A Group of Permutations that Commute with the Discrete Fourier Transform

Paulo Jorge S. G. Ferreira

***Abstract*—In this correspondence, we characterize a potentially useful set of permutation matrices that commute with the Fourier matrix of order n. The set of all such permutation matrices is a group under matrix multiplication, and every element of the group is its own inverse. We study the number of these permutations as a function of the order n of the Fourier matirx and conclude that it is a multiplicative function of n.**

I. Preliminaries

With each permutation σ defined on the set $\{0, 1, \ldots, n-1\}$, we associate a permutation matrix $\mathbf{P}$ of order n in the usual way. Let $\mathbf{F}$ be the Fourier matrix of order n, which is given by $F_{k\ell} = e^{j2\pi k\ell/n}/\sqrt{n}$, where j denotes the imaginary unit. The discrete Fourier transform (DFT) $\hat{\mathbf{x}}$ of a vector $\mathbf{x} \in C^n$ is defined as $\hat{\mathbf{x}} = \mathbf{F}\mathbf{x}$.

Chao [1] has shown that $\mathbf{PF} = \mathbf{FP}$ if and only if $\mathbf{P}$ is involutory, i.e., $\mathbf{P}^2 = \mathbf{I}$, and $\sigma(k) = \sigma(1)k \bmod n$ for all k, where σ is the permutation on $\{0, 1, 2, \ldots, n-1\}$ represented by $\mathbf{P}$. Hence, the set of $\mathbf{P}$ for which $\mathbf{PF} = \mathbf{FP}$ is a subgroup C_n of the group of permutation matrices in which each $\mathbf{P} \in C_n$ is its own inverse. Thus, a permutation matrix $\mathbf{P} \in C_n$ maps DFT pairs $\{\mathbf{x}, \hat{\mathbf{x}}\}$ into permuted DFT pairs $\{\mathbf{P}\mathbf{x}, \mathbf{P}\hat{\mathbf{x}}\}$.

We study the number of such permutations as a function of the order n of the Fourier matrix $\mathbf{F}$. It turns out that for $n > 2$, there are at least two such permutations and exactly two if n is prime. We show that the actual number of permutations is a multiplicative function of n, that is, if k and m are two relatively prime integers, the number of permutations in C_n with $n = km$ is given by the product of the number of permutations in C_k and C_m.

II. Results

Proposition 2.1: A permutation matrix $\mathbf{P}$ commutes with the Fourier matrix $\mathbf{F}$ of order n if and only if the permutation σ represented by $\mathbf{P}$ satisfies the properties $\sigma(k) = \sigma(1)k \bmod n$ for all k and $[\sigma(1)]^2 = 1 \bmod n$. Hence, the number of permutations that commute with the Fourier matrix of order n is equal to the number of square roots of unity modulo n.

It is easy to check that $\mathbf{FP} = \mathbf{PF}$ if and only if $\sigma(i)\sigma(k) = ik \bmod n$ for all $i, k = 0, 1, \ldots, n-1$. Therefore, if $\mathbf{P}$ and $\mathbf{F}$ commute, then $[\sigma(1)]^2 = 1 \bmod n$ and $\sigma(k) = k\sigma(1) \bmod n$ for all $k = 0, 1, \ldots, n-1$. Conversely, if $\sigma(k) = k\sigma(1) \bmod n$ for all $k = 0, 1, \ldots, n-1$ and $[\sigma(1)]^2 = 1 \bmod n$, then $\sigma(i)\sigma(k) = i\sigma(1)k\sigma(1) = ik \bmod n$ for all $i, k = 0, 1, \ldots, n-1$.

Obviously, the set of all such permutation matrices is a group under matrix multiplication. The order of the group depends on the number of square roots of unity mod n.

Manuscript received July 23, 1992; revised April 13, 1993. The associate editor coordinating the review of this paper and approving it for publication was Prof. James Cooley.

The author is with the Departamento de Electrónica e Telecomunicações/INESC, Universidade de Aveiro, Aveiro, Portugal.

IEEE Log Number 9214169.

TABLE I
NUMBER OF PERMUTATIONS THAT COMMUTE WITH $\mathbf{F}$ FOR A NUMBER OF POSSIBLE VALUES OF n.

Order	*Number of solutions*	*Solutions*
4	2	1,3
5	2	1,4
6	2	1,5
7	2	1,6
8	4	1,3,5,7
9	2	1,8
10	2	1,9
11	2	1,10
12	4	1,5,7,11
13	2	1,12
14	2	1,13
15	4	1,4,11,14
16	4	1,7,9,15
17	2	1,16
18	2	1,17
19	2	1,18
20	4	1,9,11,19
21	4	1,8,13,20
22	2	1,21
23	2	1,22
24	8	1,5,7,11,13,17,19,23

For each $n > 2$, there will always exist two such permutations where one is the identity. The other is defined by

$$\mathbf{J} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 1 & \cdots & 0 \end{bmatrix}$$

which is the square of the Fourier matrix; this is a fact that obviously explains the commutativity. In addition, note that $\mathbf{J}^2 = \mathbf{I}$, as is required for $\{\mathbf{I}, \mathbf{J}\}$ to be a group. The matrices $\mathbf{I}$ and $\mathbf{J}$ correspond to the two square roots of unity mod n that always exist independently of n, that is, 1 and $n-1$.

If we consider each vector in C^n to be one period of a time series, the effect of multiplication by $\mathbf{J}$ is equivalent to an inversion of the temporal axis, as expressed by $t' = -t$. The classical Fourier transform presents a similar invariance property: If $\hat{f}(\omega)$ is the Fourier transform of $f(t)$, then $\hat{f}(-\omega)$ will be the Fourier transform of $f(-t)$.

When n is prime, 1 and $n-1$ are the only solutions to $x^2 = 1 \bmod n$, but when n is composite, there might be more solutions. The exact number of solutions can be found in Table I for a few values of n.

We will now proceed to show that this number is a multiplicative function of n. Let $n = \prod_{i=1}^{k} p_i^{\gamma_i}$. The equation

$$f(x) = 0 \pmod n \tag{1}$$

where f is a polynomial in x with integer coefficients and degree at least 1, has a solution if and only if each of the equations $f(x) = 0 \bmod p_i^{\gamma_i}$ is soluble [2]. It is easy to see that each of the solutions x_i of $f(x) = 0 \bmod p_i^{\gamma_i}$ originate a different solution of (1), which implies that the number of solutions of (1) is a multiplicative function of n. Taking $f(x) = x^2 - 1$, we arrive at the following result.

Proposition 2.2 The number of permutation matrices that commute with the Fourier matrix of order n is a nontrivial multiplicative function of n.

This agrees with the results depicted in Table I.

The solutions of

$$f(x) = 0 \pmod{2^{k+1}}. \tag{2}$$

can be found [2] from the solutions of

$$f(x) = 0 \pmod{2^k} \tag{3}$$

in the following way. Let x be a solution of (3). The integer

$$x + t2^k \tag{4}$$

solves (2) if and only if

$$2tx + \frac{x^2 - 1}{2^k} = 0 \pmod 2. \tag{5}$$

Suppose, for example, that we want to find the solutions to $x^2 = 1 \bmod 8$ knowing that the solutions when $n = 4$ are 1 and 3. Equation (5) then gives $t = 1$, which, inserted in (4), immediately generates the solutions 5 and 7 from 1 and 3.

ACKNOWLEDGMENT

The author gratefully acknowledges the help and criticism of an anonymous reviewer.

REFERENCES

[1] C. -Y. Chao. "On a type of circulants," *Linear Algebra and its Applications*, vol. 6, pp. 241–248, 1973.

[2] H. E. Rose. *A Course in Number Theory*. Oxford: Oxford University Press, 1988.

On the Mean-Square Error Performance of Adaptive Minimum Variance Beamformers Based on the Sample Covariance Matrix

Jeffrey L. Krolik and David N. Swingler

***Abstract*—This correspondence examines the mean-square error (MSE) performance of two common implementations of adaptive linearly constrained minimum variance (LCMV) beamformers that employ the sample covariance matrix. The Type I beamformer is representative of block processing methods where the same input data is used both to compute the adaptive weights and to form the beamformer output. The Type II beamformer, as in many recursive schemes, applies adaptive weights computed from previous data to the current input. Due to correlation between the adaptive weights and the input data, the Type I LCMV beamformer exhibits signal cancellation, which is shown here to cause signal estimate bias. To explicitly account for signal cancellation, the mean-square error (MSE) and output signal-to-noise ratio (SNR) measures of the bias-corrected Type I beamformer are analyzed here, thus extending previous results. Further, new analytical results for these performance measures are given for the Type II LCMV beamformer. Comparison of bias-corrected Type I and Type II implementations indicate that both methods yield exactly the same MSE and output SNR performance.**

Manuscript received October 2, 1992; revised July 6, 1993. The associate editor coordinating the review of this paper and approving it for publication was Prof. John A. Stuller. This work was supported by the Canadian Defence Research Establishment Atlantic (DREA) under contract no. W7707-0-00500-(009) and the U.S. Office of Naval Research under grant N0014-92-J-1090.

J. L. Krolik is with the Department of Electrical Engineering, Duke University Durham, NC 27708-0291.

D. N. Swingler is with the Division of Engineering, Saint Mary's University, Halifax, Canada B3H 3C3.

IEEE Log Number 9214188.

I. INTRODUCTION

In an interesting recent correspondence by Van Veen [1], the expected output power and mean-square error (MSE) of the linearly constrained minimum variance (LCMV) beamformer were derived for an arbitrary number of adaptive degrees of freedom. The analysis in [1], which extends previous work of [3]–[5], [8] was based on the use of the sample covariance matrix as a covariance matrix estimate and where the same input data is used both to compute the adaptive weights and to form the beamformer output. This type of operation, which is referred to here as Type I, is representative of block-mode adaptation. The mean output power of the Type I LCMV beamformer is less than the corresponding "infinite-time" beamformer (i.e., one employing the true covariance matrix rather than a finite-time estimate). As noted in [1], this reduction in power implies that there is a signal cancellation effect at play in the finite-time Type I beamformer. This signal cancellation effect can be traced to the correlation between the adaptive beamformer weights and the current input data. In this correspondence, this signal cancellation effect is examined more closely, and it is shown that the signal component of the Type I beamformer output is, in fact, a scaled version of the input signal. In [1], calculation of the MSE is performed without regard to possible scaling of the signal output, which leads to a somewhat optimistic performance prediction. In this correspondence, the MSE of a bias-corrected Type I beamformer designed to explicitly account for signal cancellation is evaluated, thereby extending the result of [1]. In addition, the corrected MSE is used to compute output signal-to-noise ratio (SNR).

A disadvantage of block-mode processing is that the output data is available only after a delay corresponding to the data block length. An alternative implementation that is representative of recursive processing schemes is to apply weights computed using the previous data block to the current input data. This mode of operation is referred to here as Type II. For Type II LCMV beamformers, the adaptive beamformer weights are uncorrelated from the input data, and hence, signal cancellation is avoided. In this case, no bias correction is required, and new results for the MSE and output SNR of the Type II beamformer are given. Interestingly, it is shown that even though the Type I and Type II implementations differ in their use of the current data snapshot, when the Type I output is corrected for signal estimate bias, both have precisely the same MSE and output SNR performance.

II. SIGNAL CANCELLATION AND TYPE I ADAPTIVE LCMV BEAMFORMER PERFORMANCE

In this section, the signal cancellation effect exhibited by the block adaptive LCMV beamformer is examined. Adopting the notation and assumptions of [1], let the columns of the $N \times M$ data matrix X represent M independently identically distributed (i.i.d.) zero-mean complex Gaussian random vectors impinging on an N element sensor array. Using the generalized sidelobe canceler (GSC) realization of the LCMV beamformer, the beamformer weights are given by [1]

$$w = w_q - T_a(T_a^H X X^H T_a)^{-1} T_a^H X X^H w_q \tag{1}$$

where T_a denotes the N by K generalized signal-blocking matrix, and K represents the number of adaptive degrees of freedom available to the beamformer. If L is the number of constraints used in defining the quiescent beamformer weight vector w_q, then $K \leq N - L$. Note that superscript H denotes conjugate transpose, $T_a^H w_q = 0$, and $M^{-1} \cdot XX^H$ is the sample covariance matrix. The beamformer output is denoted by the M by 1 vector $y = X^H w$.