Models and Analysis of Vocal
Emissions for Biomedical Applications
(MAVEBA 1999)
Firenze, Italy, September 1-3, 1999

SPEECH SIGNAL SYNTHESIS BASED ON THE FILTER BANKS IN FINITE AND POLYNOMIAL RINGS*

Alexander M. Krot and Vadim O. Kudryavtsev
Institute of Engineering Cybernetics of the National Academy of Sciences of Belarus,
6, Surganov str. 220012, Minsk, Belarus
e-mail: alxkrot@newman.basnet.minsk.by

Abstract. High quality filters are essential part of vocoders. By means of filter banks structures we can combine modern DSP algorithms with hardware realizations having many parallel identical devices. This paper proposes digital filter realization based on filter bank structure suitable for hardware realization.

Keywords: filter banks, generalized K_N-convolution, eigen transform, fast number-theoretic transform, fast polynomial transform.

Introduction

During last years speech and data transmission is realized mainly by digital form. Vocoder devices are the most suitable for solving problems of low-speed speech transmission with subsequent information scrambling and conserving acceptable quality level of sound on receiving side. At present it is possible to realize high quality filters that are essential part of those devices on the basis of modern algorithms and modern technology. By means of filter banks structures we can combine modern DSP algorithms with hardware realizations having many parallel identical devices.

A purpose of this paper is to show how new discrete transforms can be used in filter bank structures for realizing digital FIR filters.

An aliasing error analysis of filter banks leads to the structure shown in fig.1 [1]. It was shown [2] that such structure is free from aliasing errors if matrix $\mathbf{P}(z)$ is pseudocirculant. An output vector of polyphase components is determined from input ones with equation :

$$\mathbf{Y}(z)=\mathbf{X}(z)\mathbf{P}(z)=$$

$$=\mathbf{S}(z)\begin{bmatrix} P_0(z) & P_1(z) & \cdots & P_{M-1}(z) \\ z^{-1}P_{M-1}(z) & P_0(z) & \cdots & P_{M-2}(z) \\ \vdots & \vdots & \ddots & \vdots \\ z^{-1}P_1(z) & z^{-1}P_2(z) & \cdots & P_0(z) \end{bmatrix} \quad (1)$$

where $\mathbf{Y}(z)=[Y_0(z),Y_1(z),\ldots,Y_{M-1}(z)]$, $\mathbf{X}(z)=[X_0(z),X_1(z),\ldots,X_{M-1}(z)]$, $\mathbf{P}(z)$ is pseudocirculant, i.e. next row of $\mathbf{P}(z)$ is obtained from previous one by performing a cyclic right-shift followed by the multiplication of z^{-1} to the elements below the main diagonal. In this case filter bank is a linear system with a transfer function

$$F(z)=\sum_{i=0}^{M-1}P_i(z^M)z^{-i} \qquad (2)$$

where $P_i(z)$ is i-th polyphase component of function $F(z)$. From now on we will consider only structures with FIR-analysis and synthesis filters, so $P_i(z)$, $0\le i\le M-1$ are polynomials.

An expression (1) is called a pseudocyclic convolution.

A realization of digital filter with a filter bank was described in [3],[4]. Computation of (1) was made as linear convolution (by performing fast linear convolution algorithms) of polynomials followed by reduction to pseudocirculant. However, it is of interest to find more effective methods of pseudocyclic convolution because of regularity property of $\mathbf{P}(z)$.

An efficient approach to solve this problem is based on the eigen transform methods. It is well known from [5]-[8] that Vandermonde transform is the eigen transform for generalized $\mathbf{K}_N$-convolutions being a parametric convolution in particular cases.

The generalized $\mathbf{K}_N$-convolution of $x^T=(x_0,x_1,\ldots,x_{N-1})$ and $h^T=(h_0,h_1,\ldots,h_{N-1})$ can be written as

$$y^T=x^T\mathbf{Z}_N(h) \qquad (3)$$

where $y^T=(y_0,y_1,\ldots,y_{N-1})$ is the row vector of the generalized K_N-convolution,

* This work was supported partly by International Science and Technology Center (ISTC) under project B-95 and partly by University of Firenze, Italy

$$\mathbf{Z}(h)=\begin{bmatrix} h^T\mathbf{K}_N^0 \\ h^T\mathbf{K}_N^1 \\ \vdots \\ h^T\mathbf{K}_N^{N-1} \end{bmatrix}$$ is matrix operator for the generalized $\mathbf{K}_N$-convolution,

$$\mathbf{K}_N=\begin{bmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & & & 1 \\ q_N & q_{N-1} & \cdots & q_1 \end{bmatrix}$$ is generalized $\mathbf{K}_N$-shift represented by the Frobenius matrix.

If the parameters of the generalized $\mathbf{K}_N$-shift operator are defined as $q_{N-1}=q_{N-2}=\ldots=q_1=0$ and $q_N=\beta$ then $\mathbf{K}_N=\mathbf{S}_N(\beta)$ is the parametric shift matrix and $\mathbf{Z}_N(h)=\mathbf{C}_{N,\beta}(h)$ is the parametric convolution operator with parameter β [5]-[8].

It will be shown in this paper how pseudocyclic convolution can be transformed to parametric convolution in order to use eigen transform methods for computing (1).

Pseudocyclic convolution using MNTT

An algorithm for calculation of linear convolution by means of modified number-theoretic transform (MNTT) under condition of dynamic range decreasing was described in [9]. It is possible to use such method to calculate (1). A computation of pseudocyclic convolution can be realized by means of parametric convolution in ring of integers modulo D:

$$\mathbf{Y}_\beta(z)=\mathbf{X}(z)\mathbf{P}_\beta(z)=$$
$$=\mathbf{S}(z)\begin{bmatrix} P_0(z) & P_1(z) & \cdots & P_{M-1}(z) \\ \beta P_{M-1}(z) & P_0(z) & \cdots & P_{M-2}(z) \\ \vdots & \vdots & \ddots & \vdots \\ \beta P_1(z) & \beta P_2(z) & \cdots & P_0(z) \end{bmatrix}. \quad (4)$$

If all the coefficients of polynomials of $\mathbf{Y}(z)$ are in the range $-\beta/2\ldots\beta/2$, $\beta\le\sqrt{D}$, then using uniqueness of number representation

$$a+\beta b,\ a<\beta \quad (5)$$

it is possible from samples of $\mathbf{Y}_\beta(z)$ to recover a vector of linear convolution and then to obtain vector $\mathbf{Y}(z)$, corresponding to (1) [9].

Parametric convolution (4) can be calculated by means of MNTT, which is an eigen transform of matrix operator $\mathbf{P}_\beta(z)$ [5]-[8]:

$$\mathbf{Y}_\beta(z)=\mathbf{X}(z)\ \mathbf{T}\ diag\left[\tilde{\mathbf{P}}(z)\right]\ \mathbf{T}^{-1} \quad (6)$$

where $\tilde{\mathbf{P}}(z)=\left[P_0(z),P_1(z),\ldots,P_{M-1}(z)\right]\mathbf{T}$, $\mathbf{T}=\mathbf{VW}$, $\mathbf{V}=diag[1,v,v^2,\ldots,v^{M-1}]$, $v^M=\beta\ (\mathrm{mod}\ D)$,

$\mathbf{W}=[\omega^{ik}]$, $0\le i,k\le M-1$ is Fourier matrix operator in ring modulo D, i.e. NTT matrix operator.

Calculation structure corresponding to (6) is represented in fig. 2. Samples in profile $R-R$ except r_{M-1} have to be restricted in the range $-\beta/2\ldots\beta/2$. In each of parallel channels L/M multiplications per sample are performed at rate M-times less then rate of input samples. Hence, this method requires $M\frac{L}{M}\frac{1}{M}=\frac{L}{M}$ multiplications per sample needed to implement internal filters. Direct and inverse transforms represent pre- and postadditions in Winograd sense and can be calculated by any of known algorithms.

Calculation of pseudocyclic convolution using MNTT in finite field

Let filter impulse response length is equal to L. Let we are processing input sequence dividing it by blocks with length also equal to L by means of overlap add scheme (in common case length of block B must be equal or greater than impulse response length L). Let number of channels of filter bank equal to M. We can calculate pseudocyclic convolution (1) by embedding it into finite field $GF(q^{2m})$, where $m=L/M$. For convenience we replace z^{-1} with u and write (1) in new notation

$$\mathbf{Y}'(u)=\mathbf{X}'(u)\mathbf{P}'(u)=$$
$$=\mathbf{X}'(u)\begin{bmatrix} P_0'(u) & P_1'(u) & \cdots & P_{M-1}'(u) \\ uP_{M-1}'(u) & P_0'(u) & \cdots & P_{M-2}'(u) \\ \vdots & \vdots & \ddots & \vdots \\ uP'(u)_1 & uP_2'(u) & \cdots & P_0'(u) \end{bmatrix}, \quad (7)$$

where $\mathbf{Y}'(u)=\left[Y_0'(u),Y_1'(u),\ldots,Y_{M-1}'(u)\right]$, $\mathbf{X}'(u)=\left[X_0'(u),X_1'(u),\ldots,X_{M-1}'(u)\right]$.

Polynomials $Y_i'(u)$, $X_i'(u),P_i'(u)$ have coefficients with mirrored sequence order in comparison to $Y_i(z),X_i(z),P_i(z)$, respectively.

Now we define requirements to the field.

1. Field characteristic q is chosen in accordance with the dynamic range of output sequence.

2. Field extension degree equal to $2m$

guarantees correct calculation of products $P_i(z)X_j(z)$ and $z^{-1}P_i(z)X_j(z)$, $0 \le i, j \le M-1$ in (1).

3. Operations in the field are defined modulo polynomial $f(u)$. The choice of $f(u)$ as a non-primitive polynomial guarantees, that there exist certain element $v(u)$, being an M-th root of u for certain M. For example,

$(u+u^2+u^3)^3 = u \bmod (2, 1+u+u^2+u^3+u^4)$

4. Element $\omega(u)$ of order M must exist in the field.

In the field determined like that an expression (7) represents parametric convolution and can be calculated by means of eigen transform $\mathbf{T}(u)$ of matrix operator $\mathbf{P}'(u)$ in (7):

$$\mathbf{Y}'(u) = \mathbf{X}'(u)\mathbf{T}(u)diag(\tilde{\mathbf{P}}'(u))\mathbf{T}^{-1}(u), \qquad (8)$$

where $\tilde{\mathbf{P}}'(u) = [P_0'(u), P_1'(u), \ldots, P_{M-1}'(u)]\mathbf{T}(u)$,

$$\mathbf{T}(u) = \mathbf{V}(u)\mathbf{W}(u),$$

$$\mathbf{V} = diag[1, v(u), v^2(u), \ldots, v^{M-1}(u)],$$

$$\mathbf{W}(u) = [\omega^{ik}(u)],\ 0 \le i, k \le M-1,$$

$$v^M(u) = u.$$

Calculation of (8) can be realized with a filter bank structure (fig. 3).

In each of M parallel channel a product of two degree *2m* polynomials modulo irreducible polynomial $f(u)$ is computed. Such product can be calculated with *4m-1* multiplications. Therefore, total number of multiplications required for implementing internal filters is $(4m-1)M = 4L - M$ per each block of L samples, or less than *4* multiplications per sample. Direct and inverse eigen transforms are decomposed into product of diagonal matrix and NTT matrix operator in considered finite field.

Calculation of pseudocyclic convolution using polynomial transform

If polynomial $f(u)$ is reducible convolution (7) is embedded in polynomial ring modulo $f(u)$. We add one more requirement to the previous four ones - existence of inverse number M^{-1} of M (i.e. $MM^{-1} = 1 \pmod{q}$).

Now eigen transform $\mathbf{T}(u)$ is a polynomial transform [10]. Calculations are arranged again in correspondence to equation (8) and fig. 3.

If polynomial $f(u)$ is decomposed on linear factors each polynomial product can be calculated with $2m$ multiplications. Therefore we can arrive a total number of multiplications for implementing internal filters equal to $2mM = 2L$ per each block of L samples, or 2 multiplications per sample.

Example.

Let $q = F_5 = 2^{2^5} + 1$. Let filter length $L = 8$, and number of channels $M = 4$. Then degree of polynomial $f(u)$ must equal to $2L/M = 4$. Let $f(u) = u^4 + 1$. It is evident, that $\omega(u) = u^2$ has order equal to 4 in ring modulo $f(u)$. A fourth root of u has a form $v(u) = 17821697 + 4008640513u +$

$+ 4026466545u^2 + 3855u^3$.

As a result we obtain eigen transform $\mathbf{T}(u)$ in the form:

$$\mathbf{T}(u) = diag([1, v(u), v^2(u), v^3(u)]) \times$$

$$\times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & u^2 & -1 & -u^2 \\ 1 & -1 & 1 & -1 \\ 1 & -u^2 & -1 & u^2 \end{bmatrix} . \qquad (9)$$

Now consider internal filter implementation. Polynomial $f(u)$ is decomposed in product of four linear cofactors

$f(u) = (u - 3735508651)(u - 3718731691) \times$

$\times (u - 559458646)(u - 576235606)$.

Hence, polynomial product modulo $f(u) = u^4 + 1$ representing skew-cyclic convolution can be calculated with four multiplications.

A skew-cyclic convolution is a parametric one and can be computed also by eigen transform:

$$\mathbf{T}_{SC} = diag([1, \tau, \tau^2, \tau^3]) \times$$

$$\times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \varepsilon & -1 & -\varepsilon \\ 1 & -1 & 1 & -1 \\ 1 & -\varepsilon & -1 & \varepsilon \end{bmatrix} , \qquad (10)$$

where $\varepsilon = 46837383$ is 4-th root of unity,

$\tau = 3735508651$ is 8-th root of unity.

In total, four channels require $4*4=16$ multiplications for processing of block of length 8. Eigen transforms require in this example only additions for their implementation.

Conclusion

This work proposes new methods for FIR filter realization by means of filter banks structure. New kind of transform were used to reduce number of channels in comparison with method proposed in [3] and hence to decrease arithmetical complexity of realization.

Described methods have sufficiently large flexibility for structure choice for each concrete realization. In general optimal number of channels is computed to minimize objective function

$$C = M\ C_F(L/M) + 2\ C_T(M), \qquad (11)$$

where $C_F(L/M)$ is direct filter realization complexity of length L/M,

$C_T(M)$ is transform realization complexity of length M.

Note for example that for $M = 1$ we obtain a direct filter realization and for $M = L$ we obtain a method of convolution calculation by means of MNTT's similar to one of the methods proposed in [9].

References

1. P.P. Vaidyanthan. Multirate digital filters, filter banks, polyphase networks, and applications. A tutorial. Proc. IEEE, vol. 78. pp. 56-93, Jan 1990.
2. P.P. Vaidyanathan, S.K. Mitra. Polyphase Networks, Block Digital Filtering, LPTV Systems and Alias-free System Banks: A Unified Approach Based on Pseudocirculants. IEEE Transactions on Acoustics, Speech and Signal Processing. Vol. ASSP-36, pp.381-391, Mar. 1988.
3. M. Vetterli. Running FIR and IIR Filtering Using Multirate Filter Banks. IEEE Transactions on Acoustics, Speech and Signal Processing. Vol. ASSP-36, No.5, May 1988, pp.731-738.
4. A.M. Krot, V.O. Kudryavtsev. A Theory of Filter Bank Analysis and Synthesis and Its Implementation. Achievements of Modern Radioelectronics. No.2, 1999, pp.3-17. (In Russian).
5. A.M. Krot, Discrete Models of Dynamic Systems Based on the Polynomial Algebra. Minsk: Nauka i Tekhnika, 1990 (the monograph in Russian).
6. A.M. Krot. Algorithms and Multiplicative Complexity of the Reduction a Modulo Arbitrary Polynomial, Generalized K_N-Convolution and Fast Vandermonde Transform. Proc. 13th Intern. Conf. on Digital Signal Processing (DSP97), July 2-4, 1997, Vol.2, Santorini, Greece, pp. 893-897.
7. A.M. Krot. Fast Reduction a modulo Polynomial and Fast Vandermonde Transform based on Fast Fourier Transform Algorithm. Proc. of SPIE, vol. 3374, April 13-15, 1998, Orlando, USA, pp 505-514.
8. A.M. Krot and H.B. Minervina. Fast Algorithm for Reduction a modulo Polynomial and Vandermonde Transform Using FFT. Proc. of IX European Signal Processing Conference (EUSIPCO-98), vol. 1, September 8-11, 1998, Rhodes, Greece, pp 173-176.
9. N.S. Rubanov, E.I. Bovbel, P.D. Kukharchik, V.J. Bodrov. The Modified Number-Theoretic Transform over the Direct Sum of Finite Fields to Compute the Linear Convolution. IEEE Transactions on Signal Processing, Vol.46, No. 2, February 1998, pp.813-818.
10. H.J. Nussbaumer, Fast Fourier Transform and Convolution Algorithms. Berlin, Heidelberg, and New York: Springer,1981.

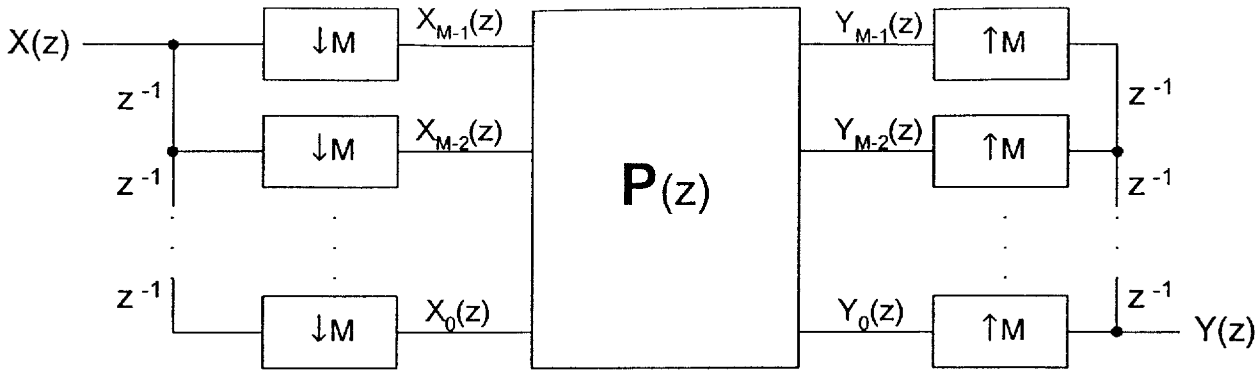

Fig. 1. Equivalent filter bank structure.

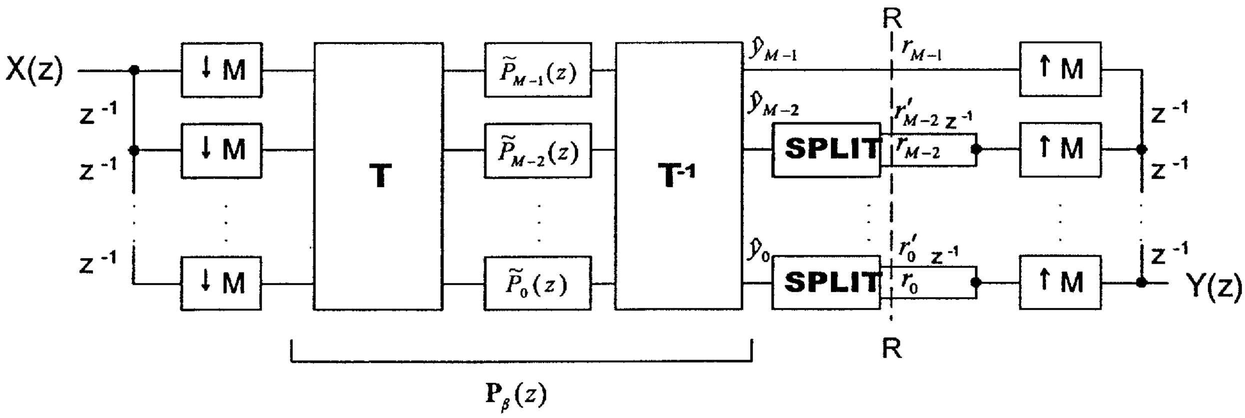

Fig. 2. Digital filter realization by means of MNTT

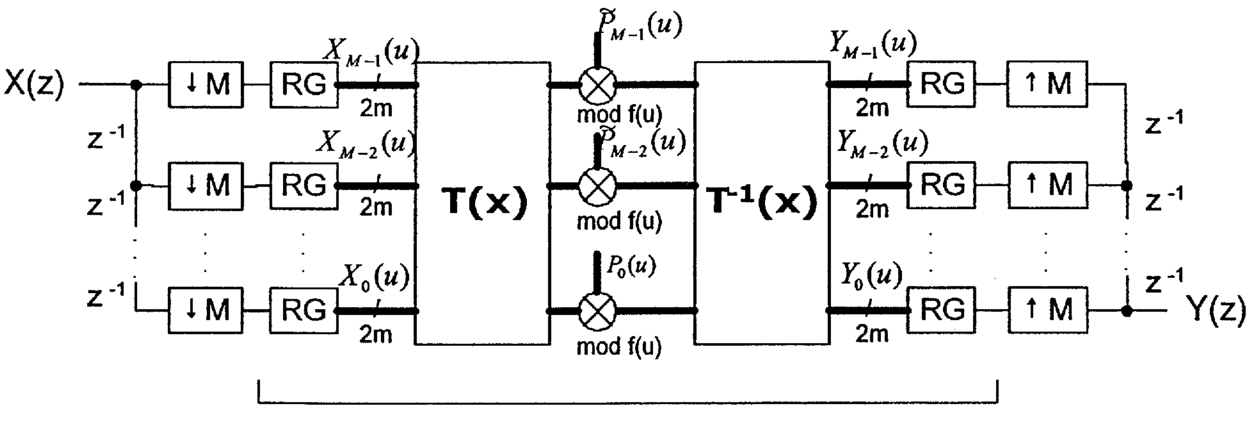

Fig. 3. Digital filter realization in polynomial fields and rings