CONVOLUTION BY p-ADIC TRANSFORMS

การประสานโดยผลการแปลงพี - แอดิก

Wanlop Surakampontorn
วัลลภ สุระกำพลธร

Vichian Laohakosol *
วิเชียร เลาหโกศล

Department of Electronics, Faculty of Engineering,
King Mongkut's Institute of Technology Ladkrabang
ภาควิชาอิเล็กทรอนิกส์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ABSTRACT

This work represents an investigation on the use of p-adic transforms to perform convolution of sequences. First, p-adic transforms are described and then are used to study cyclic convolution of short and long sequences. It is shown that to obtain error free results, usual restrictions on the nature of input and output data have to be made. In contrast to former number theoretic transforms, in general, p-adic transforms yield better dynamic ranges. As for long sequences, most relevant aspects, such as technical derivation of various computational techniques, the number of multiplications needed resemble and/or remain at least in principle as compatible as other number theoretic transforms.

บทคัดย่อ

งานวิจัยนี้แสดงถึงการใช้การแปลงพี - แอดิก เพื่อคำนวณผลการประสานของลำดับ เริ่มด้วยการกล่าวถึงการแปลงพี - แอดิก จากนั้นเป็นการนำมาประยุกต์เพื่อศึกษาผลการประสานวัฏจักรของลำดับประเภทสั้นและยาว สิ่งที่แสดงคือ การที่จะได้รับผลที่ไร้ข้อผิดพลาด จำเป็นต้องมีเงื่อนไขทั่วไปเกี่ยวกับลักษณะของข้อมูลเข้าและออก โดยทั่วไปเมื่อเทียบกับการแปลงเชิงทฤษฎีจำนวนที่มีมาก่อน การแปลงพี-แอดิกให้พิสัยพลวัตที่ดีกว่า ส่วนด้านการประยุกต์ใช้กับลำดับประเภทยาวนั้น รูปแบบลักษณะที่เกี่ยวข้อง เช่น การแสดงสูตรหรือเทคนิคการคำนวณหลาย ๆ ประเภท ปริมาณของการคูณที่ต้องใช้ ในหลักการแล้วคล้าย และ/หรือ ไม่ด้อยกว่าการแปลงเชิงทฤษฎีจำนวนประเภทอื่น ๆ

---

* Department of Mathematics, Kasetsart University

INTRODUCTION

In recent years, a number of techniques and algorithms for computing digital convolutions have been proposed.[1,2,3,9,10,12,13] One of which is the use of number theoretic transforms. These transforms have the advantages of being error free and efficient in certain cases. On the other hand, they suffer serious drawbacks such as limited dynamic range, and implementation difficulty of modular arithmetic. Quite recently, a new kind of number theoretic transforms enjoying the cyclic convolution property, called p-adic transforms, has been developed and their basic properties have also been derived.[7,8] One note worthy advantage of p-adic transforms over other usual number theoretic transforms is the longer and more flexible dynamic ranges. An analysis of the cyclic convolution based on p-adic transforms was presented in this study, and a study of the corresponding cyclic convolution was made. As may be expected, certain confinements on dynamic ranges have to be imposed so as to yield error free results, but they are certainly less restrictive than usual number theoretic transforms. We also sketch briefly the derivation relating to the computation of convolution of long sequences using higher dimensional p-adic transforms.

MATERIALS, METHODS AND RESULTS

1. p-Adic segments

Let p be a fixed prime, $\mathbb{Q}_p$ be the p-adic field, i.e. the completion of the rational field $\mathbb{Q}$ with respect to the p-adic valuation $|\ |_p$. As is well-known, any p-adic number $\alpha \in \mathbb{Q}_p$ can be uniquely represented by a(p-adically) convergent power series.[4]

$$\alpha = \sum_{i=-n}^{\infty} a_i p^i \qquad \text{.....(1)}$$

where $n = n(\alpha)$ is a non-negative integer, $a_{-n} \neq 0$ and $a_i = a_i(\alpha) \in \{0, 1, \ldots, p-1\}$. For a fixed positive integer r, define a finite r-segment (or simply, segment) of α to be

$$H(P, r, \alpha) = \sum_{i=-n}^{k} a_i p^i \qquad \text{.....(2)}$$

with $r = n+k+1$, and define a finite r-segmented p-adic (or simply, segmented field) $\hat{\mathbb{Q}}_{p,r}$ to be the collection of all such H(p, r, α)'s. When p and r are kept fixed throughout, let us simply write H(α) for H(p, r, α) and $\hat{\mathbb{Q}}$ for $\hat{\mathbb{Q}}_{p,r}$.

It was shown by Laohakosol and Surakampontorn[7] that if $\alpha = \frac{A}{B}$ is a rational p-adic integer in its reduced fraction form with dynamic ranges

$$-X \leqslant A \leqslant X \quad , \quad -Y \leqslant B \leqslant Y \quad , \qquad \text{.....(3)}$$

where X and Y are positive numbers satisfying

$$XY \leqslant \frac{1}{2} \cdot (p^r - 1) \quad , \qquad \text{.....(4)}$$

then α is uniquely representable by $H(\alpha)$. This unique representation is actually valid for a wider class of rational numbers. Indeed any reduced fraction of the form

$$p^t \cdot A/B \qquad \text{.....(5)}$$

where t, A, B, are integers with A, B having the same dynamic ranges as above, has unique segment representations because A/B has.

The finite segment p-adic arithmetic can be used in a digital signal processor to perform error-free computation. Since the input and the output data are rational numbers, an efficient conversion scheme is required. Various algorithms for computing p-adic expansions of rational number exists.[4,5] On the other hand, efficient algorithms used for recapturing a rational number from its unique segment, e.g. Krishnamurthy,[6] are awkward. However, these algorithms are quite time-consuming. In practice, particularly for real-time calculation, it seems much more convenient and expeditious, after fixing r, to construct a look up table.[11]

2. p-Adic transforms

2.1 One dimensional p-adic transforms

Let N be a positive integer satisfying the following two conditions (i) a primitive N^{th} root of unity $H(\gamma)$ exists in $\hat{\mathbb{Q}}$, i.e. the equation

$$X^N - 1 = 0 \qquad \text{.....(6)}$$

is solvable in $\hat{\mathbb{Q}}$.

(ii) 1/N is a p-adic integer with dynamic ranges conditioned as in section 2. This automatically implies that $H(1/N) = H(N)$ up to the first r digits.

As note in Nasrabadi and King,[8] a permissible value of $N \varepsilon \{0, 1, \ldots, p-1\}$ satisfying both conditions above is

$$N_0 = p - 1 \quad . \qquad \text{.....(7)}$$

Now, if we let $H(x_i)$, $i = 0, 1, \ldots, N-1$ be a sequence of points in $\hat{\mathbb{Q}}$. The (forward) p-adic transforms of $H(x_i)$ is defined as

$$H(X_k) = \sum_{i=0}^{N-1} H(x_i) \cdot H(\gamma)^{ik} \quad , \quad k = 0, 1, \ldots, N-1 \quad . \qquad \text{.....(8)}$$

It is readily checked that the following orthogonality condition holds, up to r digits,

$$\sum_{i=0}^{N-1} H(\gamma)^{k(n-i)} = \begin{cases} H(N) & , \text{ if } n-i \equiv 0 \,(\text{mod } N) \\ 0 & , \text{ otherwise.} \end{cases} \qquad \text{.....(9)}$$

Hence the inverse transform is

$$H(x_i) = H(1/N) \cdot \sum_{k=0}^{N-1} H(X_k) \cdot H(\gamma)^{-ik} \quad . \qquad \text{.....(10)}$$

Since p-adic transforms are so constructed structually to conform with transforms having the convolution property,[1] they certainly enjoy this property.

Owing to the fact that rational numbers of the form described in the last section render unique segment representations, p-adic transforms certainly provide us with an error free transform when applied to these number sequences. In addition, the dynamic ranges are relatively flexible and larger than usual number theoretic transforms (NTT's). However, to increase dynamic ranges amounts to increasing the value of r which in turn enlarges our look up table. Another noteworthy remark is that equality and all basic arithmetic operation carried out above and in what follows are interpreted up to r digits, and this suffices to yield error free results.

2.2 Multi-dimensional p-adic transforms

As shown in Laohakosol and Surakampontorn,[7] multi-dimensional p-adic transforms can be straightforwardly defined as follows:

Let N be a positive integer subject to the two requirements in section 3.1. Given an N^n – sequence of segments $\vec{H}(X_{t_1}, \ldots, X_{t_n})$, $t_i = 0, 1, \ldots, N-1$; $i = 1, \ldots, n$, we define the (forward), n-dimensional p-adic transform of $\vec{H}(x_{t_1}, \ldots, x_{t_n})$ to be

$$\vec{H}(X_{k_1}, \ldots, X_{k_n}) = \sum_{t_1=0}^{N-1} \cdots \sum_{t_n=0}^{N-1} \vec{H}(x_{t_1}, \ldots, x_{t_n}) \cdot H(\gamma)^{t_1k_1 + \ldots + t_nk_n} \quad , \quad \text{...(11)}$$

$k_i = 0, \ldots, N-1$; $i = 1, \ldots, n$, where $H(\gamma)$ is a primitive N^{th} root of unity in $\hat{\mathbb{Q}}$. Again the following orthogonality is easily checked

$$\sum_{k_1=0}^{N-1} \cdots \sum_{k_n=0}^{N-1} H(\gamma)^{k_1(i_1-t_1) + \ldots + k_n(i_n-t_n)}$$

$$= \begin{cases} H(N)^n & , \text{ if } i_m - t_m \equiv 0 (\text{mod } N),\ m = 1, \ldots, n \\ 0 & , \text{ otherwise.} \end{cases} \qquad \text{.....(12)}$$

This orthogonality immediately yields the inverse transform

$$\vec{H}(x_{t_1}, \ldots, x_{t_n}) = H(1/N)^n \sum_{k_1=0}^{N-1} \cdots \sum_{k_n=0}^{N-1} \vec{H}(X_{k_1}, \ldots, X_{k_n}) \cdot H(\gamma)^{-(t_1k_1 + \ldots + t_nk_n)} \quad , \qquad \ldots\ldots\ldots(13)$$

$$t_i = 0, \ldots, N-1 \quad ; \quad i = 1, \ldots, n.$$

3. Cyclic convolutions

Let x_i, y_i, $i = 0, 1, \ldots, N-1$ be two sequences of rational numbers which we require to find their cyclic convolutions and N be a positive integer appropriately chosen as in section 3. To ensure error free convolution after performing p-adic transforms and p-adic arithmetic, two requirements are in order :

3.1 Both input data are assumed to be rational numbers which are also p-adic integers. We do not though have to assume the output data to be rational and p-adic integral because both properties are being preserved through the convolution.

3.2 Dynamic ranges of the input and output data must be suitably adjusted. This requirement can be made explicit as follows :

Let $x_i = A_i/B_i$, $y_i = C_i/D_i$, $i = 0, 1, \ldots, N-1$, be the input sequences and $z_i = E_i/F_i$, $i = 0, 1, \ldots, N-1$ be the output data. Thus

$$z_i = x_i * y_i = \sum_{k=0}^{N-1} x_k\, y_{i-k} \quad , \quad i = 0, 1, \ldots, N-1 \qquad \ldots\ldots\ldots(14)$$

$$\text{or} \qquad \frac{E_i}{F_i} = \sum_{k=0}^{N-1} \frac{A_k}{B_k} \cdot \frac{C_{i-k}}{D_{i-k}} \qquad \ldots\ldots\ldots(15)$$

Dynamic ranges of z_i will be satisfied if

$$|B_0B_1 \ldots B_{N-1} \cdot D_0D_1 \ldots D_{N-1}| \leqslant S \qquad \ldots\ldots\ldots(16)$$

and

$$N|A_iC_jB_{k_1}B_{k_2} \ldots B_{k_{N-1}} \cdot D_{m_1} \cdot D_{m_2} \ldots D_{m_{N-1}}| \leqslant T \qquad \ldots\ldots\ldots(17)$$

where $i, j, k_1 \ldots, k_{N-1}, m_1, m_2, \ldots, m_{N-1} \in \{0, 1, \ldots, N-1\}$, and

$$ST \leqslant \frac{p^r - 1}{2} \quad . \qquad \ldots\ldots\ldots(18)$$

As a crude example, we may take sequences A_i/B_i, C_i/D_i with

$$\max(|A_i| \, , \, |B_i| \, , \, |C_i| \, , \, |D_i|) \leqslant \left(\frac{p^r - 1}{2N}\right)^{\frac{1}{4N}} \qquad \ldots\ldots\ldots(19)$$

With all above requirements met, error free cyclic convolution via p-adic transforms are computed through the following steps :

Step 1. Pre-assign a value of r.
Step 2. Obtain from the look up table the segments $H(x_i)$, $H(y_i)$ of the input sequences x_i, y_i.
Step 3. Compute the transforms $H(X_k)$, $H(Y_k)$ of $H(x_i)$, $H(y_i)$.
Step 4. Compute the products $H(Z_k) = H(X_k) \cdot H(Y_k)$.
Step 5. Compute the inverse transforms $H(z_k)$ of $H(Z_k)$.
Step 6. Obtain from the look up table the actual values z_k from the segments $H(z_k)$.

We give now an example to illustrate the necessity of the bounds on dynamic ranges mentioned above.

Take $p = 5$, $N = 4$, $r = 2$, so that $\frac{1}{2}(p^r - 1) = 12$.

Let us compute the convolution of the following two sequences of integers

$$x_0 = 3,\ x_1 = 2,\ x_2 = 2,\ x_3 = 4$$
$$y_0 = 2,\ y_1 = 3,\ y_2 = 0,\ y_3 = 4 \quad .$$

Their convolution is

$$z_i = x_i * y_i = \sum_{k=0}^{3} x_k y_{i-k} \quad , \quad i = 0, 1, 2, 3$$

where the subscripts are computed mod 4. By direct calculation

$$z_0 = x_0y_0 + x_1y_3 + x_2y_2 + x_3y_1 = 26 = 1 + 0 \cdot 5 + 1 \cdot 5^2$$

and so $H(5, 2, z_0) = H(z_0) = 1 + 0 \cdot 5$,

$$z_1 = 21,\ H(z_1) = 1 + 4 \cdot 5$$
$$z_2 = 26,\ H(z_2) = 1 + 0 \cdot 5$$
$$z_3 = 26,\ H(z_3) = 1 + 0 \cdot 5 \quad .$$

Observe that all $z_0, z_1, z_2, z_3 > \frac{1}{2}(p^r - 1)$.

Referring to the dynamic range conditions (3), (4) with $Y = 1$, $X = \frac{1}{2}(p^r - 1) = 12$, we have the following error free representation of the two sequences x_i, y_i

$H(x_0) = 3 + 0 \cdot 5$, $H(x_1) = 2 + 0 \cdot 5$, $H(x_2) = 2 + 0 \cdot 5$, $H(x_3) = 4 + 0 \cdot 5$

$H(y_0) = 2 + 0 \cdot 5$, $H(y_1) = 3 + 0 \cdot 5$, $H(y_2) = 0 + 0 \cdot 5$, $H(y_3) = 4 + 0 \cdot 5$.

Now a primitive 4^{th} root of unity in $\mathbb{Q}_5$ is[8]

$$\gamma = 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + \ldots,$$

so that $H(\gamma) = 3 + 3 \cdot 5$.

Next, we compute the p-adic transforms

$$H(X_k) = \sum_{i=0}^{3} H(x_i) \cdot H(\gamma)^{ik} \quad , \quad k = 0, 1, 2, 3,$$

$$H(X_0) = 1+2\cdot 5 \ , \qquad H(X_1) = 0+1\cdot 5 \ ,$$
$$H(X_2) = 4+4\cdot 5 \ , \qquad H(X_3) = 2+2\cdot 5 \ ,$$
$$H(Y_0) = 4+1\cdot 5 \ , \qquad H(Y_1) = 4+1\cdot 5 \ ,$$
$$H(Y_2) = 0+4\cdot 5 \ , \qquad H(Y_3) = 0+4\cdot 5 \ .$$

Next compute the products

$$H(Z_k) = H(X_k) \cdot H(Y_k) \quad , \quad k = 0, 1, 2, 3.$$

$$H(Z_0) = 4+4\cdot 5 \ , \qquad H(Z_1) = 0+4\cdot 5 \ ,$$
$$H(Z_2) = 0+1\cdot 5 \ , \qquad H(Z_3) = 0+3\cdot 5 \ .$$

Finally compute the inverse transforms

$$H(z_i) = H(\tfrac{1}{4}) \cdot \sum_{k=0}^{3} H(Z_k)\, H(\gamma)^{-ik} \quad , \quad i = 0, 1, 2, 3.$$

Here, we have $H(\frac{1}{4}) = 4+3\cdot 5$, $H(\gamma)^{-1} = 2+1\cdot 5$.

$$H(z_0) = 1+3\cdot 5 \ , \quad H(z_1) = 1+0\cdot 5 \ ,$$
$$H(z_2) = 1+1\cdot 5 \ , \quad H(z_3) = 1+4\cdot 5 \ .$$

These values obviously do not agree with actual values found at the beginning. Though the input data are represented error free, the dynamic ranges of the output convolution exceed the error free bounds, which then yields wrong results.

4. Cyclic convolution of long sequences

Although p-adic transforms of sequences of length N are possible for infinitely many values of N (one such value is $N_0 = p-1$) meeting the requirements described in section 3, we see from equation (19) that dynamic ranges of convolution are reduced if N is large. This may lead to a problem of optimizing values of r and N. However, a technique of formulating a one-dimensional convolution as a two or larger dimensional convolutions, may prove advantageous and help alleviating the above problem.[2,14] We shall pursue this formulation for p-adic transforms in this section.

4.1 Agarwal-Burrus Technique

We start with converting a one-dimensional convolution to a two-dimensional one by a technique in Agarwal and Burrus.[2] Let N be a positive integer as in section 3 and suppose that it is composite with factorization

$$N = LM \ .$$

Let $H(x_n)$ and $H(y_n)$, $n = 0, 1, \ldots, N-1$, be two sequences of segments to be cyclically convolved, namely to find $H(z_n)$ such that

$$H(z_n) = \sum_{t=0}^{N-1} H(y_{n-t})\, H(x_t) \quad , \quad n = 0, \ldots, N-1 \ ,$$

where the suffixes are evaluated mod N. We introduce a change of variables of the form

$$\begin{aligned} n &= \ell + sL \\ q &= k + tL \end{aligned}$$

$k, \ell = 0, 1, \ldots, L-1$; $s, t = 0, \ldots, M-1$. Such representation of n and q are evidently unique. Thus our convolution becomes

$$H(z_{\ell+sL}) = \sum_{k=0}^{L-1} \cdot \sum_{t=0}^{M-1} H(Y_{\ell+sL-k-tL})\, H(x_{k+tL}) \quad .$$

Define a two-dimensional $L \times M$ matrix $\hat{X}$ from the original length $N = LM$ signal, $H(x_n)$, by

$$\hat{X}(\ell, s) = H(x_{\ell+sL})$$

where columns of $\hat{X}$ are the sections of H(x) and the rows are samples of H(x) taken every L values of n. Similarly, define

$$\begin{aligned} \hat{Y}(\ell, s) &= H(Y_{\ell+sL}) \\ \hat{Z}(\ell, s) &= H(z_{\ell+sL}) \quad . \end{aligned} \qquad \text{.....(20)}$$

With these, we have two-dimensional signals

$$\hat{Z}(\ell, s) = \sum_{t=0}^{M-1} \sum_{k=0}^{L-1} \hat{Y}(\ell-k, s-t)\ \hat{X}(k, t)$$

which represent a two-dimensional convolution. For values of $\hat{Y}(\ell-k, s-t)$ outside the $L \times M$ array, we define them via (20). This amounts to extending $\hat{X}$ into a $(2L-1) \times M$ array $\hat{\hat{X}}$ by appending $L-1$ zeros to the bottom of $\hat{X}$.[2] (eqn. 8 in Agarwal and Burrus)[2].

The desired convolution is cyclic in the s dimension, while the values of $\hat{Y}$ along ℓ shows that the convolution is not cyclic in this direction. Analogous to $\hat{X}$, we extend $\hat{Y}$ into $\hat{\hat{Y}}$ so that the columns of $\hat{\hat{Y}}$ contain the periodic extension of the original $H(y_n)$ with period N. (eqn. 9 in Agarwal and Burrus)[2].

The two-dimensional cyclic convolution is then

$$\hat{\hat{Z}} = \hat{\hat{Y}} * \hat{\hat{X}}$$

Usually, one additional row is inserted to yield $2L \times M$ rather than the minimum $(2L-1) \times M$ array; this is merely for ease of implementation. The two-dimensional transform of $\hat{\hat{X}}$ is defined as

$$T(\hat{\hat{X}}) = F(j, k) = \sum_{s=0}^{M-1} \sum_{\ell=0}^{2L-1} \hat{\hat{X}}(\ell, s)\, H(\gamma_{2L})^{\ell}\, H(\gamma_M)^{sk}$$

and the inverse transform

$$T^{-1}(F) = \hat{\hat{X}}(\ell, s) = H(\tfrac{1}{2}N) \sum_{k=0}^{M-1} \sum_{j=0}^{2L-1} F(j, k)\, H(\gamma_{2L})^{-\ell j}\, H(\gamma_M)^{-sk}$$

provided that a primitive 2L-root of unity $H(\gamma_{2L})$, a primitive M^{th} root of unity $H(\gamma_M)$ both exist in $\hat{Q}$ and $H(\frac{1}{2}N) = H(2N)^{-1}$. Thus being so, by the convolution property

$$T(\hat{\hat{Z}}) = T(\hat{\hat{Y}})\, T(\hat{\hat{X}})$$

yielding

$$\hat{\hat{Z}} = T^{-1}\{T(\hat{\hat{Y}})\, T(\hat{\hat{X}})\}$$

As evident from the formulation, the amount of multiplications needed and the applicability of fast Fourier transforms (FFT) algorithm in the above-mentioned technique are the same as Agarwal and Burrus' techniques[2]. There are also drawbacks, notably the existence of two primitive roots and the requirement $H(\frac{1}{2}N) = H(2N)^{-1}$.

4.2 Siu-Constantinides Technique

A different technique avoiding these difficulties which may prove more attractive has been given in Siu and Constantinides.[14] It relies heavily on the use of Z-transforms. Suppose N is composite with factor $N = N_1 N_2$.

Let

$$n = N_2 n_1 + n_2 \quad , \quad \begin{matrix} n_1 = 0, 1, \ldots, N_1 - 1 \\ n_2 = 0, 1, \ldots, N_2 - 1 \end{matrix}$$

and $$Z_1 = Z^{N_2} \quad .$$

Then the one-dimensional Z-transform of the sequence of segments $H(x_n)$ is mapped into a two-dimensional form by

$$X(Z, Z_1) = \sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{N_1-1} H(x_{n_2, n_1})\, Z_1^{n_1}\, Z^{n_2} \quad .$$

Similarly the two-dimensional transform of the sequence of segments $H(y_n)$, $n = 0, 1, \ldots, N-1$, is defined as

$$Y(Z, Z_1) = \sum_{m_2=0}^{N_2-1} \sum_{m_1=0}^{N_1-1} H(y_{m_2,m_1})\, Z_1^{m_1} Z^{m_2} \quad .$$

Since the cyclic convolution of $H(x_n)$ and $H(y_n)$ is

$$H(w_k) = \sum_{n=0}^{N-1} H(x_n)\, H(y_{k-n}) \ , \ k = 0, 1, \ldots, N-1$$

this can be expressed as a two-dimensional Z-transform as

$$\begin{aligned} X(Z, Z_1)\, Y(Z, Z_1) &= \Big(\sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{N_1-1} H(X_{n_2, n_1})\, Z_1^{n_1} Z^{n_2} \Big) \\ &\quad \cdot \Big(\sum_{m_2=0}^{N_2-1} \sum_{m_1=0}^{N_1-1} H(y_{m_2, m_1})\, Z_1^{m_1} Z^{m_2} \Big) \pmod{Z_1^{N_1} - 1} \\ &= \sum_{n_2=0}^{N_2-1} \sum_{m_2=0}^{N_2-1} \Big[\Big(\sum_{n_1=0}^{N_1-1} H(x_{n_2,n_1})\, Z_1^{n_1} \Big) \\ &\quad \cdot \Big(\sum_{m_1=0}^{N_1-1} H(y_{m_2, m_1})\, Z_1^{m_1} \Big) \Big] Z^{n_2+m_2} \pmod{Z_1^{N_1} - 1} \end{aligned}$$

Since n_1 and m_1 are cyclic, the product inside the last square bracket corresponds to a cyclic convolution. Define

$$\begin{aligned} X_{n_2}(Z_1)\, Y_{m_2}(Z_1) &= \Big(\sum_{n_1=0}^{N_1-1} H(X_{n_2, n_1})\, Z_1^{n_1} \Big) \\ &\quad \cdot \Big(\sum_{m_1=0}^{N_1-1} H(y_{m_2, m_1})\, Z_1^{m_1} \Big) \pmod{Z_1^{N_1} - 1} \quad , \ldots\ldots\ldots(21) \end{aligned}$$

where $n_2, m_2 = 0, \ldots, N_2 - 1$. Thus

$$X(Z, Z_1) \cdot Y(Z, Z_1) = \sum_{n_2=0}^{N_2-1} \sum_{m_2=0}^{N_2-1} X_{n_2}(Z_1)\, Y_{m_2}(Z_1)\, Z^{n_2+m_2} \quad .$$

Evaluating (21) at $Z_1 = H(\gamma)^{k_1}$ where $H(\gamma)$ is a primitive N^{th} root of unity (this gives the p-adic transforms of the sequences of segments $H(x_{n_2, n_1})$ and $H(y_{m_2, m_1})$, $n_2, m_2 \in \{0, 1, \ldots, N-1\}$; $n_1, m_1 \in \{0, \ldots, N-1\}$ with respect to n_1 and m_1) and substituting into (21), we get

$$X(Z, H(\gamma)^{k_1}) \cdot Y(Z, H(\gamma)^{k_1}) = \sum_{n_2=0}^{N_2-1} \sum_{m_2=0}^{N_2-1} X_{n_2,k_1} \cdot Y_{m_2,k_1} \cdot Z^{n_2+m_2} \quad \text{.....(22)}$$

$k_1 = 0, \ldots, N_1 - 1$, where

$$X_{n_2,k_1} = \sum_{n_1=0}^{N_1-1} H(x_{n_2,n_1}) \cdot H(\gamma)^{n_1 k_1}$$

$$Y_{m_2,k_1} = \sum_{m_1=0}^{N_1-1} H(y_{m_2,m_1}) \cdot H(\gamma)^{n_1 k_1} \quad .$$

Equation (22) is a linear convolution (not cyclic in n_2) of the sequences X_{n_2,k_1} and Y_{m_2,k_1} ; $n_2, m_2 \varepsilon \{0, 1, \ldots, N_2 - 1\}$, i.e.

$$X(Z, H(\gamma)^{k_1}) \cdot Y(Z, H(\gamma)^{k_1}) = \left(\sum_{n_2=0}^{N_2-1} X_{n_2,k_1} Z^{n_2} \right) \left(\sum_{m_2=0}^{N_2-1} Y_{m_2,k_1} Z^{m_2} \right)$$

$$= W_{0,k_1} + W_{1,k_1} Z + \ldots + W_{2N_2-2,k_1} Z^{2N_2-2} \quad , \quad \text{.....(23)}$$

$k_1 = 0, \ldots, N_1 - 1$. The values of W's are to be sought.

Siu and Constantinides[14] propose two techniques for computing the W's, both of which can be carried out with respect to p-adic transforms as follows :

A. Lagrange Interpolation Techniques

Write the polynomial in (23) as a sum of interpolating polynomials

$$W_{0,k_1} + W_{1,k_1} Z + \ldots + W_{2N-2,k_1} Z^{2N_2-2} = \sum_{i=0}^{2N-2} m_{k_1,i} L_i(Z) \quad ,$$

where

$$L_i(Z) = \prod_{\substack{j=0 \\ j \neq i}}^{2N-2} \frac{Z - Z_j}{Z_i - Z_j}$$

and the interpolating coefficients are, by construction,

$$m_{k_1,i} = X(Z_i, H(\gamma)^{k_1}) \cdot Y(Z_i, H(\gamma)^{k_1}) \ , \ i = 0, \ldots, 2N-2, \quad \text{.....(24)}$$

Here the interpolating points $Z_0, \ldots, Z_{2N-2}$ are arbitrary chosen. This last equation (24) requires $2N_2 - 1$ multiplications for the calculation of N_2 points, or $2 - \frac{1}{N_2}$ per point. Hence, this method is quite good for small N_2. However, the interpolating polynomials become complicated when N_2 is large.

B. Double Transform Technique

Since (23) is a product of convolutions of two sequences each of length N_2, it can be found by a length $2N_2 - 1$ cyclic convolution of two $(2N_2 - 1)$-sequences form by appending $N_2 - 1$ zeros at the end of the original sequences, i.e.

$$\{X_{0,k_1}, \ldots, X_{N_2-1,k_1}, \underbrace{0, \ldots, 0}_{N_2-1 \text{ zeros}}\} * \{Y_{0,k_1}, \ldots, Y_{N_2-1,k_1}, \underbrace{0, \ldots, 0}_{N_2-1 \text{ zeros}}\} \quad .$$

This cyclic convolution can then be computed as in section 3. This amounts to

$$X'_{k_2',k_1} = \sum_{n_2'=0}^{2N_2-2} X_{n_2',k_1} \cdot H(\gamma_{2N_2-1})^{k_2' n_2'}$$

where $k_2' = 0, \ldots, 2N_2 - 1$, $H(\gamma_{2N_2-1})$ is a primitive $(2N_2 - 1)^{\text{th}}$ root of unity; a similar formular for Y'_{k_2',k_1}. The final required convolution is

$$W_{n_2',k_1} = H\left(\frac{1}{2N_2-1}\right) \sum_{k_2=0}^{2N_2-2} X'_{k_2',k_1} \cdot Y'_{k_2',k_1} \cdot H(\gamma_{2N_2-1})^{-k_2' n_2'}$$

where $n_2' = 0, \ldots, 2N_2 - 1$. Again, we observe as in subsection 4.1 that this second technique requires two $H(\gamma)$'s.

Both techniques A and B evidently require the same number of multiplications and whenever FFT is applicable in Siu and Constantinides' technique.[14] With just a single root of unity needed, technique A seems better than B, but this advantage is paid for by the fact that technique A becomes feasible when one of the sequence lenght factors is small.

DISCUSSION

As with other number theoretic transforms, to obtain p-adic transforms, we begin by constructing the so-called Hensel code for each rational number in the sequence. Subject to certain restrictions on the sizes of numerators and denominators, these codes can be made error free throughout. This is an aspect nicer than many number theoretic transforms.

The derivation of one and multi-dimensional p-adic transforms proceeds along the line similar to all transforms. The existence of primitive roots of unity used is guaranteed for infinitely many sequences. This is the same as other number theoretic transforms.

To compute cyclic convolution of two sequences with error free results, two requirements are needed 1) input data have to be p-adically integral and 2) dynamic ranges have to be suitably adjusted. The requirement 1) is not severe for we can always so adjust the input data, and by doing so, p-adic integrality is preserved throughout the entire calculation. The requirement 2) is common to all transforms and in fact dynamic ranges deducible via p-adic transforms are even wider than most number theoretic transforms. Worth emphasizing is that the error free output data, which are desirable but usually lacking in many number theoretic transforms, are automatic here.

For long sequences, the derivation of three computation techniques due to Agarwal-Burrus and Siu-Constantinides[2,14] is attained with equal labour as with classical situations. Considering this likeness, it is evident that the amount of operations, such as multiplications, is, if any, of little difference.

We mention one particular difficulty encountered which involves the problem of implementing p-adic transforms. This seems a real difficulty meriting more research. The principal obstacle is the lack of practical algorithms for inverting Hensel codes back to rational numbers. We hope to return to this interesting problem later.

CONCLUSION

In this paper basic facts and properties of p-adic transform are first reviewed, and its application to digital convolution is analysed. There are two main attractive features: error free computation and longer dynamic ranges than ordinary number theoretic transforms. Yet, cares must also be taken on dynamic ranges to ensure error free arithmetic, and these constraints are made explicit. For long input sequences, three techniques based on multi-dimensional approach are formulated along the same lines as classical number theoretic transforms. The number of multiplications needed are observed to be indentical and the fast Fourier transform algorithm is also applicable in the same manner as usual number theoretic transforms.

REFERENCES

1. Agarwal, R.C. and Burrus, C.S. Fast Convolution Using Fermat Number Transforms with Applications to Digital Filtering. *IEEE Trans. Acoust.,Speech, Signal Processing*, 1974, **ASSP-22**, 87-99.
2. Agarwal, R.C. and Burrus, C.S. Fast One-dimensional Digital Convolution by Multidimensional Techniques. *IEEE Trans. Acoust., Speech, Signal Processing*, 1974, **ASSP-22**, 179-188.

3. Agarwal, R.C. and Cooley, J.C. New Algorithms for Digital Convolution. *IEEE Trans. Acoust., Speech, Signal Processing*, 1977, **ASSP-25**, 392-410.
4. Bachman, G. Introduction to p-Adic Numbers and Valuation Theory. Academic Press, New York, 1964.
5. Krishnamurthy, E.V. Matrix Processors Using p-Adic Arithmetic for Exact Linear Computations. *IEEE Trans. Comput.*, 1977, **C-26**, 629-633.
6. Krishnamurthy, E.V. On the Conversion of Hensel Codes to Farey Rationals. *IEEE Trans. Comput.*, 1983, **C-32**, 331-336.
7. Laohakosol, V. and Surakampontorn, W. p-Adic Transforms. *Electron. Lett.*, 1984, **20**, 726-727.
8. Nasrabadi, N.M. and King, R.A. Fast Digital Convolution Using p-Adic Transforms. *Electron. Lett.*, 1983, **19**, 266-267.
9. Nussbaumer, H.J. Fast Polynomial Transform Algorithms for Digital Convolution. *IEEE Trans. Acoust., Speech, Signal Processing*, 1980, **ASSP-28**, 205-215.
10. Nussbaumer, H.J. and Quandalle, P. Computation of Convolutions and Discrete Fourier Transforms by Polynomial Transforms. *IBM J. Res. Develop.*, 1978, **22**, 134-144.
11. Pei, S.O. and Wu, J.A. Exact Fast Digital Convolution by Using p-Adic Numbers and Polynomial Transformations. Proceeding IEEE International Conference on Acoustic Speech and Signal Processing, 1985, 760-763.
12. Rader, C.M. Discrete Convolutions via Mersenne Transforms. *IEEE Trans. Comput.*, 1972, **C-21**, 1269-1273.
13. Reed, I.S. and Truong, T.K. The Use of Finite Fields to Compute Convolutions. *IEEE Trans. Inform. Theory*, 1975, **IT-21**, 208-213.
14. Siu, W.C. and Constantinides, A.G. Cyclic Convolution of Long Sequences Using Number Theoretic Transform. *IEEE Proc. G. Electron. Circuits Syst.*, 1984, **131**(3), 119-126.