KYBERNETIKA — VOLUME 13 (1977), NUMBER 2

Congruence of Analytic Functions Modulo a Polynomial

ZDENĚK VOSTRÝ

In the paper an algebraic approach to the numerical computation of a mapping of analytic functions into polynomials is developed. This mapping can be applied for the numerical computing of some complex integrals, transformation between Laplace and $\mathscr{Z}$ transfer functions and for more general Newton interpolation formula. Applications are in this and in the following papers.

INTRODUCTION

Some problems of linear time invariant continuous and discrete systems can be solved by using the polynomial approach [1, 2]. The extension of the polynomial approach to other problems is given in this and the following papers. The mathematical background is the congruence of analytic functions modulo a polynomial and operations in a ring of polynomials modulo a polynomial.

The basic idea is based on work by Prof. Nekolný.

Let us consider polynomials a, b with complex coefficients. We say that a divide b and write a/b, if and only if there exists a polynomial c such that $b = a \cdot c$.

The greatest common divisor of a and b is a polynomial denoted as (a, b).

The degree of a polynomial a is written as ∂a. Let $m = m_0 + m_1 x + \ldots, m_k x^k$ be a polynomial with complex coefficients and $\partial m > 0$. Then the spectrum $\mathscr{M}$ of the polynomial m is the set of all complex numbers α for which $m(\alpha) = 0$.

If f is a complex-valued function of the complex variable x defined on a neighbourhood $\mathscr{N}(\alpha)$ of a point α and if the derivative $f'(\alpha)$ exists everywhere in $\mathscr{N}(\alpha)$ then f is said to be analytic at α.

A function f is analytic on $\mathscr{M}$ if it is analytic at all points of $\mathscr{M}$. Denote $\mathscr{F}_m$ the set of all functions analytic or having at worst removable singularities on $\mathscr{M}$.

Definition 1. Let a polynomial m, $\partial m > 0$ and functions $f, g \in \mathscr{F}_m$ be given. We say that f and g are congruent modulo $m, f = g \bmod m$, if there exists an $h \in \mathscr{F}_m$ such that $f = g + hm$. The polynomial m is called modulus.

It is evident that this congruence modulo m defines an equivalence relation on $\mathscr{F}_m$ and hence the $\mathscr{F}_m$ is decomposed into disjoint equivalent classes. Each class can be represented by a polynomial with degree less then ∂m as it is shown in the following theorem.

Lemma. Let the polynomial $m = (x - \alpha)^k$ and a function $f \in \mathscr{F}_m$ be given. Then there exists only one polynomial r such that

$$f = r \bmod m\,, \quad \partial r < \partial m\,.$$

Proof. From Definition 1 the congruence

$$0 = (x - \alpha)^l \bmod m \quad \text{for} \quad l = k, k + 1, \ldots$$

follows.

Because $f \in \mathscr{F}_m$ we can write

$$f(x) = \sum_{\nu=0}^{\infty} f^{(\nu)}(\alpha) \frac{(x - \alpha)^\nu}{\nu!}\,.$$

Hence

$$f(x) = \sum_{\nu=0}^{k-1} f^{(\nu)}(\alpha) \frac{(x - \alpha)^\nu}{\nu!} \bmod m = r \bmod m$$

an the proof is complete.

Theorem 1. For any $f \in \mathscr{F}_m$, $\partial m > 0$ only one complex polynomial r exists such that

$$f = r \bmod m\,, \quad \partial r < \partial m\,. \tag{1}$$

The natural homomorfism $\mathbf{H} : f \to r$ induced by the congruence relation (1) will be called the reduction of f modulo m and denoted $[f]_m = r$.

Proof. *Existence.* Consider the modulus $m = \prod_{i=1}^{n} {}^i m$, ${}^i m = (x - \alpha_i)^{k_i}$, $\alpha_i \neq \alpha_j$ for $i \neq j$ and the equation

$$f = \sum_{j=1}^{n} {}^j q \prod_{i=1, i \neq j}^{n} {}^i m + \left(\prod_{i=1}^{n} {}^i m\right) . h \tag{i}$$

where ${}^j q$, $h \in \mathscr{F}_m$, $j = 1, 2, \ldots, n$.

Below we show that ${}^j q$ can be chosen to be a polynomial with degree less then $k_j = \partial\, {}^j m$.

Divide both sides of (i) by $\prod_{i=1, i \neq l}^{n} {}^{i}m$, $l = 1, 2, \ldots, n$. Then

$$(ii) \qquad \frac{f}{\prod_{i=1, i \neq l}^{n} {}^{i}m} = {}^{l}q + {}^{l}m \left(\sum_{j=1, j \neq l}^{n} \frac{{}^{j}q}{{}^{j}m} + h \right)$$

or in short-hand notation

$${}^{l}g = {}^{l}q + {}^{l}m \, {}^{l}h \, .$$

It is evident that ${}^{l}g, {}^{l}q, {}^{l}h \in \mathscr{F}_{{}^{l}m}$.

Using Lemma we can choose ${}^{l}q$ as a polynomial with degree less than $\partial \, {}^{l}m$ and hence the degree of the polynomial

$$r = \sum_{j=1}^{n} {}^{j}q \prod_{i=1, i \neq j}^{n} {}^{i}m$$

is less then ∂m and the existence is proven.

Uniqueness. Suppose that two polynomials r and s exist such that $\partial r < \partial m$, $\partial s < \partial m$ and

$$f = r \bmod m \, , \quad f = s \bmod m \, .$$

From these assumptions and from Definition 1 the next equations follow

$$f = r + h_1 m = s + h_2 m \, , \quad h_1 - h_2 = \frac{r - s}{m} \, ,$$

where $h_1, h_2 \in \mathscr{F}_m$.

Because $\partial(r - s) < \partial m$ and $(h_1 - h_2) \in \mathscr{F}_m$ it must be $r - s = 0$. This contradicts to the above assumption and the proof is complete.

Remark. Denote $z_1, z_2, \ldots, z_l$, $z_i \neq z_j$ for $i \neq j$, all zeros of the polynomial m and denote k_i the multiplicity of zero z_i. $(\sum_{i=1}^{l} k_i = \partial m)$.

From Definition 1

$$(2) \qquad f(z) = r(z) + h(z) \, m(z)$$

where $h(z) \in \mathscr{F}_m$.

Consider $i = 1, 2, \ldots, l$, $\nu_i = 0, 1, \ldots, (k_i - 1)$ then

$$\left. \frac{\mathrm{d}^{\nu_i} m(z)}{(\mathrm{d}z)^{\nu_i}} \right|_{z = z_i} = 0$$

and from (2)

$$(3) \qquad f^{(\nu_i)}(z_i) = r^{(\nu_i)}(z_i)$$

for all i and ν_i. In this way ∂m simultaneous linear equations for ∂m unknowns $r_0, r_1, \ldots, r_{\partial m-1}$, are obtained and the polynomial r can be computed.

Point out that the first part of the proof of Theorem 1 gives more general Newton interpolation formula. (See (i) and Remark). These interpolations can be succesfully used in many numerical problems. Computations of $[f]_m$ are given below.

PROPERTIES OF REDUCTION MODULO m

Theorem 2. Let a modulus m and the set $\mathscr{F}_m$ be given. If $f, g \in \mathscr{F}_m$, $[f]_m = a$, $[g]_m = b$ and λ is a complex number, the next equations hold:

(i) $[f + g]_m = [f]_m + [g]_m = a + b$,

(ii) $[\lambda f]_m = \lambda[f]_m = \lambda a$,

(iii) $[f \cdot g]_m = [[f]_m [g]_m]_m = [ab]_m$,

(iv) if $f/g \in \mathscr{F}_m$ then

$$\left[\frac{f}{g}\right]_m = \left[\frac{[f]_m}{[g]_m}\right]_m = \left[\frac{a}{b}\right]_m .$$

Theorem 3. Let a modulus m, the set $\mathscr{F}_m$ and a function $g \in \mathscr{F}_m$ be given. Define the set $\mathscr{N}$ as $\mathscr{N} = \{y : y = g(x), m(x) = 0\}$. If f is analytic on $\mathscr{N}$ then

$$[f(g)]_m = [f([g]_m)]_m .$$

These two theorems follow from the proof of Theorem 1.

If the function f is a polynomial then the reduction f modulo m is the remainder after dividing f by m. (see (2)).

ANNIHILATING POLYNOMIAL

Very important in applications of this approach is the so called "annihilating polynomial".

Consider polynomials $g_0, g_1, \ldots, g_N$ such that N is an integer and $\partial g_i < N$, $i = 0, 1, \ldots, N$. Then as it follows from the properties of the vector space with dimension N the complex numbers $\lambda_0, \lambda_1, \ldots, \lambda_N$ exist such that

$$(4) \qquad \sum_{i=0}^{N} \lambda_i g_i = 0 , \quad \sum_{i=0}^{N} |\lambda_i| > 0 .$$

Let a modulus m with degree N and a function $g \in \mathscr{F}_m$ be given. If (4) holds for $g_i = [f^i]_m$ then the polynomial $\sum_{i=0}^{N} \lambda_i x^i$ corresponds to the concept of characteristic polynomial in matrix algebra.

Definition 2. Consider a modulus m and a function $f \in \mathscr{F}_m$. The annihilating polynomial of a function f modulo m, denoted $\mathscr{A}[f]_m$, is a nonzero polynomial $p = p_0 + p_1 x + \ldots + p_k x^k$ with minimal degree for which

$$[p(f)]_m = 0 .$$

It is evident that

(i) $\partial p \leqq \partial m$,

(ii) for any $f \in \mathscr{F}_m$ an annihilating polynomial modulo polynomial m exists,

(iii) if p, q are annihilating polynomials of f modulo m then $p = \mu q$ for some complex number μ.

COMPUTING THE ANNIHILATING POLYNOMIAL

Let a modulus m and a function $f \in \mathscr{F}_m$ be given. Set $k = \partial m - 1$ and denote the polynomials

$$g_{(i)} = [f^i]_m \quad \text{for} \quad i = 0, 1, \ldots, \partial m , \tag{5}$$

where $g_{(i)} = g_{i0} + g_{i1}x + \ldots + g_{ik}x^k$.
Write the coefficients of the polynomial $g_{(i)}$ in the vector form

$$G_i = \begin{bmatrix} g_{i0} \\ g_{i1} \\ \vdots \\ g_{ik} \end{bmatrix} .$$

If $p = \mathscr{A}[f]_m$ then using Definition 2 and $[f^0]_m = 1$ we obtain

$$[p(f)]_m = p_0 + p_1[f]_m + p_2[f^2]_m + \ldots + p_{\partial m}[f^{\partial m}]_m = \sum_{i=0}^{\partial m} p_i g_{(i)} . \tag{6}$$

In the matrix shorthand notation

$$[G_0, G_1, \ldots, G_{\partial m}] \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{\partial m} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} . \tag{7}$$

It is evident that the minimal degree of the polynomial p is equal to the rank of the

matrix $G = [G_0, G_1, \ldots, G_{\partial m}]$. Let $n = \operatorname{rank} G$ then for $p_n = 1$ and $p_{n+1}, p_{n+2}, \ldots$
$\ldots, p_{\partial m} = 0$ the coefficients of the annihilating polynomial are given by (7).

Example 1. Find the annihilating polynomial of $f = x^2$ modulo

$$m = 6 + 5x + x^2 .$$

By (5)

$$g_{(0)} = 1$$

$$g_{(1)} = [x^2]_m = -6 - 5x$$

$$g_{(2)} = [g_{(1)}^2]_m = [(-6 - 5x)^2]_m = -144 - 65x .$$

The equation (6) has the form

$$\begin{bmatrix} 1 & -6 & -144 \\ 0 & -5 & -55 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} .$$

The rank $(G) = 2$ and for $p_2 = 1$ the solution of equation (7) gives

$$\mathscr{A}[x^2]_{6+5x+x^2} = 46 - 13x + x^2 .$$

Consider a modulus m, a function $f \in \mathscr{F}_m$ and the annihilating polynomial $p = \mathscr{A}[f]_m$ then for $m(\lambda) = 0$ the equation (6) and (3) gives $p(f(\lambda)) = 0$. The relations between the zeros of m and the zeros of p play the important role in applications.

Theorem 4. Let a modulus m and a function $f \in \mathscr{F}$ be given such that

$$\left.\frac{\mathrm{d}f}{\mathrm{d}x}\right|_{x=x_i} \neq 0$$

for all x_i for which $(x - x_i)^2 \mid m(x)$ then

$$a = \mathscr{A}[f(x)]_m = \mathrm{LCM}\left((x - f(x_1))^{n_1}, (x - f(x_2))^{n_2}, \ldots, (x - f(x_l))^{n_l}\right)$$

where LCM denotes least common multiple and n_i is the multiplicity of zero x_j of the polynomial m.

Proof. Denote $\mathscr{A}[f]_m = a_0 + a_1 x + \ldots + a_n x^n = a$.
The annihilating polynomial f modulo m is a polynomial with minimal degree for which

$$[a(f)]_m = 0 .$$

From the properties of $[\cdot]_m$ see, the proof of Theorem 1, the next equation holds

$$\left.\frac{\mathrm{d}^k}{\mathrm{d}x^k} a(f(x))\right|_{x=x_i} = 0 , \quad \text{for} \quad k = 0, 1, \ldots, (n_i - 1) .$$

Set $k = 0$ then

$$a(f) = 0 \quad \text{for} \quad x = x_i .$$

Set $k = 1$ then

$$\frac{\mathrm{d}a}{\mathrm{d}x} = \frac{\mathrm{d}a}{\mathrm{d}f}\frac{\mathrm{d}f}{\mathrm{d}x} = 0 \quad \text{for} \quad x = x_i .$$

From the assumption $\left.\frac{\mathrm{d}f}{\mathrm{d}x}\right|_{x=x_i} \neq 0$ we obtain

$$\frac{\mathrm{d}a}{\mathrm{d}f} = 0 \quad \text{for} \quad x = x_i .$$

Set $k = 2$ then

$$\frac{\mathrm{d}^2 a}{\mathrm{d}x^2} = \frac{\mathrm{d}^2 a}{\mathrm{d}f^2}\left(\frac{\mathrm{d}f}{\mathrm{d}x}\right)^2 + \underbrace{\frac{\mathrm{d}a}{\mathrm{d}f}\frac{\mathrm{d}^2 f}{\mathrm{d}x}}_{0} = 0$$

and from this

$$\frac{\mathrm{d}^2 a}{\mathrm{d}f^2} = 0 .$$

Set $k = n_i - 1$ then

$$\frac{\mathrm{d}^{n_i-1}}{\mathrm{d}x^{n_i-1}} = \frac{\mathrm{d}^{n_i-1}a}{\mathrm{d}f^{n_i-1}}\left(\frac{\mathrm{d}f}{\mathrm{d}x}\right)^{n_i-1} + \underbrace{\ldots}_{0} = 0$$

and

$$\frac{\mathrm{d}^{n_i-1}a}{\mathrm{d}f^{n_i-1}} = 0 .$$

From $\left.\frac{\mathrm{d}^k a}{\mathrm{d}f^k}\right|_{x=x_i} = 0$ for $k = 0, 1, \ldots, (n_i - 1)$ and $i = 1, 2, \ldots, l$ the property

$$(i) \qquad (x - f(x_i))^{n_i} \mid a$$

follows for any zero x_i, $i = 1, 2, \ldots, l$. A polynomial a with minimal degree satisfying (i) is evidently the LCM of $(x - f(x_i))^{n_i}$, $i = 1, 2, \ldots, l$.

Remark 1. By adding the conditions

$$f(x_i) \neq f(x_j), \quad x_i \neq x_j \quad \text{for} \quad i \neq j$$

to Theorem 4 we obtain

$$\partial a = \partial m ,$$

$$a = \prod_{i=1}^{l} (x - f(_i))^{n_i} = \mathscr{A}[f]_m .$$

Example 2. For $m = -1 + x^2$ and $f = x^2$ compute $\mathscr{A}[f]_m$.

$$[f^0]_m = 1\,,$$
$$[f^1]_m = +1\,,$$
$$[f^2]_m = \quad 1\,.$$

Construct the equation (5)

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

The rank of the matrix G is equal to 1 and

$$\mathscr{A}[x^2]_{x^2-1} = -1 + x\,.$$

It can be seen that in this example the conditions of Theorem 4 are satisfied and the conditions of Remark 1 are not satisfied.

DIOPHANTINE EQUATIONS IN POLYNOMIALS

Consider the equation

(i) $$ax + by = c$$

for unknown polynomials x, y and given polynomials a, b, c with complex coefficients.

Equation (i) has a solution if and only if $(a, b) \mid c$ (see [1]).

If $\hat{x}$, $\hat{y}$ is a particular solution of (i), then all solutions are of the form

$$x = \hat{x} + \frac{b}{(a, b)}\,t\,,$$

$$y = \hat{y} + \frac{b}{(a, b)}\,t\,,$$

where t is an arbitrary polynomial. We can obtain

$$\hat{x} = (-1)^n\, z_{n-1}\frac{c}{r_{n-1}}\,, \quad \frac{b}{(a, b)} = z_n\,,$$

$$\hat{y} = (-1)^{n-1}\, w_{n-1}\frac{c}{r_{n-1}}\,, \quad \frac{a}{(a, b)} = w_n\,,$$

where w_{n-1}, w_n and z_{n-1}, z_n are the polynomials given via recurrent equations

$$w_0 = 1, \quad w_1 = q_1, \quad w_k = q_k w_{k-1} + w_{k-2},$$
$$z_0 = 0, \quad z_1 = 1, \quad z_k = q_k z_{k-1} + z_{k-2},$$
$$k = 2, 3, \ldots, n,$$

the polynomials $q_1, q_2, \ldots, q_n$ and r_{n-1} come from euclidean algorithm for (a, b).
Euclidean algorithm for (a, b).

$$a = q_1 b + r_1 \quad \partial r_1 < \partial b$$
$$b = q_2 r_1 + r_2 \quad \partial r_2 < \partial r_1$$
$$r_1 = q_3 r_2 + r_3 \quad \partial r_3 < \partial r_2$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_{n-2} = q_n r_{n-1}.$$
$$(a, b) = r_{n-1}.$$

Theorem 5. Let a modulus m and polynomials a, c be given such that $c/a \in \mathscr{F}_m$ then

$$\left[\frac{c}{a}\right]_m = r$$

where $r = [\hat{x}]_m$, and $\hat{x}$ is a particular solution of diophantine equation

$$(d) \qquad a^* x + m y = c^*, \quad \text{where} \quad a^* = \frac{a}{(a, c)}, \quad c^* = \frac{c}{(a, c)}$$

Proof. Divide (d) by a^* then

$$x + \frac{my}{a^*} = \frac{c^*}{a^*} = \frac{c}{a}$$

and because $[gm]_m = 0$ holds for any $g \in \mathscr{F}_m$, we obtain

$$[x]_m = \left[\frac{c}{a}\right]_m.$$

Note that the condition $c/a \in \mathscr{F}_m$ agrees to condition $(a^*, m) \mid c^*$ of the diophantine equation (d). To compute the reduction modulo m of functions e^x, $\ln x$, $\sqrt{x}$, x^k etc. we use some theorems on uniform convergence and define a norm of a function modulo m. Any sequence of analytic functions f_i, $i = 1, 2, \ldots$, uniformly convergent over common region, converges to an analytic function F within that region. From this

$$\lim_{i \to \infty} f_i^{(v)} = F^{(v)} \quad \text{for} \quad v = 0, 1, 2 \ldots.$$

Theorem 6. Let a modulus m and a sequence $f_0, f_1, \ldots,$ be given such that $f_i \in \mathscr{F}_m$,
$i = 1, 2, \ldots,$ and $f_0, f_1, \ldots$ uniformly converges over some closed region containing spectrum of the modulus m to a function F. Then

$$\lim_{i \to \infty} [f_i]_m = [F]_m .$$

Proof follows from the proof of Theorem 1.

In this way the reduction $[F]_m$ can be computed by a limit process of $[f_i]_m$.

MODULAR NORM

For proofs of uniform convergence a norm is needed.

Theorem 7. Let a modulus $m = m_0 + m_1 x + \ldots, m_{k-1}x^{k-1} + m_k x^k, \; m_k \neq 0$ and $f, g \in \mathscr{F}_m$ be given. Consider $a = [f]_m$, $b = [g]_m$ and the Chebychev vector norm of the polynomial a as $\|a\| = \sum_{i=0}^{k-1} |a_i|$. Then the number

$$(n) \qquad \varrho = \max_{0 \leqq j \leqq k-1} \|[x^j f]_m\|$$

is the norm in $\mathscr{F}_m$, written as $\|f\|_m$, with the property

$$\|f \cdot g\|_m \leqq \|f\|_m \, \|g\|_m .$$

We say that $\|f\|_m$ is the modular norm of the function f with respect to the modulus m.

Proof. At first, the following norm axioms

(i) $\|f\|_m = 0$ if and only if $[f]_m = 0$,

(ii) $\|f\|_m > 0$ if and only if $[f]_m \neq 0$,

(iii) $\|\lambda f\|_m = |\lambda| \, \|f\|_m$,

(iv) $\|f + g\|_m \leqq \|f\|_m + \|g\|_m$,

are evidently held.

Product inequality

From (n) $\|fg\|_m = \|ab\|_m$ follows. Denote $[x^j b]_m = b^{(j)} = b_0^{(j)} + b_1^{(j)} x + \ldots + \ldots, b_{k-1}^{(j)} x^{k-1}$ then

$$\|ab\|_m = \max_{0 \leqq j \leqq k-1} \|[x^j ba]_m\| = \max_{0 \leqq j \leqq k-1} \|[b^{(j)} a]_m\| =$$

$$= \max_{0 \leqq j \leqq k-1} \left\| \sum_{i=0}^{k-1} b_i^{(j)} [x^i a]_m \right\| \leqq \max_{0 \leqq j < k-1} \|a\|_m \sum_{i=1}^{k-1} |b_i^{(j)}| \leqq \|a\|_m \|b\|_m$$

using the properties of the vector norm.

This norm is well adapted for computer calculations.

Remark. Consider modulus $m = m_0 + m_1 x + \ldots m_{k-1} x^{k-1} + m_k x^k$, $k \geqq 1$, then from Theorem 7 $\|x\|_m = \max_{0 \leqq j < k-1} \|[x^j x]_m\| = \max(1, (|m_0| + |m_1| + \ldots + |m_{k-1}|)/(m_k)$ using $[x^n]_m = x^n$ for $n < \partial m$ and $[x^{\partial m}]_m = -(m_0 + m_1 x + \ldots \ldots m_{k-1} x^{k-1})/m_k$. Consider the matrix

$$A = \begin{bmatrix} 0 & 0 & . & & -m_0 \\ 1 & 0 & . & & -m_1 \\ \vdots & 1 & \vdots & & \\ \vdots & & \vdots & & -m_{k-1} \\ 0 & & \vdots & 1 & -m_{k-1} \end{bmatrix}$$

then $\|x\|_m$ defines the column norm of the matrix A and as it is known

$$\max_{m(\lambda)=0} |\lambda| \leqq \|A\| = \|x\|_m \,.$$

The other properties of the modular norm are mentioned in the section Power series.

POWER SERIES

As it is well known a power series converges uniformly in any closed set that can be enclosed in a circle which in turn lies wholly in the interior of the circle of convergence.

Theorem 8. Let a modulus m and a power series $a_0 + a_1 x + a_2 x^2 + \ldots$ with the radius of convergence R defining a function $F(x) = \sum_{i=0}^{\infty} a_i x_i$ be given such that $\|x\|_m < R$ then

$$[F(x)]_m = \sum_{i=0}^{\infty} a_i [x^i]_m \,.$$

Proof. Define the closed disk $\mathscr{D}$ centred in the origin with radius $\varrho = \|x\|_m$. Then all zeros of $m(x)$ lie inside $\mathscr{D}$ and hence the above series converges uniformly over $\mathscr{D}$. Using Theorem 6 for partial sums of the given series the proof is complete.

Lemma 1. Let a modulus m and functions f, g be given such that $f(g) \in \mathscr{F}_m$ and the function f can be expressed as the power series

$$f(z) = \sum_{i=0}^{\infty} a_i z^i$$

with radius of convergence $R > \|g\|_m$. Then

$$(i) \qquad [f(g)]_m = \sum_{i=0}^{\infty} a_i [g^i]_m$$

and

$$(ii) \qquad \|f(g)\|_m \leqq |f(\|g\|_m)| .$$

Proof. (i) follows from the properties of Taylor series. (ii) following from (i) using the properties of the modular norm, especially $\|g^i\|_m \leqq (\|g\|_m)^i$.

The next algorithms are established for a modulus with real coefficients and they can be adapted for a modulus with complex coefficients with small modifications.

Let a modulus with real coefficients and a function $f \in \mathscr{F}_m$ be given such that $f^*(x) = f(x^*)$ denote the complex conjugate of x, then $[f]_m$ is the polynomial with real coefficients and it can be evaluated by real arithmetics.

NUMERICAL RESTRICTIONS

In the recommended numerical algorithms the range of numbers $(10^{-72}, 10^{72})$ and double precision real arithmetics wiht 16 decimal digits are supposed.

COMPUTATION OF $[e^{qx}]_m$.

Using Numerical restriction the value of e^{qx} can be computed for

$$|qx| < 166 < 2^8 .$$

Hence, this restriction must hold for all x for which $m(x) = 0$.

Theorem 9. Let a modulus $m = m_0 + m_1 x + \ldots + m_k x^k$, $m_k \neq \emptyset$ and a real number q be given then

$$[e^{qx}]_m = \left[\left[\sum_{i=0}^{8} \frac{1}{i!}\left(\frac{qx}{2}\right)^i\right]^{2^L}\right]_m + R$$

where

L is the least natural number for which

$$\|qx\|_m \leqq 2^{L-3}$$

and

$$\|e^{-qx} R\|_m \leqq 3.2^L \, 10^{-14} .$$

The sum is computed by Horner scheme.

Proof. Denote

$$s = \sum_{i=0}^{8} \frac{1}{i!}\left[\frac{qx}{2^L}\right]_m, \quad \varrho = \left\|\frac{qx}{2^L}\right\|_m$$

then

$$[e^{qx2^{-L}}]_m = s + [r]_m$$

where r is the remainder of the known power series for the exponential function.

From the assumption $\varrho \leqq \frac{1}{8}$ the norm $\|r\|_m$ can be bounded as

$$\|r\|_m \leqq \frac{\varrho^9 e^{1/8}}{9!} \doteq 2.4 \,.\, 10^{-14},$$

because

$$\sum_{i=9}^{\infty} \frac{\varrho^i}{i!} < \frac{\varrho^9}{9!} \sum_{i=0}^{\infty} \frac{\varrho^i}{i!} = \frac{\varrho^9}{9!} e^{\varrho}.$$

The error R is defined as

$$[e^{qx}]_m = [s^{2^L}]_m + R\,.$$

For $\|r^2\|_m \ll \|r\|_m$ we can write

$$[e^{qx}]_m = [(s + r)^{2^L}]_m \doteq [s^{2^L} + 2^L s^{2^L-1} r]_m$$

and

$$R \doteq 2^L s^{2^L-1}[r]_m\,.$$

Hence the relative error can be given as

$$\|e^{-qx}R\|_m \doteq \|2^L e^{-qx/2^L} r\|_m\,.$$

Using Lemma 1 $\|e^{-qx/2^L}\|_m \leqq e^{1/8}$ and we obtain

$$\|e^{-qx}R\| \leqq \frac{e^{1/8}e^{1/8}}{8^9 9!} 2^L < 3 \,.\, 2^L \,.\, 10^{-14}\,.$$

In usual cases $L \ll 11$ and hence $[e^{qx}]_m$ is approximated at least at 12 decimal digits.

Remark 1. Computation of $[e^{f(x)}]_m$, $f \in \mathscr{F}_m$ can be performed in the same way as $e^{q.x}$ and L is the least natural number for which

$$\|f(x)\|_m \leqq 2^{L-3}\,.$$

Point out that the practical computation of s is without numerical difficulties due to $\varrho \leqq \frac{1}{8}$.

The bilinear transformation

$$w = \frac{1 - z}{1 + z}$$

maps the right half-plane, $\mathscr{R}e\, z > 0$, onto the domain $|w| < 1$. The equation

$$\left|\frac{1 - z}{1 + z}\right| = r$$

defines for all r, $0 < r < 1$, the family of nonintersecting coaxial circles in the right half-plane.

Hence for any complex number s, $\mathscr{R}e\, s > 0$, there exists a real number $\varrho < 1$ such that

$$\frac{1 - s}{1 + s} < \varrho\,.$$

Consider the principal value of the square root of a complex number x, $x \neq t$, $t \leqq 0$ then $\mathscr{R}e \sqrt{x} > 0$.

Theorem 10. Define the domain $\mathscr{D} = \{x : \mathscr{R}e \sqrt{x} > 0\}$ then the sequence

$$(1) \qquad y_{i+1} = \frac{1}{2}\left(y_i + \frac{x}{y_i}\right), \quad y_0 = 1\,, \quad i = 0, 1, 2 \ldots$$

uniformly converges to the principal value of $\sqrt{x}$ on any finite closed set $\mathscr{S}$ contained in the domain $\mathscr{D}$.

Proof. Let a set $\mathscr{S}$ be given, then there exists a number ϱ such that the closed set $\mathscr{P} = \{x : |1 - \sqrt{x}/1 + \sqrt{x}| \leqq \varrho < 1\}$ contains the set $\mathscr{S}$ and if $x \in \mathscr{S}$ then $|1 - \sqrt{x}/1 + \sqrt{x}| < \varrho$. This follows from the property of the bilinear transformation. From (1)

$$(8) \qquad y_{i+1} - \sqrt{x} = \frac{1}{2y_i}(y_i - \sqrt{x})^2\,, \quad y_i \neq 0\,,$$

$$y_{i+1} + \sqrt{x} = \frac{1}{2y_i}(y_i + \sqrt{x})^2$$

and hence

$$(9) \qquad \frac{y_{i+1} - \sqrt{x}}{y_{i+1} + \sqrt{x}} = \left(\frac{y_i - \sqrt{x}}{y_i + \sqrt{x}}\right)^2 = \left(\frac{y_{i-1} - \sqrt{x}}{y_{i-1} + \sqrt{x}}\right)^2 \ldots = \left(\frac{y_0 - \sqrt{x}}{y_0 + \sqrt{x}}\right)^{2^{i+1}}.$$

 For $y_0 = 1$ we obtain

$$\left|\frac{y_i - \sqrt{x}}{y_i + \sqrt{x}}\right| = \left|\frac{1 - \sqrt{x}}{1 + \sqrt{x}}\right|^{2^i} < \varrho^{2^i}, \quad \text{for all} \quad x \in \mathscr{S},$$

hence $y_i - \sqrt{x}/y_i + \sqrt{x}$ and in turn $y_i - \sqrt{x}$, uniformly converges to zero on $\mathscr{S}$. The convergence is quadratic on $\mathscr{S}$.

Theorem 11. Let a modulus $m = m_0 + m_1 x + \ldots m_k x^k$, $m_k \neq 0$ be given such that $m(t) \neq 0$ for $t \leqq 0$. Then

$$(i) \qquad [\sqrt{x}]_m = \frac{1}{\sqrt{\lambda}}\, y_{N+1} + R_{N+1}$$

where

$$\lambda = \left(\frac{m_0}{m_k}(-1)^k\right)^{1/k},$$

$$y_0 = 1,$$

$$y_{i+1} = \frac{1}{2}\left[y_i + \frac{\lambda x}{y_i}\right]_m, \quad i = 0, 1, 2, \ldots, N,$$

$$\frac{\|R_{N+1}\|_m}{\|\sqrt{x}\|_m} < 10^{-14},$$

N is the least natural number for which $\|y_{N+1} - y_N\|_m / \|y_N\| < 10^{-14}$, $\|y_N\|$ is the Chebyshev vector norm (see Theorem 7).

Proof. It is known that $\lambda^k = \prod_{i=1}^{k} x_i$ where x_i is a zero of the modulus m. Hence, the values of λx, $m(x) = 0$, are "centred" about the number 1, $\prod_{i=1}^{k} \lambda x_i = 1$ and faster convergence and better numerical properties are obtained. In view of the quadratic convergence of the given algorithm (see Theorem 10) the number N is a small number, usually $N < 6$.

The error R_{N+1} can be estimated in terms of the following formulae:

$$R_{N+1} = [\sqrt{x}]_m - \frac{1}{\sqrt{\lambda}}\, y_{N+1}, \quad \text{using } (i),$$

$$-\left[\frac{R_{N+1}}{y_N}\right]_m = \frac{1}{2}\left[\left(\frac{\sqrt{(\lambda)}\, R_N}{y_N}\right)^2\right]_m, \quad \text{using } (8),$$

$$\left\|\frac{\sqrt{(\lambda)}\, R_N}{y_N}\right\|_m \ll 1$$

for $N > L$, where L is an integer number, using $R_N \to 0$ and

$$\left\|\frac{R_N}{\sqrt{x}}\right\|_m \gg \left\|\frac{R_{N+1}}{\sqrt{x}}\right\|_m .$$

Finally, we write,

$$\left[\frac{R_N}{\sqrt{x}}\right]_m \doteq \left[\frac{R_N - R_{N+1}}{\sqrt{x}}\right]_m = \left[\frac{1}{\sqrt{\lambda x}}(y_{N+1} - y_N)\right]_m \doteq \left[\frac{y_{N+1} - y_N}{y_N}\right]_m$$

and

$$\frac{\|R_{N+1}\|_m}{\|\sqrt{x}\|_m} < \frac{\|y_{N+1} - y_N\|_m}{\|y_N\|_m} \leqq \|y_{N+1} - y_n\|_m / \|y_N\|$$

by using $\|y_N\| < \|y_N\|_m$ (see Theorem 7).

Remark 2. Let a modulus m and a function f be given such that $f(x_i) \neq t$, $t \leqq 0$, $m(x_i) = 0$, then

$$[\sqrt{f(x)}]_m = z_{N+1} ,$$

where

$$z_0 = 1 , \quad z_{i+1} = \frac{1}{2}\left[z_i + \frac{f}{z_i}\right]_m$$

and N is the least natural number for which

$$\|z_{i+1} - z_i\|_m / \|z_i\| < 10^{-14} .$$

COMPUTATION OF $[x^\alpha]_m$.

Consider a real number α expressed in a computer binary form

$$\alpha = \sum_{i=-N}^{+N} 2^i \beta_i , \quad \beta_i = 0 \quad \text{or} \quad 1 , \quad (\text{usually} \quad N = 15)$$

then $x^\alpha = x^{2^i \beta_i}, \ldots, x^{2\beta_1} x^{\beta_0} \sqrt{x^{\beta_{-1}}} \sqrt{\sqrt{x^{\beta_{-2}}}} + x^{(1/2N)\beta_{-N}}$ and $[x^\alpha]_m$ can be computed using Theorem 2 and highly efficient algorithm for $[\sqrt{\ }]_m$.

Point out that $[\sqrt{\sqrt{x}}]_m$ is computed with less number of iterations then $[\sqrt{x}]_m$ because

$$\lim_{n \to \infty} [x^{1/2^n}]_m = 1 .$$

Remark 3. Computation of $[(f(x)^\alpha]_m$, $f \in \mathscr{F}_m$ is carried out in the same way as the computation of $[x^\alpha]_m$.

which converges uniformly to the principal value of $\ln(x)$ on any finite closed set $\mathscr{S}$ contained in the domain $\mathscr{D} = \{x : \mathscr{Re}\sqrt{x} > 0\}$ (see the proof of Theorem 10).

Theorem 12. Let the modulus $m = m_0 + m_1 x + \ldots + m_k x^k$, $m_k \neq 0$ be given such that $m(t) \neq 0$ for $t \leqq 0$. Then

$$(i) \qquad [\ln(x)]_m = -\ln(\lambda) + 2^{N+1} \sum_{i=0}^{7} \frac{1}{2i+1} \left(\frac{(\lambda x)^{(1/2^N)} - 1}{(\lambda x)^{(1/2^N)} + 1} \right)^{2i+1} + R$$

where

$$\lambda = \left(\frac{m_k}{m_0} (-1)^k \right)^{1/k},$$

$$\varrho = \left\| \frac{(\lambda x)^{1/2^N} - 1}{(\lambda x)^{1/2^N} + 1} \right\|_m.$$

N is the least natural number for which $\varrho \leqq \frac{1}{8}$, $N \geqq 1$. and

$$\|R\|_m \leqq 2^{N-3} \varrho^{17} < 2^N \,.\, 10^{-16} \,.$$

Proof. The number λ is defined in the same way as in Theorem 11. The equation (i) follows from $\ln(\lambda x)^{1/2^N} = (1/2^N)\ln(\lambda) + (1/2^N)\ln(x)$ and from the above series for $\ln(x)$.

Denote

$$y = \frac{(\lambda x)^{1/2^N} - 1}{(\lambda x)^{1/2^N} + 1}$$

then from (i)

$$\|R\|_m = 2^{N+1} \left\| \sum_{i=8}^{\infty} \frac{1}{2i+1} y^{2i+1} \right\|_m \leqq 2^{N+1} \frac{1}{17} \sum_{i=8}^{\infty} \|y\|_m^{2i+1} .$$

Because $\|y\|_m \leqq \varrho \leqq \frac{1}{8}$,

$$\|R\|_m \leqq 2^{N+1} \frac{1}{17} \frac{\varrho^{17}}{1-\varrho^2} < 2^{N-3} \varrho^{17} < 2^N \,.\, 10^{-16} \,.$$

Considering numerical restriction we can see that $N < 11$ because

$$\frac{(10^{72})^{1/2^{11}} - 1}{(10^{72})^{1/2^{11}} + 1} \doteq 0.044 < \frac{1}{8} .$$

If $\varrho = \|y\|_m < \frac{1}{8}$ for $N = 1$, i.e. all zeros of m tends to 1, then $\|R\|_m \leqq \frac{1}{4}\varrho^{17}$. Consider that $\|x - 1\|_m$ tends to zero, then

$$\left[\frac{\sqrt{x} - 1}{\sqrt{x} + 1} \right]_m \doteq \tfrac{1}{4} [x - 1]_m \quad \text{and} \quad [\ln(x)]_m \doteq [x - 1]_m \,.$$

Hence, for $\varrho = \frac{1}{4}\|x - 1\|_m \leqq 0.1$

$$\|\ln x\|_m \doteq 4\varrho\,, \quad \|R\|_m < \tfrac{1}{4}\varrho^{17}\,.$$

The computation of $[\ln x]_m$ is correct to fifteen decimal digits.

Remark 4. Computation of $[\ln(f(x))]_m$, $\ln(f) \in \mathscr{F}_m$ is given in the same way as the computation of $[\ln x]_m$, only $\lambda = 1$ and

$$\varrho = \left\|\frac{(f)^{1/2^N} - 1}{(f)^{1/2^N} + 1}\right\|_m\,.$$

EVALUATION OF SOME CONTOUR INTEGRALS

Theorem 13. Let a polynomial a and a function $F \in \mathscr{F}_a$ be given. Consider a closed curve $\mathscr{C}$ such that all zeros of a lie inside $\mathscr{C}$ and the function F is analytic inside $\mathscr{C}$ and on $\mathscr{C}$.

$$\int_{\mathscr{C}} \frac{F}{a}\,\mathrm{d}x = \int_{(a)} \frac{F}{a}\,\mathrm{d}x = \int_{(a)} \frac{[F]_a}{a}\,\mathrm{d}x = \frac{f_{n-1}}{a_n}\,2\pi\mathrm{j}\,,$$

where

$$n = \partial a$$

$$[F]_a = f = f_0 + f_1 x + \ldots + f_{n-1}x^{n-1}\,,$$

$$\frac{1}{2\pi\mathrm{j}}\int_{(a)} \frac{F}{a}\,\mathrm{d}x$$

denotes the sum of residues inside $\mathscr{C}$ (in the zeros of m). j imaginary unit.

Proof. Residue theorem gives

$$\int_{\mathscr{C}} \frac{F}{a}\,\mathrm{d}x = \int_{(a)} \frac{F}{a}\,\mathrm{d}x\,.$$

It is evident that

$$\int_{(a)} h\,\mathrm{d}x = 0 \quad \text{for any} \quad h \in \mathscr{F}_a$$

and hence

$$\int_{(a)} \frac{F}{a}\,\mathrm{d}x = \int_{(a)} \frac{F + ha}{a}\,\mathrm{d}x\,.$$

Choosing the function h such that $F + ha = [F]_a$ we obtain

$$\int_{(a)} \frac{F}{a}\,\mathrm{d}x = \int_{(a)} \frac{f}{a}\,\mathrm{d}x\,.$$

The integral

$$\int_{(a)} \frac{f}{a} \mathrm{d}x\,, \quad f, a \text{ polynomials}\,, \quad \partial f < \partial a\,,$$

can be evaluated by using

$$\int_{(a)} \frac{f}{a} \mathrm{d}x = -2\pi\mathrm{j}\,.\ \text{residuum at } \infty\,.$$

$$\int_{(a)} \frac{f}{a} \mathrm{d}x = \frac{f_{n-1}}{a_n} 2\pi\mathrm{j}\,.$$

Example 3. Given the Laplace transform of a function f in the form $b(s)/a(s)$ where b, a polynomials, $\partial b < \partial a$. Compute $f(\alpha)$ for some real α.

Inversion theorem for Laplace transform gives

$$f(t) = \frac{1}{2\pi\mathrm{j}} \int_{\gamma-\mathrm{j}\infty}^{\gamma+\mathrm{j}\infty} \mathrm{e}^{st} \frac{b(s)}{a(s)} \mathrm{d}s$$

where γ is any positive real number greater than the maximum real part of all zeros of $a(s)$.

In our case using Jordan's Lemma we can write

$$f(t) = \frac{1}{2\pi\mathrm{j}} \int_{\gamma-\mathrm{j}\infty}^{\gamma+\mathrm{j}\infty} \mathrm{e}^{st} \frac{b(s)}{a(s)} \mathrm{d}s = \frac{1}{2\pi\mathrm{j}} \int_{(a)} \mathrm{e}^{st} \frac{b(s)}{a(s)} \mathrm{d}s\,.$$

Using Theorem 13 we obtain

$$f(t) = \frac{1}{2\pi\mathrm{j}} \int_{(a)} \frac{[\mathrm{e}^{st}\, b(s)]_{a(s)}}{a(s)} \mathrm{d}s = \frac{c_{n-1}}{a_n}$$

where

$$n = \partial a\,,$$

$$c = c_0 + c_1 s + \ldots + c_{n-1} s^{n-1} = [\mathrm{e}^{st}\, b(s)]_{a(s)}\,.$$

For

$$F(s) = \frac{s}{6 + 11s + 6s^2 + s^3}$$

and $\alpha = 0.5$ we obtain

$$f(0.5) = 4.695096611976623\,.\,10^{-2}$$

using Theorem 3 and Theorem 9 in computer algorithm.

Example 4. The following rational function

$$F(s) = 5\,\frac{3024 - 1344s + 252s^2 - 24s^3 + s^4}{15\,120s + 8400s^2 + 2100s^3 + 300s^4 + 25s^5 + s^6}$$

giving the Laplace transform of a function $f(t)$ was previously inverted by the conventional method with the aid of a computer (Longman 1966).

Some values of $f(t)$ obtained analytically are compared in Table below with values obtained by the tadious method of Longman and Sharir [3] and by the method based on the congruence of analytic functions modulo a polynomial described in this paper.

TABLE

t	$f(t)$	$f_1(t) - f(t)$	$f_2(t) - f(t)$
0	0	0	0
0·2	−0·061994089	-10^{-9}	-10^{-9}
0·4	0·108183033	-2.10^{-9}	-2.10^{-9}
0·6	0·141936276	0	0
0·8	0·018957791	-10^{-9}	-10^{-9}
1·0	0·564698377	-2.10^{-9}	-10^{-9}
1·2	0·946068875	-2.10^{-9}	0
1·4	1·03645770	-10^{-9}	0
1·6	1.01057147	0	0
1·8	0·993023461	-26.10^{-9}	10^{-9}
2·0	0·996131698	-6.10^{-9}	0

where $f_1(t)$ is computed by the method given in [3], $f_2(t)$ is computed by the recommended method. The computations reported in this paper were carried out on the IBM 370/135 computer with double precision arithmetics and PL/I language.

CONCLUSION

This paper is the first part of a series of papers to be published on the polynomial approach to some numerical problems related to the Laplace and Z transformations, evaluation of some complex integrals etc. This approach is based on algorithms for the numerical computation of the reduction of an analytic function modulo a polynomial.

(Received June 8, 1976.)

REFERENCES

[1] V. Kučera: Algebraic Theory of Discrete Optimal control for single-variable systems I. Kybernetika *9* (1973), 2, 94–107.

[2] Z. Vostrý: New Algorithm for Polynomial Spectral Factorization with Quadratic Convergence I. Kybernetika *11* (1975), 6, 415–422.

[3] I. M. Longman, M. Sharir: Laplace Transform Inversion of Rational Functions. Geophys. J. R. astr. Soc. (1971), 25, 299–305.

[4] G. F. Carrier: Functions of a Complex Variable: Theory and Technique. McGraw-Hill, 1966.

Ing. Zdeněk Vostrý, CSc. Ústav teorie informace a automatizace ČSAV (Institute of Information Theory and Automation — Czechoslovak Academy of Sciences), Pod vodárenskou věží 4, 180 76 Praha 8. Czechoslovakia.