Generalized Subspace-based Algorithms For Blind Channel Estimation In Cyclic Prefix Systems

Borching Su
Department of Electrical Engineering
California Institute of Technology
Pasadena, California 91125
Email: borching@systems.caltech.edu

P. P. Vaidyanathan
Department of Electrical Engineering
California Institute of Technology
Pasadena, California 91125
Email: ppvnath@systems.caltech.edu

***Abstract*— In this paper a novel generalization of subspace-based blind channel identification methods in cyclic prefix (CP) systems is proposed. For the generalization, a new system parameter called *repetition index* is introduced whose value is unity for previously reported special cases. By choosing a repetition index larger than unity, the number of received blocks needed for blind identification is significantly reduced compared to *all* previously reported methods. This feature makes it more realistic especially in wireless environments where the channel state is usually fast-varying. Given the number of received blocks available, the minimum value of repetition index is derived. Theoretical limit allows the proposed method to perform blind identification using only three received blocks. Simulation results not only demonstrate the capability of the algorithm to perform blind identification using fewer received blocks, but also show that in some cases system performance can be improved by choosing a repetition index larger than needed. If the number of received blocks and the repetition index are optimally chosen, the proposed method outperforms previously reported special cases, especially in time-varying channel environments.** [1]

I. Introduction

In digital communication systems, it is well-known that linear redundant precoding (LRP) facilitates block equalization of frequency-selective channels by eliminating inter-block interference (IBI). Two major types of LRP techniques are zero-padding (ZP) and cyclic prefix (CP). ZP systems are superior in the sense they guarantee symbol recovery regardless of channel null locations. But the CP precoders are more widely used in many current standards such as orthogonal frequency division multiplexing (OFDM) and single-carrier cyclic prefix (SC-CP).

Blind channel estimation algorithms exploiting redundancy introduced by LRP have long been of great interest. Systems using these techniques require very few, if any, further redundant symbols and hence possess better bandwidth efficiency compared to those using training-based methods. However, many blind estimation methods [1] require accumulation of a large number of received data so that they usually become unrealistic over time-varying channels. Recently, several new subspace-based methods exploiting ZP structures have been reported to require much fewer blocks [2]–[4]. These advances suggest blind channel estimation can be done in a much shorter time and hence become more applicable to time-varying channels.

However, ZP structures do not fit the currently most popular wireless standards such as OFDM and hence the applications of these blind methods are seriously limited. Blind identification methods in CP systems have completely different and usually much more sophisticated designs. Most existing blind identification methods for CP/OFDM systems fall into either subspace-based [5] or non-subspace-based categories. Non-subspace-based methods often take advantage of finite-alphabet property of transmitted symbols and involve considerable computational complexity especially when the size of constellation is large [6], [7]. Subspace-based methods, on the other hand, require no knowledge on symbol constellations, but many of them [8]–[12] involve calculating statistics of received blocks and hence converge much slower than methods exploiting finite constellations. The number of received blocks needed for estimation is high in order to satisfy the persistency of excitation (p.o.e) criterion of the input [11].

In this paper, we propose a generalization to previously reported subspace-based blind methods for CP systems by introducing a new system parameter called *repetition index*, whose value is unity for all previously reported subspace-based methods. When the repetition index is chosen to be greater than one, the number of received blocks needed can be significantly reduced. The rest of the paper is organized as follows. Section II reviews a known prototype algorithm for subspace-based blind identification in CP systems. In section III we present the generalized algorithm. Simulation results are presented in Section IV and conclusions are made in section V.

A. Notations

Boldfaced lower case letters represent column vectors. Boldfaced upper case letters and calligraphic upper case letters are reserved for matrices. Superscripts ^{T} and † as in $\mathbf{A}^T$ and $\mathbf{A}^\dagger$ denote the transpose and transpose-conjugate operations, respectively, of a matrix or a vector. $[\mathbf{v}]_k$ denotes the kth entry of vector $\mathbf{v}$. All the vectors and matrices in this paper are complex-valued. $\mathbf{W}_M$ is an $M \times M$ DFT matrix whose kl-th entry is $e^{-j2\pi(k-1)(l-1)/M}$. Column and row indices of all matrices and vectors begin at one. If $\mathbf{v} = [\ v_1 \quad v_2 \quad \cdots \quad v_m\ ]^T$ is an $m \times 1$ vector, we use $\mathcal{T}_n(\mathbf{v})$ to denote the $(m+n-1) \times n$ Toeplitz matrix [14] whose first column is $\begin{bmatrix} \mathbf{v}^T & \mathbf{0}^T_{(n-1)\times 1} \end{bmatrix}^T$ and whose first row is $\begin{bmatrix} v_1 & \mathbf{0}_{1\times(n-1)} \end{bmatrix}$. $\mathcal{K}_l(\mathbf{v})$ denotes the $l \times (m-l+1)$ Hankel matrix [14] whose first column is $[\ v_1 \quad v_2 \quad \cdots \quad v_l\ ]^T$ and whose last row is $[\ v_l \quad v_{l+1} \quad \cdots \quad v_m\ ]$. Due to the special property of cyclic prefixes, we will use the following notation extensively in this paper. $[\mathbf{v}]_b^a$ denotes the $(b-a+1) \times 1$

[1]Work supported in parts by the NSF grant CCF-0428326 and the Moore Fellowship of the California Institute of Technology.

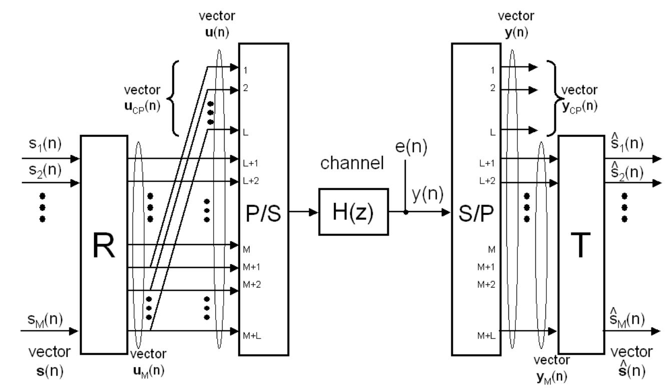

Fig. 1. A typical cyclic prefix system

vector $\left[\begin{array}{cccc} v_a & v_{a+1} & \cdots & v_b \end{array}\right]^T$ if $1 \leq a \leq b \leq m$. An extension of this definition to any arbitrary pair of integers a and b satisfying $a \leq b$ is made by defining v_k as $v_{(k-1 \bmod m)+1}$ for any $k > m$ or $k < 1$. For example, if $\mathbf{v} = \left[\begin{array}{ccc} v_1 & v_2 & v_3 \end{array}\right]^T$, then $[\mathbf{v}]_7^{-1}$ denotes the vector $\left[\begin{array}{ccccccccc} v_2 & v_3 & v_1 & v_2 & v_3 & v_1 & v_2 & v_3 & v_1 \end{array}\right]^T$.

II. Problem Formulation and Literature Review

A. Cyclic Prefix System Overview

Consider the communication system using cyclic prefix(CP) depicted in Fig. 1. The source symbols $s_1(n), s_2(n), ..., s_M(n)$ are in a blocked form of vectors $\mathbf{s}(n)$ of size M. The vector $\mathbf{s}(n)$ is precoded by an $M \times M$ constant matrix $\mathbf{R}$ and results in precoded data $\mathbf{u}_M(n)$. For OFDM or multi-carrier (MC) systems, $\mathbf{R} = \frac{1}{\sqrt{M}}\mathbf{W}_M^\dagger$ is the IDFT matrix. For single-carrier cyclic prefix (SC-CP) systems, $\mathbf{R}$ is chosen as $\mathbf{I}_M$. A cyclic prefix of length L, taking from the last L elements of $\mathbf{u}_M(n)$, is defined as $\mathbf{u}_{cp}(n) = \left[\begin{array}{cc} \mathbf{0}_{L\times(M-L)} & \mathbf{I}_L \end{array}\right]\mathbf{u}_M(n)$. The cyclic prefix is appended to $\mathbf{u}_M(n)$, forming a vector $\mathbf{u}(n) = \left[\begin{array}{c} \mathbf{u}_{cp}(n)^T \mathbf{u}_M(n)^T \end{array}\right]^T$ whose length is $P = M + L$. The information with redundancy is then sent over the channel $H(z)$. We assume $H(z)$ is an FIR channel with a maximum order L, i.e., $H(z) = \sum_{k=0}^{L} h_k z^{-k}$, and define $\mathbf{h}$ as the column vector $\left[\begin{array}{cccc} h_0 & h_1 & \cdots & h_L \end{array}\right]^T$. The signal is corrupted by channel noise $e(n)$. The received symbols $y(n)$ are blocked into $P \times 1$ vectors $\mathbf{y}(n)$. Also let $\mathbf{e}(n)$ denote the blocked version of the noise $e(n)$. Denote $\mathbf{y}_{cp}(n)$ as the first L and $\mathbf{y}_M(n)$ as the last M entries of $\mathbf{y}(n)$ so that $\mathbf{y}(n) = \left[\begin{array}{cc} \mathbf{y}_{cp}(n)^T & \mathbf{y}_M(n)^T \end{array}\right]^T$. It can be shown that

$$\mathbf{y}_M(n) = \mathbf{H}_{cir}\mathbf{u}_M(n) + \mathbf{e}_M(n) \tag{1}$$

where $\mathbf{H}_{cir}$ is an $M \times M$ circulant matrix [15] whose first column is $\left[\begin{array}{cc} \mathbf{h}^T & \mathbf{0}_{M-L-1}^T \end{array}\right]^T$ and $\mathbf{e}_M(n) = [\mathbf{e}(n)]_P^{L+1}$ is the noise vector. The $L \times 1$ vector $\mathbf{y}_{cp}(n)$ contains inter-block interference (IBI) and can be expressed as

$$\mathbf{y}_{cp}(n) = \mathbf{H}_l\mathbf{u}_{cp}(n) + \mathbf{H}_u\mathbf{u}_{cp}(n-1) + \mathbf{e}_{cp}(n) \tag{2}$$

where

$$\mathbf{H}_l \triangleq \left[\begin{array}{ccc} h_0 & & \mathbf{0} \\ \vdots & \ddots & \\ h_{L-1} & \cdots & h_0 \end{array}\right] \text{ and } \mathbf{H}_u \triangleq \left[\begin{array}{ccc} h_L & \cdots & h_1 \\ & \ddots & \vdots \\ \mathbf{0} & & h_L \end{array}\right]$$

are $L \times L$ matrices and $\mathbf{e}_{cp}(n) = [\mathbf{e}(n)]_L^1$ represents the noise. $\mathbf{y}_{cp}(n)$ is usually dropped for channel equalization and only $\mathbf{y}_M(n)$ passes through the $M \times M$ equalizer $\mathbf{T}$ and results in recovered symbol $\hat{\mathbf{s}}(n)$. When the channel coefficients are known, the optimal equalizer $\mathbf{T}$ can be derived to minimize mean square error of equalized symbols.

B. Subspace-based Blind Channel Identification

The problem of interest in this paper is to estimate channel coefficients $\mathbf{h}$ using only measurements of $\mathbf{y}(n)$ without knowledge of $\mathbf{u}(n)$. In this subsection we review an algorithm which has been used in three previously reported methods [9], [11], [12]. For simplicity we first ignore the noise term $\mathbf{e}(n)$. Define a *composite block* containing information from two consecutive blocks as

$$\bar{\mathbf{y}}(n) = \left[\begin{array}{ccc} \mathbf{y}_M(n-1)^T & \mathbf{y}_{cp}(n)^T & \mathbf{y}_M(n)^T \end{array}\right]^T. \tag{3}$$

Then from Eqs. (1) and (2) we have

$$\bar{\mathbf{y}}(n) = \left[\begin{array}{c} \mathbf{H}_{cir}\mathbf{u}_M(n-1) \\ \mathbf{H}_l\mathbf{u}_{cp}(n) + \mathbf{H}_u\mathbf{u}_{cp}(n-1) \\ \mathbf{H}_{cir}\mathbf{u}_M(n) \end{array}\right] = \bar{\mathbf{H}}\bar{\mathbf{u}}(n) \tag{4}$$

where

$$\bar{\mathbf{H}} = \left[\begin{array}{c|c} \mathbf{H}_{cir} & \mathbf{0}_{M\times M} \\ \hline \mathbf{0}_{L\times(M-L)}\mathbf{H}_u & \mathbf{H}_l\mathbf{0}_{L\times(M-L)} \\ \hline \mathbf{0}_{M\times M} & \mathbf{H}_{cir2} \end{array}\right], \bar{\mathbf{u}}(n) = \left[\begin{array}{c} \mathbf{u}_M(n-1) \\ [\mathbf{u}_M(n)]_{M-L}^{-L+1} \end{array}\right],$$

and $\mathbf{H}_{cir2}$ is obtained by permuting the last L columns of $\mathbf{H}_{cir}$ to the leftmost and is still a circulant matrix [15]. A special case of Eq. (4) when $M = 4$ and $L = 2$ is shown as

$$\left[\begin{array}{c} y_{01} \\ y_{02} \\ y_{03} \\ y_{04} \\ \hline y_{cp1} \\ y_{cp2} \\ \hline y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \end{array}\right] = \left[\begin{array}{cccc|cccc} h_0 & 0 & h_2 & h_1 & & & & \\ h_1 & h_0 & 0 & h_2 & & \mathbf{0} & & \\ h_2 & h_1 & h_0 & 0 & & & & \\ 0 & h_2 & h_1 & h_0 & & & & \\ \hline 0 & 0 & h_2 & h_1 & h_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & h_2 & h_1 & h_0 & 0 & 0 \\ \hline & & & & h_2 & h_1 & h_0 & 0 \\ & & & & 0 & h_2 & h_1 & h_0 \\ & \mathbf{0} & & & h_0 & 0 & h_2 & h_1 \\ & & & & h_1 & h_0 & 0 & h_2 \end{array}\right] \left[\begin{array}{c} u_{01} \\ u_{02} \\ u_{03} \\ u_{04} \\ \hline u_{13} \\ u_{14} \\ u_{11} \\ u_{12} \end{array}\right]. \tag{5}$$

For notational convenience, here we set $y_{0k} = [\mathbf{y}_M(n-1)]_k$, $y_{1k} = [\mathbf{y}_M(n)]_k$, and $y_{cpk} = [\mathbf{y}_{cp}(n)]_k$.

Theorem 1: The $(2M+L)\times 2M$ matrix $\bar{\mathbf{H}}$ has full column rank if and only if $H(z) = \sum_{k=0}^{L} h_k z^{-k}$ does not have any zero at $z = e^{j2\pi l/M}, 0 \leq l \leq M-1$.

Proof: See [11]. ■

Suppose we gather J consecutive received blocks $\mathbf{y}(0), \mathbf{y}(1), \cdots, \mathbf{y}(J-1)$ at the receiver, then we have $J-1$ composite blocks defined as in Eq. (3). We can construct the $(2M+L)\times(J-1)$ matrix by placing these composite blocks together as $\mathbf{Y}^{(J)} = \left[\begin{array}{cccc} \bar{\mathbf{y}}(1) & \bar{\mathbf{y}}(2) & \cdots & \bar{\mathbf{y}}(J-1) \end{array}\right]$. Then we have $\mathbf{Y}^{(J)} = \bar{\mathbf{H}}\mathbf{U}^{(J)}$ where $\mathbf{U}^{(J)} = \left[\begin{array}{cccc} \bar{\mathbf{u}}(1) & \bar{\mathbf{u}}(2) & \cdots & \bar{\mathbf{u}}(J-1) \end{array}\right]$ is a $2M \times (J-1)$ matrix. Assume there exists an integer $J \geq 2M+1$ such that $\mathbf{U}^{(J)}$ has full row rank $2M$. Also assume the channel does not have zeros at $z = e^{j2\pi l/M}$ so that $\bar{\mathbf{H}}$ has full rank. Then rank$(\mathbf{Y}^{(J)}) = 2M$ and hence $\mathbf{Y}^{(J)}$ has L linearly independent left annihilators. These annihilators are also left annihilators of $\bar{\mathbf{H}}$ since $\mathbf{U}^{(J)}$ has full rank. Given each annihilator $\mathbf{g}_k^\dagger$, we can

$$
\left[\begin{array}{ccc}
y_{01} & y_{04} & y_{03} \\
y_{02} & y_{01} & y_{04} \\
y_{03} & y_{02} & y_{01} \\
y_{04} & y_{03} & y_{02} \\ \hline
y_{cp1} & y_{04} & y_{03} \\
y_{cp2} & y_{cp1} & y_{04} \\
y_{11} & y_{cp2} & y_{cp1} \\
y_{12} & y_{11} & y_{cp2} \\ \hline
y_{13} & y_{12} & y_{11} \\
y_{14} & y_{13} & y_{12} \\
y_{11} & y_{14} & y_{13} \\
y_{12} & y_{11} & y_{14}
\end{array}\right]
=
\left[\begin{array}{cccc|cc|cccc}
h_0 & 0 & h_2 & h_1 & 0 & 0 & 0 & 0 & 0 & 0 \\
h_1 & h_0 & 0 & h_2 & 0 & 0 & 0 & 0 & 0 & 0 \\
h_2 & h_1 & h_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & h_2 & h_1 & h_0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline
0 & 0 & h_2 & h_1 & h_0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & h_2 & h_1 & h_0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & h_2 & h_1 & h_0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & h_2 & h_1 & h_0 & 0 & 0 \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & h_2 & h_1 & h_0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & h_2 & h_1 & h_0 \\
0 & 0 & 0 & 0 & 0 & 0 & h_0 & 0 & h_2 & h_1 \\
0 & 0 & 0 & 0 & 0 & 0 & h_1 & h_0 & 0 & h_2
\end{array}\right]
\left[\begin{array}{ccc}
u_{01} & u_{04} & u_{03} \\
u_{02} & u_{01} & u_{04} \\
u_{03} & u_{02} & u_{01} \\
u_{04} & u_{03} & u_{02} \\ \hline
u_{13} & u_{04} & u_{03} \\
u_{14} & u_{13} & u_{04} \\ \hline
u_{11} & u_{14} & u_{13} \\
u_{12} & u_{11} & u_{14} \\
u_{13} & u_{12} & u_{11} \\
u_{14} & u_{13} & u_{12}
\end{array}\right]
\tag{10}
$$

construct a $2M \times (L+1)$ matrix $\mathcal{G}_k$ such that $\mathcal{G}_k \mathbf{h} = \mathbf{0}$. Define $\mathcal{G} = \begin{bmatrix} \mathcal{G}_1^T & \mathcal{G}_2^T & \cdots & \mathcal{G}_L^T \end{bmatrix}^T$, then the channel coefficients $\mathbf{h}$ can be recovered within a scalar ambiguity by solving the equation $\mathcal{G}\mathbf{h} = \mathbf{0}$. The specific construction of the matrix $\mathcal{G}$ as well as the algorithm in presence of noise will be automatically covered when we describe the generalized method in Section III. Due to space limit, they are omitted here.

A necessary condition for the method presented above is that the $2M \times (J-1)$ matrix $\mathbf{U}^{(J)}$ must have full row rank $2M$, which implies $J \geq 2M+1$. This means it requires a large number of received blocks and makes these previously reported algorithms unrealistic in fast-fading channel environments since the channel coefficients may have changed significantly during accumulation of the data. Even though some adaptive techniques have been proposed (e.g., [11]) by using a forgetting factor which gives larger weighting to newer blocks than to older blocks, the usage of received symbols as old as $2M+1$ blocks earlier, is still unavoidable. The method we propose in Section III will overcome this limitation.

III. Proposed Method

A. Algorithm Development

We will derive our algorithm based on Eq. (4). Due to the properties of circulant matrices [15], it can be shown that if Eq. (4) is true, then we have

$$
[\mathbf{y}_M(n-1)]_M^{1-k} = \begin{bmatrix} \mathbf{H}_{cir} & \mathbf{0}_{M\times k} \\ \mathbf{0}_{k\times(M-L)} & \mathcal{H}_k \end{bmatrix} [\mathbf{u}_M(n-1)]_M^{1-k} \tag{6}
$$

for any $k \geq 0$. Here $\mathcal{H}_k = \mathcal{T}_k(\mathbf{h})^T$ is a $k \times (L+k)$ Toeplitz matrix. Similarly we have

$$
[\mathbf{y}_M(n)]_{M+l}^{1} = \begin{bmatrix} \mathcal{H}_l & \mathbf{0}_{l\times(M-L)} \\ \mathbf{0}_{M\times l} & \mathbf{H}_{cir2} \end{bmatrix} [\mathbf{u}_M(n)]_{M+l}^{1} \tag{7}
$$

for any $l \geq 0$. Using knowledge of Eqs. (6) and (7), we can "expand" the composite block $\bar{\mathbf{y}}(n)$ in Eq. (4) by k symbols upward and l symbols downward at our choice of arbitrary nonnegative integers k and l. It can be shown that, if we choose k and l such that $k+l = Q-1$ for some positive integer Q, we can write a new channel equation as described in the following theorem.

Theorem 2: Given a positive integer Q and nonnegative integers k, l such that $k+l = Q-1$, then Eq. (4) implies

$$
\bar{\mathbf{y}}_{kl}(n) = \bar{\mathbf{H}}_Q \bar{\mathbf{u}}_{kl}(n) \tag{8}
$$

where

$$
\bar{\mathbf{y}}_{kl}(n) = \begin{bmatrix} [\mathbf{y}_M(n-1)^T]_M^{-k+1} & \mathbf{y}_{cp}(n)^T & [\mathbf{y}_M(n)^T]_{M+l}^{1} \end{bmatrix}^T,
$$

$$
\bar{\mathbf{H}}_Q = \begin{bmatrix} \mathbf{H}_{cir} & & \mathbf{0}_{M\times(M+Q-1)} \\ \mathbf{0}_{(L+Q-1)\times(M-L)} & \mathcal{H}_{L+Q-1} & \mathbf{0}_{(L+Q-1)\times(M-L)} \\ \mathbf{0}_{M\times(M+Q-1)} & & \mathbf{H}_{cir2} \end{bmatrix},
$$

and $\bar{\mathbf{u}}_{kl}(n) = \begin{bmatrix} [\mathbf{u}_M(n-1)^T]_M^{-k+1} & [\mathbf{u}_M(n)^T]_{M+l}^{1} \end{bmatrix}^T$. ■

Now, by choosing k from 0 to $Q-1$ (and so l from $Q-1$ to 0) in Eq. (8) and putting $\bar{\mathbf{y}}_{kl}(n)$ together in a matrix, we get

$$
\mathbf{Y}_Q(n) = \bar{\mathbf{H}}_Q \mathbf{U}_Q(n) \tag{9}
$$

where

$$
\mathbf{Y}_Q(n) = \begin{bmatrix} \bar{\mathbf{y}}_{0,Q-1}(n) & \bar{\mathbf{y}}_{1,Q-2}(n) & \cdots & \bar{\mathbf{y}}_{Q-1,0}(n) \end{bmatrix}
$$

is a $(2M+Q+L-1) \times Q$ matrix and

$$
\mathbf{U}_Q(n) = \begin{bmatrix} \bar{\mathbf{u}}_{0,Q-1}(n) & \bar{\mathbf{u}}_{1,Q-2}(n) & \cdots & \bar{\mathbf{u}}_{Q-1,0}(n) \end{bmatrix}
$$

is a $(2M+Q-1) \times Q$ matrix. A special case of Eq. (9) when $M = 4, L = 2$, and $Q = 3$ is shown in Eq. (10) at the top of this page. Note that Eq. (4) implies Eq. (9) without any additional assumptions. We can see this, for example, by verifying that Eq. (5) is equivalent to Eq. (10). We call the parameter Q the *repetition index* since for each received block we can generate a matrix $\mathbf{Y}_Q(n)$ which has Q columns.

Finally, if we accumulate J consecutive blocks $\mathbf{y}(n)$, $0 \leq n \leq J-1$, we have $J-1$ composite blocks and can construct the $(2M+Q+L-1) \times Q(J-1)$ matrix as

$$
\mathbf{Y}_Q^{(J)} = \begin{bmatrix} \mathbf{Y}_Q(1) & \mathbf{Y}_Q(2) & \cdots & \mathbf{Y}_Q(J-1) \end{bmatrix}. \tag{11}
$$

Then we have $\mathbf{Y}_Q^{(J)} = \bar{\mathbf{H}}_Q \mathbf{U}_Q^{(J)}$ where

$$
\mathbf{U}_Q^{(J)} = \begin{bmatrix} \mathbf{U}_Q(1) & \mathbf{U}_Q(2) & \cdots & \mathbf{U}_Q(J-1) \end{bmatrix} \tag{12}
$$

is a $(2M+Q-1) \times Q(J-1)$ matrix.

Theorem 3: The $(2M+Q+L-1) \times (2M+Q-1)$ matrix $\bar{\mathbf{H}}_Q$ has full column rank if and only if $H(z)$ does not have any zero at $z = e^{j2\pi l/M}, 0 \leq l \leq M-1$.

Proof: See [13]. ■

Assume the channel $H(z)$ does not have zeros at $z = e^{j2\pi l/M}$ for any l. Then $\bar{\mathbf{H}}_Q$ has full column rank $2M+Q-1$. We also assume that there exists J such that $\mathbf{U}_Q^{(J)}$ achieves full row rank $2M+Q-1$. Under these two assumptions, we obtain that the $(2M+L+Q-1)$-row matrix $\mathbf{Y}_Q^{(J)}$ has rank $2M+Q-1$. This means there exist L linearly independent vectors $\mathbf{g}_k, 1 \leq k \leq L$ such that $\mathbf{g}_k^\dagger \mathbf{Y}_Q^{(J)} = \mathbf{0}^T$. Since $\mathbf{U}_Q^{(J)}$ has full row rank, these vectors $\mathbf{g}_k$ are also annihilators of $\bar{\mathbf{H}}_Q$. For each annihilator $\mathbf{g}_k^\dagger$ of $\bar{\mathbf{H}}_Q$, we can construct a $(2M+Q-1) \times (L+1)$ matrix $\mathcal{G}_k$ such that $\mathcal{G}_k \mathbf{h} = \mathbf{0}$. The construction of $\mathcal{G}_k$ can be conceptually easy by simply inspecting each column of $\bar{\mathbf{H}}_Q$ and finding locations of each channel coefficient h_k. Nevertheless, we write our construction explicitly as follows. Let $\mathcal{G}_k = \mathbf{G}_H + \mathbf{G}_s$ where $\mathbf{G}_H$ is a Hankel matrix $\mathcal{K}_{2M+Q-1}(\mathbf{g}_k^\dagger)$ and $\mathbf{G}_s$ is a sparse matrix defined as

$$\mathbf{G}_s = \left[\begin{array}{c} \mathbf{0}_{(M-L)\times(L+1)} \\ \hline \mathcal{K}_L([0,\ldots,0,g_1,g_2,\ldots,g_L]) \\ \hline \mathbf{0}_{(Q-1)\times(L+1)} \\ \hline \mathcal{K}_L([g_{2M+Q},\ldots,g_{2M+Q+L-1},0,\ldots,0]) \\ \hline \mathbf{0}_{(M-L)\times(L+1)} \end{array} \right].$$

Now define the $(2M+Q-1)L \times (L+1)$ matrix $\mathcal{G} = \left[\begin{array}{cccc} \mathcal{G}_1^T & \mathcal{G}_2^T & \cdots & \mathcal{G}_L^T \end{array} \right]^T$. We have $\mathcal{G}\mathbf{h} = \mathbf{0}$ and the channel coefficients $\mathbf{h}$ can be identified within a scalar ambiguity.

In presence of noise, the annihilators $\mathbf{g}_k^\dagger$ can be found by taking SVD on $\mathbf{Y}_Q^{(J)}$ and be chosen as the L singular vectors associated with the L smallest singular values. Also, after constructing the $\mathcal{G}$ matrix, we choose the vector $\hat{\mathbf{h}}$ which minimizes the norm of $\mathcal{G}\mathbf{h}$ as the estimated channel coefficients. This optimal estimation can be written as

$$\hat{\mathbf{h}} = \arg \min_{||\mathbf{h}||=1} ||\mathcal{G}\mathbf{h}||^2 = \arg \min_{||\mathbf{h}||=1} \mathbf{h}^\dagger(\mathcal{G}^\dagger\mathcal{G})\mathbf{h}.$$

Note that by choosing $Q = 1$, the proposed algorithm reduced to the special case in Section II.

B. Necessary Condition

Recall that the matrix $\mathbf{U}_Q^{(J)}$ defined in Eq. (12) must have full row rank so that the algorithm proposed above would work. Since $\mathbf{U}_Q^{(J)}$ has size $(2M+Q-1) \times (J-1)Q$, it has full row rank only when $(J-1)Q \geq 2M+Q-1$, or

$$Q \geq \frac{2M-1}{J-2}. \tag{13}$$

This necessary condition for $\mathbf{U}_Q^{(J)}$ to have full row rank $(2M+Q-1)$ is not sufficient since it still depends on the values of transmitted symbols $\mathbf{u}_M(n)$. However, simulations show that once inequality (13) is satisfied, the probability that $\mathbf{U}_Q^{(J)}$ has full rank is very close to unity for all commonly used constellations so that $Q = \lceil (2M-1)/(J-2) \rceil$ is usually a valid choice in practice. More detailed sufficient conditions will be presented elsewhere [13]. As long as $J \geq 3$, there exists Q such that $\mathbf{U}_Q^{(J)}$ could have full rank. This suggests the capability of the proposed algorithm to identify channel coefficients with *only three received blocks*.

C. Equalization and Resolving the Scalar Ambiguity

After estimating the channel coefficients, the receiver proceeds to equalize the channel. A standard linear minimum mean square error (L-MMSE) equalizer is used at the receiver. Since there is a scalar ambiguity in the estimated channel coefficients, all equalized symbols will be scaled by a same unknown scalar. A usual way to resolve this scalar is to introduce *one* extra pilot symbol and compare it with the corresponding received symbol. We set the first symbol of the source block $\mathbf{s}(n)$ as a known symbol defined as $\sqrt{E_s} p_{(n \bmod 4)}$, where E_s is the average symbol energy and $\left[\begin{array}{cccc} p_0 & p_1 & p_2 & p_3 \end{array} \right] = \left[\begin{array}{cccc} 1 & j & -j & -1 \end{array} \right]$. There are definitely many other alternative designs of these pilot symbols. The choice here is just to make sure that $\mathbf{U}_Q^{(J)}$ defined in Eq. (12) would not become rank deficient due to the introduction of these pilot symbols.

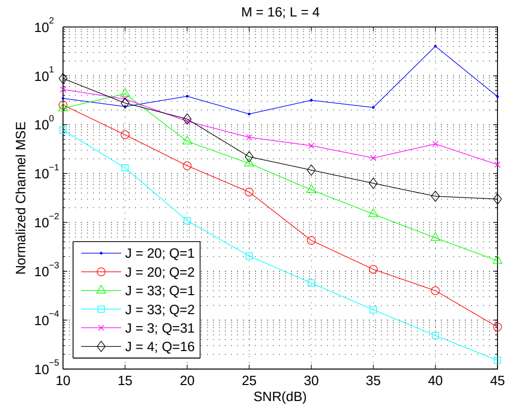

Fig. 2. Normalized mean squared error of channel estimation for static channels.

IV. Simulation Results and Discussion

In this section, we conduct several Monte Carlo simulations to demonstrate the performance of the proposed method under different system parameters: the number of collected blocks J and the repetition index Q. The number of informational symbols per block M is chosen as 16 and the length of cyclic prefix is $L = 4$. The constellation of source symbols is QPSK.

A. Static Channels

We first test our methods in static channel environments. The channel is assume to be FIR whose order is upper bounded by the CP length $L = 4$. The simulation is performed over 500 different channels generated by Raleigh fading statistics. The normalized least squared channel estimation error, denoted as E_{ch}, is used as the figure of merit for channel identification and is defined as $E_{ch} = (||\hat{\mathbf{h}} - \mathbf{h}||^2)/||\mathbf{h}||^2$ where $\hat{\mathbf{h}}$ and $\mathbf{h}$ are the estimated and the true channel vectors, respectively. The simulation result is shown in Figure 2 and the corresponding bit-error-rate (BER) plot is presented in Figure 3. When $J = 20$ and $Q = 1$ (corresponding to previously reported methods reviewed in Section II), the algorithm simply does not work since inequality (13) is not satisfied. This means all previously reported methods are unable to perform blind channel identification using only 20 blocks. When we choose $Q = 2$, the algorithm works with a fairly satisfactory result.

When the number of received blocks is $J = 33$, the algorithm works well with $Q = 1$. In view of inequality (13), this is the minimum number of blocks needed for any previously reported algorithm. If we use $Q = 2$, the performance has a significant boost. This suggests that choosing Q larger than necessary sometimes yields a better performance.

In order to test the theoretical limit of the proposed algorithm, the simulation is also performed with $J = 3$ and $J = 4$. The parameters Q are chosen as the minimum values required by inequality (13) for both cases. Although the system performances are not as good as those when J is larger and the computational complexity is very high due to large Q, these results do suggest that *subspace-based blind channel estimation is possible with data gathered in a very short time.*

B. Time-Varying Channels

We further test our algorithm in an environment of time-varying channels. The channel model considered here is a random FIR channel whose order is upper bounded by the

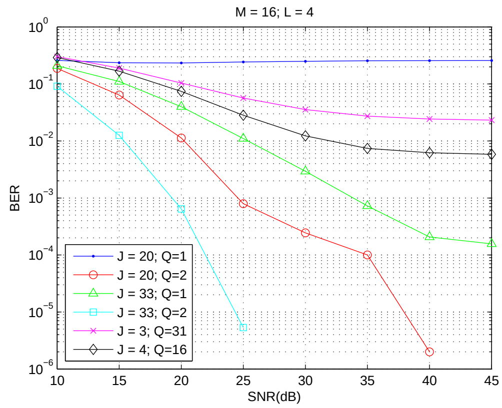

Fig. 3. Bit error rate performance for static channels.

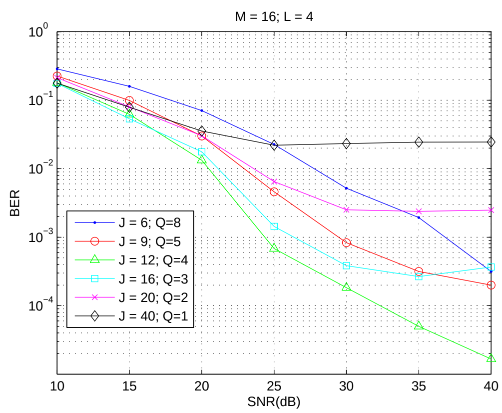

Fig. 4. Bit error rate performance for blind identification systems when the object speed is $v = 30$m/s.

CP length. The channel characteristics is shown in Table I. A standard Jakes' Doppler spectrum is used and Rayleigh fading statistics are assumed for all taps. The Doppler frequency is chosen as 100 (Hz), which corresponds to an object speed 30 m/s (108 km/hr) if the carrier frequency is 1 GHz. The symbol duration is 10^{-6} seconds.

Since the channel coefficients are changing during the time when the received blocks are collected, we do not define the figure of merit in terms of channel estimation error. Instead, we evaluate the system performance by the BER performance as shown in Figure 4. The number of blocks J is ranging from 6 to 40, and the repetition index Q is chosen as the minimum value required by (13) for each J. When $J = 40$ and $Q = 1$ (representing the previously reported algorithms), the performance is fairly poor since the estimated channel coefficients are hardly accurate due to channel variation. When the number of received blocks J is reduced, the performance becomes better and $J = 12$ yields the best performance for this particular channel model. When an even smaller J is chosen, performance becomes worse again due to lack of data available for estimation. This result suggests that an optimal number of blocks J can be chosen to compromise between the channel variation and lack of data. A finite repetition index Q can always be chosen as long as $J \geq 3$.

Tap	Delays (μs)	Avg. Power (dB)
1	0	0.0
2	1	-0.9
3	2	-1.7
4	3	-2.6
5	4	-3.5

TABLE I

TIME-VARYING CHANNEL MODEL

V. CONCLUSIONS

In this paper we proposed a generalized algorithm for subspace-based blind channel estimation in cyclic prefix systems. Two system parameters, the number of received blocks (J) and repetition index (Q) of the system, can be chosen freely depending on channel variation as long as they satisfy the necessary condition derived in the paper. By using a repetition index Q larger than unity, the number of received blocks needed is significantly reduced compared to previously reported methods. Simulation shows that when the repetition index Q is properly chosen, the generalized algorithm outperforms previously reported special cases, especially in a time-varying channel environments. The proposed method can be directly applied to existing systems such as OFDM, SC-CP, etc., without any modification of the transmitter structure. In the future, developing the strategy to find the optimal J and Q given knowledge of channel variation can be a challenging yet important problem. Extending this scheme for multi-input-multi-output (MIMO) channels is also of great interest.

REFERENCES

[1] A. Scaglione, G. B. Giannakis, and S. Barbarossa, "Redundant filter bank precoders and equalizers Part II: Unification and Optimal Designs", IEEE Trans. SP, vol. 47, pp. 2007-2022, Jul. 1999.

[2] D. H. Pham and J. H. Manton, "A Subspace Algorithm for Guard Interval Based Channel Identification and Source Recovery Requiring Just Two Received Blocks", Proc. of ICASSP 2003, pp. 317 - 320, Hong Kong, China.

[3] B. Su and P. P. Vaidyanathan, "A Generalized Algorithm for Blind Channel Identification with Linearly Redundant Precoding," *in print, EURASIP Journal on Applied Signal Processing Special Issue on Multirate Systems.*

[4] B. Su and P. P. Vaidyanathan, "A Generalization of Deterministic Algorithm for Blind Channel Identification with Filter Bank Precoders", in *Proc. ISCAS 2006*, Kos Island, Greece, May 2006.

[5] E. Moulines, P. Duhamel, J. F. Cardoso, S. Mayrargue, "Subspace Methods for the Blind Identification of Multichannel FIR Filters," IEEE Trans. on SP, pp. 516-525, Feb. 1995.

[6] S. Zhou and G. B. Giannakis, "Finite-alphabet based channel estimation for OFDM and related multicarrier systems," *IEEE Trans. Commun.*, vol. 49, pp. 1402-1414, Aug. 2001.

[7] A. P. Petropulu, R. Zhang, and R. Lin, "Blind OFDM channel estimation through simple linear precoding," *IEEE Trans. on Wireless Communications*, vol. 3, no. 2, pp. 647-655, Mar. 2004.

[8] R. W. Heath Jr. and G. B. Giannakis, "Exploting input cyclostationarity for blind channel identification in OFDM systems," *IEEE Trans. Signal Process.*, vol. 47, no. 3, pp. 848-856, Mar. 1999.

[9] X. Cai and A. Akansu, "A subspace method for blind channel identification in OFDM systems," in Proc. Int. Conf. Commun., vol 2, New Orleans, LA, Jun. 2000, pp. 929-933.

[10] X. Zhuang, Z. Ding, and A. L. Swindlehurst, "A statistical subspace method for blind channel identification in OFDM communications," in *Proc. ICASSP*, vol. 5, Istanbul, Turkey, Jun. 2000, pp. 2493-2496.

[11] B. Muquet, M. de Courville, and P. Duhamel, "Subspace-based blind and semi-blind channel estimation for OFDM systems," *IEEE Trans. Signal Process.*, vol. 50, no. 7, pp. 1699-1712, Jul. 2002.

[12] C. Li and S. Roy, "Subspace-based blind channel estimation for OFDM by exploiting virtual carriers," *IEEE Trans. Wireless Commun.*, vol. 2, no. 1, pp. 141-150, Jan. 2003.

[13] B. Su and P. P. Vaidyanathan, "Subspace-based blind channel estimation for time-varying channel," *in preparation.*

[14] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 1996.

[15] P. P. Vaidyanathan, *Multirate systems and filter banks*, Prentice-Hall, 1993.