Full Diversity Blind Signal Designs for Unique Identification of Frequency Selective Channels

Jian-Kang Zhang, *Senior Member, IEEE*, Chau Yuen, *Member, IEEE*, and Fei Huang

***Abstract*—In this paper, we develop two kinds of closed-form decompositions on phase-shift-keying (PSK) constellations by exploiting linear congruence equation theory: the one for factorizing a pq-PSK constellation into a product of p- and q-PSK constellations and the other for decomposing a specific complex number into a difference of a point in p-PSK constellation and a point in q-PSK constellation. With this, we present a novel and simple signal design technique to blindly and uniquely identify frequency selective channels with zero-padded block transmission by only processing the first two block received signals. In a noise-free case, a closed-form solution to determine the transmitted signals and the channel coefficients is obtained. In a Gaussian noise and Rayleigh fading environment, we prove that our scheme enables full diversity for the generalized likelihood ratio test (GLRT) receiver. When only finite received data are given, the linearity of our signal design allows us to use iterative sphere decoders to approximate GLRT detection so that the joint estimation of the channel and symbols can be efficiently implemented.**

***Index Terms*—Blind modulation and blind unique identification, coprime phase-shift-keying (PSK) constellations, frequency selective channels, full diversity, linear congruence equations.**

I. Introduction

IN THIS paper, we are interested in wireless communication systems having a single transmitting antenna and a single receiving antenna that transmit data through a frequency-selective fading channel. The systems that we consider alleviate the intersymbol interference produced by the channel by transmitting the data stream in consecutive equal-size blocks, which are subsequently processed at the receiver on a block-by-block basis. To eliminate interblock interference, some redundancy is padded to each block before transmission. There are several ways to add redundancy (e.g., [1] and [2]), but in this paper, we will restrict ourselves to block-by-block communication systems with zero-padding redundancy [1]. When the receiver possesses perfect knowledge of the channel and employs maximum likelihood (ML) detection, it was shown [3], [4] that such a system not only enables full diversity but provides maximum coding gain as well.

Unfortunately, perfect channel state information at the receiver, in practice, is not easily achievable. If the coherence time is sufficiently long, then the transmitter can send training signals that enable the receiver to estimate the channel coefficients accurately. For mobile wireless communications, however, the fading coefficients may fluctuate so rapidly that the coherence time may be too short to allow reliable estimation of the coefficients. Therefore, the time cost on transmitting training signals cannot be neglected because of the necessity of transmitting more training signals for the accurate estimation of the channel [5]–[7].

To get rid of having to transmit training signals, considerable research efforts have been made to develop techniques of "blind channel estimation" [8]–[10] recently. Basically, these techniques utilize only the received signals at the receiver to identify and estimate the transmission channel. The essence of these algorithms is to take advantage of the structure of the channel and/or the property of the transmitted signals. The subspace method is one such method exploiting the channel structure and the second order statistics of input signals [11]–[16]. In digital communication applications, the input signals possess finite alphabet property such as the constant modulus for phase-shift-keying (PSK) modulation or integers for quadrature amplitude modulation. This property can be further exploited to reliably estimate the channel even if the coherence time is short [8], [17]–[24]. Thus far, to the best knowledge of the authors, all currently available blind methods for frequency selective fading channel estimation incur scale ambiguity and, as a consequence, cannot identify the channel coefficients uniquely. In addition, wireless communication applications demand the accurate estimate of the channel as well as of the signal. To resolve this issue, we propose a novel signaling and transmitting technique for the frequency-selective channel with zero-padded block transmission, in which neither the transmitter nor the receiver knows the channel state information. Our main contributions in this paper are as follows.

1) A novel modulation technique using a pair of coprime p-PSK and q-PSK constellations is proposed to blindly and uniquely identify frequency-selective channels with zero-padded block transmission by only processing the first two block received signals. In addition, a closed-form solution to determine the transmitted signals and the channel coefficients is obtained by exploiting the linear congruence equation theory.

Manuscript received June 14, 2011; revised November 14, 2011 and January 27, 2012; accepted February 1, 2012. Date of publication March 10, 2012; date of current version June 12, 2012. The work of J.-K. Zhang was supported in part by the Natural Sciences and Engineering Research Council of Canada. The work of C. Yuen was supported in part by the International Design Center under Grant IDG31100102 and Grant IDD11100101. The review of this paper was coordinated by Prof. H.-F. Lu.

J.-K. Zhang is with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON L8S 4K1, Canada (e-mail: jkzhang@mail.ece.mcmaster.ca).

C. Yuen is with the Singapore University of Technology and Design, Singapore 138682 (e-mail: yuenchau@sutd.edu.sg).

F. Huang is with the Shanghai Institute of Radio Equipment, Shanghai 200090, China (e-mail: feihuang1206@hotmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2012.2190629

2) In the Gaussian noise and Rayleigh fading environment, we prove that our scheme enables full diversity for the generalized likelihood ratio test (GLRT) receiver.
3) When only finite received data are given, the linearity of our signal design allows us to utilize the iterative least squares [14], [18]–[21], [25] with parallel sphere decoders [26]–[35] to approximate GLRT detection so that the joint estimation of the channel and symbols can be efficiently implemented.

Here, we should point out that similar hybrid signaling schemes [36]–[41] were used to eliminate the ambiguity of the blind orthogonal space–time block codes. However, there are the following three major differences between the work presented in [36]–[41] and that to be developed in this paper.

1) The work in [36]–[41] mainly focused on flat fading channels with multiple transmitter antennas and a single receiver antenna. Specifically, the authors in [39] and [40] utilized a hybrid binary PSK (b-PSK) and quadrature PSK (q-PSK) signaling scheme with 1 bit as a pilot to eliminate the ambiguity for general orthogonal space–time block codes, whereas the authors in [36]–[38] and [41] alternatively transmitted the two Alamouti codes with a pair of coprime PSK modulations to get rid of the ambiguity for the flat fading channel with two transmitter antennas and a single receiver antenna. However, the work in this paper considers a noncoherent frequency selective channel with a single transmitter antenna and a single receiver antenna. For such a system, to the best knowledge of the authors, no work has been reported in the literature so far that deals with the unique identification of both the channel coefficients and the transmitted signals as well as with full diversity.
2) In spite of the fact that the work in [36]–[38] and [41] also employed a pair of coprime PSK constellations and a rigorous proof for the unique identification of the channel and transmitted signal as well as for full diversity was presented in [41], the mathematical technique developed in [36], [38], and [41] only involves the unique product factorization of a pair of coprime PSK constellations, i.e., uniquely factorizing a pq-PSK constellation into a product of p- and q-PSK constellations. In this paper, we not only significantly simplify this property but also develop a novel unique difference decomposition, i.e., uniquely decomposing an eligible complex number into a difference of p- and q-PSK constellation symbols.
3) Combining the zero-padded block transmission with proper coprime PSK constellation pair modulations, we rigorously prove that the signaling scheme proposed in this paper enables the unique identification of both the frequency selective channel and the transmitted signals as well as full diversity.

Here, it is worth emphasizing the fact that using a pair of coprime PSK constellations does not necessarily enable the unique identification of the channel and the transmitted signal and full diversity (see more details on the comments after Theorems 1 and 2). They also depend on the way of how to transmit signals. Different transmission schemes need different unique factorization properties such that the unique identification of the channel and the transmitted signal and full diversity are guaranteed. Therefore, developing a variety of unique factorizations of a coprime PSK constellations not only provides us with some deep understandings of these constellations mathematically but also gives us some theoretic guidelines of how to properly design the corresponding transmission schemes for a general frequency-selective multiple-input–multiple-output channel so that the unique identification of the channel and the transmitted signal and full diversity are assured.

In addition, despite the fact that the focus of this paper is only on the zero-padded block transmission for the frequency-selective channel, the signal design and full diversity analysis can be extended in a straightforward manner into the Toeplitz space–time block-coded channel [42] in a noncoherent case.

Notation: Most notations used throughout this paper are standard. Column vectors and matrices are boldface lowercase and uppercase letters, respectively. The matrix transpose, complex conjugate, and Hermitian are denoted by $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$, respectively. $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. $\gcd(m, n)$ denotes the greatest common divisor of positive integers m and n. Particularly when $\gcd(m, n) = 1$, we say that m and n are coprime integers. $\varphi(n)$ denotes the Euler function, i.e., the number of all positive integers that do not exceed n and are prime to n. The (i, j)th element of matrix $\mathbf{A}$ is denoted by a_{ij}.

II. Channel Model and a Novel Blind Modulation

If the channel is assumed to be of length at most L, then the block transmission system with zero padding operates as follows: First, $L - 1$ zeros are appended to $\mathbf{s}$ to form $\mathbf{s}'$, which is of length $P = K + L - 1$. The elements of $\mathbf{s}'$ are serially transmitted through the channel. The channel impulse response is denoted by $\mathbf{h} = [h_0, h_1, \ldots, h_{L-1}]^T$. The received signal vector $\mathbf{r}$ can be represented as

$$\mathbf{r} = \mathcal{T}_c(\mathbf{h})\mathbf{s} + \boldsymbol{\xi} \tag{1}$$

where $\mathbf{r}$ is a $P \times 1$ received signal vector, $\mathbf{s}$ is a $K \times 1$ transmitted signal vector, $\boldsymbol{\xi}$ denotes the vector of noise samples at the receiver, and $\mathcal{T}_c(\mathbf{h})$ denotes the $P \times K$ Toeplitz channel matrix

$$\mathcal{T}_c(\mathbf{h}) = \begin{pmatrix} h_0 & 0 & \ldots & 0 \\ h_1 & h_0 & \ldots & 0 \\ \vdots & h_1 & \ddots & \vdots \\ h_{L-1} & \ddots & \ddots & h_0 \\ 0 & \ddots & \ddots & h_1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ddots & 0 & h_{L-1} \end{pmatrix}_{P\times K}.$$

For blind channel estimation, it is convenient to rewrite the channel model (1) as

$$\mathbf{r} = \mathcal{T}(\mathbf{s})\mathbf{h} + \boldsymbol{\xi} \tag{2}$$

where we have used the following fact:

$$\mathcal{T}_c(\mathbf{h})\mathbf{s} = \mathcal{T}(\mathbf{s})\mathbf{h} \tag{3}$$

with the $P \times L$ Toeplitz signal matrix $\mathcal{T}(\mathbf{s})$ defined by

$$\mathcal{T}(\mathbf{s}) = \begin{pmatrix} s_1 & 0 & \dots & 0 \\ s_2 & s_1 & \dots & 0 \\ \vdots & s_2 & \ddots & \vdots \\ s_k & \ddots & \ddots & s_1 \\ 0 & \ddots & \ddots & s_2 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ddots & 0 & s_k \end{pmatrix}_{P \times L}.$$

Now, we assume that during a T block transmission period, the channel coefficients stay constant and after that will randomly change. Our novel blind modulation scheme is described as follows. During the first block transmission, each symbol of a transmitted signal vector $\mathbf{s} = \mathbf{x} = \mathbf{z}_1$ is chosen from p-PSK constellation $\mathcal{X}$, i.e.,

$$\mathbf{r}_1 = \mathcal{T}(\mathbf{x})\mathbf{h} + \boldsymbol{\xi}_1, \qquad \mathbf{x} \in \mathcal{X}^K. \tag{4}$$

During the second block transmission, each symbol of a transmitted signal vector $\mathbf{s} = \mathbf{y} = \mathbf{z}_2$ is chosen from q-PSK constellation $\mathcal{Y}$, i.e.,

$$\mathbf{r}_2 = \mathcal{T}(\mathbf{y})\mathbf{h} + \boldsymbol{\xi}_2, \qquad \mathbf{y} \in \mathcal{Y}^K \tag{5}$$

where p and q are coprimes. Then, during the ith block transmission for $3 \le i \le T$, each symbol of a transmitted signal vector $\mathbf{s} = \mathbf{z}_i$ can be chosen from any constellation $\mathcal{Z}_i$, i.e.,

$$\mathbf{r}_i = \mathcal{T}(\mathbf{z}_i)\mathbf{h} + \boldsymbol{\xi}_i, \qquad \mathbf{z}_i \in \mathcal{Z}_i^K. \tag{6}$$

Collecting all the block received signals, we have

$$\mathbf{r} = \mathbf{S}\mathbf{h} + \boldsymbol{\eta} \tag{7a}$$

where $\boldsymbol{\eta} = (\boldsymbol{\xi}_1^T, \boldsymbol{\xi}_2^T, \dots, \boldsymbol{\xi}_T^T)^T$ and

$$\mathbf{S} = \begin{pmatrix} \mathcal{T}(\mathbf{x}) \\ \mathcal{T}(\mathbf{y}) \\ \mathcal{T}(\mathbf{z}_3) \\ \vdots \\ \mathcal{T}(\mathbf{z}_T) \end{pmatrix}, \qquad \mathbf{x} \in \mathcal{X}^K, \mathbf{y} \in \mathcal{Y}^K, \mathbf{z}_i \in \mathcal{Z}_i^K. \tag{7b}$$

Throughout this paper, we make the following assumptions.

1) The channel coefficients h_ℓ for $\ell = 0, 1, \dots, L-1$ are samples of independent circularly symmetric zero-mean complex white Gaussian random variables with unit variances and remain constant for the first PT ($T \ge 2$) time slots, after which, they change to new independent values that are fixed for the next PT time slots, and so on.[1] $\boldsymbol{\eta}$ is circularly symmetric zero-mean complex Gaussian samples with covariance matrix $\sigma^2\mathbf{I}_{PT}$.
2) During PT observable time slots, consecutive length T blocks $\mathbf{z}_i$ are transmitted with each entry z_{ik} for $i = 3, 4, \dots, T$ and $k = 1, 2, \dots, K$ being independently and equally likely chosen from the constellation $\mathcal{Z}_i$, whereas components x_k and y_k for $k = 1, 2, \dots, K$ in the previous two blocks are independently and equally likely chosen from the respective p-PSK and q-PSK constellations $\mathcal{X}$ and $\mathcal{Y}$, where p and q are coprimes.
3) Channel state information is not available at either the transmitter or the receiver.

Our goal in this paper is to prove that our designed signaling scheme (7)

1) enables the unique identification of the channel and the transmitted signals for any given nonzero received signal vector $\mathbf{r}$ in a noise-free case;
2) provides full diversity for the GLRT receiver in the Gaussian noise and the Rayleigh fading environment.

III. Blind Unique Identification and Full Diversity

In this section, we first develop some decomposition properties on a pair of coprime PSK constellations and then prove that our blind modulation scheme proposed in the previous section enables the unique identification of the channel coefficients and the transmitted signals in a noise-free case as well as full diversity for the GLRT receiver in a noise environment.

A. Decompositions of PSK Constellations

First, we introduce some fundamental properties on the Euler function, whose proofs can be found in [44] and [45].

Lemma 1: The Euler function $\varphi(m)$ has the following properties:

1) Multiplicative property, i.e., if $\gcd(m, m') = 1$, then $\varphi(mm') = \varphi(m)\varphi(m')$.
2) For any integer m, if the standard factorization is given by

$$m = p_1^{l_1} \cdots p_s^{l_s}, \quad p_1 < p_2 < \cdots < p_s \tag{8}$$

where $p_1, p_2, \dots, p_s$ are the prime numbers, and each l_i for $i = 1, 2, \dots, s$ is a positive integer, then we have

$$\varphi(m) = \varphi\left(p_1^{l_1}\right) \cdots \varphi\left(p_s^{l_s}\right). \tag{9}$$

3) For any integer m, we have

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) \tag{10}$$

where p runs over the distinct prime divisors of m.

Example: $\varphi(20) = \varphi(2^2 \times 3 \times 5) = 2^2 \times 3 \times 5 \times (1 - 1/2) \times (1 - 1/3) \times (1 - 1/5) = 16$.

A typical application of the Euler function is the following well-known Euler theorem in congruence equation theory [45].

Lemma 2: Let $a \equiv b (\mathrm{mod}\ c)$ denote that $a - b$ is a multiple of c. Then, if $\gcd(d, c) = 1$, then, $d^{\varphi(c)} \equiv 1 (\mathrm{mod}\ c)$.

[1] Since the time-varying behaviors of channels are often caused by the movement of the transmitter and the receiver or environmental scatters, it would be more practical to assume that the channel coefficients change gradually instead of the changing suddenly. However, in this paper, we have to adopt the assumption on the block fading made in [7], [43] for the theoretic necessity of the diversity analysis on our transmission scheme.

By Lemma 2, we can immediately obtain the following corollary [44], [45].

Corollary 1: Let $\gcd(d, c) = 1$. Then, the solution of congruent equation $dx \equiv k (\bmod\ c)$ is given by $x \equiv k\bar{d}_c (\bmod\ c)$, where $\bar{d}_c \equiv d^{\varphi(c)-1}$ and $d\bar{d}_d \equiv 1 (\bmod\ c)$ for $1 \le \bar{d}_c \le c-1$.

We also need the following Chinese reminder theorem.

Lemma 3: Chinese Reminder Theorem: Let p and q be coprimes. Then, for a given integer k, solving the congruent equation $np + mq \equiv k (\bmod\ pq)$ for m and n is equivalent to solving a system of congruent equations

$$mq \equiv k (\bmod\ p) \quad (11a)$$

$$np \equiv k (\bmod\ q). \quad (11b)$$

Now, we establish the first property of uniquely decomposing a pq-PSK constellation into the product of p- and q-PSK constellations.

Proposition 1: Let two positive integers p and q be coprimes. Then, for any integer k with $0 \le k < pq$, there exists a pair of x and y such that

$$xy = \exp\left(j\frac{2\pi k}{pq}\right), \quad \text{for } 0 \le k < pq. \quad (12)$$

Furthermore, x and y can be uniquely determined by

$$x = \exp\left(j\frac{2\pi k \bar{q}_p}{p}\right) \quad (13a)$$

$$y = \exp\left(j\frac{2\pi k \bar{p}_q}{q}\right) \quad (13b)$$

where $\bar{q}_p$ is the inverse element of q under modulus p, and $\bar{p}_q$ is the inverse element of p under modulus q, i.e., $q\bar{q}_p \equiv 1 (\bmod\ p)$ and $p\bar{p}_q \equiv 1 (\bmod\ q)$ for $1 \le \bar{q}_p \le p-1$ and $1 \le \bar{p}_q \le q-1$.

Proposition 1, whose proof is given in Appendix A, tells us that any pq-PSK symbol can be uniquely factored into the product of a pair of the coprime p- and q-PSK symbols. This factorization was first discovered in [38] and [41]. Now, Proposition 1 significantly simplifies the original representation reported in [38] and [41]. The following property gives a necessary and sufficient condition for a complex number to be able to be decomposed into a difference of a pair of coprime p- and q-PSK symbols.

Proposition 2: Let $w \neq 0$ be a given nonzero complex number and $w = |w|e^{j\theta}$. Then, there exists a pair of $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ satisfying equation

$$x - y = w \quad (14)$$

if and only if there exist three integers m, n, and k such that

$$\theta = \frac{\pi(pn + qm)}{pq} + k\pi + \frac{\pi}{2} \quad \text{for some } k \in \mathbb{Z} \quad (15a)$$

$$|w| = 2(-1)^{k+1}\sin\left(\frac{\pi(pn - qm)}{pq}\right). \quad (15b)$$

Furthermore, under the condition (15), if p and q are coprimes, then (14) has the unique solution that can be explicitly determined as follows:

1) $w = 0$. In this case, $x = y = 1$.
2) $w \neq 0$. Then, x and y are given by

$$x = \exp\left(j\frac{2\pi \ell \bar{q}_p}{p}\right) \quad (16a)$$

$$y = \exp\left(j\frac{2\pi \ell \bar{q}_p}{p}\right) \quad (16b)$$

with integer $\ell = pq(\theta/\pi - 1/2)$.

The proof of Proposition 2 is provided in Appendix B. Propositions 1 and 2 together play an important role in the unique identification of the channel and the transmitted signals as well as in the analysis of full diversity in this paper.

B. Blind Unique Identification of the Channel

Our main purpose in this section is to prove that the blind modulation scheme (7) is capable of uniquely identifying the channel coefficients and the transmitted symbols. To do this, let $\mathbf{u}$ and $\mathbf{v}$ be two consecutive block received signal vectors in the first two block transmissions from the channel model (2) in a noise-free environment, i.e.,

$$\mathbf{u} = \mathcal{T}(\mathbf{x})\mathbf{h}, \qquad \mathbf{x} \in \mathcal{X}^K \quad (17)$$

$$\mathbf{v} = \mathcal{T}(\mathbf{y})\mathbf{h}, \qquad \mathbf{y} \in \mathcal{Y}^K. \quad (18)$$

Now, we formally state the first result.

Theorem 1—Unique Identification: For two coprime positive integers p and q, let $\mathbf{u} = (u_1, u_2, \dots, u_P)^T$ and $\mathbf{v} = (v_1, v_2, \dots, v_P)^T$ be the first two consecutive block nonzero received signal vectors given by (17) and (18), respectively. If J denotes the maximum integers such that $u_1v_1 = u_2v_2 = \cdots = u_Jv_J = 0$, then, $h_0 = h_1 = \cdots = h_{J-1} = 0$. In addition, the other remaining channel coefficients $h_J, h_{J+1}, \dots, h_{L-1}$ and all the transmitted symbols in $\mathbf{x}$ and $\mathbf{y}$ can be uniquely determined as follows.

1) Let w_1 be defined by $w_1 = u_{J+1}/v_{J+1} = |w_1|e^{j\theta_1}$ and $\ell_1 = pq\theta_1/2\pi$. Then, we have

$$x_1 = \exp\left(j\frac{2\pi \ell_1 q^{\varphi(p)-1}}{p}\right) \quad (19a)$$

$$y_1 = \exp\left(-j\frac{2\pi \ell_1 p^{\varphi(q)-1}}{q}\right) \quad (19b)$$

$$h_J = x_1^* u_{J+1}. \quad (19c)$$

2) For $1 < m \le L - J$, let w_m be defined by

$$w_m = h_J^{-1}\left(x_1^*\left(u_{J+m} - \sum_{i=1}^{m-2} h_{J+i}x_{m-i}\right) - y_1^*\left(v_\ell - \sum_{i=1}^{m-2} h_{J+i}x_{m-i}\right)\right). \quad (20)$$

a) If $w_m = 0$, then we have

$$x_m = x_1 \tag{21a}$$

$$y_m = y_1 \tag{21b}$$

$$h_{J+m-1} = x_1^* \left(u_{J+m} - \sum_{i=0}^{m-2} h_{J+i} x_{m-i} \right). \tag{21c}$$

b) If $w_m \neq 0$, let $w_m = |w_m| e^{j\theta_m}$ and $\ell_m = pq(\theta_m/\pi - 1/2)$. Then, we have

$$x_m = x_1 \exp\left(j \frac{2\pi \ell_m q^{\varphi(p)-1}}{p} \right) \tag{22a}$$

$$y_m = y_1 \exp\left(j \frac{2\pi \ell_m p^{\varphi(q)-1}}{q} \right) \tag{22b}$$

$$h_{J+m-1} = x_1^* \left(u_{J+m} - \sum_{i=0}^{m-2} h_{J+i} x_{m-i} \right). \tag{22c}$$

3) For $L - J + 1 \leq m \leq K$, we have

$$x_m = \frac{u_{m+J} - \sum_{i=1}^{L-J-1} h_{L-i}\, x_{m-L+J+i}}{h_J} \tag{23a}$$

$$y_m = \frac{u_{m+J} - \sum_{i=1}^{L-J-1} h_{L-i}\, y_{m-L+J+i}}{h_J}. \tag{23b}$$

Proof: Basically, the proof of Theorem 1 captures the following four steps:

Step 1. First, we consider the first received signals in each block. In this case, we have

$$h_0 x_1 = u_1 \tag{24a}$$

$$h_0 y_1 = v_1. \tag{24b}$$

Therefore, if either u_1 or v_1 is zero, then h_0 is zero. Similarly, we can obtain $h_1 = h_2 = \cdots, h_{J-1} = 0$ if $u_1 v_1 = u_2 v_2 = \cdots = u_J v_J = 0$.

Step 2. We continue to proceed to the $(J+1)$th received signals for each block. In this case, we have received

$$h_J x_1 = u_{J+1} \tag{25a}$$

$$h_J y_1 = v_{J+1}. \tag{25b}$$

Since $u_{J+1} v_{J+1} \neq 0$, eliminating h_J from (25) results in

$$x_1 y_1^* = \frac{u_{J+1}}{v_{J+1}} = w_1. \tag{26}$$

Now, by Proposition 1, x_1 and y_1 can uniquely be determined by (19a) and (19b), respectively, and thus, h_J is uniquely determined by (19c).

Step 3. Let us consider the $(J+2)$th received signals for each block

$$h_{J+1} x_1 + h_J x_2 = u_{J+2} \tag{27a}$$

$$h_{J+1} y_1 + h_J y_2 = v_{J+2}. \tag{27b}$$

Eliminating h_{J+1} from (27) yields

$$x_1^* x_2 - y_1^* y_2 = \frac{u_{J+2} x_1^* - v_{J+2} y_1^*}{h_J} = w_2. \tag{28}$$

Since $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ for $i = 1, 2$, we have $x_1^* x_2 \in \mathcal{X}$ and $y_1^* y_2 \in \mathcal{Y}$, as well. Now, by Proposition 2, x_2 and y_2 can uniquely be determined by (21a) or (22a) and (21b) or (22b), respectively, and thus, h_{J+1} is uniquely determined by (21c) or (22c) with $m = 2$.

In general, we proceed to consider determining the $(J+m)$th channel coefficient for $2 < m \leq L - J - 1$. In this case, we have received

$$h_{J+m-1} x_1 + h_{J+m-2} x_2 + \cdots + h_J x_m = u_{J+m} \tag{29a}$$

$$h_{J+m-1} y_1 + h_{J+m-2} y_2 + \cdots + h_J y_m = v_{J+m}. \tag{29b}$$

This is equivalent to

$$h_{J+m-1} x_1 + h_J x_m = u_{J+m} - \sum_{i=1}^{m-2} h_{J+i} x_{m-i} \tag{30a}$$

$$h_{J+m-1} y_1 + h_J y_m = v_{J+m} - \sum_{i=1}^{m-2} h_{J+i} x_{m-i}. \tag{30b}$$

Eliminating h_{J+m-1} from (30) yields

$$\begin{aligned} x_1^* x_m - y_1^* y_m = h_J^{-1} \Bigg(x_1^* \left(u_{r+m} - \sum_{i=1}^{m-2} h_{J+i} x_{m-i} \right) \\ - y_1^* \left(v_{J+m} - \sum_{i=1}^{m-2} h_{J+i} x_{mi} \right) \Bigg) \\ = w_m. \end{aligned}$$

Now, by Proposition 2, x_m and y_m can uniquely be determined by (21a) or (22a) and (21b) or (22b), respectively, and thus, h_{J+m-1} is uniquely determined by (21c) or (22c).

Step 4. $L - J - 1 < m \leq K$. In this case, since the channel coefficients have been determined by the previous three steps, we can determine the other remaining transmitted signals from the remaining received signals of each block. In this case, we have

$$h_{L-1} x_{mL+J+1} + h_{L-2} x_{mL+J+2} + \cdots + h_J x_m = u_{J+m}$$

$$h_{L-1} y_{mL+J+1} + h_{L-2} y_{mL+J+2} + \cdots + h_J y_m = v_{J+m}.$$

From this, we can obtain (23). This completes the proof of Theorem 1. ■

We would like to make the following observations on Theorem 1.

1) Theorem 1 not only tells us that the channel coefficients can be uniquely identified by only transmitting two block signals with each symbol selected from two coprime PSK constellations but provides simple and closed-form solutions to both the channel coefficients and the transmitted symbols as well.

2) If we set $p = 2^m$ and $q = 2^m + 1$ with m being a positive integer, then it is clear that p and q are coprimes. Therefore, Theorems 1 holds for such a pair of p and q. In addition, if we need the original symbol sets $\mathcal{X}$ and $\mathcal{Y}$ to contain the same integer bits, we can delete the only one common element 1 from $\mathcal{Y}$, i.e., $\overline{\mathcal{Y}} = \mathcal{Y} - \{1\}$. Thus, there are totally 2^m elements in the remaining set $\overline{\mathcal{Y}}$, and Theorems 1 still holds for such a pair of constellations $\mathcal{X}$ and $\overline{\mathcal{Y}}$. Therefore, instead of a pair of coprime PSK constellations $\mathcal{X}$ and $\mathcal{Y}$, a pair of constellations $\mathcal{X}$ and $\overline{\mathcal{Y}}_1$, in practice, can be used in the bit/constellation mapping.
3) By Theorem 1, if we let m_0 denote the maximum positive integer such that $u_{J+m} - \sum_{i=1}^{m-2} h_{J+i}x_{m-i} = 0$ for $m_0 < m \le L - J$ but $u_{J+m_0} - \sum_{i=1}^{m_0-2} h_{J+i}x_{m_0-i} = 0$, then the length of the channel is actually equal to $m_0 - J + 1$. Therefore, our blind modulation scheme enables the receiver to exactly determine the length of the channel by only utilizing the first two block received signals.
4) It should be explicitly pointed out here that the unique identification of both the channel coefficients and the transmitted signals in Theorem 1 depends not only on the two unique factorizations characterized by Propositions 1 and 2 but on the scheme of how to transmit the signals as well. A natural question is whether orthogonal frequency-division multiplexing (OFDM) with a pair of coprime PSK constellations enables the unique identification of both the channel coefficients and the transmitted signals. Unfortunately, the answer to this question is negative. The reason is as follows. For discussion simplicity, let us consider a noncoherent OFDM system with four subcarriers, the channel length of 2, and the coherence time being 8. In the noise-free case, there are in total eight received signals, i.e., $\mathbf{r}_x = \mathrm{diag}(H_0, H_1, H_2, H_3)\mathbf{x}$ and $\mathbf{r}_y = \mathrm{diag}(H_0, H_1, H_2, H_3)\mathbf{y}$, where $\mathbf{x} \in \mathcal{X}^4$, $\mathbf{y} \in \mathcal{Y}^4$, and $H_i = h_0 + h_1 \exp(-j2\pi i/4)$ for $i = 0, 1, 2, 3$. If we take $h_0 = h_1 = 1$, then we have $H_2 = 0$. As a result, the signals x_3 and y_3 are completely lost in the third subcarrier.

C. Full Diversity

When the channel statistics of the fading and the noise is available at the receiver, the ML criterion can be utilized for noncoherent detection [46]. Under the assumptions made in Section II, the noncoherent ML detector for our channel model (7) is a quadratic receiver, i.e., $\hat{\mathbf{S}} = \arg\min_{\mathbf{S}}\{\Delta_s - \mathbf{r}^H\boldsymbol{\Theta}_s\mathbf{r}\}$, where $\boldsymbol{\Theta}_s = (1/\sigma^2)\mathbf{S}(\sigma^2\mathbf{I} + \mathbf{S}^H\mathbf{S})^{-1}\mathbf{S}^H$, and $\Delta_s = \log\det(\sigma^2\mathbf{I} + \mathbf{S}^H\mathbf{S})$. The GLRT receiver requires neither the knowledge of the fading and noise statistics nor the knowledge of their realizations [43], [47], [48]. The criterion can be simply stated as $\hat{\mathbf{S}} = \arg\max_{\mathbf{S}}\{\mathbf{r}^H\mathbf{S}(\mathbf{S}^H\mathbf{S})^{-1}\mathbf{S}^H\mathbf{r}\}$. In fact, the GLRT receiver projects the received signal $\mathbf{r}$ on the different subspaces spanned by $\mathbf{S}$ and then compute the energies of all the projections and choose the projection maximizing the energy. In general, the GLRT receiver provides a suboptimal solution. However, the GLRT receiver that does not require fading information makes it an appealing detection candidate [43]. Now, suppose we use the GLRT receiver. To examine full diversity, for any pair of distinct codewords $\mathbf{S}$ and $\widetilde{\mathbf{S}}$, let

$$\begin{pmatrix} \mathbf{S}^H \\ \tilde{\mathbf{S}}^H \end{pmatrix} (\mathbf{S}, \tilde{\mathbf{S}}) = \mathbf{A}. \tag{31}$$

Brehler and Varanasi [43] proved the following lemma.

Lemma 4: If matrices $\mathbf{A}$ have full rank for all pairs of distinct codewords $\mathbf{S}$ and $\widetilde{\mathbf{S}}$, then the codebook provides full diversity for the GLRT receiver.

Now, we are in position to formally state the second result in this paper.

Theorem 2: The blind modulation designed in Section II with p and q being coprime enables the full diversity gain of L for the GLRT receiver.

Proof: By Lemma 4, we only need to prove that $(\mathbf{S}, \widetilde{\mathbf{S}})$ has full column rank for any pair of distinct signal matrices $\mathbf{S}$ and $\widetilde{\mathbf{S}}$. Otherwise, if there existed a pair of distinct codeword matrices $\mathbf{S}$ and $\widetilde{\mathbf{S}}$ for which the matrix $(\mathbf{S}, \widetilde{\mathbf{S}})$ does not have full column rank, then the following linear equations with respect to variables $\mathbf{h}$ and $-\widetilde{\mathbf{h}}$

$$(\mathbf{S}, \tilde{\mathbf{S}}) \begin{pmatrix} \mathbf{h} \\ -\tilde{\mathbf{h}} \end{pmatrix} = 0 \tag{32}$$

would have a nonzero solution $\mathbf{h}_0$ and $\widetilde{\mathbf{h}}_0$. Let $\mathbf{r}_0 = \mathbf{S}\mathbf{h}_0$. Then, we would also have $\mathbf{r}_0 = \widetilde{\mathbf{S}}\widetilde{\mathbf{h}}_0$. In other words, for a given nonzero received signal $\mathbf{r}_0$, equation $\mathbf{r}_0 = \mathbf{S}\mathbf{h}$ has two distinct pairs of solutions. By Theorem 1, we have that $\mathcal{T}(\mathbf{x}) = \mathcal{T}(\widetilde{\mathbf{x}})$ and $\mathcal{T}(\mathbf{y}) = \mathcal{T}(\widetilde{\mathbf{y}})$. Since $\mathbf{S} \neq \widetilde{\mathbf{S}}$, there is a pair of distinct signal submatrices in $\mathbf{S}$ and $\widetilde{\mathbf{S}}$, $\mathcal{T}(\mathbf{z}_i)$ and $\mathcal{T}(\widetilde{\mathbf{z}}_i)$ for some $3 \le i \le qL$. That being said, $\mathbf{z}_i \neq \widetilde{\mathbf{z}}_i$. If we let $\mathbf{z}_i = (z_{i1}, z_{i2}, \ldots, z_{iK})^T$ and $\widetilde{\mathbf{z}}_i = (\widetilde{z}_{i1}, \widetilde{z}_{i2}, \ldots, \widetilde{z}_{iK})^T$, then there exists a positive integer k such that $z_{ik} \neq \widetilde{z}_{ik}$ but $z_{i\ell} = \widetilde{z}_{i\ell}$ for $\ell = 1, 2, \ldots, k-1$. For notional simplicity, we use $\mathbf{B}[M : N]$ to denote the submatrix of a matrix $\mathbf{B}$ consisting of all the columns and rows from M to N. Then, we have (33), shown at the bottom of the next page, since $\mathcal{T}(\widetilde{\mathbf{z}}_i)[k : K+k-1] - \mathcal{T}(\mathbf{z}_i)[k : K+k-1]$ is actually a $K \times K$ lower triangular matrix with the diagonal entries being all equal to $z_{ik} - \widetilde{z}_{ik}$. Therefore, the submatrix of $(\mathbf{S}, \widetilde{\mathbf{S}})$

$$\begin{pmatrix} \mathcal{T}(\mathbf{x})[1:K] & \mathcal{T}(\tilde{\mathbf{x}})[1:K] \\ \mathcal{T}(\mathbf{z}_i)[k:K+k-1] & \mathcal{T}(\tilde{\mathbf{z}}_i)[k:K+k-1] \end{pmatrix}$$

is a $2K \times 2K$ invertible matrix, and hence, $(\mathbf{S}, \widetilde{\mathbf{S}})$ has full column rank, which contradicts with the previous assumption. This completes the proof of Theorem 2. ■

So far, we have shown that our blind modulation scheme enables the unique identification of the channel coefficients in the noise-free case as well as full diversity in the noise environment. Similar to Comment 2 on Theorem 1, our Theorem 2 is also true for both a particular pair of $p = 2^m$ and $q = 2^m + 1$ and the derived pair of constellations $\mathcal{X}$ and $\overline{\mathcal{Y}}$. In addition, full diversity relies on the two unique factorizations enabled by Propositions 1 and 2 as well as on the way of how to transmit the signals. For example, consider a noncoherent OFDM system with four subcarriers, the channel length of 2, and the coherence time being 8. In this case, the signal matrix is given by

$$\mathbf{S} = \begin{pmatrix} x_1 & x_1 \\ x_2 & -jx_2 \\ x_3 & -x_3 \\ x_4 & jx_4 \\ y_1 & y_1 \\ y_2 & -jy_2 \\ y_3 & -y_3 \\ y_4 & jy_4 \end{pmatrix}.$$

If we take $x_i = \tilde{x}_i$ for $i = 1, 2, 3, 4$, $y_k = \tilde{y}_k$ for $k = 2, 3, 4$ and $y_1 \neq \tilde{y}_1$, the rank of the matrix $(\mathbf{S}, \tilde{\mathbf{S}})$ is 3 at most. As a consequence, the OFDM system with a pair of coprime PSK constellations cannot enable full diversity for the GLRT receiver.

IV. Iterative Least-Square Errors With Parallel Sphere Decoders and Simulations

Our task in this section is to provide an efficient algorithm to approximate the GLRT receiver by making use of the iterative least squares [14], [18]–[21], [25] with the parallel sphere decoders [26]–[35], the semidefinite relaxation algorithm [49], or the Viterbi algorithm [50].

A. Iterative Least-Square Errors With Parallel Sphere Decoders

Essentially, the GLRT receiver for our channel model deals with the following optimization problem:

$$\hat{\mathbf{S}} = \arg\max_{\mathbf{S}} \left\{ \mathbf{r}^H \mathbf{S} (\mathbf{S}^H \mathbf{S})^{-1} \mathbf{S}^H \mathbf{r} \right\}. \tag{34}$$

The global solution of (34) can be computed by an exhaust search over the whole codewords. However, the number of all possible codewords that need to be checked grows exponentially, which is practically prohibitive. It was proved [25] that the optimization problem (34) is equivalent to the following least squares for jointly estimating the channel and the signal:

$$\{\hat{\mathbf{S}}, \hat{\mathbf{h}}\} = \arg\min_{\mathbf{S},\mathbf{h}} \|\mathbf{r} - \mathbf{S}\mathbf{h}\|_2^2. \tag{35}$$

This optimization problem can be approached by employing iterative least squares [14], [18]–[21] with parallel ML decoders. Given an initial estimate $\hat{\mathbf{h}}^{(0)}$ of $\mathbf{h}$, since $\|\mathbf{r} - \mathbf{S}\hat{\mathbf{h}}^{(0)}\|_2^2 = \sum_{i=1}^{T} \|\mathbf{r}_i - \mathcal{T}(\mathbf{z}_i)\hat{\mathbf{h}}^{(0)}\|_2^2$ and the information symbols between each two codeword matrixes $\mathcal{T}(\mathbf{z}_i)$ and $\mathcal{T}(\mathbf{z}_\ell)$ for $i \neq \ell$ are independent, the minimization problem of $\|\mathbf{r} - \mathbf{S}\hat{\mathbf{h}}^{(0)}\|_2^2$ with respect to the signal matrix $\mathbf{S}$ is equivalent to each minimization problem with respect to the individual signal submatrix $\mathcal{T}(\mathbf{z}_i)$, i.e.,

$$\begin{aligned} \hat{\mathbf{z}}_i^{(0)} &= \arg\min \left\| \mathbf{r}_i - \mathcal{T}(\mathbf{z}_i)\hat{\mathbf{h}}^{(0)} \right\|_2^2 \\ &= \arg\min \left\| \mathbf{r}_i - \mathcal{T}_c\left(\hat{\mathbf{h}}^{(0)}\right)\mathbf{z}_i \right\|_2^2, \quad \text{for } i = 1, 2, \cdots, T. \end{aligned} \tag{36}$$

Due to the structure of $\mathcal{T}_c(\hat{\mathbf{h}}^{(0)})$, the minimization problem (36) can be efficiently solved using parallel sphere decoders [26]–[35] or Viterbi algorithm [50] if either L or the size of constellations is small. Once we have all the estimates $\hat{\mathbf{z}}_i^{(0)}$ of $\mathbf{z}_i$ for $i = 1, 2, \ldots, T$, then a better estimate of $\mathbf{h}$ can be obtained by minimizing $\|\mathbf{r} - \hat{\mathbf{S}}^{(0)}\mathbf{h}\|_2^2$ with respect to complex continuous variable $\mathbf{h}$, which gives $\hat{\mathbf{h}}^{(1)} = ((\mathbf{S}^{(0)})^H \mathbf{S}^{(0)})^{-1} (\mathbf{S}^{(0)})^H \mathbf{r}$. Hereafter, we let $\mathbf{S}^{(m)}$ denote $\mathbf{S}^{(m)} = [\mathcal{T}^T(\hat{\mathbf{z}}_1^{(m)}), \mathcal{T}^T(\hat{\mathbf{z}}_2^{(m)}), \ldots, \mathcal{T}^T(\hat{\mathbf{z}}_T^{(m)})]^T$. We keep continuing this process until $\|\hat{\mathbf{h}}^{(m+1)} - \hat{\mathbf{h}}^{(m)}\|$ is less than a given threshold $\delta > 0$. The above whole procedure can be summarized as the following algorithm:

Algorithm 1: Iterative least squares with parallel sphere decoders or the Viterbi algorithm

1) *Initialization:* $\hat{\mathbf{h}}^{(m)}, m = 0$ and estimate $\hat{\mathbf{S}}^{(0)}$ using the parallel linear ML decoders or the Viterbi algorithm based on (36).

2) *Update:* $\hat{\mathbf{h}}^{(m+1)} = ((\mathbf{S}^{(m)})^H \mathbf{S}^{(m)})^{-1} (\mathbf{S}^{(m)})^H \mathbf{r}$.

3) *Stop:* Continue until $\|\hat{\mathbf{h}}^{(m+1)} - \hat{\mathbf{h}}^{(m)}\| < \delta$.

B. Initialization of Channel Estimation

The performance of the decoding Algorithm 1 heavily depends on how to properly choose the initial estimate of $\mathbf{h}$, i.e., $\mathbf{h}^{(0)}$. In this section, we develop an efficient algorithm to

$$\begin{aligned} &\begin{vmatrix} \mathcal{T}(\mathbf{x})[1:K] & \mathcal{T}(\widetilde{\mathbf{x}})[1:K] \\ \mathcal{T}(\mathbf{z}_i)[k:K+k-1] & \mathcal{T}(\widetilde{\mathbf{z}}_i)[k:K+k-1] \end{vmatrix} \\ &= \begin{vmatrix} \mathcal{T}(\mathbf{x})[1:K] & \mathcal{T}(\widetilde{\mathbf{x}})[1:K] - \mathcal{T}(\mathbf{x})[1:K] \\ \mathcal{T}(\mathbf{z}_i)[k:K+k-1] & \mathcal{T}(\widetilde{\mathbf{z}}_i)[k:K+k-1] - \mathcal{T}(\mathbf{z}_i)[k:K+k-1] \end{vmatrix} \\ &= \begin{vmatrix} \mathcal{T}(\mathbf{x})[1:K] & \mathbf{0} \\ \mathcal{T}(\mathbf{z}_i)[k:K+k-1] & \mathcal{T}(\widetilde{\mathbf{z}}_i)[k:K+k-1] - \mathcal{T}(\mathbf{z}_i)[k:K+k-1] \end{vmatrix} = x_1^K (z_{ik} - \widetilde{z}_{ik})^K \neq 0. \end{aligned} \tag{33}$$

obtain an initial estimate of the channel. Let us consider the relationship between the inputs and outputs in the first two blocks. In this case, we rewrite (4) and (5) here as

$$\mathbf{r}_1 = \mathcal{T}(\mathbf{x})\mathbf{h} + \boldsymbol{\xi}_1, \quad \mathbf{x} \in \mathcal{X}^K \tag{37a}$$

$$\mathbf{r}_2 = \mathcal{T}(\mathbf{y})\mathbf{h} + \boldsymbol{\xi}_2, \quad \mathbf{y} \in \mathcal{Y}^K. \tag{37b}$$

Let $\mathbf{r}_m = (r_{m1}, r_{m2}, \ldots, r_{mT})^T$ and $\boldsymbol{\xi}_m = (\xi_{m1}, \xi_{m2}, \ldots, \xi_{mT})^T$ for $m = 1, 2$. Then, from the first two equations of (37a) and (37b), we have

$$r_{11} = x_1 h_0 + \xi_{11} \tag{38}$$

$$r_{21} = y_1 h_0 + \xi_{21}. \tag{39}$$

These two equations can be written in a more compact vector form as

$$\begin{pmatrix} r_{11} \\ r_{21} \end{pmatrix} = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} h_0 + \begin{pmatrix} \xi_{11} \\ \xi_{21} \end{pmatrix}. \tag{40}$$

Then, an estimate of h_0 is given by

$$\hat{h}_{f,0}^{(0)} = \frac{\hat{x}_{f,1}^* r_{11} + \hat{y}_{f,1}^* r_{21}}{2} \tag{41}$$

where $\hat{x}_{f,1}$ and $\hat{y}_{f,1}$ can be obtained by solving the following optimization problem:

$$\begin{aligned} \{\hat{x}_{f,1}, \hat{y}_{f,1}\} &= \arg \max_{x_1 \in \mathcal{X}, y_1 \in \mathcal{Y}} |x_1^* r_{11} + y_1^* r_{21}|^2 \\ &= \arg \max_{x_1 \in \mathcal{X}, y_1 \in \mathcal{Y}} \\ &\quad \times \left(|r_{11}|^2 + |r_{21}|^2 + r_{11}^* r_{21} x_1 y_1^* + r_{11} r_{21}^* x_1^* y_1 \right) \\ &= \arg \max_{x_1 \in \mathcal{X}, y_1 \in \mathcal{Y}} \\ &\quad \times \left(|r_{11}|^2 + |r_{21}|^2 + |r_{11}^* r_{21}|^2 - |r_{11}^* r_{21} - x_1^* y_1|^2 \right). \end{aligned} \tag{42}$$

Hence, the maximization optimization problem (42) is equivalent to the following minimization optimization problem:

$$\hat{s}_{pq} = \arg \min_{s_{pq} \in \mathcal{S}_{pq}} |r_{11}^* r_{21} - s_{pq}|^2 \tag{43}$$

where $\mathcal{S}_{pq}$ denotes the pq-PSK constellation and $s_{pq} = x_1^* y_1 = \exp(j(2\pi k/pq))$ is a pq-PSK symbol. The solution to (43), i.e., an optimal estimate of k, is determined as follows: $\hat{k}_f = \lfloor pq \arg(\alpha)/2\pi \rfloor$ if $0 \le pq \arg(\alpha)/2\pi - \lfloor pq \arg(\alpha)/2\pi \rfloor < 1/2$. Otherwise, $\hat{k}_f = \lfloor pq \arg(\alpha)/2\pi \rfloor + 1$. Here, α is defined by $\alpha = r_{11}^* r_{21}$. Then, using Proposition 1, we obtain the estimates of x_1 and y_1 as

$$\hat{x}_{f,1} = \exp\left(-j\frac{2\pi \hat{k}_f q^{\varphi(p)-1}}{p}\right)$$

$$\hat{y}_{f,1} = \exp\left(j\frac{2\pi \hat{k}_f p^{\varphi(q)-1}}{q}\right).$$

In general, suppose that both the estimates $\hat{h}_{f,i-1}^{(0)}$ of h_{i-1} and those of signals x_i and y_i are all correct, i.e., $\hat{h}_{f,i-1}^{(0)} = h_{i-1}, \hat{x}_{f,i} = x_i$ and $\hat{y}_{f,i} = y_i$ for $i = 1, 2, \ldots, n < L$. Now, consider the $(n+1)$th equations in (37), i.e.,

$$r_{1(n+1)} = \sum_{i=1}^{n} x_{n+2-i} h_{i-1} + x_1 h_n + \xi_{1(n+1)} \tag{44}$$

$$r_{2(n+1)} = \sum_{i=1}^{n} y_{n+2-i} h_{i-1} + y_1 h_n + \xi_{2(n+1)} \tag{45}$$

which can equivalently be rewritten as

$$\begin{aligned} \tilde{r}_{1(n+1)} &= r_{1(n+1)} - \sum_{i=2}^{n} x_{n+2-i} h_{i-1} \\ &= x_{n+1} h_0 + x_1 h_n + \xi_{1(n+1)} \\ \tilde{r}_{2(n+1)} &= r_{2(n+1)} - \sum_{i=2}^{n} y_{n+2-i} h_{i-1} \\ &= y_{n+1} h_0 + y_1 h_n + \xi_{2(n+1)}. \end{aligned}$$

Therefore, based on the above two received signals, the least-square error estimate of h_n is given by

$$\hat{h}_{f,n}^{(0)} = \frac{x_1^* \tilde{r}_{1(n+1)} + y_1^* \tilde{r}_{2(n+1)} - (x_1^* \tilde{x}_{f,n+1} + y_1^* \hat{y}_{f,n+1}) h_0}{2} \tag{46}$$

where the estimates of x_{n+1} and y_{n+1} are obtained by solving the following optimization problem:

$$\{\hat{x}_{f,n+1}, \hat{y}_{f,n+1}\} = \arg \min_{x_{n+1} \in \mathcal{X}, y_{n+1} \in \mathcal{Y}} \times \left\| \mathbf{F} \begin{pmatrix} \tilde{r}_{1(n+1)} \\ \tilde{r}_{2(n+1)} \end{pmatrix} - h_0 \mathbf{F} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \right\|^2$$

with $\mathbf{F}$ being defined by $\mathbf{F} = \mathbf{I}_2 - 1/2\binom{x_1}{y_1}(x_1^*, y_1^*)$. The preceding whole procedure can be summarized as the following algorithm:

Algorithm 2: Initial forward successive estimates of the channel coefficients

1) *Initialization:* The estimate of h_0 is given by $\hat{h}_{f,0}^{(0)} = (\hat{x}_{f,1}^* r_{11} + \hat{y}_{f,1}^* r_{21}/2)$, where the estimates of x_1 and y_1 are

$$\hat{x}_{f,1} = \exp\left(-j\frac{2\pi \hat{k}_f q^{\varphi(p)-1}}{p}\right)$$

$$\hat{y}_{f,1} = \exp\left(j\frac{2\pi \hat{k}_f p^{\varphi(q)-1}}{q}\right)$$

an optimal estimate of k is determined as follows. $\hat{k}_f = \lfloor pq \arg(\hat{\alpha})/2\pi \rfloor$ if $0 \le pq \arg(\hat{\alpha})/2\pi - \lfloor pq \arg(\hat{\alpha})/2\pi \rfloor < 1/2$. Otherwise, $\hat{k}_f = \lfloor pq \arg(\hat{\alpha})/2\pi \rfloor + 1$. Here, α is defined by $\alpha = r_{11}^* r_{21}$.

2) *Recursion:* Under the assumption on the perfect estimates of x_i, y_i and h_i, i.e., $\hat{h}_{f,i-1}^{(0)} = h_{i-1}, \hat{x}_{f,i} = x_i$ and $\hat{y}_{f,i} = y_i$

for $i = 1, 2, \ldots, n < L$, the estimates of x_{n+1} and y_{n+1} are obtained by solving the following optimization problem:

$$\{\hat{x}_{f,n+1}, \hat{y}_{f,n+1}\} = \arg \min_{x_{n+1}\in\mathcal{X}, y_{n+1}\in\mathcal{Y}} \times \left\| \mathbf{F} \begin{pmatrix} \tilde{r}_{1(n+1)} \\ \tilde{r}_{2(n+1)} \end{pmatrix} - h_0 \mathbf{F} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \right\|^2$$

and thus, the estimate of h_n is provided by

$$\hat{h}_{f,n}^{(0)} = \frac{x_1^* \tilde{r}_{1(n+1)} + y_1^* \tilde{r}_{2(n+1)} - (x_1^* \tilde{x}_{f,n+1} + y_1^* \hat{y}_{f,n+1}) h_0}{2}$$

where $\widetilde{r}_{1(n+1)}$ and $\widetilde{r}_{2(n+1)}$ are determined by

$$\tilde{r}_{1(n+1)} = r_{1(n+1)} - \sum_{i=2}^{n} x_{n+2-i} h_{i-1}$$

$$\tilde{r}_{2(n+1)} = r_{2(n+1)} - \sum_{i=2}^{n} y_{n+2-i} h_{i-1}.$$

For $n = L, L+1, \ldots, K$ and under the condition of no error propagation, the estimates of x_n and y_n are obtained as follows. Let $\gamma_{f,n} = r_{1n} - \sum_{i=1}^{L-1} h_{i-1} x_{n-i}/h_0$ and $\delta_{f,n} = r_{2n} - \sum_{i=1}^{L-1} h_{i-1} y_{n-i}/h_0$. Then

a) $\hat{x}_{f,n} = \exp(j(2\pi\hat{\ell}_{f,n}/p)$, where $\hat{\ell}_{f,n} = \lfloor p \arg(\gamma_{f,n})/2\pi \rfloor$ if $0 \le (p \arg(\gamma_{f,n})/2\pi) - \lfloor p \arg(\gamma_{f,n})/2\pi \rfloor < 1/2$, and otherwise, $\hat{\ell}_{f,n} = \lfloor p \arg(\gamma_{f,n})/2\pi \rfloor + 1$;

b) $\hat{y}_{f,n} = \exp(j(2\pi\hat{m}_{f,n}/q)$, where $\hat{m}_{f,n} = \lfloor q \arg(\delta_{f,n})/2\pi \rfloor$ if $0 \le q \arg(\delta_{f,n})/2\pi - \lfloor q \arg(\delta_{f,n})/2\pi \rfloor < 1/2$, and otherwise, $\hat{m}_{f,n} = \lfloor p \arg(\delta_{f,n})/2\pi \rfloor + 1$.

If we start with the last L equations of (37a) and (37b) and take advantage of the upper triangular structure, we can obtain the following initial backward successive algorithm similar to Algorithm 2.

Algorithm 3: Initial backward successive estimates of the channel coefficients

1) *Initialization:* The estimate of h_{L-1} is given by $\hat{h}_{b,L-1}^{(0)} = (\hat{x}_{b,K}^* r_{1P} + \hat{y}_{b,K}^* r_{2P})/2$, where the estimates of x_K and y_K are

$$\hat{x}_{b,k} = \exp\left(-j \frac{2\pi \hat{k}_f q^{\varphi(p)-1}}{bp}\right)$$

$$\hat{y}_{b,k} = \exp\left(j \frac{2\pi \hat{k}_b p^{\varphi(q)-1}}{q}\right)$$

and an optimal estimate of k is determined as follows: $\hat{k}_b = \lfloor pq \arg(\hat{\beta})/2\pi \rfloor$ if $0 \le pq \arg(\hat{\beta})/2\pi - \lfloor pq \arg(\hat{\beta})/2\pi \rfloor < 1/2$. Otherwise, $\hat{k}_b = \lfloor pq \arg(\hat{\beta})/2\pi \rfloor + 1$. Here, β is defined by $\beta = r_{1P}^* r_{2P}$.

2) *Recursion:* Under the assumption on the perfect estimates of x_{K+1-i}, y_{K+1-i} and h_{L-i}, i.e., $\hat{h}_{b,L-i}^{(0)} = h_{L-i}, \hat{x}_{b,K+1-i} = x_{K+1-i}$ and $\hat{y}_{b,K+1-i} = y_{K+1-i}$ for $i = 1, 2, \ldots, n < L$, the estimates of x_{K-n} and y_{K-n} are obtained by solving the following optimization problem:

$$\{\hat{x}_{b,K-n}, \hat{y}_{b,K+n}\} = \arg \min_{x_{K-n}\in\mathcal{X}, y_{K-n}\in\mathcal{Y}} \times \left\| \mathbf{B} \begin{pmatrix} \tilde{r}_{1(P-n)} \\ \tilde{r}_{2(P-n)} \end{pmatrix} - h_{L-1} \mathbf{B} \begin{pmatrix} x_{K-n} \\ y_{K-n} \end{pmatrix} \right\|^2$$

and thus, the estimate of h_{L-n-1} is provided by

$$\hat{h}_{b,L-n-1}^{(0)} = \left(x_K^* \tilde{r}_{1(P-n)} + y_K^* \tilde{r}_{2(P-n)} - \left(x_K^* \hat{x}_{b,K-n} + y_K^* \hat{y}_{b,K-n}\right) h_{L-1}\right)/2$$

where $\widetilde{r}_{1(P-n)}$ and $\widetilde{r}_{2(P-n)}$ are determined by

$$\tilde{r}_{1(P-n)} = r_{1(P-n)} - \sum_{i=1}^{n} x_{K-n+i} h_{L-i-1}$$

$$\tilde{r}_{2(P-n)} = r_{2(P-n)} - \sum_{i=1}^{n} y_{K-n+i} h_{L-i-1}.$$

For $n = L, L+1, \ldots, K$ and under the condition of no error propagation, the estimates of x_{K-n} and y_{K-n} are obtained as follows: Let $\gamma_{b,n} = (r_{1(P-n)} - \sum_{i=1}^{L-1} h_{L-i-1} x_{K-n+i})/h_{L-1}$ and $\delta_{b,n} = (r_{2(P-n)} - \sum_{i=1}^{L-1} h_{L-i-1} y_{K-n+i})/h_{L-1}$. Then

a) $\hat{x}_{b,K-n} = \exp(j(2\pi\hat{\ell}_{b,n}/p))$, where $\hat{\ell}_{b,n} = \lfloor p \arg(\gamma_{b,n})/2\pi \rfloor$ if $0 \le p \arg(\gamma_{b,n})/2\pi - \lfloor p \arg(\gamma_{b,n})/2\pi \rfloor < 1/2$, and otherwise, $\hat{\ell}_{b,n} = \lfloor p \arg(\gamma_{b,n})/2\pi \rfloor + 1$;

b) $\hat{y}_{b,K-n} = \exp(j(2\pi\hat{m}_{b,n}/q))$, where $\hat{m}_{b,n} = \lfloor q \arg(\delta_{b,n})/2\pi \rfloor$ if $0 \le q \arg(\delta_{b,n})/2\pi - \lfloor q \arg(\delta_{b,n})/2\pi \rfloor < 1/2$, and otherwise, $\hat{m}_{b,n} = \lfloor p \arg(\delta_{b,n})/2\pi \rfloor + 1$.

Once we have had two estimates of $\mathbf{x}$ and $\mathbf{y}$ using Algorithms 2 and 3, we can compare $\mathbf{r}^H \mathbf{S}_f (\mathbf{S}_f^H \mathbf{S}_f)^{-1} \mathbf{S}_f^H \mathbf{r}$ with $\mathbf{r}^H \mathbf{S}_b (\mathbf{S}_b^H \mathbf{S}_b)^{-1} \mathbf{S}_b^H \mathbf{r}$ and select the greater one to obtain the final initial estimate of $\mathbf{h}$ for Algorithm 1, where $\mathbf{S}_f = (\mathcal{T}^T(\mathbf{x}_f), \mathcal{T}^T(\mathbf{y}_f))^T$, and $\mathbf{S}_b = (\mathcal{T}^T(\mathbf{x}_b), \mathcal{T}^T(\mathbf{y}_b))^T$. That is

$$\hat{\mathbf{h}}^{(0)} = \begin{cases} \left(\mathbf{S}_f^H \mathbf{S}_f\right)^{-1} \mathbf{S}_f^H \mathbf{r} & \text{if } \mathbf{r}^H \mathbf{S}_f \left(\mathbf{S}_f^H \mathbf{S}_f\right)^{-1} \mathbf{S}_f^H \mathbf{r} > \mathbf{r}^H \mathbf{S}_b \left(\mathbf{S}_b^H \mathbf{S}_b\right)^{-1} \mathbf{S}_b^H \mathbf{r} \\ \left(\mathbf{S}_b^H \mathbf{S}_b\right)^{-1} \mathbf{S}_b^H \mathbf{r} & \text{if } \mathbf{r}^H \mathbf{S}_f \left(\mathbf{S}_f^H \mathbf{S}_f\right)^{-1} \mathbf{S}_f^H \mathbf{r} < \mathbf{r}^H \mathbf{S}_b \left(\mathbf{S}_b^H \mathbf{S}_b\right)^{-1} \mathbf{S}_b^H \mathbf{r}. \end{cases}$$

Here, we must point out clearly that in spite of the fact that our proposed scheme enables full diversity for the GLRT receiver shown in Theorem 2, the decoding Algorithm 1 with Algorithms 2 and 3 for initialization is just a suboptimal decoding algorithm, and in general, it cannot assure full diversity.

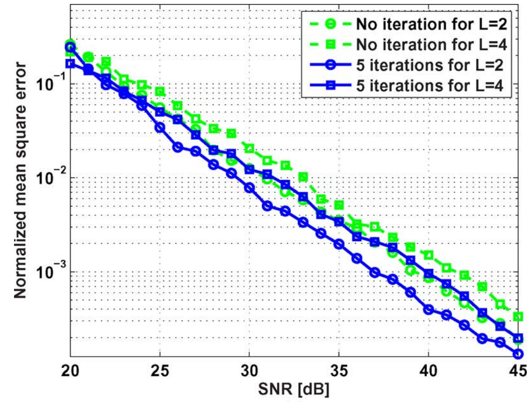
C. Simulations

In this section, we examine the performance of our blind modulation scheme and iterative decoding algorithms. Here, in all our computer simulations, we fix $T = 2$. At the receiver, we jointly estimate the channel coefficients and the transmitted symbols using the iterative least squares with parallel sphere detectors, as described in the previous section. First, we use Algorithms 2 and 3 to obtain an initial estimate of the channel vector $\mathbf{h}$. Then, we utilize this estimate as starting point in the iteration of Algorithm 1.

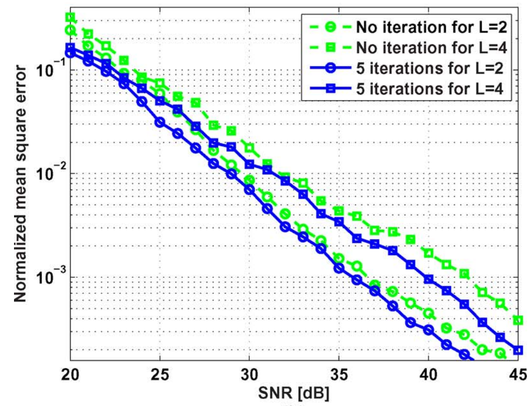
For each SNR, 200 channel realizations are implemented. We calculate the normalized mean square error $((1/200)\sum_{k=1}^{200}\|\mathbf{h}_k - \hat{\mathbf{h}}\|^2/\|\mathbf{h}_k\|^2)$ between the true channel coefficients and their estimates and evaluate the average symbol error rate using the decoding Algorithm 1. We test the performance of our hybrid signaling scheme when different lengths of channels, different sizes of transmission blocks, and different modulations are utilized. Figs. 1(a) and (b) and 2(a) and (b) show the normalized mean square errors, whereas Figs. 1(c) and (d) and 2(c) and (d) show the corresponding average symbol error rates. To put our decoding Algorithm 1 into perspective, we also compare its error performance using Algorithms 2 and 3 as initialization to that using random channel initialization when either $L = 2$ or $L = 4$ and $K = 16$. From Fig. 1(c), it can be observed that the decoding Algorithm 1 with random channel initialization completely fails. This means that the iterative decoding Algorithm 1 significantly depends on the initialization. On the other hand, from Figs. 1(c) and (d) and 2(c) and (d), it can also be observed that for the fixed K, p, and q, the symbol error rate for $L = 2$ is better than that for $L = 4$. This implies that decoding Algorithm 1 with Algorithms 2 and 3 for initialization does not achieve full diversity as proved by Theorem 2. In addition, in spite of the fact that the convergent issue on the iterative least squares with some pilot symbols was discussed and analyzed in [18], [19], and [21] only for linear receivers and the binary constellation, our computer simulations show that the iterative least-square algorithm using the sphere decoder and a pair of the coprime PSK constellations is still numerically convergent. All the aforementioned issues motivate us to further investigate how to properly choose the initialization of Algorithm 1 to improve its error performance in our future research.

V. Conclusion

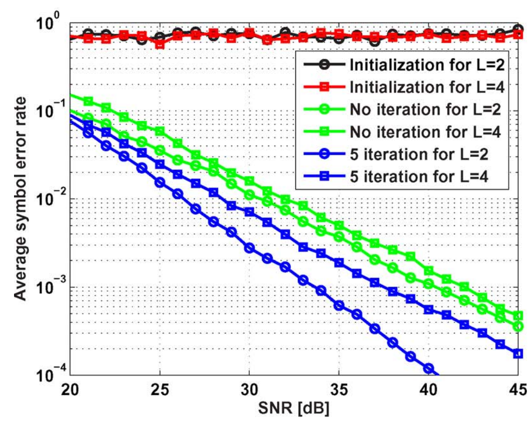
In this paper, we have proposed a novel and simple blind modulation technique to uniquely identify frequency-selective channels with zero-padded block transmission under noise-free environments by only processing the first two block received signal vectors. Furthermore, a closed-form solution to determine the transmitted signals and the channel coefficients has been derived by using linear congruence equation theory. In the Gaussian noise and Rayleigh fading environment, we have proved that our new scheme enables full diversity for the GLRT receiver. When only finite received data are available, we have provided the iterative least squares with parallel sphere decoders to approximate the GLRT detector by taking advantage of the linearity and triangular structure of our signal design.



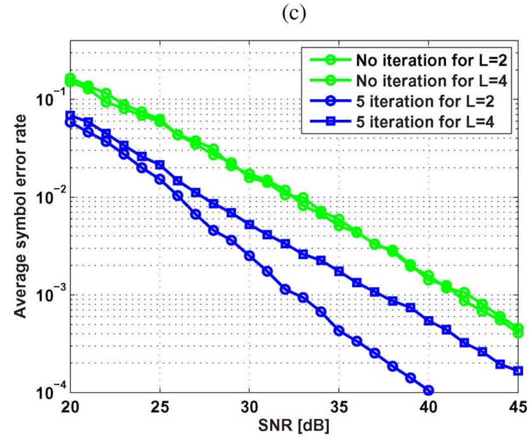
(a)



(b)



(c)



(d)

Fig. 1. Normalized mean square errors and average symbol error rates for $p = 4$ and $q = 3$. (a) $K = 16$. (b) $K = 20$. (c) $K = 16$. (d) $K = 20$.

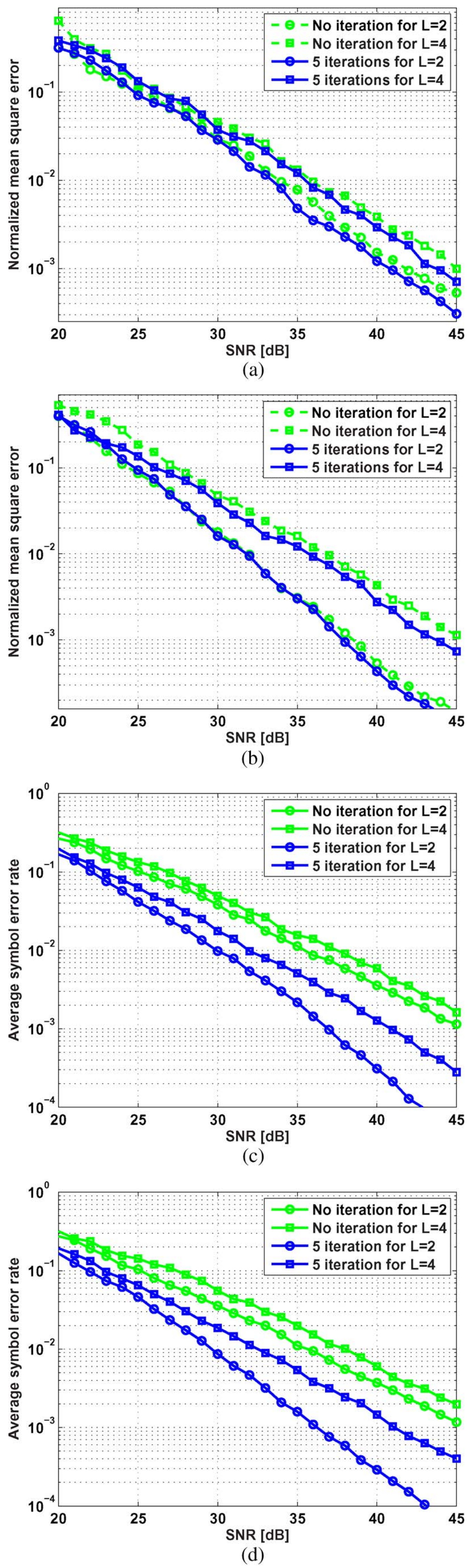


Fig. 2. Normalized mean square errors and average symbol error rates for $p = 5$ and $q = 4$. (a) $K = 16$. (b) $K = 20$. (c) $K = 16$. (d) $K = 20$.

APPENDIX A
PROOF OF PROPOSITION

First, we notice that $\exp(j(2\pi k/pq)) = \exp(j(2\pi n/p)) \exp(j(2\pi m/q))$ is equivalent to following linear congruence equation:

$$mp + nq \equiv k \ (\mathrm{mod} pq). \tag{47}$$

Since p and q are coprimes, by Lemma 3, solving (47) for m and n is equivalent to solving the following system of linear congruent equations:

$$nq \equiv k(\mathrm{mod} p) \tag{48a}$$

$$mp \equiv k(\mathrm{mod} q). \tag{48b}$$

By Lemma 2 and its Corollary 1, the solutions of (48) can be expressed by $n \equiv k\bar{q}_p \equiv kq^{\varphi(p)-1}(\mathrm{mod} p)$ and $m \equiv k\bar{p}_q \equiv kp^{\varphi(q)-1}(\mathrm{mod} q)$.

In the following, we will prove the uniqueness of the solutions. To do that, suppose there exists another pair of symbols $x' \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that $xy = x'y'$. Let $x = \exp(j(2\pi n/p)$, $x' = \exp(j(2\pi n'/p)), 0 \le nn' < p$, and $y = \exp(j(2\pi m/q)$, $y' = \exp(j(2\pi m'/q), 0 \le m, m' < q$. Then, we have

$$\exp\left(j2\pi\left(\frac{n}{p} + \frac{m}{q}\right)\right) = \exp\left(j2\pi\left(\frac{n'}{p} + \frac{m'}{q}\right)\right). \tag{49}$$

This is equivalent to $(n - n')q \equiv (m' - m)p \quad (\mathrm{mod} pq)$. Therefore, $m' - m \equiv 0 \quad (\mathrm{mod} q)$ and $n - n' \equiv 0 \quad (\mathrm{mod} p)$. Since $0 \le m < q$ and $0 \le n < p$, we have $m = m'$ and $n = n'$. This completes the proof of Proposition 1. ■

APPENDIX B
PROOF OF PROPOSITION

Proof: Let $w = |w| \exp(j\theta)$. If we write $x = \exp(j(2\pi m/p)$ and $y = \exp(j(2\pi n/q)$, then (14) is equivalent to

$$\exp\left(j\frac{2\pi m}{p}\right) - \exp\left(j\frac{2\pi n}{q}\right) = |w| \exp(j\theta). \tag{50}$$

Since

$$\begin{aligned}
&\exp\left(j\frac{2\pi m}{p}\right) - \exp\left(j\frac{2\pi n}{q}\right)\\
&\quad = \exp\left(j\frac{2\pi m}{p}\right)\left(1 - \exp\left(j\frac{2\pi(pn - qm)}{pq}\right)\right)\\
&\quad = -2j \sin\left(\frac{\pi(pn - qm)}{pq}\right) \exp\left(j\frac{\pi(pn + qm)}{pq}\right)
\end{aligned} \tag{51}$$

substituting (51) into (50) yields

$$-2j \sin\left(\frac{\pi(pn-qm)}{pq}\right) = |w| \exp\left(j\left(\theta - \frac{\pi(pn+qm)}{pq}\right)\right).$$

Therefore, we have

$$\theta = \frac{\pi(pn+qm)}{pq} + k\pi + \frac{\pi}{2} \quad \text{for some } k \in \mathbb{Z} \tag{52}$$

$$|w| = 2(-1)^{k+1}\sin\left(\frac{\pi(pn-qm)}{pq}\right). \tag{53}$$

Moreover, if (15) is satisfied, i.e., there exists a pair of $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ satisfying (14), then we have

$$mp + nq \equiv \ell\,(\mathrm{mod} pq) \tag{54}$$

with $\ell = pq(\theta/\pi - 1/2)$. Since p and q are coprimes, solving (54) for m and n is equivalent to solving the system of linear congruent equations

$$nq \equiv k(\mathrm{mod} p) \tag{55a}$$

$$mp \equiv k(\mathrm{mod} q). \tag{55b}$$

By Corollary 1, the solutions of (55) can be expressed by $n \equiv k\bar{q}_p \equiv kq^{\varphi(p)-1}(\mathrm{mod} p)$ and $m \equiv k\bar{p}_q \equiv kp^{\varphi(q)-1}(\mathrm{mod} q)$. This completes the proof of Proposition 2. ■

References

[1] Z. Wang and G. B. Giannakis, "Wireless multicarrier communications: Where Fourier meets Shannon," *IEEE Signal Process. Mag.*, vol. 17, no. 3, pp. 29–48, May 2000.

[2] N. Al-Dhahir and N. Diggavi, "Guard sequence optimization for block transmission over linear frequency-selective channels," *IEEE Trans. Commun.*, vol. 50, no. 6, pp. 938–946, Jun. 2002.

[3] J.-K. Zhang, T. N. Davidson, and K. M. Wong, "Optimal precoder for block transmission over frequency-selective fading channels," *Proc. Inst. Elect. Eng.—Commun.*, vol. 152, no. 4, pp. 463–468, Aug. 2005.

[4] Z. Wang, X. Ma, and G. B. Giannakis, "Optimality of single-carrier zero-padded block transmissions," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Orlando, FL, Mar. 2002, pp. 660–664.

[5] T. L. Marzetta, "BLAST training: Estimation channel characteristics for high-capacity space–time wireless," in *Proc. 37th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, Sep. 22–24, 1999.

[6] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.

[7] L. Zheng and D. N. C. Tse, "Communication on the Grassmann manifold: A geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 2, pp. 359–383, Feb. 2002.

[8] A. J. van der Veen, "Algebraic methods for deterministic blind beamforming," *Proc. IEEE*, vol. 86, no. 10, pp. 1987–2008, Oct. 1998.

[9] L. Tong and S. Perreau, "Multichannel blind identification: From subspace to maximum likelihood methods," *Proc. IEEE*, vol. 86, no. 10, pp. 1951–1968, Oct. 1998.

[10] G. Xu, H. Liu, L. Tong, and T. Kailath, "A least-squares approach to blind channel identification," *IEEE Trans. Signal Process.*, vol. 43, no. 12, pp. 2982–2993, Dec. 1995.

[11] L. Tong, G. Xu, and T. Kailath, "Blind identification and equalization based on second-order statistics: A time domain approach," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 340–349, Mar. 1994.

[12] L. Tong, G.-K. Xu, B. Hassibi, and T. Kailath, "Blind identification and equalization based on second-order statistics: A frequency-domain approach," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 329–334, Jan. 1995.

[13] E. Moulines, P. Duhamel, J. F. Cardoso, and S. Mayrargue, "Subspace methods for the blind identification of multichannel FIR filters," *IEEE Trans. Signal Process.*, vol. 43, no. 2, pp. 516–525, Feb. 1995.

[14] A. J. van der Veen, S. Talwar, and A. Paulraj, "A subspace approach to blind space–time signal processing for wireless communication systems," *IEEE Trans. Signal Process.*, vol. 45, no. 1, pp. 173–190, Jan. 1997.

[15] G. B. Giannakis and S. D. Halford, "Blind fractionally spaced equalization of noisy FIR channel: Direct and adaptive solutions," *IEEE Trans. Signal Process.*, vol. 45, no. 9, pp. 2277–2292, Sep. 1997.

[16] C. B. Papadias and D. T. M. Slock, "Fractionally spaced equalization of linear polyphase channels and related blind techniques based on multichannel linear prediction," *IEEE Trans. Signal Process.*, vol. 47, no. 3, pp. 641–654, Mar. 1999.

[17] Z. Ding, "Application aspects of blind adaptive equalizers in QAM data communications," Ph.D. dissertation, Cornell Univ., Ithaca, NY, 1990.

[18] S. Talwar, M. Viberg, and A. Paulraj, "Blind estimation of multiple cochannel digital signals using an antenna array," *IEEE Signal Process. Lett.*, vol. 1, no. 2, pp. 29–31, Feb. 1994.

[19] S. Talwar, M. Viberg, and A. Paulraj, "Blind separation synchronous cochannel digital signals using an antenna array-space—Part I: Algorithms," *IEEE Trans. Signal Process.*, vol. 44, no. 5, pp. 1184–1197, May 1996.

[20] A. J. van der Veen and A. Paulraj, "An analytical constant modulus algorithm," *IEEE Trans. Signal Process.*, vol. 44, no. 5, pp. 1136–1155, May 1996.

[21] S. Talwar, M. Viberg, and A. Paulraj, "Blind separation synchronous co-channel digital signals using an antenna array-space—Part II: Performance analysis," *IEEE Trans. Signal Process.*, vol. 45, no. 3, pp. 706–718, Mar. 1997.

[22] C. R. Johnson, P. Schniter, T. J. Endres, J. D. Behm, D. R. Brown, and R. A. Casas, "Blind equalization using the constant modulus criterion: A review," *Proc. IEEE*, vol. 86, no. 10, pp. 1927–1950, Oct. 1998.

[23] Z. Ding and Z.-Q. Luo, "A fast linear programming algorithm for blind equalization," *IEEE Trans. Commun.*, vol. 48, no. 9, pp. 1432–1436, Sep. 2000.

[24] Z.-Q. Luo, M. Meng, K. M. Wong, and J.-K. Zhang, "A fractionally spaced blind equalizer based on linear programming," *IEEE Trans. Signal Process.*, vol. 50, no. 7, pp. 1650–1660, Jul. 2002.

[25] G. H. Golub and V. Pereyra, "The differentiation of pseudo-inverses and nonlinear least squares problems whose variables separate," *SIAM J. Num. Anal.*, vol. 10, no. 2, pp. 413–432, 1973.

[26] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications," *ACM SIGSAM Bull.*, vol. 15, no. 1, pp. 37–44, Feb. 1981.

[27] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, no. 170, pp. 463–471, Apr. 1985.

[28] L. Babai, "On Lovsz lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, p. 113, Mar. 1986.

[29] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.

[30] C. P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Programm.*, vol. 66, no. 2, pp. 181–199, Sep. 1994.

[31] W. H. Mow, "Maximum likelihood sequence estimation from the lattice viewpoint," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1591–1600, Sep. 1994.

[32] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.

[33] L. Lampe, R. Schober, V. Pauli, and C. Windpassinger, "Application of sphere decoding to MSDD," in *Proc. 5th Int. ITG Conf. Source Channel Coding*, Erlangen, Germany, Jan. 2004, pp. 251–258.

[34] O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice code decoder for space–time codes," *IEEE Commun. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.

[35] M. O. Damen and N. C. Beaulieu, "On two high-rate algebraic space–time codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1059–1063, Apr. 2003.

[36] L. Zhou, J.-K. Zhang, and K. M. Wong, "Blind unique identification of Alamouti space–time coded channel via signal design and transmission technique," in *Proc. 18th Int. Symp. Signal Process. Appl.*, Aug. 2005, pp. 691–694.

[37] T. Cui and C. Tellambura, "Efficient blind receiver design for orthogonal space–time block codes," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1890–1899, May 2007.

[38] L. Zhou, J.-K. Zhang, and K. M. Wong, "A novel signaling scheme for blind unique identification of Alamouti space–time block coded channel," *IEEE Trans. Signal Process.*, vol. 55, no. 6, pp. 2570–2582, Jun. 2007.

[39] W.-K. Ma, "Blind ML detection of orthogonal space–time block codes: identifiability and code construction," *IEEE Trans. Signal Process.*, vol. 55, no. 7, pp. 3312–3324, Jul. 2007.

[40] T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Maximum-likelihood detection of orthogonal space–time block coded OFDM in unknown block fading channels," *IEEE Trans. Signal Process.*, vol. 56, no. 4, pp. 1637–1649, Apr. 2008.

[41] J.-K. Zhang and W.-K. Ma, “Full diversity blind Alamouti space–time block codes for unique identification of flat fading channels,” *IEEE Trans. Signal Process.*, vol. 57, no. 2, pp. 635–644, Feb. 2009.

[42] J. Liu, J.-K. Zhang, and K. M. Wong, “Full diversity codes for MISO systems equipped with linear or ML detectors,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4511–4527, Oct. 2008.

[43] M. Brehler and M. K. Varanasi, “Asymptotic error probability analysis of quadratic receiver in Rayleigh-fading channels with applications to a unified analysis of coherent and noncoherent space–time receivers,” *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2383–2399, Sep. 2001.

[44] T. M. Apostol, *Introduction to Analytic Number Theory*. New York: Springer-Verlag, 1976.

[45] L.-K. Hua, *Introduction to Number Theory*. Berlin, Germany: Springer-Verlag, 1982.

[46] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.

[47] A. Lapidoth and P. Narayan, “Reliable communication under channel uncertainty,” *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2148–2177, Oct. 1998.

[48] D. Warrier and U. Madhow, “Spectrally efficient noncoherent communication,” *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 651–668, Mar. 2002.

[49] Z.-Q. Luo and M. Kisialiou, An efficient SDR algorithm, Jun. 2006. [Online]. Available: http://www.ece.umn.edu/users/luozq

[50] G. D. Forney, Jr., “The Viterbi algorithm,” *Proc. IEEE*, vol. 61, no. 3, pp. 268–278, Mar. 1973.

Jian-Kang Zhang (M’04–SM’09) received the B.S. degree in information science (math) from Shaanxi Normal University, Xi’an, China, in 1983, the M.S. degree in information and computational science (math) from Northwest University, Xi’an, in 1988, and the Ph.D. degree in electrical engineering from Xidian University, Xi’an, in 1999.

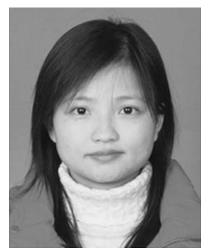
He has held research positions with McMaster University, Hamilton, ON, Canada, and Harvard University, Cambridge, MA. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, McMaster University. His research interests include multirate filterbanks, wavelet and multiwavelet transforms and their applications, and number theory transform and their applications in signal processing. His current research focuses on random matrices, channel capacity, and coherent and noncoherent multiple-input–multiple-output communication systems.

Dr. Zhang is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE SIGNAL PROCESSING LETTERS, and the *Journal of Electrical and Computer Engineering*. He is the coauthor of the paper that received the “IEEE Signal Processing Society Best Young Author Award” in 2008.

Chau Yuen (M’08) received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively.

He was a Post Doctoral Fellow with Lucent Technologies Bell Labs, Murray Hill, NJ, during 2005 and a Visiting Assistant Professor with the Hong Kong Polytechnic University, Hong Kong, in 2008. During the period of 2006–2010, he was a Senior Research Engineer with the Institute for Infocomm Research, Singapore. Since June 2010, he has been an Assistant Professor with the Singapore University of Technology and Design. He has published more than 80 research papers at international journals or conferences. His present research interests include green communications, cognitive networks, cooperative transmissions, and network coding.

Dr. Yuen also serves as an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.



Fei Huang was born in Jiangxi, China, on December 1983. She received the B.S. degree in electronics and communications engineering from Nanjing University of Science and Technology, Nanjing, China, in 2005 and the M.S. and Ph.D. degrees in electronics science and technology from the Nanjing University of Science and Technology, in 2007 and 2011, respectively.

She is currently with the Shanghai Institute of Radio Equipment, Shanghai, China. Her research interests include smart antenna and radar array signal processing.