THEORY OF NUMBERS AS APPLIED TO SYSTOLIZATION OF ALGORITHMS FOR NUMERICAL HANDLING OF IMAGES

A.I. Brodovich, S.A. Ikonnikov, E.I. Shabakov, and A.N. Kalinenko

Institute of Atmospheric Optics
Siberian Branch of the Russian Academy of Sciences, Tomsk
Received December 23, 1994

A method for processing video information obtained from space based on data flow splitting is proposed. The method allows time of the data flow processing to be decreased significantly (by a factor about 100*).*

Potentialities of modern photographic, TV, and optoelectronic observation systems are mainly determined by characteristics of means for processing the information acquired in the form of videosignals and images. Necessity of processing the high–density flows of videodata in real time requires certain improvements in both the hardware and software of processors. For this purpose such mathematical structures of the abstract algebra and theory of numbers as the residue class rings, Galois fields, and hypercomplex fields are widely used now in the problem of digital processing of videosignals and images.

Large number of fast processing algorithms based on the structure theorems of algebra and theory of numbers can be divided conditionally into two large groups. Algorithms of the first group use the number–theoretic features of data addresses or their numbers in a segment of the videodata flow processed. This group of algorithms is well described in Refs. 1, 2, and 3 and it is widely used in the digital signal processing. Among them there are the Agarval––Cooley and Vinograd algorithms for convolution computation, Cooley––Tukey and Tomas––Good algorithms for the discrete Fourier transform, and others.

Algorithms of the second group based on the number–theoretic features of the quantum values of the signal readouts themselves are not completely developed and are under way now.[4] Of special interest is the application of these algorithms to digital processing of videosignals and images with some specific features. First, the initial data take the values belonging to a set of integer positive numbers. Second, this set is limited by a number of brightness gradations permitted. Third, the dimensions of the processing segments are finite.[5]

Integer character of the data under processing allows the fast calculation algorithms to be constructed not only for some elements of output sequences but for the entire sequences as well. To this end, the processing algorithm or its part ought to be placed in the algebraic structure of polynomial rings.

Purpose of this paper is to discuss the algorithms for videodata processing in the polynomial rings by an example of calculation of the most cumbersome operation, i.e., the convolution of the digital sequences describing images.

The linear convolution of two sequences of integers, $\{r_i\}$ and $\{h_i\}$, of the lengths l_r and l_h described by the polynomials $r(x)$ and $h(x)$ yields a polynomial

$$s(x) = r(x)\, h(x)\ , \tag{1}$$

where the polynomial degrees are: $\deg r(x) = l_r - 1$, $\deg h(x) = l_h - 1$, and $\deg s(x) = l_r + l_h - 2$.

The polynomial coefficients are elements of a ring of integer numbers Z, therefore, the convolution can be nested into the ring of polynomials with the integer coefficients which is referred to as the ring of polynomials over the ring Z and designated as $Z[x]$.

If the polynomial coefficients are presented as elements of the residue ring Z_m, where the values of the modulus m are greater than any coefficient of the polynomials $r(x)$, $h(x)$, and $s(x)$, the convolution can be nested into the polynomial ring over the residue ring Z_m, $Z_m[x]$

$$s(x) = r(x)\, h(x)\ (\mathrm{mod}\ m),\ \ Z_m[x]\ . \tag{2}$$

The problem of calculating linear convolution can be nested into the problem of calculation of the product of polynomials modulo a fixed polynomial $m(x)$ of the degree n. If an integer number is chosen as n, which is greater than the degree of the polynomial $s(x)$, and an arbitrary polynomial of the degree n is chosen as $m(x)$, then the problem of calculating the output polynomial

$$s(x) = r(x)\, h(x)\ (\mathrm{mod}\ m(x)) \tag{3}$$

is reduced to the problem of calculating linear convolution, since the modulo $m(x)$ reduction does not change $s(x)$. Taking $m(x) = x^n - 1$, we can calculate the cyclic convolution in the same manner

$$s(x) = r(x)\ (\mathrm{mod}\ x^n - 1)\ h(x)\ . \tag{4}$$

Depending on the algebraic structure over which the polynomials $r(x)$, $h(x)$, and $s(x)$ are defined, the convolution can be nested into the problem of calculation of the polynomial product in various rings of residues of the polynomials to their moduli. If the polynomials are defined over the ring of integer numbers Z then

$$s(x) = r(x)\, h(x)\ (\mathrm{mod}\ m(x));\ \ Z[x]\ /\ m(x)\ . \tag{5}$$

If the polynomials are defined over the ring of residue classes Z_m then

$$s(x) = r(x)\, h(x)\ (\mathrm{mod}\ m)\ (\mathrm{mod}\ m(x))\ ;\ \ Z_m[x]\ /\ m(x)\ . \tag{6}$$

If the polynomials are defined over the Galois field then

$$s(x) = r(x)h(x)(\mathrm{mod}\ p)(\mathrm{mod}\ m(x))\ ;\ GF(p)[x]/m(x)\ . \tag{7}$$

In Eqs. (5)–(7) $Z[x]/m(x)$ is the ring of modulo $m(x)$ residues of polinomials over the ring of integer numbers, $Z_m[x]/m(x)$ is the same over the ring of modulo $m(x)$ residues of integer numbers, $GF(p)[x]/m(x)$ is the same over the Galois field $GF(p)$, and p is the prime integer positive number.

0235-6880/95/07 570-03 $02.00

If the polynomial $m(x)$ is expanded into polynomials irreducible above the Galois field $p_1(x)$, $p_2(x)$, ..., $p_j(x)$, ..., $p_k(x)$, the calculation of the convolution in the ring $GF(p)/m(x)$ can be reduced to calculation of the short convolutions $s_j(x)$ in the rings $GF(p)/p_j(x)$:

$$s_1(x) = r(x)\ h(x)\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ p_1(x))\ ;$$

$$s_2(x) = r(x)\ h(x)\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ p_2(x))\ ;$$

. . . .

$$s_k(x) = r(x)\ h(x)\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ p_k(x))\ .$$

Use of the polynomial version of the chinese remainder theorem (CRT)[6] allows all polynomials $s_j(x)$ to be transformed into single polynomial $s(x)$. Such a method of transition to the short convolutions is taken as a basis for the Vinograd convolution method which provides the least number of products.[1,2] The Vinograd method is applied to calculation of convolution over any fields, where the irreducible polynomials of low degree exist. The field of real and complex numbers and also the finite Galois fields fall in this group. Having calculated the convolution in the ring $Z_m[x]/m(x)$, the Vinograd method can be supplemented by the methods of convolution calculation in the direct sum of the polynomials residue rings to the modulus $m(x)$, allowing several convolutions to be calculated simultaneously.

Consider now the calculation of K different integer convolutions as a product of K polynomials $r_j(x)$ by corresponding polynomials $h_j(x)$, where $j = 1, 2, ..., K$:

$$s_1(x) = r_1(x)\ h_1(x)\ ;$$

$$s_2(x) = r_2(x)\ h_2(x)\ ;$$

. . . .

$$s_k(x) = r_k(x)\ h_k(x)\ .$$

Unipolarity and relatively narrow dynamic range of the input videosignal allow every such a product of polynomials to be nested into the polynomial residue ring $Z_{m_j}[x]/m(x)$, where m_1, m_2, ..., m_k are integer prime–in–pair numbers, and the polynomial degree $m(x)$ is greater than the degree of any of the polynomials $s_1(x)$, $s_2(x)$, ..., $s_k(x)$:

$$s_1(x) = r_1(x)\ h_1(x)\ (\mathrm{mod}\ m_1)\ (\mathrm{mod}\ m(x)),\ Z_{m_1}[x]\ /\ m(x)\ ;$$

$$s_2(x) = r_2(x)\ h_2(x)\ (\mathrm{mod}\ m_2)\ (\mathrm{mod}\ m(x)),\ Z_{m_2}[x]\ /\ m(x)\ ;$$

. . . .

$$s_k(x) = r_k(x)\ h_k(x)\ (\mathrm{mod}\ m_k)\ (\mathrm{mod}\ m(x)),\ Z_{m_k}[x]\ /\ m(x)\ .$$

The chinese remainder theorem allows K polynomial products to be reduced to calculation of a single polynomial product

$$s(x) = r(x)\ h(x)\ (\mathrm{mod}\ m)\ (\mathrm{mod}\ m(x)) \tag{8}$$

in the polynomial ring $Z_m[x]/m(x)$, which is isomorphic to the direct sum of the polynomial rings $Z_{m_j}[x]/m(x)$:

$$Z_m[x]/m(x) \sim Z_{m_1}[x]/m(x)+Z_{m_2}[x]/m(x) +...+Z_{m_k}[x]/m(x). \tag{9}$$

In this case the values of the polynomial–multipliers are formed according to the following rules:

$$r(x) = \sum_{j=1}^{K} r_j(x)\ M_j\ T_j\ (\mathrm{mod}\ m)\ (\mathrm{mod}\ m(x))\ ; \tag{10}$$

$$h(x) = \sum_{j=1}^{K} h_j(x)\ M_j\ T_j\ (\mathrm{mod}\ m)\ (\mathrm{mod}\ m(x))\ , \tag{11}$$

where $M_j = m/m_j$ and $M_jT_j = (\mathrm{mod}\ m)$.

Every polynomial $s_j(x)$ results from the polynomial $s(x)$ by calculation of the residue to the corresponding modulus m_j :

$$s_1(x) = s(x)\ (\mathrm{mod}\ m_1)\ ;$$

$$s_2(x) = s(x)\ (\mathrm{mod}\ m_2)\ ;$$

. . . .

$$s_k(x) = s(x)\ (\mathrm{mod}\ m_k)\ .$$

To calculate the polynomial $s(x)$, the Vinograd method can be used if the polynomial $m(x)$ is chosen in such a manner that it permits the expansion into several irreducible polynomials $p_1(x)$, $p_2(x)$, ..., $p_k(x)$. If $h_1(x) = h_2(x) = ... = h_k(x)$ then processing in the direct sum of the polynomial rings allows a filtration of the several segments of videosignal readouts or several fragments of an image to be carried out simultaneously, as it is shown in Fig. 1. If the necessity exists to process videodata array by several filters, describing by the polynomials $h_1(x)$, ..., $h_k(x)$, in parallel, the above approach allows the filtration to be carried out with the use of a single filter as shown in Fig. 2.

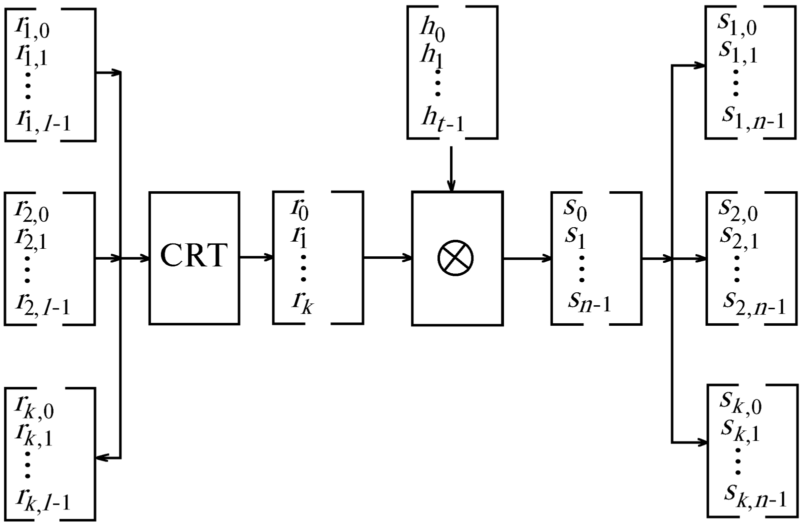

FIG. 1. Scheme of the algorithm for processing of several fragments with a single filter.

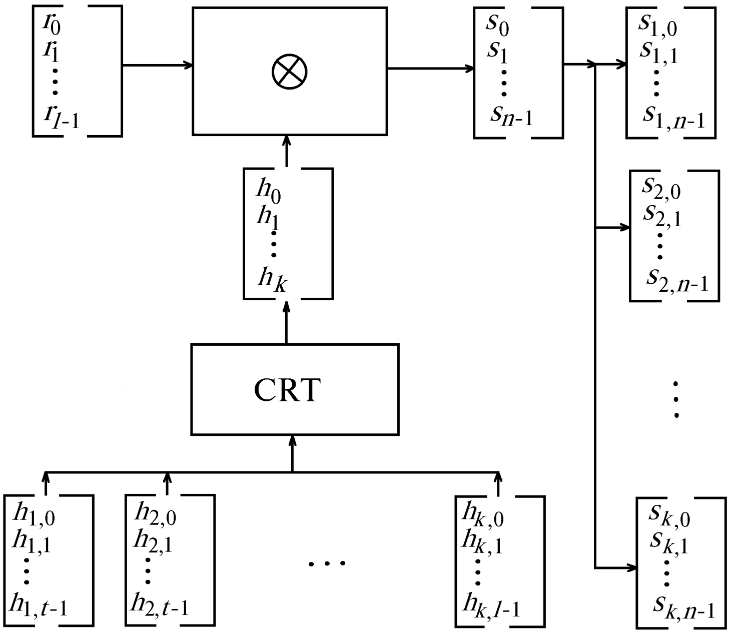

FIG. 2. Scheme of the algorithm for parallel processing of a fragment with several filters.

As is clear from the figures, the dimensions of the segments and filters transformed with the use of chinese remainder theorem do not exceed dimensions of the input data arrays. If values of the transformed filter can be calculated beforehand then a number of operations needed for convolution decreases by a factor of K. The only limitation on the number K of simultaneously calculated convolutions is the necessity to satisfy the condition $m < 2^{l_p}$, where l_p is the length of the processor word. There are several ways to overcome this limitation in calculations with the use of modular arithmetic,[7] but all of them lead to a decrease in the processing rate.

Thus, a reduction of the processing time with a universal computer can be achieved using the algorithms of simultaneous calculation of several convolutions in the ring isomorphic to the direct sum of the polynomials over the residue class rings to the prime–in–pair modulus.

These algorithms allow several fragments of an image to be processed or several filters to be used simultaneously. The latter version is preferable since the weighting function of the synthesized filters can be calculated beforehand.

It is most reasonable to use the synthesized filters in the problems of localization, detection, determination of coordinates and spatial orientation of objects in an image by the methods of coordinated filtration. The only limitation on the number of simultaneously generated filters is the word size of an arithmetic device.

REFERENCES

1. R.E. Bleyhoot, *Fast Algorithms of Signal Digital Processing* [Russian translation] (Mir, Moscow, 1989), 448 pp.

2. J.H. McClelan and Ch.M. Reyder, *Application of the Theory of Numbers to the Digital Processing of Signals* [Russian translation] (Radio i Svyaz', Moscow, 1983), pp.8–59, pp.186–202.
3. V.G. Labunets, *Algebraic Theory of Signals and Systems. Digital Signal Processing* (Krasnoyarsk University Press, Krasnoyarsk, 1984), 244 pp.
4. A.I. Brodovich and E.I. Shabakov, *Integer Processing of Videosignals and Images* (A.F. Mozhaiskii Military Space–Engineering Academy, St. Petersburg, 1993), Vol. 2, 152 pp.
5. A.S. Batrakov, A.I. Brodovich, and E.I. Shabakov, SPIE **1961**, Visual Information Processing II, 456–466 (1993).
6. B.V. Titkov and E.I. Shabakov, Tekhnika Sredstv Svyazi. Ser. Tekhn. Televideniya, No. 4, 26–33 (1985).
7. D. Knut, *Computer Programming Art.* Vol. 2. *Seminumerical Algorithms* [Russian translation] (Mir, Moscow, 1978), pp. 74–76, pp. 411–419, p. 476.