A Blind Despreading and Demodulation Method for QPSK-DSSS Signal with Unknown Carrier Offset Based on Matrix Subspace Analysis

Zhaoyang Qiu1, Hua Peng1, Member, IEEE, and Tianyun Li1

1 Information Engineering University of PLA Strategic Support Force, Zhengzhou, Henan 450001 China

Corresponding author: Zhaoyang Qiu (e-mail: qiuzaoyang2010100@163.com)

This work was supported by the National Natural Science Foundation of China(No.61401511) and the National Natural Science Foundation of China(No.U1736107)

ABSTRACT Direct sequence spread spectrum (DSSS) signals are widely used in various military and civilian communication systems. It adopts the pseudorandom (PN) sequence to modulate baseband signal before transmission, leading to some unique and useful properties such as lower working signal to noise ratio (SNR), strong anti-jamming capability, and robustness to the effect of multi-path fading. In past few years, blind despreading for DSSS signals has been a hot topic in cognitive radio field. Previous works are mostly concentrated on BPSK-DSSS signals, and have developed theories and methods to estimate the PN sequence effectively. But unfortunately, most of them are powerless to process QPSK-DSSS signals. This work proposes a method based on matrix subspace analysis to recover the PN sequences and transmitted symbols for QPSK-DSSS signals with unknown carrier offset under non-cooperative reception occasion. To recover spreading sequences from subspace of self-covariance matrix, we derive the theoretical expressions of eigenvector by studying the complex hermit matrix decomposition and then investigate the influence of carrier residual. Finally, a structure is designed to complete blind despreading and demodulation from the received waveform to bit stream. Simulation verifies pretty good bit-error-rate (BER) performance of proposed algorithm.

INDEX TERMS QPSK-DSSS, blind despreading and demodulation, matrix subspace analysis, hermit matrix,

I. INTRODUCTION DSSS signals are widely used in satellite, short wave, underwater and mobile communication systems because of its low probability of detection and interception (LPD, LPI) [1][2][3][4]. The analysis for it is urgently demanded in the field of cognitive radio, spectrum monitoring and radio management as well. DSSS transmitters use a spreading sequence to modulate the baseband signal before transmission as a result that signal becomes similar to white noise statistically. The receiver conducts correlation between local PN sequence and received symbols to despread the signal and obtain the transmitted symbols. Without the PN code, however, it can be almost impossible to recover the transmitted bits. In past few years, researchers have done a lot of work to estimate the PN code of DSSS signals in non-cooperative context. Given no prior knowledge about the sequence, it’s really a challenge in blind signal processing area.

Matrix decomposition is one of the classical and representative methods to complete the subspace estimation with great anti-noise performance [5][6][7][8]. For BPSK-DSSS signal, when the code synchronization is completed, the eigenvector corresponding to the maximum eigenvalue is proved to be an unbiased estimate of PN waveform. When the carrier residual exists, the eigenvector will absorb the carrier into the waveform so that we can still recover the PN code by demodulate the waveform of eigenvector.

The neuron network is also an effective method to obtain the PN code. By setting the objective function based on constant modulus property or Hebbian criterion [9][10][11], the connection weight of the network will converge to the PN code by updating with the training. Compared to matrix decomposition, it extracts the principle component of the
segmented signals by neuron learning, resulting in a reduction in computational afford but loss in precision and stability.

However, most of previous works are concentrated on BPSK-DSSS signal and cannot be applied into the higher order modulation type like QPSK. For QPSK-DSSS signals, two different \( n \) sequences are used to modulate the data of homophase and orthogonal branches respectively. Due to the possible existence of residual carrier or phase offset, we cannot directly separate the data by simply extracting the real part and imaginary part of the signal. As a result, the subspace is spanned by the two PN sequences, indicating that the eigenvectors will appear as mixtures of the PN sequences, leading to difficulties to obtain the PN codes from the eigenvectors, especially in non-cooperative reception occasion.

Researchers have proposed several methods to solve the PN code extraction problem for QPSK-DSSS signal. Multi-user model is put forward to separate the linear mixed signals. It adopts blind source separation (BSS) algorithm based on independent component analysis (ICA) to recover the PN code from the eigenvectors [12][13]. Given two unrelated linear combination of the PN sequences, the positive definite model in BSS is satisfied to separate the components and obtain two independent PN sequences. However, it is only able to work with the real signal and fails to run when carrier residual exists. Traversal based on the constant modulus characteristic of the PN code is also a way by searching the linear combination coefficients to realize the estimation of PN codes [14][15]. By calculating the variance of the separated sequences, the estimation with least variance can be obtained. Nevertheless, the monotonicity of objective function is rarely proved yet and the local extremums are sometimes inevitable, leading to limitations to engineering application. Furthermore, the methods are all discussed in synchronization condition and unable to process the signal with a stochastic carrier residual. In non-cooperative reception occasion, carrier offset is usually inevitable while the estimation appears almost impossible in extremely low SNR or small data volume condition, especially for high order modulated signals such as QPSK [16][17].

This work proposes a PN waveform extraction method based on matrix subspace theory. By decomposing real part and the whole of self-covariance matrix respectively, we try to derive the theoretical form of the eigenvectors and discover the relationship with PN codes. The derivation will start from the complex baseband signal without any residual carrier. And then a more complex form of signals with an unknown carrier offset will be considered. Finally, the whole process from waveform to bits is carried out to accomplish the blind despreading and demodulation for QPSK-DSSS signals. Our contributions mainly cover as below.

1) Given no carrier residual, by decomposing the real part of self-covariance matrix, we derive the mathematical expression of the eigenvectors and conclude that the two eigenvectors are just corresponding to the summation and subtraction of two PN sequences.

2) To analyze the effect of carrier to the subspace, we try to derive the form of the eigenvectors of complex self-covariance matrix of baseband signal. We conclude that the coefficients of eigenvectors depend on parameters including the length, orthogonal degree of PN sequences, and also the distribution of transmitted data. At the same time, we find the real and imaginary part of the eigenvectors are orthogonal, corresponding to the summation and subtraction of two PN sequences respectively with unbalanced amplitude.

3) Given a stochastic carrier residual, we have a discussion on carrier elimination and PN codes estimation. Due to the orthogonality of the real and imaginary part in baseband condition, the eigenvectors can be regarded as a rotated and imbalanced QPSK constellation. We propose a carrier frequency and phase offset estimation method and realize a blind despreading and demodulation structure.

Initially, and unless stated otherwise, we assume in this paper that the PN code cycle, chip rate and symbol timing have been perfectly estimated [18][19][20]. And the synchronization point has been located. The rest of the paper is organized as follows. The overall systematic model of QPSK-DSSS are presented in Section II. In section III, we develop the methodology of blind despreading and demodulation for complex baseband signal with no or stochastic frequency offset. Section IV highlights numerical results and analysis. Concluding remarks and future work directions are expressed in section V.

II. SYSTEM MODEL

![FIGURE 1. The transmitter structure of QPSK-DSSS.](image)

DSSS signal is generated by using \( m \) sequences to modulate the information bits. For QPSK-DSSS, the homophase and orthogonal branches are modulated by two different \( m \) sequences which have same length and period. The
receivers use coherent demodulation technique to recover the symbols of 2 branches respectively [21]. Fig.1 shows the QPSK-DSSS modulation structure.

The binary information bit stream $d(t)$ is divided to homophase and orthogonal branches respectively by deserializer. Then the data is sent to multiplier with the $m$ sequences to complete the spread of the spectrum. Finally, the orthogonal carrier is generated to modulate the waveform to emit after passing the bandpass filter (BPF) and superposition.

The received signal waveforms $r(t)$ may be expressed as

$$r(t) = \sum_{i=0}^{\infty} [c(i)a(t - iT_c - \tau) + jq(i)b(t - iT_c - \tau)]e^{j2\pi f_i t} + v(t)$$

where $c(i)$ and $q(i)$ represent the information bits of homophase and orthogonal branches respectively. $T_c$ is the chip duration while $T_0$ denotes the time width of information symbol. We have $T_0 = LT_c$, where $L$ denotes the length of the $m$ sequence. $\tau$ is the transmission delay and can be regarded as out-of-sync time which denotes the synchronization point of the $m$ sequences, and $v(t)$ is additive complex white Gaussian noise with zero mean and standard deviation $\sigma_r$. $f_c$ denotes the carrier offset which comes from the frequency deviation between the oscillators of transmitter and receiver. $a(t), b(t)$ denote the combination waveform of PN code and channel filter of two branches, including shaping and matching filter.

$$a(t) = \sum_{i=0}^{\infty} a_i g(t - iT_c)$$

$$b(t) = \sum_{i=0}^{\infty} b_i g(t - iT_c)$$

where $a_i, b_i$ represent the $i$-th bit of $m$ sequences $a$ and $b$, $g(t)$ usually adopts the raised cosine filter.

There are several methods to estimate the period of PN code and the chip rate, such as self-correlation algorithm [22], secondary spectrum method [23], and so on. Here, assume the information symbol period $T_0$, chip duration $T_c$ and transmission delay $\tau$ have been obtained or estimated accurately and the received signal has been chip period sampled. The discrete signal waveform may be expressed as

$$r(n) = \sum_{i=0}^{\infty} [c(i)a(n - iT_c) + jq(i)b(n - iT_c)]e^{j2\pi f_i n} + v(n)$$

where $w_i$ is normalized digital angular frequency and given by $w_i = 2\pi f_i / f_b$ .

Our objective in this work is to estimate the $m$ sequences $a$, $b$ and moreover to obtain the transmitted bits $c$ and $q$.

### III. METHOD

#### A. Decomposition method for real part of the self-covariance matrix (EVD-R)

We start the derivation from the baseband signal, meaning that $w_i = 0$ in (3). Matrix decomposition method requires to construct the period self-covariance matrix $R$ defined as

$$R = \frac{1}{M} \sum_{m=0}^{M-1} x_m x_m^H$$

where $M$ denotes the number of the information symbols, and $x_m$ is one-period long signal vector which may be expressed as

$$x_m = c_m a + jq_m b$$

where $a, b$ denotes the spreading sequences of homophase and orthogonal branches respectively. Therefore

$$x_m x_m^H = c_m^2 a a^H + q_m^2 b b^H + j c_m q_m (b a^H - a b^H)$$

$c_i$ and $q_i$ are the transmitted bits and take value of $\pm 1$, then we have $c_i^2 = q_i^2$ . We define

$$A = a a^H + b b^H$$

$$B = b a^H - a b^H$$

$A$ is a real symmetric matrix that contains all information about both PN code $a$ and $b$ . Thus, we can try to obtain them by analyzing the feature subspace of $A$ . Eigenvalue decomposition method is a classical method to obtain the feature subspace of the matrix. Consider the expression of $A$ , the eigenvector which is spanned by some base vectors may have such form as

$$\theta = a + \alpha b$$

By the definition of eigenvector

$$A \theta = \lambda \theta$$

and according to the property of $m$ sequence, we note

$$p_1 = a^\alpha a + b^\beta b$$

$$p_2 = a^\beta b + b^\alpha a$$

By combining (8) to (10), we obtain the relationship of $p_1, p_2$ and $\alpha$

$$p_1 \alpha + p_2 = \alpha$$

We observe that when $p_2 = 0$ , $\alpha$ can take any value. In this case, the PN code $a$ and $b$ is orthogonal mutually and the any linear combination of them is an eigenvector of $A$ . It can be viewed as an ideal case whereas in practice the sequences cannot be orthogonal totally And when $p_2 \neq 0$ , $\alpha$ can take value of $\pm 1$. That is to say, the eigenvectors of $A$ may be expressed as $\theta_1 = c_1(a + b)$ , $\theta_2 = c_2(a - b)$ . The eigenvalues corresponding to eigenvectors $\theta_1$ and $\theta_2$ are $p_1 + p_2$ and $p_1 - p_2$ . And now we can reconstruct the PN codes $a$ and $b$ by combining $\theta_1$ and $\theta_2$ . However, the coefficients $c_1$ and $c_2$ existing to normalize the modulus of vector result in an amplitude imbalance in $\theta_1$ and $\theta_2$ . Consequently, we cannot combine the vectors directly except that the estimation for $c_1$ and $c_2$ is accomplished.

The orthogonal unitary matrix obtained from eigenvalue decomposition for matrix ensures the norm of eigenvectors to 1. Hence, we have
which can be decomposed as the form $R = V^H D V$ where $D$ is a diagonal real matrix and $V$ is an unitary matrix that satisfies $V^H V = V V^H = I$.

The columns of $V$ is the eigenvectors of $R$, which are all spanned by base vectors $a, b$ and maybe expressed as $v = c(\theta'_1 + j\alpha\theta'_2)$ (18) where

$$
\begin{align*}
\theta'_1 &= a + \beta b \\
\theta'_2 &= a + \beta b
\end{align*}
$$

By the definition of eigenvectors

$$
\begin{align*}
(m(A + jB) + n(A - jB))(\theta'_1 + j\alpha\theta'_2) &= \lambda(\theta'_1 + j\alpha\theta'_2)
\end{align*}
$$

Equation (20) can be simplified as

$$
\begin{align*}
(m + n)A\theta'_1 - \alpha(m - n)B\theta'_2 &= \lambda\theta'_1 \\
(m + n)A\theta'_2 + (m - n)B\theta'_1 &= \lambda\alpha\theta'_2
\end{align*}
$$

According to (7) - (10), we get

$$
\begin{align*}
AA &= p_1 a + p_2 b \\
AB &= p_1 b + p_2 a \\
BA &= p_1 b + p_2 a \\
BB &= p_2 b - p_1 a
\end{align*}
$$

Substitute (22) into (21) and define $\sigma = \frac{n + m}{n - m}$, we obtain equations as below

$$
\begin{align*}
\frac{(p_2 + \beta_1 p_1) + \frac{\alpha}{\sigma}(p_1 + \beta_2 p_2)}{(p_1 + \beta_1 p_2) - \frac{\alpha}{\sigma}(p_2 + \beta_2 p_1)} &= \beta_1 \\
\frac{\alpha\sigma(p_2 + \beta_1 p_1) - (p_1 + \beta_2 p_2)}{\alpha\sigma(p_1 + \beta_2 p_2) + (p_2 + \beta_1 p_1)} &= \beta_2
\end{align*}
$$

Equations (23) and (24) are satisfied with any reasonable value of $p_1, p_2$ and $\sigma$. In the special case that $p_2 = 0$, $\beta_1\beta_2 = -1$ was obtained. And then we assume that $\alpha$ approaches to infinity, by analyzing the form of $\alpha/\sigma$ and $\alpha\sigma$, we conclude that $|\alpha/\sigma| \to 0$. Alternatively, $|\alpha\sigma|$ approaches to infinity. Suppose $|\alpha/\sigma| \to 0$, we have

$$
\begin{align*}
\frac{p_2 + \beta_1 p_1}{p_1 + \beta_2 p_2} &= \beta_1 \\
\frac{\alpha\sigma(p_2 + \beta_1 p_1) - (p_1 + \beta_2 p_2)}{\alpha\sigma(p_1 + \beta_2 p_2) + (p_2 + \beta_1 p_1)} &= \beta_2
\end{align*}
$$

And $\beta_2^2 = 1$ is obtained and similarly, if we assume $|\alpha\sigma| \to \infty$, (24) can be simplified as

$$
\begin{align*}
\frac{p_2 + \beta_1 p_1}{p_1 + \beta_2 p_2} &= \beta_1 \\
\frac{p_2 + \beta_1 p_1}{p_1 + \beta_2 p_2} &= \beta_2
\end{align*}
$$

from where $\beta_2^2 = 1$ can be concluded. By now, the value of $\beta_1$ and $\beta_2$ can be given by

$$
\begin{align*}
\{ \beta_1 = 1 \} \text{ or } \{ \beta_1 = -1 \} \\
\{ \beta_2 = 1 \} \text{ or } \{ \beta_2 = -1 \}
\end{align*}
$$

Above two cases can be transformed by the operation of conjugation for $\theta'_1$ or $\theta'_2$. We select $\beta_1 = 1, \beta_2 = -1$ to continue our derivation, and as a result, $\theta'_1 = a + \beta b$ and $\theta'_2 = a - b$ are obtained.

B. Decomposition method for the entire self-covariance matrix (EVD-C)

To analyze the effect of carrier to the subspace, we try to derive the form of the combination coefficients of eigenvectors when decomposing the complex self-covariance matrix. Firstly, let us consider the complex baseband signal.

**1) THE SUBSPACE OF SELF-COVARIANCE MATRIX**

In (6), we observe that $E(c_i q_i) = 0$ statistically. However, the imaginary part of the matrix $R$ is usually not equal to zero due to the stochastic noise and data. To keep the model lossless in original data, we write $R$ as

$$
R = \sum_{k=0}^{N} x_k x_k^H = m(A + jB) + n(A - jB)
$$

where $m$ denotes the number of symbols that satisfies $c_i q_k = 1$, and $n$ denotes the number of symbols that satisfies $c_i q_k = -1$. We observe that $R$ is a hermit matrix Consequently, $c_i$ can be obtained as

$$
\begin{align*}
c_i &= \pm \frac{1}{\|a + b\|} = \pm \frac{1}{\sqrt{2(p_1 + p_2)}} \\
c_i &= \pm \frac{1}{\|a - b\|} = \frac{1}{\sqrt{2(p_1 - p_2)}}
\end{align*}
$$

(12)

$$
\begin{align*}
c_i &= \pm \frac{1}{\|a - b\|} = \pm \frac{1}{\sqrt{2(p_1 - p_2)}}
\end{align*}
$$

(13)

When $p_2 > 0$, the maximum eigenvalue is $\lambda_1 = p_1 + p_2$, and secondary maximum eigenvalue is $\lambda_2 = p_1 - p_2$, and (13) can be expressed as

$$
\begin{align*}
c_1 &= \pm \sqrt{\frac{p_1 - p_2}{p_1 + p_2}} \\
c_2 &= \pm \sqrt{\frac{p_1 + p_2}{p_1 - p_2}}
\end{align*}
$$

(14)

When $p_2 < 0$, the maximum eigenvalue is $\lambda_1 = p_1 - p_2$, and secondary maximum eigenvalue is $\lambda_2 = p_1 + p_2$, corresponding to the eigenvectors $\theta_1 = c_2(a - b)$ and $\theta_2 = c_1(a + b)$ respectively. Similarly,

$$
\begin{align*}
c_2 &= \pm \sqrt{\frac{p_1 - p_2}{p_1 + p_2}} \\
c_1 &= \pm \sqrt{\frac{p_1 + p_2}{p_1 - p_2}}
\end{align*}
$$

(15)

we conclude that the eigenvalues can be used to equalize the coefficients of eigenvectors exactly. The PN codes $a$ and $b$ can be extracted from the combination of eigenvectors as

$$
[a b] = [\theta_1 \theta_2] \begin{bmatrix} 1 & 1 \\
\sqrt{\frac{p_1 - p_2}{p_1 + p_2}} & -\sqrt{\frac{p_1 + p_2}{p_1 - p_2}} \end{bmatrix}
$$

(16)

where $[a b]$ denotes the possible position exchange of the two vectors.
Then let us consider the value of \(\alpha\). From (22), we note that
\[
\begin{align*}
A\theta'_1 &= (p_1 + p_2)\theta'_1, \\
A\theta'_2 &= (p_1 - p_2)\theta'_2, \\
B\theta'_1 &= -(p_1 + p_2)\theta'_2, \\
B\theta'_2 &= -(p_1 - p_2)\theta'_1.
\end{align*}
\] (28)

And substituting (28) with (20), we obtain
\[
(n-m)(p_1-p_2)\alpha^2 + 2p_2(n+m)\alpha - (n-m)(p_1 + p_2) = 0
\] (29)

When \(n = m\), the matrix \(R\) degrades as a real matrix, and \(\alpha = 0\) can be concluded from (29), corresponding to the conclusion of section A. And when \(n \neq m\), the roots of the quadratic equation may be expressed as
\[
\alpha_{t,2} = -\sigma p_2 \pm \sqrt{p_1^2 - p_2^2 + \sigma^2 p_2^2}
\] (30)

And the corresponding eigenvalues are
\[
\lambda_{t,2} = (n+m)(p_1 + p_2) \pm (n-m)(p_1 - p_2)
\] (31)

Observe from (30) that when \(p_2 = 0\) which means \(a\) is totally orthogonal with \(b\), \(\alpha_{t,2}\) will equal to \(\pm 1\) indicating that the real and imaginary part of eigenvectors of \(R\) will have a balanced coefficient and power. The eigenvalues and eigenvectors in this case can be written as
\[
v = \theta'_1 \pm j\theta'_2.
\] (32)

When \(p_2 \neq 0\), which means \(a\) is not totally orthogonal with \(b\), we define \(\eta = p_2 / p_1\) where \(\eta \in (-1,1)\) can be used to evaluate the orthogonality between \(a\) and \(b\). (30) may be expressed as
\[
\alpha_{t,2} = -\sigma\eta \pm \sqrt{1-\eta^2 + \sigma^2 \eta^2}
\] (33)

and \(\alpha_1\), \(\alpha_2\) satisfy the orthogonality of the eigenvectors
\[
(\theta'_1 + j\alpha_2\theta'_2)(\theta'_1 + j\alpha_2\theta'_2) = 0
\] (34)

\(\alpha_{t,2}\) varies continuously with the parameters \(\sigma\) and \(\eta\). The relationship of them is shown in Fig.2. As is shown in Fig.2(a)(b), the coefficients \(\alpha_{t,2}\) shows different variation trend. We observe that the curved surface of \(\alpha_{t,2}\) may be divided into two parts according to the sign of \(\sigma\). When \(\sigma > 0\), the half surface of \(\alpha_2\) is nearly flat, and the half surface of \(\alpha_1\) dramatically drop down with the increasing of \(\eta\). On the contrary, When \(\sigma < 0\), the other half surface of \(\alpha_2\) is nearly flat, and the other half surface of \(\alpha_1\) dramatically rise up with the increasing of \(\eta\). Fig.2 (c)(d) are slices of Fig.2(a)(b) displaying the change of \(\alpha_1\), \(\alpha_2\) as a function of \(\eta\) while \(\sigma = 500\) and \(\sigma = -500\). When \(\sigma\) takes a constant value and \(\eta = 0\), \(\alpha_{t,2} = \pm 1\) is obtained from the insets of Fig.2 (c)(d). With the increasing of \(\eta\), \(\alpha_1\) becomes close to zero while \(\alpha_2\) close to infinity. On the other hand, given constant \(\eta\), with the increasing of value \(|\sigma|\), we observe one of the coefficients becomes close to zero while the other close to infinity as shown in Fig.2 (e). The sequence can be extracted based on the phenomenon of unbalanced coefficients.

**FIGURE 2.** The value of \(\alpha_1\), \(\alpha_2\).
2) THE ESTIMATION FOR M-SEQUENCES

Generally, the orthogonality can be very significant between m sequences, which means \( \eta \rightarrow 0 \). And suppose stochastic information symbols, \( [\delta] \) takes a very big value. Under the effect of both parameters, \( \alpha_1 \) and \( \alpha_2 \) can have very different and unpredictable values. But which is doubtless is that one of the two coefficients \( |\alpha_1| \) and \( |\alpha_2| \) will be smaller than 1 while the other become larger than 1 at the same time resulting in different SNRs of real and imaginary part of the eigenvectors. According to this important conclusion, to obtain a good signal to noise ratio(SNR), we can choose the prominent part (real or imaginary part) with a larger coefficient to the eigenvectors \( v_1 \) and \( v_2 \) as two linear combination of PN codes, i.e., the real part of eigenvector \( v_1 \) is selected as \( \vec{v}_{1\_base} \) if \( \vec{v}_1^HV_1^T > \vec{v}_2^HV_1^T \), and vice versa. Hence, the \( \vec{v}_{1\_base} \) and \( \vec{v}_{2\_base} \) are obtained accordingly.

As described in section A, the coefficients of eigenvectors obtained from decomposition for matrix is usually unbalanced resulting in difficulty to compute \( a \) and \( b \) from the direct linear combination of \( \vec{v}_{1\_base} \) and \( \vec{v}_{2\_base} \). Let us consider the coefficients \( c_3 \) and \( c_4 \) which satisfy

\[
\| \vec{v}_1 \| = \| c_3 (\theta_1 + j\alpha_2 \theta_2) \| = 1 \quad \text{and} \quad \| \vec{v}_2 \| = \| c_4 (\theta_1 + j\alpha_2 \theta_2) \| = 1
\]

(35)

Therefore

\[
c_3 = \frac{2(\alpha_1^2 + \alpha_2^2)(p_1 - p_2)}{2(\alpha_1^2 + \alpha_2^2)(p_1 - p_2) + 2\alpha_2^2(p_1 - p_2)} \quad \text{and} \quad c_4 = \frac{2(\alpha_1^2 + \alpha_2^2)(p_1 - p_2)}{2(\alpha_1^2 + \alpha_2^2)(p_1 - p_2) + 2\alpha_2^2(p_1 - p_2)}
\]

(36)

We observe from (29) that the product of \( \alpha_{1,2} \) is \( p_1 + p_2 \) \( p_1 - p_2 \). Substitution of this result into (36) yields

\[
c_3 = \frac{2\alpha_2(\alpha_1^2 + \alpha_2^2)(p_1 + p_2) + 2\alpha_2^2(\alpha_1^2 + \alpha_2^2)(p_1 - p_2)}{2\alpha_1(\alpha_1^2 + \alpha_2^2)(p_1 + p_2) + 2\alpha_2^2(\alpha_1^2 + \alpha_2^2)(p_1 - p_2)}
\]

Thus, we have

\[
c_3 = \frac{p_1 - p_2}{\alpha_1 \alpha_2}
\]

(37)

As derived in (13)(14)(15)(38), \( \rho \) is just equal to \( \pm \sqrt{\lambda_1/\lambda_2} \) in this case. However, \( \rho \) may have different expressions in different cases. We consider the value of \( \rho \) in different cases and the result is shown in Table I.

| \( \sigma, \nu \) | \( |\alpha_1|/|\alpha_2| \) | \( v_1/v_2 \) | \( \rho \) | Value of \( \rho \) |
|----------------|----------------|----------------|---------|----------------|
| \( \sigma > 0 \), \( \nu > 0 \) | \( |\alpha_1| < 1 \) | \( \vec{v}_1 = c_3 (\theta_1 + j\alpha_2 \theta_2) \) | \( c_3 \alpha_2 \) | \( \pm \sqrt{\lambda_2/\lambda_1} \) |
| \( \sigma > 0 \), \( \nu < 0 \) | \( |\alpha_1| > 1 \) | \( \vec{v}_2 = c_4 (\theta_1 + j\alpha_2 \theta_2) \) | \( c_4 \alpha_2 \) | \( \pm \sqrt{\lambda_2/\lambda_1} \) |
| \( \sigma < 0 \), \( \nu > 0 \) | \( |\alpha_1| < 1 \) | \( \vec{v}_1 = c_3 (\theta_1 + j\alpha_2 \theta_2) \) | \( c_3 \alpha_2 \) | \( \pm \sqrt{\lambda_2/\lambda_1} \) |
| \( \sigma < 0 \), \( \nu < 0 \) | \( |\alpha_1| > 1 \) | \( \vec{v}_2 = c_4 (\theta_1 + j\alpha_2 \theta_2) \) | \( c_4 \alpha_2 \) | \( \pm \sqrt{\lambda_2/\lambda_1} \) |

We conclude that \( \rho \) is constant and equal to \( \pm \sqrt{\lambda_2/\lambda_1} \) in all cases. Consequently, when neglecting the polarity or order of the vectors \( a \) and \( b \), the unbalanced coefficients of extracted part \( \vec{v}_{1\_base} \) and \( \vec{v}_{2\_base} \) can be equalized and \( a, b \) may be reconstructed by

\[
[a \ b] = [\vec{v}_{1\_base} \vec{v}_{2\_base}] \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

(39)

FIGURE 3. The comparison of PN code estimates with true sequences.

Note that due to the phase ambiguity of eigenvectors, the estimate of PN code may be an inverse of original sequence as shown in Fig.3 and the order can be reversed at the same time. Unfortunately, we are unable to ensure the phase and order theoretically. The effect to despersing will be discussed in part 3 of this section.

We should also mention that \( \lambda_1 \) and \( \lambda_2 \) are eigenvalues in section A. Consequently, in order to obtain a more precise ratio of coefficients, eigenvalue decomposition is supposed to be conducted for the real part of \( R \) to compute \( \rho \).

3) CORRELATED DESPREADING AND DEMODULATION

To despread the received baseband QPSK-DSSS signal, we construct the template waveform \( a - b \) for correlation with original signal. Observe the correlation value

\[
C_g = (c_g a + jq_g b)^T (a - b)
\]

\[
= c_g a^T a + jq_g b^T b - c_g a^T b - jq_g b^T a
\]

(40)

\[
= (p_1 - p_2)(c_g + jq_g)
\]
The value $C_k$ is a complex number corresponding to a symbol in QPSK constellation. Although there may be phase ambiguity in $a$ and $b$ which may cause a rotation or symmetric transformation of the constellation as demonstrated in Table II, it is inevitable under non-cooperative reception occasion and can be eliminated by differentially decoding process or other post-processing techniques.

**TABLE II**

<table>
<thead>
<tr>
<th>Template waveform</th>
<th>Correlation result</th>
<th>Constellation form</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a - b$</td>
<td>$\langle p_1 - p_2 \rangle (c_i + jq_i)$</td>
<td>Standard</td>
</tr>
<tr>
<td>$a + b$</td>
<td>$\langle p_1 - p_2 \rangle (c_i - jq_i)$</td>
<td>Symmetry transformation</td>
</tr>
<tr>
<td>$-a + b$</td>
<td>$\langle p_1 - p_2 \rangle (-c_i - jq_i)$</td>
<td>$\pi$ rotation</td>
</tr>
<tr>
<td>$-a - b$</td>
<td>$\langle p_1 - p_2 \rangle (-c_i + jq_i)$</td>
<td>Symmetry transformation</td>
</tr>
</tbody>
</table>

As analyzed above, it is not necessary to ensure the order and polarity of the obtained sequences and a stable constellation can be recovered directly. Thus, template $a - b$ can be a choice for correlation demodulation. Then, we will evaluate the performance of this despread way.

Suppose perfect carrier synchronization, the correlation result with noise is given by

$$C_k = [c_i, a + w_y + j(q_i b + w_i)]^H (a - b)$$  \hspace{1cm} (41)

where $w_y$, $w_i$ denote the real Gaussian white noise of homophase and orthogonal branches respectively, with variance of $\sigma^2$. The SNR of received signal is defined as

$$SNR_r = \frac{E[c_i^2 (a^+ b)]}{E[w_y^2] E[w_i^2]} = \frac{p_1}{L \sigma^2}$$  \hspace{1cm} (42)

Let us consider the SNR of $C_k$ (41) can be simplified as

$$C_k = \langle p_1 - p_2 \rangle c_i + w_y^T (a - b) + j \times [(p_1 - p_2)q_i + w_i^T (a - b)]$$

The variance of noise component is

$$E[\langle a - b \rangle ^T w_y^T (a - b)] = E[(a - b)^T \sigma^2 I (a - b)]$$

$$= 2(p_1 - p_2) \sigma^2$$

Consequently, the SNR of $C_k$ may be expressed as

$$SNR_{c_k} = \frac{E[c_i^2(p_1 - p_2)^2]} {2(p_1 - p_2) \sigma^2} = \frac{(p_1 - p_2)} {2 \sigma^2}$$  \hspace{1cm} (45)

The gain from despreadig is

$$G = 10 \times \log 10 \frac{SNR_{c_k}} {SNR_r} = 10 \times \log 10 \frac{(p_1 - p_2)} {p_1} \frac{L} {2}$$

$$\approx 10 \times \log 10 \left( \frac{L} {2} \right) - 3$$ (dB)

We observe that it brings a loss of about 3dB in spreading gain by employing the template $a - b$. We should find a more robust way to work out it with a loss as little as possible.

To avoid the cross-multiplication, we adopt single $m$-sequence to correlate with the signal. That is

$$C_u = [c_i, a + w_y - j(q_i b + w_i)]^T a$$

$$C_u = [c_i, a + w_y - j(q_i b + w_i)]^T b$$

And the real part of $C_u$ and the imaginary part of $C_u$ are extracted to reconstitute the symbol given by

$$C_u = (c_i a + w_y - j(q_i b + w_i)) b$$

In a similar way, the SNR can be obtained as

$$SNR_{c_u} = \frac{(a^T a)^2 E[c_i^2]} {E[a^T w_y] E[w_y^T a] E[a^T b] E[b^T w_y] E[w_y^T b]} \frac{p_i} {\sigma^2}$$  \hspace{1cm} (49)

Clearly, compared with (42), the spreading gain was fully achieved. Since the order and polarity of the PN code estimation in section B are not ensured, just as selecting $v_{1, \text{base}}$ and $v_{2, \text{base}}$ in $v_1$ and $v_2$, we shall choose the prominent part of $C_u$ and $C_v$ to reconstruct the constellation. The recovered constellations adopting two different methods are shown in Fig.4.

![Fig.4](image)

**FIGURE 4**. The comparison of two different correlation results.

Obviously, the second isolated correlation method has a better performance in separability corresponding to a lower BER.

However, under non-cooperative occasion, it is difficult to achieve the isolated correlation directly. Due to the residual carrier frequency and phase, some pre-processing is required to avoid the occurrence of cross-multiply. And we will discuss it in next section.

### C. Decomposition method for signal with a stochastic carrier offset

Under most of non-cooperative reception occasion, the carrier offset is inevitable. The signal model with carrier may be expressed as

$$\mathbf{x}_k = \mathbf{A}_k (c_i a + j q_i b)$$  \hspace{1cm} (50)

where $\mathbf{A}_k$ is a carrier matrix with the form as

$$\mathbf{A}_k = \begin{bmatrix} e^{j(\phi_0 + kn + \phi_k)} & 0 \\ 0 & \ddots & \ddots \\ \vdots & \ddots & \ddots & \ddots \\ 0 & \cdots & \cdots & e^{j(\phi_0 + (kn+N-1)+\phi_k)} \end{bmatrix}_{N \times N}$$

$\phi_0$ is the initial carrier phase. Therefore, the self-covariance matrix may be expressed as

$$\mathbf{R}_x = \mathbf{A}_k \mathbf{c}_k \mathbf{a}^T + \mathbf{c}_k \mathbf{b}^T + j \mathbf{c}_k q_i (\mathbf{b}^T a - \mathbf{a}^T b) \mathbf{A}_k^H$$

And $\mathbf{R}$ in (17) becomes

$$\mathbf{R}_e = \mathbf{A}_k [m(A + j \mathbf{B}) + n(A - j \mathbf{B})] \mathbf{A}_k^H = \mathbf{A}_k \mathbf{R} \mathbf{A}_k^H$$

(53)
\( R_u \) is a hermit matrix as well and can be decomposed as 
\[
R_u = V_u D_u V_u^H.
\]
Compared with baseband form \( R = VDV^H \), an obvious conclusion is
\[
\begin{align*}
D_w &= D, \\
V_w &= AV,
\end{align*}
\]
(54)

We observe that the carrier is absorbed into the eigenvectors as a result that \( \theta_1 \) and \( \theta_2 \) can’t be directly extracted. Consequently, the estimation of carrier frequency offset is unavoidable to recover the column vectors of \( V \). Let us consider the form of eigenvectors of \( R \) which can be expressed as 
\[
v = c_i (\theta_1 + j \alpha \theta_2),
\]
where \( c_i \) is a real-number coefficient. There are two meaningful properties of \( v \).

(i) Given the conclusion in section B that \( \theta_1' = a + b \) and \( \theta_2' = a - b \) the real part and imaginary part of \( v \) are orthogonal totally.

(ii) Define \( \theta_{k1} \) as the \( k \)-th bit of \( \theta_1' \), \( \theta_{k2} \) as the \( k \)-th bit of \( \theta_2' \). Due to the binary value of \( \pm 1 \) for PN codes \( a \) and \( b \), for every \( k \), if \( |\theta_{k1}| = 0 \), then \( |\theta_{k2}| = 2 \) occurs. Alternatively, if \( |\theta_{k1}| = 0 \), \( |\theta_{k2}| \) equals to 2. This special property indicates the modulus-constant and four-phase-quadrature characteristic of the eigenvector, making it QPSK constellation-like pattern of \( V_u \) with possible IQ imbalance.

The conclusions can be just used to estimate carrier frequency offset \( \omega_c \) and phase offset \( \theta \) [24] by
\[
\begin{align*}
\hat{\omega}_c &= \frac{1}{M} \arg \max_{\omega_c} \left\{ \sum_{i=0}^{N-1} v_u(i)e^{-j\omega_c i} \right\}, \\
\hat{\theta} &= \frac{1}{M} \arg \left\{ \sum_{i=0}^{N-1} v_u(i)e^{-j\omega_c i} \right\},
\end{align*}
\]
(55)

where \( M = 4 \), \( v_u(i) \) is the \( i \)-th element of \( v_u \) which represents the \( n \)-th (\( n = 1, 2 \)) column of \( V_u \).

Fig. 5 shows the operation procedure for \( v \), to obtain the form \( \theta_1 + j \alpha \theta_2 \). Firstly, the constellation of \( v \) after directly eigenvalue decomposition is shown in (a) which is seriously disturbed by the carrier. And then the estimation for the value of carrier frequency and phase is operated according to (55), the position of the peak value in the spectrum is just corresponding to \( 4 \omega_c \) and its phase is \( 4\theta \). If we look into the summation form of equation (54), it can be found as the Discrete Fourier transform (DFT) and can be realized by one-time Fast Fourier transform (FFT). Due to the fast realization algorithm, the computation afford is easily acceptable. Fig. 5(c) shows the constellation without carrier frequency offset and Fig. 5(d) without phase offset. With this, we can extract \( \theta_1 \) and \( \theta_2 \) without aliasing. At the same time, the digital down-conversion (DDC) can be done for received signal.

Due to the unknown carrier phase error, we are supposed to estimate the initial phase \( \phi_0 \) before degrading the signal. To accomplish this, we reconstitute the waveform template \( a - b \) and correlate with \( k \)-th segment. Then we have
\[
C_k = (a - b)^T(c_k a - j q_k b)e^{j\phi_0} = (c_k a^T a + j q_k b^T b)e^{j\phi_0} = p_k (c_k + j q_k)e^{j\phi_0}.
\]
(56)

\( \phi_0 \) can be estimated by reusing non-data aided (NDA) algorithm of (55) and the pure baseband signal is obtained. Then the isolated correlation can be conducted as (47) to acquire a constellation of higher quality.

We should also mention that the phase ambiguity may be unavoidable when estimating \( \phi_0 \), the influence is just as discussed in Table I and can be eliminated by some post-processing techniques.

D. Procedure of blind despreading and demodulation

The structure of proposed algorithm is shown in Fig. 6 and the procedure is arranged as follow.

Step 1. Estimate the primary parameters including chip rate \( R_c \), PN code period \( T_0 \) and out of step time \( \tau \).

Step 2. Symbol timing and synchronization for the signal can be completed. And then segment the signal into one-period long segments from \( t = \tau \), compute the average self-covariance matrix \( R_w \).

Step 3. Decompose the matrix \( R_w \) and obtain the two main eigenvectors \( v_{w1} \) and \( v_{w2} \) corresponding to the two maximum eigenvalues.

Step 4. Estimate and then eliminate the residual carrier \( \omega_c \) and phase offset \( \theta \) of the vector \( v_{w1} \) and \( v_{w2} \) using (55), the baseband waveform of eigenvectors \( v_1 \) and \( v_2 \) is obtained.

Step 5. Eliminate carrier offset for received signal, and decompose the real part of the segment self-covariance matrix to obtain the ratio \( \rho = \pm \sqrt{\lambda_2 / \lambda_1} \).
Step 6. Extract the prominent part (real or imaginary part) of $v_1$ and $v_2$ as $v_{1,\text{base}}$ and $v_{2,\text{base}}$, the $m$ sequences of two branches $a$ and $b$ can be computed as (39).

Step 7. Use the PN code waveform template $a-b$ to correlate with the segments $x_{0}, x_{1}, \ldots, x_{n}$. The rotated constellation $C$ is obtained as (55), then the initial phase $\phi_{0}$ can be estimated by reusing (54).

Step 8. Eliminate the initial phase offset of the baseband signal, and isolated correlation as (47) can be operated to obtain $C_{v}$ and $C_{u}$.

Step 9. Select the prominent part of correlation result $C_{v}$ and $C_{u}$ to reconstruct the symbol $C_{w} + jC_{i}$ and the bit stream can be acquired.

IV. SIMULATION

In order to verify the validity of the proposed algorithm, simulation experiments are carried out in Matlab R2015b. To compare the performance of proposed algorithms with theory bound and other algorithms, we define

$$\text{SNR}_{e} = E_{b}/N0 - 10 \times \log10(L)$$

where $\text{SNR}_{e}$ denotes SNR subtracting the spreading gain.

The BER of PN codes and information are computed and compared to demonstrate the superiority of proposed algorithm.

A. The performance of PN code estimation

QPSK-DSSS signal is selected and the root raised cosine shaping and matching filter are adopted. Other parameters are shown in Table III. We test and compare the performance of our baseband EVD-R, EVD-C, BSS and optimization algorithms based on constant modulus characteristic (CM Algorithm). We choose Mean BER of PN codes is chosen as the performance index. In addition, the signal with carrier residual is considered as well to exhibit the anti-carrier-offset capability of our algorithm (named as EVD-C Algorithm (Fc)). The value of normalized offset is set to 0.02, corresponding to $f_{r}/f_{b}$, where $f_{r}$ denotes the actual carrier offset and $f_{b}$ is the chip rate of the received DSSS signal.

The graph of the probability of a binary digital error as a function of $\text{SNR}_{e}$ is shown in Fig.7 for different 5 algorithms. The figure illustrates that, for baseband signal without any residual carrier, the performance of proposed EVD-R and EVD-C algorithms are superior than BSS and CM algorithms. Meanwhile, the performance of CM algorithm is seriously restricted by the orthogonality of double PN sequences resulting in estimation error even in high $\text{SNR}_{e}$ condition as demon-stated in [15]. Moreover, BSS and CM algorithms are completely unable to process signals with residual carrier. All of above make them
suboptimal choices. When existing carrier offset, as shown in Fig.7, although restricted by the accuracy of carrier estimation under strong noise environment, proposed EVD-C\( (F_c) \) algorithm has almost the same performance with baseband EVD-R algorithms in most of noise condition, exhibiting a good anti-carrier-offset capability.

The influence of symbol number is evaluated next. The \( SNR \) was set to 7dB while the number range is \( [100, 1000] \). We conduct 10000 times Monte Carlo simulation to plot the curve in Fig.8.

![FIGURE 8: BER of \( m \) sequences as a function symbol number](image1)

With the increasing of data volume, the proposed two algorithms exhibited pretty better performance in BER of PN code estimation than the other two algorithms when compared under same \( SNR \), indicating its superiority and feasibility in non-cooperative context.

To evaluate the sensitivity of proposed algorithm to different carrier offset values, we test the performance of EVD-C\( (F_c) \) algorithm with different carrier value. The normalized carrier offset range is set to \( [-0.1, 0.1] \), and the \( SNR \) is set to 7dB, 500 symbols was adopted to run the proposed estimation algorithm.

![FIGURE 9: BER of \( m \) sequences as a function carrier offset](image2)

Fig.9 illustrates that the proposed algorithm performs well without loss of BER under a wide range of unknown and stochastic carrier offset, making it a suitable and practical choice for engineering purpose.

### B. BER performance

To test the performance of proposed algorithms directly, we select the BER of transmitted symbols as the evaluation index. The same signal parameters as section 4.1 are adopted to test the BER of information symbols for QPSK-DSSS signal. we conduct the simulation on baseband signals and complex baseband signals with normalized carrier offset \( f_c = 0.02 \) respectively.

![FIGURE 10: BER performance of proposed algorithms](image3)

As shown in Fig.10(a), when the number of symbols is 500 and \( SNR \geq 3dB \), the proposed algorithm has almost the same BER performance which attains the theory bound. And the carrier offset affects the performance only in pretty low SNR condition due to the failure of estimating the value of carrier. Similar phenomenon is appeared in Fig.10(b). The poor performance under lower \( SNR \) or smaller data volume is caused by the limited precision of carrier or phase estimation which is still a common issue attracting lots of attention. By contrast, the proposed
algorithms have exhibited pretty good performance in most experiment conditions.

V. CONCLUSION

In this paper, based on the subspace theory, we propose a blind despreading and demodulation method for QPSK-DSSS signal. Firstly, the double PN codes estimation is considered. By analysing different signal model (with or without carrier residual), the theoretical eigenvector expression of self-covariance matrix is derived, which indicates that the eigenvector displays just an imbalanced QPSK constellation-like pattern. The property makes it impossible to eliminate the carrier residual. Furthermore, the eigenvalues ignored before are found to be closely related to the coefficients of eigenvectors and can be used to recover the PN codes. Simulations indicate the performance attains the theory bound demonstrating the effectiveness and superiority of the proposed method.

Although this paper only deals with QPSK-DSSS systems, it has reference value for multi-user synchronous CDMA systems. When the number of users is large, the subspace would be much more complicate which make it a significant challenge especially in non-cooperative reception context.

REFERENCES