J. Indian Inst. Sci., Nov.–Dec. 2006, **86**, 791–796

Short Communication

A number-theoretic transform for signal processing

SUSHANTA SRIVASTAVA
39 Gladstone Drive, East Brunswick, NJ 08816, USA.
email: sushantasrivastava@yahoo.com; Phone: 1 732 257 4858.

Received on October 17, 2005; Revised on December 26, 2006.

Abstract

We describe a new transform for signal processing applications, and explain its basis using multiplicative number theory. Applying this transform, any signal can be resolved into its transformed spectrum in less than $2N(1 + \log_e N)$ computations, where N is the number of signal samples. Re-synthesis of the signal from the transformed spectrum also takes about the same number of computations. We also discuss the likely applications of this new transform and outline recommendations for further research.

Keywords: Digital signal processing, multiplicative number theory, signal analysis and synthesis, signal encryption and decryption.

1. Introduction

Let N samples of a discrete time signal be denoted by the vector $s = [s(1), s(2), \ldots, s(N)]^T$. Let a transform of s be defined through the relation

$$s = A.x, \quad \text{or} \quad s(i) = \sum_{j=1}^{N} A_{ij}\, x(j), \tag{1}$$

where A is a nonsingular $N \times N$ matrix. In the above, i and j are the row and column numbers.

In this paper, we are concerned with a particular type of transformation matrix A whose elements are expressed as

$$A_{ij} = f(\lceil i/j \rceil), \tag{2}$$

where $\lceil i/j \rceil$ denotes the ceiling of the number i/j, and $f(m)$ is any arithmetic function subject to the constraints $f(1) \neq 0$ and $f(1) \neq f(2)$. An arithmetic function $f(m)$ is defined as any complex-valued function that vanishes when m is not a finite non-negative integer [1–3].

The class of matrix A, stated above, has some special characteristics:

(a) A is a square $N \times N$ matrix with at least 2 and at most N distinct entries $f(1)$, $f(2)$, … $f(N)$, with $f(1) \neq 0$, $f(2) \neq f(1)$.

(b) In the n^{th} row of A, the last $(N - n + 1)$ elements are equal to $f(1)$, the proceeding $n - \lceil n/2 \rceil$ elements are equal to $f(2)$, the preceding $\lceil n/2 \rceil - \lceil n/3 \rceil$ elements are equal to $f(3)$, etc.

(c) The entry $f(m)$ appears $\lceil n/(m-1) \rceil - \lceil n/m \rceil$ times consecutively in the n^{th} row if $m \le n$.

(d) The entry $f(m)$ does not appear in the n^{th} row if (i) $m > n$ or if (ii) $m < n$ and $\lceil n/(m-1) \rceil - \lceil n/m \rceil = 0$.

For the restrictions stated on the arithmetic function $f(m)$ in eqn (2), the nonsingularity of matrix A is ensured by the fact that a sequential subtraction of the rows of the matrix leads to

$$\det[A] = f(1) \cdot \{f(1) - f(2)\}^{(N-1)}. \tag{3}$$

To compute the spectral coefficients $\{x(j), j = 1,..., N\}$ of the signal s, we need to evaluate

$$X = A^{-1}.s = B.s. \tag{4}$$

Thus, the problem of spectral decomposition is reduced to computation of inverse matrix B. We shall refer to the transform defined by eqn (4) as number-theoretic transform, since several of its properties are derived through the application of multiplicative number theory [4, 5].

During the investigation of the problem by numerical matrix inversion, it was discovered that the structure of matrix B is surprisingly simple and sparse. In addition, as it is shown later in the paper, the inverse matrix B has at the most $2N(1 + \log_e N)$ nonzero entries. Further investigation also revealed that most of the entries of matrix B are repetitive and they can be computed without an explicit inversion of matrix A.

2. Some definitions

The matrix transformation we are dealing with is characterized by the selected arithmetic function. Any arithmetic function that satisfies the restriction stated in eqn (2) can be used.

The *Dirichlet product* (or multiplicative convolution) of any two arithmetic functions $f(m)$ and $g(m)$ is defined as [4]

$$\sum_{\substack{k|m \\ 1\le k\le m}} f(m/k).g(k) \equiv \sum_{\substack{k|m \\ 1\le k\le m}} f(k).g(m/k) \equiv f(m) \otimes g(m), \tag{5}$$

where $k|m$ denotes k divides m. The complimentary symbol $k \nmid m$ denotes k does not divide m, which is used or implied elsewhere in the paper. Also in the above, the symbol $\otimes$ denotes the *multiplicative convolution*. This convolution has commutative and associative properties [5].

Two arithmetic functions, $f(m)$ and $g(m)$, are said to be Dirichlet inverses of one another if they satisfy the condition

$$f(m) \otimes g(m) = d(m, 1), \tag{6}$$

where $d(i,j) = 1$, for $i = j$ and is zero otherwise [6].

The *Dirichlet transform* of an arithmetic function $f(m)$ is defined as

$$F(s) = \sum_{1 \le m \le \infty} f(m).m^{-s} \tag{7}$$

where s is a complex variable. The transform is defined only over that region of the complex s plane where the infinite sum in eqn (7) converges.

A necessary and sufficient condition for the convolution (6) to hold [6], i.e. the necessary and sufficient condition for any two arithmetic functions to be Dirichlet inverse is

$$F(s).G(s) \equiv 1 \Leftrightarrow f(m) \otimes g(m) = d(m,1). \tag{8}$$

3. An elementary arithmetic identity

Next, I establish an elementary arithmetic identity which is invoked in our later analysis. It establishes a relationship between any finitely bound function $f(\lceil i/j \rceil)$ and the corresponding arithmetic function $f(i/j)$.

Theorem 1: Any function $f(\lceil i/j \rceil)$ whose indices i and j are positive integers, and the corresponding arithmetic function $f(i/j)$, satisfy the identity

$$f\{\lceil i/j \rceil\} - f\{\lceil (i+1)/j \rceil\} \equiv f\{i/j\} - f\{(i/j)+1\}. \tag{9}$$

Proof (outline): Since $f(i/j)$ is an arithmetic function, the left-hand side of the above identity is zero (0) whenever $j \nmid k$; i.e. the left-hand side vanishes in such cases. The validity of the identity can be readily verified in only two other cases, namely, ($j|i$; $j = 1$) and ($j|i$; $j > 1$). □

4. Inverse transformation matrices; *B*

Using the above definition of Dirichlet inverses, we state and prove the following *inverse transformation matrix theorem.*

Theorem 2: The inverse of the matrix $A_{ij} = f(\lceil i/j \rceil)$ is

$$B_{ij} = \left\{ \begin{array}{l} g\{i/j\} - g\{i/(j-1)\}, \text{ if } 1 \le i < N \\ \dfrac{1}{f(1)}.d(j,1) - \displaystyle\sum_{1 \le l \prec N} B_{l,j}, \text{ if } i = N \end{array} \right\}, \tag{10}$$

where $g(m)$ is the Dirichlet inverse of the difference $\overline{f}(m) = f(m) - f(m+1)$, i.e.

$$\sum_{k|m} g(m/k).\{f(k) - f(k+1)\} = d(m,1) \Leftrightarrow g(m) \otimes \overline{f}(m) = d(m,1). \tag{11}$$

Proof: Considering the product, $C_{ij} = \sum_{1\le k\le N} A_{ik}B_{kj}$, we need to show that $C_{ij} = d(i, j)$, the Kronecker delta function. For, $1 \le i < N$ manipulation of the summation indices and using the fact that $g(m)$ vanishes when m is not a finite non-negative integer, yields

$$\begin{aligned} C_{\substack{i\,j\\ 1\le i\le N\\ 1\le j\le N}} &= \sum_{1\le k\le N} B_{i\,k}.A_{kj} = \sum_{1\le k\le N} [g(i/k) - g\{i/(k-1)\}].f(\lceil k/j\rceil) \\ &= \sum_{\substack{k\,|\,i\\ 1\le k< N}} g(i/k).[f\{\lceil k/j\rceil\} - f\{\lceil (k+1)/j\rceil\}]. \end{aligned} \tag{12}$$

Using the identity (9) and the convolution (11), the above becomes

$$C_{\substack{i\,j\\ 1\le i\le N\\ 1\le j\le N}} = \sum_{j\le k\le i} g(i/k).[f\{k/j\} - f\{(k/j)+1\}] = \sum_{j\le k\le i} g\left(\frac{i/j}{k/j}\right).\bar{f}(k/j). \tag{13}$$

For the last row of the product

$$\begin{aligned} C_{\substack{Nj\\ 1\le j\le N}} &= \sum_{1\le k\le N} B_{Nk}.A_{kj} = \sum_{1\le k\le N}\left\{\frac{1}{f(1)}.d(k,1) - \sum_{1\le l\le N} B_{l\,k}\right\}.f(\lceil k/j\rceil) \\ &= \frac{1}{f(1)}.f(\lceil 1/j\rceil) - \sum_{1\le l\le N}\left\{\sum_{1\le k\prec N} B_{l\,k}.f(\lceil k/j\rceil)\right\}. \end{aligned} \tag{14}$$

Using (13) in the above, and considering the cases $j = N$ and $j \ne N$, yields

$$C_{\substack{Nj\\ 1\le j\le N}} = 1 - \sum_{\substack{1\le l\prec N\\ 1\le j\le N}} C_{l\,j} = 1 - \sum_{\substack{1\le l\prec N\\ 1\le j\le N}} d(l, j) = 1 - \{1 - d(N, j)\} = d(N, j). \tag{15}$$

Combining (13) and (15), we have

$$C_{ij} = d(i, j) \text{ for } 1 \le \{i, j\} \le N. \tag{16}$$

This completes the proof. □

5. Structure of the inverse transformation matrix

On examining the structure of $g\{i/j\}$ and $g\{i/(j-1)\}$ in (10), we observe certain characteristic sparse structure of the inverse transformation matrices:

(a) For $1 \le i < N$, the entries of the matrix are nonzero only when i/j or $i/(j-1)$ are finite integers, and $g\{i/j\}$ and $g\{i/(j-1)\}$ are nonzeros. Some of the entries satisfying both these conditions may also be zero because of the cancellation of the $g\{i/j\}$ and $g\{i/(j-1)\}$ terms. Matrix $B_{i,j}$ may be viewed as the difference of two matrices having the same entries but shifted by a column.

(b) The last row of B is a negative summation of the other rows, with the exception of $1/f(1)$ added to element B_{N1}.

Next, we determine an upper bound of nonzero entries of B. For the entry $g(i/j) = g(p)$ to be nonzero, p must be an integer. For $i \neq N$, the number of $g(p)$s for each value of p is at the most $\lfloor (n-1)/p \rfloor$. So is the case for $g[i/(j-1)].(1 - d_{j,1})$. The Nth row has at the most N entries. Therefore, an upper bound of number of nonzero entries of B is

$$\sum_{\substack{B_{i,j} \neq 0 \\ 1 \leq \{i,j\} \leq N}} 1 \leq N + 2 \sum_{1 \leq p \leq N} \lfloor (N-1)/p \rfloor \leq 2N + 2(N-1)\log_e(N-1) \leq 2N(1+\log_e N). \quad (17)$$

6. Conclusions and recommendations for further research

In this paper, we state and prove the key results of a new class of number-theoretic transforms. We expect that this class of transform will find wide-scale application in signal processing, coding and encryption, design of telecommunication equipment and other applications. Particular attractions of these transforms are their computational efficiency, and design flexibility through the choice of a variety of arithmetic functions.

One particular subclass of these transforms is called the alternating pulse transform. Here, any signal can be represented by unit-magnitude (i.e., alternating +1 and –1) uniform pulse-widths of 1, 2, 3,…, N. Comparable to the fast Fourier transforms (FFT), the alternating pulse spectra of a signal yield much useful information about its characteristics. This work by the author is yet unpublished; it is available on request [7].

Another remark about the transform described should be relevant for researchers in signal processing. The differential form of representation of the spectra as expressed in eqn (10) leads to a process of sequential computation of the signal spectra. That is, it is possible to construct a signal processor that will start computing the spectral coefficients as soon as the signal sample starts arriving; it is not necessary to wait for the entire block of signal to arrive to start the spectral computation process. The relevant Dirichlet inverses required for computation of the spectrum can be pre-computed and stored.

Some of the applications of the new transform are likely to be in the following areas:

(a) Signal processing and analysis: The choice of the associated arithmetic function will decide the type of signal spectrum and the type of representation. Therefore, the arithmetic function chosen will depend on the specific signal-processing application.

(b) Real-time coding, encryption and decryption: The transform's efficacy in fast processing of signals should make real-time applications attractive. Furthermore, sequential computation of the spectrum gives ability to generate nearly real-time spectrum of the signal. These facts should be of significance for small portable communication equipment, e.g. cell phones, onboard satellite equipment.

(c) Efficient utilization of airwave telecommunication spectra: Applications for these are likely to be similar to that of code division multiplexing (CDM). The present crowding of the airwaves is likely to lead to the utilization of the new transform in quest of efficient packing of users within the available bandwidth.

7. Dedication

I dedicate this work on the new transforms to two of my *gurus*, with whom I had privilege to work and study. My mentor at the Indian Institute of Science, Late Prof. Satish Dhawan [8] coaxed us to '*be fascinated by un-chartered territories.*' My teacher at the University of Delhi, Late Prof. Daulat Singh Kothari [9], impressed on us that '*every phenomenon behoves an explanation.*' Undoubtedly, schooling of these inimitable *gurus* greatly influenced the reported work.

References

1. K. T. Atanassov, An arithmetic function and some of its applications, *Bull. Number Theory Related Topics*, **9**, 18–27 (1985).
2. G. A. Jones, and J. M. Jones, Arithmetic functions, *Elementary number theory*, Ch. 8, pp. 143–162, Springer-Verlag (1998).
3. P. J. McCarthy, *Introduction to arithmetic functions*, Springer-Verlag (1985)
4. G. H. Hardy, and E. M. Wright, *An introduction to the theory of numbers*, 5th edn, p. 248, Clarendon (1976).
5. T. F. Apostol, *Introduction to analytic number theory*, p. 29, Th. 2.6, Springer-Verlag (1976).
6. J. Knopfmacher, *Abstract analytic number theory*, p. 26, Proposition 1.3, Dover (1990).
7. Sushanta Srivastava, *Alternating pulse transform and the associated arithmetic function S(m)*. To be published. Summary of this work is available from the author on request (sushantasrivastava@yahoo.com).
8. http://en.wikipedia.org/wiki/Satish_Dhawan
9. http://www.vigyanprasar.gov.in/scientists/DKothari.htm