the fundamental theorems establishing correspondences between operations on originals and on images, which are important in the analysis and synthesis of sequential machines. A summary of these theorems is given in Table 1.

The proofs of these theorems, taking into account the special features of the field $GF(2^k)$, are analogous to the proofs of the theorems for the discrete Laplace transform ([7]). Theorems 1-8 make it possible to establish operations on images corresponding to operations in the domain of originals. Apart from the linear operations (negation, equivalence, and exclusion), all other operations are expressed through the convolution operation in the image domain or conjunction in the domain of originals. Theorem 9 is useful when considering clock-rate transformation problems.

Let us consider the class of linear sequential machines ([1–6]), in which all operations reduce to delay, exclusion, and multiplication by a binary number. The difference equation relating the output quantity

Table 1

Basic theorems of the Laplace-Galois transform

No.	Theorem	Domain of originals	Domain of images
1	Linearity	$\sum_{\nu=1}^{m} a_\nu f_\nu[n]$	$\sum_{\nu=1}^{m} a_\nu F_\nu^*(q)$
2	Shift of the independent variable in the domain of originals (shift theorem)	$f[n+m]$, $f[n-m]$	$\varepsilon^{mq}\left[F^*(q) \oplus \sum_{r=0}^{m-1} \varepsilon^{-rq} f[r]\right]$ $\varepsilon^{-mq}\left[F^*(q) \oplus \sum_{r=1}^{m} \varepsilon^{rq} f[-r]\right]$

No.	Theorem	Domain of originals	Domain of images
3	Shift of the independent variable in the domain of images (shift theorem)	$\varepsilon^{\lambda n},\ \varepsilon^{-\lambda n}$, λ is an integer less than $2^k - 1$	$F^*(q - \lambda), F^*(q + \lambda)$
4	Image of differences	$\Delta^m f[n],\ m < 2^k - 1$	$(\varepsilon^q \oplus 1)F^*(q) \oplus$ $\oplus\, \varepsilon^q \sum_{\nu=0}^{m-1} (\varepsilon^q \oplus 1)^{m-1-\nu} \Delta^\nu f[0]$
5	Image of a sum	$\sum_{m=0}^{n} f[m]$	$\frac{F^*(q)}{\varepsilon^q \oplus 1}$
6	Differentiation of the image with respect to ε^{-q}	$b[n]f[n]$, where $b[n] = 0$, n even; $b[n] = 1$, n odd	$\varepsilon^{-q} \frac{dF^*(q)}{d\varepsilon^{-q}}$
7	Multiplication of images (convolution theorem in the domain of originals)	$\sum_{m=0}^{n} f_1[m] f_2[n-m] =$ $= \sum_{m=0}^{n} f_1[n-m] f_2[n-m]$	$F_1^*(q) F_2^*(q)$
8	Multiplication of originals (convolution theorem in the domain of images)	$f_1[n] f_2[n]$	$\sum_{q=-N}^{N} F_1^*(s) F_2^*(q-s) = =$ $\sum_{s=-N}^{N} F_1^*(q-s) F_2^*(s)$
9	Change of the repetition period of a lattice Boolean function	$f[\lambda n]$	$F_\lambda^*(\lambda q)$, for integer λ that is a divisor of $2^k - 1$, $F_\lambda^*(\lambda q) = \sum_{\nu=0}^{\lambda-1} F^* \left[q + \frac{(2^k-1)}{\lambda} \nu \right]$

with the input of such a linear sequential machine (LSM), can be represented in the form

$$y[n] = \sum_{\nu=0}^{l} b_{l-\nu} \cdot x[n-\nu] \oplus \sum_{\nu=1}^{l} a_{l-\nu} \cdot y[n-\nu], \tag{11}$$

where

$$a_i,\ b_i \in GF(2), \quad x[n] = y[n] = 0 \text{ for } n < 0.$$

Subjecting (11) to the Laplace-Galois transform and taking into account the shift theorem, after elementary operations, we obtain the transfer function

LSM (1)

$$\frac{Y^*(q)}{X^*(q)} = K^*(q) = \frac{P^*(q)}{Q^*(q)} = \frac{\sum_{\nu=0}^{l} b_{l-\nu} \cdot \varepsilon^{-q_\nu}}{\sum_{\nu=0}^{l} a_{l-\nu} \cdot \varepsilon^{-q_\nu}} = \frac{\sum_{\nu=0}^{l} b_\nu \cdot \varepsilon^{q_\nu}}{\sum_{\nu=0}^{l} a_\nu \cdot \varepsilon^{q_\nu}}. \quad (12)$$

Here it is assumed that $a_l = 1$; the polynomial $Q^*(q)$ is the characteristic polynomial of the LSM.

The various equivalent representations of the original transfer function $K^*(q)$ solve the problem of synthesizing an LSM. The original $k[n]$ corresponding to the transfer function $K^*(q)$ defines the impulse response of the LSM and, according to (8) and (10), is expressed in the form

$$k[n] = \sum_{\nu=1}^{l} \frac{P^*(q_\nu)}{\varepsilon^{q_\nu} \dot{Q}^*(q_\nu)} \varepsilon^{q_\nu n}, \quad GF(2^k), \quad (13)$$

where $\dot{Q}^*(q_\nu) = [dQ^*(q)/d\varepsilon^q]_{\varepsilon^q = \varepsilon^{q_\nu}}$, $GF(2^k)$; ε^{q_ν} are the zeros of the characteristic polynomial, which are assumed to be simple. It is convenient to introduce into consideration the transition function (7)

$$b[n] = \sum_{m=0}^{n} k[m] = \frac{P^*(0)}{Q^*(0)} \oplus \sum_{\nu=1}^{l} \frac{P^*(q_\nu)}{(1 \oplus \varepsilon^{q_\nu}) \dot{Q}^*(q_\nu)} \varepsilon^{q_\nu n}, \quad GF(2^k). \quad (14)$$

The impulse response $k[n]$ and the transition function $b[n]$ determine the responses of the LSM to impulse and step-like input actions. If the input action $x[n] = \varepsilon^{\bar{\omega} n}$ is a simple periodic lattice function, then the response of the LSM is determined by the formula

$$y[n] = K^*(\bar{\omega}) \varepsilon^{\bar{\omega} n} \oplus \sum_{\nu=1}^{l} \frac{P^*(q_\nu)}{(\varepsilon^{\bar{\omega}} \oplus \varepsilon^{q_\nu}) \dot{Q}^*(q_\nu)} \varepsilon^{q_\nu n}, \quad GF(2^k). \quad (15)$$

The first term in (15) corresponds to the forced process, the second sum of terms to the transient process, and $K^*(\bar{\omega})$ may be physically interpreted as the "frequency" characteristic of the LSM. $K^*(\bar{\omega})$ is obtained from $K^*(q)$ for $q = \bar{\omega}$. Since $\bar{\omega}$ is a divisor of the number $2^k - 1$, the frequency characteristic of the LSM is determined by a finite number of frequencies, and not by a continuum of frequencies on an interval or an infinite straight line, as is the case for impulse and continuous systems.

The expansion formulas given above and their generalizations to the case of multiple zeros of the characteristic polynomial, an arbitrary input action, etc., make it possible to determine the forced and transient processes (including zero sequences) in an LSM.

Thus the Laplace-Galois transform plays, with respect to sequential machines, the same role as the discrete or ordinary Laplace transform does with respect to impulse and continuous circuits.

Institute of Automation and Telemechanics

Received
29 IV 1965

CITED LITERATURE

1. D. A. Huffman, in: *Collected Papers. Theory of Information Transmission*, Foreign Literature Publishing House, 1957.
2. D. A. Huffman, *IRE Trans. on Circuit Theory*, CT-2, No. 3 (1956).
3. B. Friedland, ibid., CT-6, No. 1 (1959).
4. J. Riehalet, *L' onde Electrique*, 43, No. 439 (1963).
5. T. L. Booth, *Proc. Symposium on Math. Theory of Automata*, 12, 1963.
6. R. T. Faradzhev, *Izv. AN SSSR, Tekhnicheskaya kibernetika*, 5 (1965).
7. Ya. Z. Tsypkin, *Theory of Linear Impulse Systems*, Moscow, 1963.
8. R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, N. Y., 1937.
9. Pr. Moisil, *Algebraic Theory of Discrete Automaton Devices*, Foreign Literature Publishing House, 1963.
10. M. A. Aizerman, L. A. Gusev, L. I. Rozonoer, I. M. Smirnov, A. A. Tal' , *Logic, Automata, Algorithms*, Moscow, 1963.

Note: Figure translations are in progress. See original paper for figures.