HIGH-RATE SPACE-TIME BLOCK CODES FROM TWISTED LAURENT SERIES RINGS

HASSAN KHODAIEMEHR
Department of Mathematics and Computer Science
Amirkabir University of Technology (Tehran Polytechnic)
424 Hafez Ave., Tehran 15914, Iran

DARIUSH KIANI
Department of Mathematics and Computer Science
Amirkabir University of Technology (Tehran Polytechnic)
424 Hafez Ave., Tehran 15914, Iran
and
School of Mathematics
Institute for Research in Fundamental Sciences (IPM)
P.O. Box 19395-5746, Tehran, Iran

(Communicated by Iwan Duursma)

Abstract. We construct full-diversity, arbitrary rate STBCs for specific number of transmit antennas over an apriori specified signal set using twisted Laurent series rings. Constructing full-diversity space-time block codes from algebraic constructions like division algebras has been done by Shashidhar et al. Constructing STBCs from crossed product algebras arises this question in mind that besides these constructions, which one of the well-known division algebras are appropriate for constructing space-time block codes. This paper deals with twisted Laurent series rings and their subrings twisted function fields, to construct STBCs. First, we introduce twisted Laurent series rings over field extensions of $\mathbb{Q}$. Then, we generalize this construction to the case that coefficients come from a division algebra. Finally, we use an algorithm to construct twisted function fields, which are noncrossed product division algebras, and we propose a method for constructing STBC from them.

1. Introduction

It is shown in [8], [9] and [32], that the capacity of fading channels with multiple transmit and receive antennas approximately increases linearly with the increase in the minimum of the transmit and the receive antennas. Signal design for such situations, i.e., for fading channels with multiple transmit and receive antennas is called space-time coding (STC) ([31]). A class of STC called space-time block coding (STBC) has attracted wide attention because of the availability of low-complexity decoders for them. In [10], an \((n \times l)\), \((n \leq l)\), STBC, \(\mathcal{C}\), is defined to be a finite set of \((n \times l)\) matrices (codewords) over the complex field \(\mathbb{C}\). One of the main performance criteria for an STBC, \(\mathcal{C}\), is the minimum of the ranks of any two distinct codewords in \(\mathcal{C}\), known as rank or diversity of the STBC (see, e.g., [31] and [29]). If the rank...
of an STBC is equal to \( n \), then we call it a full-rank STBC. We have summarized the STBC design criteria in the following two conditions.

Let \( C \subset M_n(C) \) be an space-time block code. In order to perform \( C \) well, it should satisfy property (1) as many of the other properties as possible.

1. It is fully diverse: \( \det(X - X') \neq 0 \) for all matrices \( X \neq X', X, X' \in C \).
2. It has full rate, which means that the \( n^2 \) degrees of freedom are used to transmit \( n^2 \) information symbols. It is high-rate if the rate of the code is greater than 1.

In [13], it is shown that the Alamouti code is the only rate-1, \((2 \times 2)\) design which achieves capacity, among all the orthogonal designs. In [24], [25], [23], [26], [28] and [30], full-rank arbitrary-rate and information-lossless STBCs were constructed for an arbitrary number of transmit antennas, over any finite subsets of any subfields of \( C \), using commutative and noncommutative (cyclic) division algebras. In [29], designs have been obtained using crossed product algebras and a sufficient condition introduced for the STBCs obtained from them to be information-lossless. These STBCs are very close to the capacity of the channel with QAM symbols as the input.

In Section 2, we describe the system model, and define equivalent channel of an STBC and information-lossless STBC. In Section 3, we give a brief introduction to twisted Laurent series rings. The main principle and construction of the STBCs from such algebras are given in Section 4. In Section 5, we introduce some classes of division algebras which are noncrossed product and we use these division algebras to construct full-rank STBCs. Using of these constructions is illustrated with some examples. Finally, we present simulation results in Section 6, to show the performance of these codes.

2. System model

In this section, we give a brief description of the system model which we use, and define equivalent channel of an STBC and information-lossless STBC. The following definition enables one to describe STBCs for \( n \) transmit antennas, with a signal set, \( S \), and a matrix which avoids exhaustive listing of codewords of an STBC.

**Definition 2.1.** A rate-\( k/n \), \((n \times l)\) linear design over a field \( F \subseteq C \) is an \((n \times l)\) matrix with all its entries \( F \)-linear combinations of \( k \) variables and their complex conjugates, which are allowed to take values from the field \( F \). If we restrict the variables to take values from a finite subset \( S \) of \( F \), then we get an \((n \times l)\) STBC \( C \) over that finite subset \( S \), for \( n \) transmit antennas.

Let \( n \) and \( r \) be the numbers of transmit and receive antennas, respectively, \( f \in C^{r \times 1} \) be the transmitted vector for one time instant and \( x \in C^{r \times 1} \) be the received vector. Also, let \( H \in C^{r \times n} \) is the channel matrix whose entries are independent and identically distributed (i.i.d.) with zero-mean, unit-variance, complex Gaussian. Then, we have

\[
(1) \quad x = \sqrt{\frac{\rho}{n}} H f + w,
\]

where \( w \in C^{r \times 1} \) is the additive noise vector whose entries are i.i.d. with zero-mean, unit-variance, complex Gaussian. We assume that the vector \( f \) has entries with unit variance i.e., \( E(f^H f) = n \). The term \( \rho \) is the signal-to-noise ratio (SNR) at each receive antenna. The channel matrix \( H \) is assumed to be known at the receiver.
but not at the transmitter. Under the assumption that the distribution of $H$ is rotationally invariant, by [32] and [9], the resulting channel capacity is

$$C(\rho, n, r) = E_H \log_2 \left( \det \left( I_r + \frac{\rho}{n} HH^H \right) \right).$$

The preceding expression gives channel capacity when we transmit independent vectors at every time instant. However, if we use an $(n \times l)$ STBC, then we transmit $l$ vectors in $l$ time instants which need not be independent of each other. So, if the transmitted $(n \times l)$ matrix over $l$ time instants is $F$, then we have

$$X = \sqrt{\frac{\rho}{n}} HF + W,$$

where $X$ and $W$ are the received $(r \times l)$ and additive noise $(r \times l)$ matrices, respectively. Let the STBC used in the above equation be of rate $R$ symbols per channel use. Then, we have $lR$ independent variables describing the matrix $F$. Let us denote them by $f_1, \ldots, f_{lR}$ and let $f = [f_1, \ldots, f_{lR}]^T$. Suppose that we can rewrite (3) as

$$\hat{x} = \sqrt{\frac{\rho}{n}} \hat{H} f + \hat{w},$$

where $\hat{x}$ and $\hat{w}$ are the matrices $X$ and $W$, respectively, arranged in a single column, by serializing the columns. Notice that this can be done for any linear design. The size of the matrix $\hat{H}$ is $(rl \times rl)$. Then, the capacity of the new channel $\hat{H}$, known as equivalent channel, is given by (2), by replacing $n, r$ and $H$ with $lR, lr$ and $\hat{H}$, respectively (except $n$ in the term $\sqrt{\frac{\rho}{n}}$). So, by introducing coding, the maximum mutual information between the actual information vector $f$ and the received matrix $X$ (or $\hat{x}$) is

$$C_{STBC}(\rho, n, r) = \frac{1}{l} E_H \log_2 \left( \det \left( I_r + \frac{\rho}{n} \hat{H} \hat{H}^H \right) \right),$$

where $C_{STBC}(\rho, n, r)$ denotes the maximum mutual information when the STBC is introduced. Clearly, this can be at most equal to $C(\rho, n, r)$.

**Definition 2.2.** If the maximum mutual information when an STBC, $C$, is used for $n$ transmit and $r$ receive antennas, is equal to the capacity of the channel for $n$ transmit and $r$ receive antennas given by $C(\rho, n, r)$, then $C$ is called an information-lossless STBC [5]. We call the design used to describe $C$, a capacity achieving design.

3. Twisted Laurent series ring

In this section, we give a brief introduction to twisted Laurent rings. Let $L$ be a commutative field and $\sigma$ be an automorphism of $L$. Call $K = \text{Fix}_L(\sigma) = \{x \in L \mid \sigma(x) = x\}$, the fixed field of $\sigma$ in $L$.

**Definition 3.1.** Denote by $L((T, \sigma))$, the ring of formal Laurent series $\sum_{i=\infty}^R a_i T^i$ in the indeterminate $T$ with coefficients $a_i \in L$ and $R \in \mathbb{Z}$, with usual addition but skew multiplication such that $Ta = \sigma(a)T$, i.e., $T^a = \sigma^i(a)T^i$, where $a \in L$.

If $\sigma = id_L$ is the identity map of $L$, then $L((T))$ is the usual commutative field of formal Laurent series over $L$ in the indeterminate $T$, customarily denoted by $L((T))$. It is shown in [6] that $L((T, \sigma))$ is always a skew field (or a division ring).
Now let $L$ be again a commutative field, then we have the following lemma (see, e.g., [6]):

**Lemma 3.2.** Let $D = L((T, \sigma))$ be given. If $\sigma$ has infinite order, then $Z(D) = K$, hence $|D : Z(D)| = \infty$; if $\sigma$ has the finite order $n$ in $\text{Aut}(L)$, then $Z(D) = K((T^n))$, hence $|D : Z(D)| = n^2$ ($K = \text{Fix}_L(\sigma)$).

If $\sigma$ has the finite order $n$, then we want to calculate the dimension $|D : Z(D)|$ in the latter case. First we observe that $L$ is a Galois extension of $K$ and $|L : K| = n$ (see Galois Theory, in particular Artin’s Lemma [17]) for $L/K$ is obviously cyclic with generating automorphism $\sigma$. Now choose a basis $\{1, t, t^2, \ldots, t^{n-1}\}$ of $L$ as a $K$-space (in the case of separable extensions always this basis exists and we can see that $L = K(t)$ for a primitive element $t \in L$). Then our considerations show immediately that $\{t^iT^j | 0 \leq i, j < n\}$ is a basis of $D$ as a $K((T^n))$-space, hence $|D : Z(D)| = n^2$.

### 4. STBCs from twisted Laurent series rings

In the previous section, we gave the definition of twisted laurent rings, and we saw that $D = L((T, \sigma))$ is a division algebra over its center. Now we want to construct a class of STBCs from these division algebras by embedding them into the ring of matrices. We will see in Section 5, that a twisted laurent series ring like $D$, can be a crossed product or a noncrossed product algebra. Consequently, it may not have any Galois maximal subfield to consider the representation over that. In order to avoid ambiguity, and such a difficulty as occurred in the latter case, we consider the representation of $D$ over its center.

#### 4.1. STBCs for a perfect square numbers of transmit antennas

Consider $D = L((T, \sigma))$ and let $F = Z(D)$. Then we can view $D$ as a left $F$-space, i.e., the action of scalar multiplication is given by left multiplication. In this section, we use this property and construct arbitrary rate, full-rank STBCs.

Consider the map $L : D \rightarrow \text{End}_F(D)$, given by $L(\beta) = \lambda_\beta$, where $\lambda_\beta(u) = u\beta$ for all $u \in D$. Since the scalar multiplication is via left and the action of $\lambda_\beta$ gives right multiplication, these actions commute. That is, $k(\lambda_\beta(u)) = k(u\beta) = (ku)\beta = \lambda_\beta(ku)$. This implies that $\lambda_\beta$ is an $F$-linear transform of $D$ (here $F$ is the center of $D$ and the terms left or right in the action of scalar multiplication are equivalent). Clearly, $L$ is a ring homomorphism from $D$ to $\text{End}_F(D)$ i.e., $\lambda_{\beta+\beta'} = \lambda_\beta + \lambda_{\beta'}$ and $\lambda_{\beta\beta'} = \lambda_\beta\lambda_{\beta'}$. Since $D$ is a simple algebra, $L$ is injective. That is, $\beta - \beta' \neq 0$ implies that $\lambda_{\beta-\beta'}(u) = \lambda_\beta(u) - \lambda_{\beta'}(u) \neq 0$. Whereas $D$ is a division algebra, $\beta - \beta'$ is invertible, say its inverse is $\beta''$, which results that $\lambda_{\beta-\beta'}$ is also invertible. Thus, the image of $L$ is also a division algebra.

Now, since $D = L((T, \sigma))$ is an $F$-space, we can view the elements of $\text{End}_F(D)$ as matrices over $F$, with respect to a basis. We saw in the previous section that the set $B = \{t^iT^j | 0 \leq i, j < n\}$, forms a basis for the algebra $D = L((T, \sigma))$ over its center $F = Z(D) = K((T^n))$. With respect to this basis, we shall find the matrix representation of $\lambda_\beta$. Let $\beta = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{ij}t^iT^j$, where $f_{ij} \in F = K((T^n))$ for $0 \leq i, j \leq n - 1$. Then, in order to find the matrix representation of $\lambda_\beta$, it is sufficient to find the action of $\lambda_\beta$ on each of the basis elements. Thus,

$$
\lambda_\beta(t^iT^j) = (t^iT^j)\beta = (t^iT^j)(\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{ij}t^iT^j)
$$
By knowing the minimal polynomial of \( t \) over \( \mathbb{F} \), we can write all powers of \( t \) as an \( \mathbb{F} \)-linear combination of \( 1, t, t^2, \ldots, t^{n-1} \). When \( l + j \geq n - 1 \), we can put \( T^l + j = T^n T^{l + j - n} \), and we know that \( T^n \in \mathbb{F} \). So, we can write \( (6) \) as an \( \mathbb{F} \)-linear combination of the basis \( \mathcal{B} = \{ t^i T^j | 0 \leq i, j < n \} \). We put the coefficients of \( (6) \) (with respect to the basis \( \mathcal{B} \)) on the \( (ln + k)^{th} \) column of matrix \( \lambda_\beta \). By doing this for all \( 0 \leq k, l \leq n - 1 \), we will get full rank \( (n^2 \times n^2) \) matrix representation of \( \lambda_\beta \). If we do this for another \( \beta' \neq \beta \), \( (\beta' \in \mathbb{D}) \), then \( (\beta - \beta') \in \mathbb{D} \). So, its matrix representation will be a full rank matrix. Thus, we have the following theorem:

**Theorem 4.1.** If \( \sigma \) is an automorphism in Galois group of \( \mathbb{L}/\mathbb{K} \) and \( \text{ord}(\sigma) = n \), with \( \mathbb{D} = \mathbb{L}(T, \sigma) \) and \( T^n = x \), then the set of matrices of the form described in previous paragraph has the property that the difference of any two such matrices is invertible. In addition, we have \( \mathbb{D} \hookrightarrow M_{n^2}(\mathbb{K}(x)) \).

**Proof:** The result follows from the fact that the set of matrices of the form as in previous paragraph is isomorphic to the division algebra \( \mathbb{D} \). \( \square \)

In representation of the matrices in Theorem 4.1, \( f_{ij} \)'s are series in terms of indeterminate \( x = T^n \). We can consider them in a special case to be polynomials in terms of \( x \). From the preceding theorem it is clear that if \( \mathbb{K} \) is a subfield of \( \mathbb{C} \) and we restrict coefficients of \( f_{ij} \) to some finite subset \( \mathbb{S} \) of \( \mathbb{K} \), then we obtain a full-rank arbitrary-rate STBC for \( n^2 \) transmit antennas. In the following example, we obtain a full-rank STBC from a twisted Laurent series ring by the stated method.

**Example 4.1.** Let \( \mathbb{S} \) be an arbitrary signal set (for example we can consider QAM or PSK signal sets). We want to construct a full-rank STBC for 4 transmit antennas. We put \( \mathbb{L} = \mathbb{Q}(\mathbb{S})(\sqrt{2}) \) and \( \mathbb{D} = \mathbb{L}(T, \sigma) \). By the used notation, \( t = \sqrt{2} \). If we consider \( \sigma : \mathbb{L} \rightarrow \mathbb{L}, \sigma(\sqrt{2}) = -\sqrt{2} \) and \( \sigma = \text{id} \) for elements which are in \( \mathbb{Q}(\mathbb{S}) \), then \( n = \text{ord}(\sigma) = 2 \) and \( \mathbb{K} = Fix_{\mathbb{L}}(\sigma) = \mathbb{Q}(\mathbb{S}) \) and by Lemma 3.2, \( \mathbb{F} = Z(\mathbb{D}) = \mathbb{K}((T^2)) = \mathbb{Q}(\mathbb{S})(\langle x \rangle) \), where \( T^2 = x \). It is clear that \( \mathbb{L}/\mathbb{K} \) is a Galois extension, and the basis of \( \mathbb{D} \) over \( \mathbb{F} \) is \( \mathcal{B} = \{ 1, \sqrt{2}, T, \sqrt{2}T \} \). If \( \beta = f_0 + f_1 \sqrt{2} + f_2 T + f_3 \sqrt{2}T \), then we have

\[
\lambda_\beta(1) = f_0 + f_1 \sqrt{2} + f_2 T + f_3 \sqrt{2}T,
\]

\[
\lambda_\beta(\sqrt{2}) = 2f_1 + f_0 \sqrt{2} + 2f_3 T + f_2 \sqrt{2}T,
\]

\[
\lambda_\beta(T) = f_2 T^2 - f_3 T^2 \sqrt{2} + f_0 T - f_1 \sqrt{2}T,
\]

\[
\lambda_\beta(\sqrt{2}T) = -2f_3 T^2 + f_2 T^2 \sqrt{2} - 2f_1 T + f_0 \sqrt{2}T.
\]

With these notations, the obtained STBC has codewords of the form

\[
C_\beta = \begin{bmatrix}
f_0 & 2f_1 & x f_2 & -2x f_3 \\
f_1 & f_0 & -x f_3 & x f_2 \\
f_2 & 2f_3 & f_0 & -2f_1 \\
f_3 & f_2 & -f_1 & f_0
\end{bmatrix},
\]
where \( f_i = \sum_{k=R_i}^{\infty} f_{k,i} x^k \) for \( i = 0, 1, 2, 3 \), and \( f_{k,i} \in K = \mathbb{Q}(S) \) for all \( k \geq R_i \). If we want to have the rate of \( R \) bits per channel use, then it is enough to put \( f_i = \sum_{k=0}^{R-1} f_{k,i} x^k \), where \( f_{k,i} \)'s come from an arbitrary finite subset of the field \( \mathbb{Q}(S) \subseteq \mathbb{C} \).

It remains to replace indeterminate \( x \) with appropriate element in \( \mathbb{C} \) to have an STBC with rate \( R \) for 4 transmit antennas over signal set \( S \). We are going to present two candidates for indeterminate \( x \). First one is an algebraic element over \( K = \mathbb{Q}(S) \), and we construct it as following.

Let \( n^2 \) be the number of transmit antennas and let \( S \) be the signal set with cardinality \( |S| = m \). If we use \( M\text{-PSK} \) signal set, then \( m = M \), and if we use \( \mathbb{Q} \text{-QAM} \) signal set, then \( m = 4 \). In order to obtain a full-rank STBC, \( C \), with the rate \( R \) bits per channel use, it is enough to replace indeterminate \( x \) in matrices of codewords with an element \( \alpha \in \mathbb{C} \) such that \( \Delta(\beta, \beta')(x) = (\det(C_{\beta} - C_{\beta'})) |_{x=\alpha} \neq 0 \) for every \( C_{\beta}, C_{\beta'} \in \mathbb{C} \) (or equivalently \( \beta, \beta' \in D \)). Let \( P \) be a prime number. Then \([\mathbb{Q}(\omega_P) : \mathbb{Q}] = \varphi(P) = P - 1 \), where \( \varphi \) is the Euler function and \( \omega_P = e^{\frac{2\pi i}{P}} \) is the \( P \)th root of unity and \( j = \sqrt{-1} \). In general case, for every natural number \( k \) we have \([\mathbb{Q}(\omega_k) : \mathbb{Q}] = \varphi(k) \). We know that \( \Delta(\beta, \beta')(x) \) is a polynomial in terms of \( x \) with coefficients which are in \( K = \mathbb{Q}(S) \), since every matrix element of \( C_{\beta} - C_{\beta'} \) is a polynomial of degree at most \( R + 1 \), the degree of the polynomial \( \Delta(\beta, \beta')(x) \) will be upper bounded by \( n^2(R + 1) \). If we consider a prime number \( P > n^2(R + 1) \), then the degree of minimal polynomial of \( \omega_P \) over \( \mathbb{Q} \) is \( P - 1 \) which is greater than \( n^2(R + 1) \). So, it can not satisfy in any polynomial in \( \mathbb{Q}[x] \) with degree less than \( n^2(R + 1) \).

If we extend \( \mathbb{Q} \) to \( K = \mathbb{Q}(S) \), then the degree of minimal polynomial of \( \omega_P \) over \( K \) can be decreased and \( \omega_P \) may satisfy in \( \Delta(\beta, \beta')(x) \) which is unsightly here. If we choose a prime number \( P > n^2(R + 1) \times \varphi(m) \), where \( m = |S| \), then it can be easily checked that the degree of the minimal polynomial of \( \omega_P \) over \( \mathbb{Q}(S) \) is greater than \( n^2(R + 1) \). So, \( \alpha = \omega_P \) can not satisfy in \( \Delta(\beta, \beta')(x) \) i.e., \( \Delta(\beta, \beta')(\alpha) \neq 0 \). This method can be replaced by the method of [28], which guaranties that \((K/F, \sigma, \gamma)\) is a division algebra, by choosing \( \gamma \) to be a non-norm element of \( K/F \).

For example, if we use this method in Example 4.1, where \( S \) is the \( 8 - \text{PSK} \) signal set i.e., \( S = \{ \omega_8^k \mid k = 0, 1, \ldots, 7 \} \) and \( R = 4 \) is the rate of \( C \), then we need a prime number \( P > 4 \times 5 \times 4 = 80 \). So, \( P = 83 \) is appropriate and let \( \alpha = \omega_{83} \). Then, the STBC we obtain in (7) will have codewords of the form

\[
\begin{bmatrix}
    f_0(\alpha) & 2f_1(\alpha) & \alpha f_2(\alpha) & -2\alpha f_3(\alpha) \\
    f_1(\alpha) & f_0(\alpha) & -\alpha f_2(\alpha) & \alpha f_3(\alpha) \\
    f_2(\alpha) & 2f_3(\alpha) & f_0(\alpha) & -2f_1(\alpha) \\
    f_3(\alpha) & f_2(\alpha) & -f_1(\alpha) & f_0(\alpha)
\end{bmatrix},
\]

where \( f_i(\alpha) = f_{i0} + f_{i1}\alpha + f_{i2}\alpha^2 + f_{i3}\alpha^3 \), for \( i = 0, 1, 2, 3 \), and \( f_{ij} \in \mathbb{Q}(S) \) for \( i, j = 0, 1, 2, 3 \).

Now we present second candidate of indeterminate \( x \), which is a transcendental number [29]. The Lindemann-Weierstrass theorem suggests a method to find algebraically independent transcendental numbers. By using this theorem, we can put \( \alpha = e^{\sqrt{2}} \) (or any transcendental element over \( \mathbb{Q} \)) in (8).

Until here, we construct full-rate STBCs for arbitrary signal constellation and arbitrary rate from twisted Laurent series in the cases that the number of transmit antennas is a perfect square number, say \( n^2 \). It is a natural question that why we consider the representation of a division ring over its center rather than one over
its maximal commutative subfield as is commonly done in the STC literature and would result in higher rate codes consisting of \((n \times n)\) matrices. The answer to this question is that as we will see in the sequel, a Laurent series ring like \(D(x, \sigma)\) is not necessarily a crossed product algebra. So, the representation of a Laurent series ring over its maximal subfield is not specified. We must use a technique to increase the rate of the obtained STBCs, and mitigate the condition that makes us choose a perfect square number of transmit antennas. In the next section, we will construct STBCs in the cases that the number of transmit antennas is one of the numbers \(n, 2n, \ldots, (n-1)n, n^2\), for any natural number \(n\).

In previous examples, we used polynomials instead of series in representation of elements. In the succeeding example, we construct an STBC that uses infinite series in the representation of codewords.

**Example 4.2.** Let \(S = \{1, \omega_4, \omega_4^2, \omega_4^3\}\) be the 4-PSK signal set and another parameters of the code be like (4.1), but at this time we choose \(f_0, f_1, f_2, f_3\) as following. The code \(C\) is a finite set of matrices of the form (4.1) and its main entries come from 4 sets \(C_0, C_1, C_2, C_3\), i.e., \(f_0 \in C_0, f_1 \in C_1, f_2 \in C_2, f_3 \in C_3\). We define

\[
C_0 = \left\{ \sum_{j=0}^{n-1} f_{0,j} x^j + \omega_4^k \sum_{j=n}^{\infty} \frac{x^j}{j!} f_{0,j} \in Q(S) \right\} = \left\{ \sum_{j=0}^{n-1} f_{0,j} x^j + \omega_4 x^j | f_{0,j} \in Q(S) \right\},
\]

\[
C_1 = \left\{ \sum_{j=0}^{n-1} f_{1,j} x^j + \omega_4^k \sum_{j=n}^{\infty} \frac{(-1)^j x^j}{j!} f_{1,j} \in Q(S) \right\} = \left\{ \sum_{j=0}^{n-1} f_{1,j} x^j + \omega_4 x^j | f_{1,j} \in Q(S) \right\},
\]

\[
C_2 = \left\{ \sum_{j=0}^{n-1} f_{2,j} x^j + \omega_4^k \sum_{j=n}^{\infty} \frac{(-1)^j x^j}{2j} f_{2,j} \in Q(S) \right\} = \left\{ \sum_{j=0}^{n-1} f_{2,j} x^j + \omega_4^2 \cos(x) | f_{2,j} \in Q(S) \right\},
\]

\[
C_3 = \left\{ \sum_{j=0}^{n-1} f_{3,j} x^j + \omega_4^k \sum_{j=n}^{\infty} \frac{(-1)^j x^j}{2j+1} f_{3,j} \in Q(S) \right\} = \left\{ \sum_{j=0}^{n-1} f_{3,j} x^j + \omega_4^2 \sin(x) | f_{3,j} \in Q(S) \right\}.
\]

We now show that by the above assumptions and choosing \(x\) appropriately, the set of matrices of the form (8) gives us an STBC. Let \(X\) and \(X'\) be two arbitrary codewords in \(C\). Then, their difference is

\[
X - X' = \begin{bmatrix}
   s_0(x) + e^x \\
   s_1(x) + \omega_4 e^{-x} \\
   s_2(x) + \omega_4^2 \cos(x) \\
   s_3(x) + \omega_4^2 \sin(x)
\end{bmatrix}
\]

\[
= \begin{bmatrix}
   2(s_1(x) + \omega_4^2 \cos(x)) - 2s_0(x) \\
   2(s_2(x) + \omega_4^2 \sin(x)) - 2s_1(x) \\
   -2s_0(x) + \omega_4^2 e^{-x} \\
   -2s_1(x) + \omega_4^2 \cos(x)
\end{bmatrix}
\]

\[
= \begin{bmatrix}
   (s_0(x) - s_1(x)) + \omega_4^2 \cos(x) \\
   (s_0(x) - s_1(x)) - \omega_4^2 \cos(x) \\
   (s_0(x) - s_1(x)) + \omega_4^2 \sin(x) \\
   (s_0(x) - s_1(x)) - \omega_4^2 \sin(x)
\end{bmatrix}
\]

where \(s_i\) and \(s_i'\) for \(i = 0, 1, 2, 3\), are polynomials of degree less than \(n\) in \(Q(S)[x]\). So, it is enough to choose \(\alpha \in C\) by using one of the criteria which are stated in the previous example and replace \(x\) with \(\alpha\) in the elements of \(C\).

**Remark 1.** As we see in Example 4.2, the number of distinct coefficients of the main entries, i.e., the first column in each codeword, is a finite number. It makes sense, because a code is a finite set and at least one symbol must be repeated infinitely. It seems impracticable work and we use this example to show that instead of polynomials, analytic functions can appear in the representation of codewords.
However, this may help us in receivers to detect and uncouple the signals of each transmit antenna from the others. Also, note that if we use arbitrary analytic function in the codewords representation, we must take care about choosing an appropriate replacement for $x$ which satisfies in STBC design criteria and is in the convergence regions of all used series.

4.2. STBCs which are useable with non-perfect square number of transmit antennas. Now, we are going to construct STBCs from Laurent series rings in the cases that the number of transmit antennas is a non-perfect square number. Like previous section, let $L = K(t)$ be a Galois extension of field $K$ and $\sigma$ be an automorphism in Galois group of $L$ with order $n$ and $D = L((T, \sigma))$ be the twisted Laurent series ring in terms of indeterminate $T$. By Lemma 3.2, we have that if we put $x = T^n$, then $D$ is a $K((x))$-division algebra with the basis $B = \{t^iT^j : i, j = 0, 1, \ldots, n-1\}$. Now, let $V_k$, for $k = 1, \ldots, n$, be the $F$-subspace generated by the basis $B_k = \{t^iT^j : i = 0, 1, \ldots, n-1 & j = 0, 1, \ldots, k-1\}$.

This is clear that $|B_k| = kn$. If we consider $\beta = f_0 + f_1 t + f_2 t^2 + \cdots + f_{n-1} t^{n-1}$, where $f_i \in F = K((x))$ for $i = 0, \ldots, n-1$, then $\lambda_\beta$ is a linear transform that preserves $V_k$ invariant for $k = 1, \ldots, n$, i.e., $\lambda_\beta(V_k) \subseteq V_k$, because for $i = 0, 1, \ldots, n-1$ and $j = 0, 1, \ldots, k-1$, we have

$$\lambda_\beta(t^iT^j) = (t^iT^j)(f_0 + f_1 t + f_2 t^2 + \cdots + f_{n-1} t^{n-1})$$

$$= \sum_{k=0}^{n-1} f_k t^i \sigma^j(t^k)T^j = \sum_{k=0}^{n-1} f_k (\sum_{l=0}^{n} \alpha_l t^{kl})^j T^j$$

$$= \sum_{k=0}^{n-1} \sum_{l=0}^{n} \alpha_l f_k t^{kl} T^j.$$ 

If we use minimal polynomial of $t$ over $K$, then we can write all terms in (9) with respect to elements of $B_k$. So, we can write matrix representation of $\lambda_\beta$ by using $B_k$ as the basis, where $\beta = f_0 + f_1 t + f_2 t^2 + \cdots + f_{n-1} t^{n-1}$, and we will get a set of $(kn \times kn)$ matrices with this property that the difference of any couple of them is a full-rank matrix. This result follows from the fact that if we extend $B_k$ to $B$, the basis of $D$ over $F$, and let $X$ and $X'$ be the matrix representations of $\lambda_\beta$ and $\lambda_{\beta'}$ with respect the basis $B_k$ ($\beta \neq \beta'$) and $C$ and $C'$ be the matrix representations of $\lambda_\beta$ and $\lambda_{\beta'}$ with respect to the basis $B$, then we have

$$C - C' = \begin{bmatrix} [X - X']_{nk \times nk} & [A - A']_{nk \times n(n-k)} \\ [O_{n(n-k) \times nk}]_{nk \times n(n-k)} & [B - B']_{n(n-k) \times n(n-k)} \end{bmatrix}.$$ 

Since $\det(C - C') \neq 0$ and $\det(C - C') = \det(X - X') \det(B - B')$, we have $\det(X - X') \neq 0$ and $X - X'$ is a full-rank matrix, as desired.

By using what stated in the above paragraph, we can construct STBCs for $kn$ transmit antennas, where $k = 1, \ldots, n-1$. Here we need Galois extensions of order $n$. We use cyclic extensions and the idea used in [27, p. 89].

Let $K$ be a field and $L$ an extension of $K$, such that $[L : K] = n$. Also, let the extension $L/K$ be a cyclic extension, i.e., the Galois group of the extension be a cyclic group generated by a single element, say $\sigma$. We now give a general method of obtaining a cyclic extension from [27, p. 89]. Towards finding such a method, we state the following lemma from [20].
Theorem 4.2. Let $K$ be a field containing a primitive $n^{th}$ root of unity. Then, $L/K$ is cyclic of degree $n$ if and only if $L$ is the splitting field over $K$ of an irreducible polynomial $x^n - a \in K[x]$.

Let $S$ be the signal set of interest and $n$ be the number of transmit antennas. Then, consider the field $K = \mathbb{Q}(S, \omega_n, \omega_m)$, where $m$ is such that the polynomial $x^n - \omega_m$ is irreducible in $K[x]$. We can always find such $m$ as $S$ is a finite subset of $\mathbb{C}$. However, depending on the structure of $S$, the difficulty in finding such $m$ varies.

Let $L = K(\omega_{mn})$. For using Theorem 4.2, it is enough to show that $L$ is the splitting field of $x^n - \omega_m$. The roots of this polynomial are $\omega_{mn}\omega_i^n$, for $i = 0, \ldots, n-1$. Since $L$ contains $\omega_{mn}n$, all these roots also lie in $L$. Thus, $L$ contains the splitting field of $x^n - \omega_m$. Since $L$ is the smallest subfield containing $K$ and $\omega_{mn}$, $L$ itself is the splitting field of $x^n - \omega_m$. Thus, by Theorem 4.2, $L/K$ is a cyclic extension. We give some examples to illustrate the above construction.

Example 4.3. Let $n = 2$, $K = \mathbb{Q}(j)$ and $L = K(\sqrt{j})$. Clearly, $L$ is the splitting field of the polynomial $x^2 - j \in K[x]$ and hence $L/K$ is cyclic of degree 2. Note that $x^2 - j$ is irreducible over $K$, since its only roots are $\pm \sqrt{j}$ and none of them are in $K$. The generator of the Galois group is given by $\sigma : \sqrt{j} \mapsto -\sqrt{j}$. We can use the notations of Example 4.1 and construct codewords with the following form

$$
\begin{bmatrix}
    f_0(a) & jf_1(a) & \alpha f_2(a) & -j\alpha f_3(a) \\
    f_1(a) & f_0(a) & -\alpha f_2(a) & \alpha f_3(a) \\
    f_2(a) & jf_3(a) & f_0(a) & -j f_1(a) \\
    f_3(a) & f_2(a) & -f_1(a) & f_0(a)
\end{bmatrix},
$$

where $f_0, f_1, f_2, f_3 \in K[\alpha]$ and $\alpha = e^{j\sqrt{2}}$.

Example 4.4. Let $n = 3$. Suppose that we want $S$ to be a QAM signal constellation. Let $K = \mathbb{Q}(j, \omega_3)$. Then, the polynomial $x^3 - \omega_3$ is irreducible in $K[x]$, because if it is reducible, then it should have a linear factor, which implies that this polynomial has a root in $K$, which is not true. Thus, $L = K(\omega_3)$ is a cyclic extension of $K$ and $\sigma : \omega_3 \mapsto \omega_3\omega_3$ is a generator of the Galois group. Now let $D = L((T, \sigma))$, where $T$ is an indeterminate and put $x = T^j$. Then, by Lemma 3.2, $B = \{\omega_i^jT^j : i, j = 0, 1, 2\}$ is the basis of $D$ over $F = K(\langle x \rangle)$ and by using this basis, we can construct an STBC $C$ for 9 transmit antennas. Let $\beta = f_0 + f_1\omega_3 + f_2\omega_3^2 + f_3T + f_4\omega_3T + f_5\omega_3^2T + f_6T^2 + f_7\omega_3T^2 + f_8\omega_3^2T^2$. Then, $C$ has codewords as following:

$$
\begin{bmatrix}
    f_0 & \omega_3f_2 & \omega_3f_1 & xf_6 & xf_8 & x\omega_3^2f_7 & xf_3 & x\omega_3f_5 & xf_4 \\
    f_1 & f_0 & \omega_3f_2 & xf_6 & xf_8 & x\omega_3^2f_7 & xf_3 & x\omega_3f_5 & xf_4 \\
    f_2 & f_1 & f_0 & xf_6 & x\omega_3f_7 & xf_3 & x\omega_3f_5 & x\omega_3^2f_4 & xf_3 \\
    f_3 & \omega_3f_5 & \omega_3f_4 & f_0 & f_2 & \omega_3^2f_1 & xf_6 & x\omega_3^2f_8 & xf_7 \\
    f_4 & f_3 & \omega_3f_5 & \omega_3f_1 & f_0 & f_2 & x\omega_3^2f_7 & xf_6 & x\omega_3f_8 \\
    f_5 & f_4 & f_3 & \omega_3f_2 & \omega_3f_1 & f_0 & x\omega_3f_8 & x\omega_3^2f_7 & xf_6 \\
    f_6 & f_5 & f_4 & f_3 & \omega_3f_4 & f_0 & f_2 & x\omega_3f_8 & x\omega_3^2f_7 \\
    f_7 & f_6 & f_5 & \omega_3f_8 & \omega_3f_4 & f_3 & f_5 & \omega_3^2f_1 & f_0 \\
    f_8 & f_7 & f_6 & \omega_3f_8 & \omega_3f_4 & f_3 & f_5 & \omega_3^2f_1 & f_0
\end{bmatrix},
$$

where $f_0, \ldots, f_8$ are series in terms of indeterminate $x$ with coefficients which come from $K = \mathbb{Q}(j, \omega_3)$. We can put $f_0, \ldots, f_8$ to be polynomials in terms of $\alpha$, where $x = \alpha = e^{j\sqrt{2}}$ and we will get a full-rank STBC with arbitrary rate for 9 transmit antennas.
Now let $\mathcal{B}_2 = \{1, \omega_9, \omega_9^2, T, \omega_9 T, \omega_9^2 T\}$. Then, by using $\mathcal{B}_2$ as basis of $F$-space $V_2$, and those elements of $D$ which have the form $\beta = f_0 + f_1 \omega_9 + f_2 \omega_9^2$, where $f_0, f_1, f_2 \in K((x)) = \mathbb{Q}(j, \omega_3)((x))$, we can construct the following STBC for 6 transmit antennas

\begin{align*}
\begin{bmatrix}
 f_0 & \omega_3 f_2 & \omega_3 f_1 & 0 & 0 & 0 \\
 f_1 & f_0 & \omega_3 f_2 & 0 & 0 & 0 \\
 f_2 & f_1 & f_0 & 0 & 0 & 0 \\
 0 & 0 & 0 & f_0 & f_2 & \omega_3^2 f_1 \\
 0 & 0 & 0 & \omega_3 f_1 & f_0 & f_2 \\
 0 & 0 & 0 & \omega_3^2 f_2 & \omega_3 f_1 & f_0
\end{bmatrix}.
\end{align*}

Finally, if we use $\mathcal{B}_3 = \{1, \omega_9, \omega_9^2\}$ as the basis, then we can construct an STBC for 3 transmit antennas as in [27].

The idea which is used in Example 4.4 can be used for constructing another STBC. Let $\mathcal{B}_k = \{1, t, \ldots, t^k, T, \ldots, t^k T, T^2, \ldots, t^k T^2, \ldots, T^{n-1}, \ldots, t^k T^{n-1}\}$ and $\beta = f_0 + f_1 T + f_2 T^2 + \cdots + f_{n-1} T^{n-1}$, where $f_0, \ldots, f_{n-1} \in K((x))$. Then, $\lambda_\beta$ preserves the $F$-subspace generated by $\mathcal{B}_k$, invariant. So, we can construct an STBC for $kn$ transmit antennas, where $k = 1, \ldots, n$, as the following

\begin{align*}
\begin{bmatrix}
 f_0 I_k & x f_{n-1} I_k & \cdots & x f_1 I_k \\
 f_1 I_k & f_0 I_k & \cdots & x f_2 I_k \\
 \vdots & \vdots & \ddots & \vdots \\
 f_{n-1} I_k & f_n - 2 I_k & \cdots & f_0 I_k
\end{bmatrix},
\end{align*}

where $I_k$ is the $(k \times k)$ identity matrix and $f_i \in K((x)) = \mathbb{Q}(j, \omega_3)((x))$, for $i = 0, \ldots, n-1$.

For example, if $\beta = f_0 + f_1 T + f_2 T^2$ and $\mathcal{B}_2 = \{1, \omega_9, T, \omega_9 T, T^2, \omega_9 T^2\}$, then we obtain

\begin{align*}
\begin{bmatrix}
 f_0 & 0 & x f_2 & 0 & x f_1 & 0 \\
 0 & f_0 & 0 & x f_2 & 0 & x f_1 \\
 f_1 & 0 & f_0 & 0 & x f_2 & 0 \\
 0 & f_1 & 0 & f_0 & 0 & x f_2 \\
 f_2 & 0 & f_1 & 0 & f_0 & 0 \\
 0 & f_2 & 0 & f_1 & 0 & f_0
\end{bmatrix},
\end{align*}

where $f_0, f_1, f_2 \in K((x)) = \mathbb{Q}(j, \omega_3)((x))$. If $f_0, f_1, f_2 \in K[\alpha] = \mathbb{Q}(j, \omega_3)[\alpha]$ and $\alpha = e^{i \sqrt{2}}$, then we have a full-rank arbitrary rate STBC for 6 transmit antennas.

In the next section, we present some examples of twisted Laurent series rings and twisted function fields, which are noncrossed product algebras, and we construct STBCs from them.

5. STBCs from noncrossed product algebras

In [29], high-rate and full diversity STBCs were constructed from crossed product algebras. In this section, we are going to construct high-rate and full diversity STBCs from a family of twisted Laurent series rings and twisted function fields, which are noncrossed product algebras [11]. First, we give a brief introduction to crossed product algebras. Let the associative $F$-algebra, $A$, be a central simple algebra and $n^2$ be the dimension of $A$ over its center, $F$. By a subfield $K$ of $A$, we mean $F \subset K \subset A$. Let $K$ be a maximal subfield of $A$. Also, let $K$ be such that the centralizer of $K$ in $A$ is $K$ itself. Then, $K$ is called a strictly maximal subfield and
it is well known that $[K : F] = n$, where $n$ is the degree of the algebra $A$. When $A$ is a division algebra, then every maximal subfield is its own centralizer in $A$ and thus $[K : F] = n$, for every maximal subfield $K$. In STC literature, we always consider central simple algebras which have at least one strictly maximal subfield as a subfield of the complex field $C$. In addition, let the extension $K/F$ be a Galois extension and let $G = \{\sigma_0 = 1, \sigma_1, \ldots, \sigma_{n-1}\}$ be the Galois group of $K/F$. Then, by the Skolem-Noether theorem [15], we can find the representation of elements in $A$ over $F$ and then, use them to construct an STBC (see, e.g., [29]).

**Definition 5.1.** An $F$-central simple algebra $A$ is called a crossed product algebra if it can be written as a crossed product, i.e., if it has a strictly maximal subfield which is Galois over the center $F$. Otherwise, $A$ is called a noncrossed product.

### 5.1. Constructing Noncrossed Product Division Algebras

In this subsection, an explicit example of a noncrossed product division algebra is given from [11]. By [11], the degree of this example is 8, which is the smallest one for which the existence of noncrossed products is currently known. The direct construction used here is the one of iterated twisted function fields in two variables over division algebras over number fields. These algebras are denoted by $D(x, \sigma)(y, \tau)$ where $D$ is a division algebra and $\sigma$ and $\tau$ are outer automorphisms of $D$ that define conjugation of elements of $D$ with the indeterminate $x$ and $y$, respectively. By choosing the parameters involved carefully, this construction yields a noncrossed product. For instance, $D$ can be chosen to be the quaternion division algebra $(3 + \sqrt{3}, -7 + \sqrt{-7})$ over the biquadratic number field $K = \mathbb{Q}(\sqrt{3}, \sqrt{-7})$ or a cyclic division algebra (see, e.g., [12]).

**Definition 5.2.** Let $A$ be a central simple algebra with center $K$, and let $\text{Aut}(A)$ be its automorphism group. We write $\text{Inn}(A) \leq \text{Aut}(A)$ for the normal subgroup of all inner automorphisms $\text{Inn}(x) : a \mapsto xax^{-1}, x \in A^*$. The outer automorphism group is defined as $\text{Out}(A) := \text{Aut}(A)/\text{Inn}(A)$. Every element of $\text{Out}(A)$ is called an outer automorphism of $A$.

For the proofs of the theorems which are used in this section, see [11]. Also, the valuation theory of algebraic number fields [21], the basic facts on quaternion algebras [22], and central simple algebras and their subfields, [22] and [18], are needed.

### 5.1.1. Construction of iterated twisted function fields and twisted Laurent series rings

Twisted function fields and twisted Laurent series rings are introduced at various points in the literature, for instance in [1]. Twisted Laurent series are also discussed in [19] and in more details in [22] and [18].

Let $K/F$ be a finite cyclic field extension with $\text{Gal}(K/F) = \langle \sigma \rangle$ and $[K : F] = n$. Furthermore, let $D$ be a finite-dimensional central $K$-division algebra, and suppose that $\sigma$ extends to an $F$-algebra automorphism $\tilde{\sigma}$ of $D$. Denote by $D[x; \tilde{\sigma}]$, the set of all polynomials

$$D[x; \tilde{\sigma}] := \left\{ \sum_{i=0}^{k} d_i x^i \mid k \in \mathbb{N} \cup \{0\}, d_i \in D \right\},$$

and by $D((x; \tilde{\sigma}))$, the set of all formal series

$$D((x; \tilde{\sigma})) := \left\{ \sum_{i \geq k} d_i x^i \mid k \in \mathbb{Z}, d_i \in D \right\}.$$
A ring structure on $D[x, \tilde{\sigma}]$ and $D((x; \tilde{\sigma}))$, is given by componentwise addition and the multiplication rule

$$xd = \tilde{\sigma}(d)x, \quad \text{for all } d \in D.$$

Denote by $D(x; \tilde{\sigma})$, the ring of central quotients of $D[x; \tilde{\sigma}]$, i.e.

$$D(x; \tilde{\sigma}) := \left\{ \frac{f}{g} \mid f, g \in D[x; \tilde{\sigma}], g \in Z(D[x; \tilde{\sigma}]) \right\},$$

with $Z(-)$ denoting the center. It is easy to verify that $D(x; \tilde{\sigma})$ and $D((x; \tilde{\sigma}))$ are division rings. $D(x; \tilde{\sigma})$ can be regarded as a subring of $D((x; \tilde{\sigma}))$. By the Skolem-Noether theorem, $\tilde{\sigma}^n$ is an inner automorphism of $D$ since it is the identity on the center $K$. Moreover, as a consequence of Hilbert’s Theorem 90, we have

**Lemma 5.3.** There exists an $\alpha \in D^*$ with

$$\tilde{\sigma}^n = \text{Inn}(\alpha) \quad \text{and} \quad \tilde{\sigma}(\alpha) = \alpha.$$

Here, Inn$(\alpha)$ denotes the inner automorphism of $D$ defined by $\text{Inn}(\alpha)(x) := \alpha x \alpha^{-1}$ for all $x \in D$. Moreover, such an element $\alpha$ can be found by solving systems of linear equations only. Note that (17) determines $\alpha \in D^*$ up to multiplication by elements from $F^*$.

Let $\alpha \in D^*$ be an element as in Lemma 5.3. Then $s := \alpha^{-1} x^n$ is a commuting indeterminate over $D$ and the centers of $D[x; \tilde{\sigma}]$, $D((x; \tilde{\sigma}))$ and $D(x; \tilde{\sigma})$ are

$$Z(D[x; \tilde{\sigma}]) = F[s] = \left\{ \sum_{i=0}^{k} a_i (\alpha^{-1} x^n)^i \mid k \in \mathbb{N} \cup \{0\}, a_i \in F \right\},$$

$$Z(D((x; \tilde{\sigma}))) = F((s)) = \left\{ \sum_{i \geq k} a_i (\alpha^{-1} x^n)^i \mid k \in \mathbb{Z}, a_i \in F \right\},$$

and

$$Z(D(x; \tilde{\sigma})) = F(s),$$

respectively. Obviously, the set $\{1, x, \ldots, x^{n-1}\}$ forms a basis of $D[x; \tilde{\sigma}]$, $D((x; \tilde{\sigma}))$ and $D(x; \tilde{\sigma})$ over $D[s]$, $D((s))$ and $D(s)$ (as free modules). Hence

$$[D(x; \tilde{\sigma}) : F(s)] = [D((x; \tilde{\sigma})) : F((s))] = n[D : F].$$

We see in the following theorem that the constructions which are used in previous sections, are examples of crossed product algebras and they can be presented as (cyclic) generalized crossed products. This theorem shows that twisted function fields and Laurent series rings are rich sources to obtain crossed product or noncrossed product division algebras.

**Lemma 5.4 ([33, Theorem 2.3]).** The algebras $D((x; \tilde{\sigma}))$ and $D(x; \tilde{\sigma})$ are central simple $F((s))$- and $F(s)$-algebras, respectively and

$$D((x; \tilde{\sigma})) \cong (D((s)), \tilde{\sigma}, \alpha s), \quad D(x; \tilde{\sigma}) \cong (D(s), \tilde{\sigma}, \alpha s).$$

Here $\tilde{\sigma}$ also denotes the extension of $\sigma$ to $D((s))$ and $D(s)$ that fixes $s$.

**Definition 5.5.** Let $A$ be a central simple algebra. Then by [22, Proposition 12.5b], there is a division algebra $D$ and a suitable $n \in \mathbb{N}$ such that $A \cong M_n(D)$; the Schur index (or index) of $A$ is

$$\text{Ind}(A) = \text{deg}(D).$$
high-rate STBCs from Laurent series rings 267

So, if \(D\) is a division algebra, then \(\text{Ind}(D) = \text{deg}(D)\). By using Definition 5.5, we have
\[
\text{Ind}(D(x; \hat{\sigma})) = \text{Ind}(D((x; \hat{\sigma}))) = n\text{Ind}(D).
\]

**Remark 2.** As mentioned before, in construction of STBC we use polynomials instead of infinite series. Hereinafter, we shall use twisted function fields instead of twisted Laurent series rings.

Now we iterate the process of building twisted function fields and twisted Laurent series rings from \(D\). The following will be carried out only for \(D(x; \hat{\sigma})\) and is analogous for \(D((x; \hat{\sigma}))\). Let \(K/F\) be a finite Abelian Galois extension with \(\text{Gal}(K/F) = \langle \sigma \rangle \oplus \langle \tau \rangle\), \(\text{ord}(\sigma) = n_1\), \(\text{ord}(\tau) = n_2\), \([K:F] = n_1n_2 = n\). Let \(D\) be a finite-dimensional central \(K\)-division algebra and suppose that \(\sigma\) and \(\tau\) extend to \(F\)-algebra automorphisms \(\hat{\sigma}\) and \(\hat{\tau}\) of \(D\), respectively. Let \(F_\sigma \subseteq K\) be the fixed field of \(\sigma\). Then, since \(K/F_\sigma\) is cyclic with \(\text{Gal}(K/F_\sigma) = \langle \sigma \rangle\), we can build \(D(x; \hat{\sigma})\) as in (16). By (20), \(Z(D(x; \hat{\sigma})) = F_\sigma(s)\) for some indeterminate \(s\) over \(F_\sigma\). If we set \(\tau(s) := s\), then \(F_\sigma(s)/F(s)\) is cyclic with \(\text{Gal}(F_\sigma(s)/F(s)) = \langle \tau \rangle\). To build an iterated twisted function field, which is a twisted function field of the form \(D(x; \hat{\sigma})(y; \hat{\tau})\), we need to extend \(\tau\) to an \(F(s)\)-automorphism \(\hat{\tau}\) of \(D(x; \hat{\sigma})\). The following theorem gives a criterion when this is possible. Note that \(s = \alpha^{-1}x^{n_1}\) is not uniquely determined, since \(\alpha\) is only determined up to multiplication by elements from \(F_\sigma^*\).

**Theorem 5.6 ([11, Theorem 2.2]).** If there are elements \(\alpha, \beta, \gamma \in D^*\) satisfying
\[
\begin{align*}
\text{(i)} \quad & \hat{\sigma}^n = \text{Inn}(\alpha), \hat{\sigma}(\alpha) = \alpha, \\
\text{(ii)} \quad & \hat{\tau}^n = \text{Inn}(\beta), \hat{\tau}(\beta) = \beta, \\
\text{(iii)} \quad & \hat{\sigma} = \text{Inn}(\gamma)\hat{\sigma}\hat{\tau}, \\
\text{(iv)} \quad & \hat{\tau}(\alpha)^{-1} = \gamma\hat{\sigma}(\gamma)\ldots\hat{\sigma}^{n_1-1}(\gamma), \\
\text{(v)} \quad & \hat{\tau}(\beta) = \hat{\tau}(\hat{\sigma}(\gamma)\gamma),
\end{align*}
\]
then \(\tau\) extends to the automorphism \(\hat{\tau}\) of \(D(x; \hat{\sigma})\), defined by
\[
\hat{\tau}\left(\sum d_ix^i\right) := \sum \hat{\tau}(d_i)(\gamma x)^i,
\]
such that \(\hat{\tau}(s) = s\) for \(s := \alpha^{-1}x^{n_1}\). Moreover,
\[
Z(D(x; \hat{\sigma})(y; \hat{\tau})) = F(s(t),
\]
for \(t := \beta^{-1}y^{n_2}\), and
\[
\text{Ind}(D(x; \hat{\sigma})(y; \hat{\tau})) = n\text{Ind}(D).
\]

**Remark 3 ([11, Remark 2.3]).** The algebra \(D(x; \hat{\sigma})(y; \hat{\tau})\) in Theorem 5.6 is completely described by the rules
\[
xd = \hat{\sigma}(d)x, \quad yd = \hat{\tau}(d)y, \quad yx = \gamma xy,
\]
for all \(d \in D\). Therefore it is denoted by \(D(x, y; \hat{\sigma}, \hat{\tau}, \gamma)\) and analogously we can build Laurent series ring \(D((x, y; \hat{\sigma}, \hat{\tau}, \gamma))\).

Thus we can construct a class of noncrossed products division algebras by using the following algorithm:

**Algorithm 5.1 ([11, Algorithm 2.4]).** If there exist elements \(\alpha, \beta, \gamma \in D^*\) satisfying (i) -- (v) of Theorem 5.6, then such elements can be constructed by performing the following steps:

1. Choose any \(\alpha', \beta', \gamma' \in D^*\) satisfying (i), (ii) & (iii), respectively.
2. Set
\begin{align*}
x & := \gamma' \sigma(\gamma') \cdots \sigma^{-1}(\gamma') \alpha' \tau(\alpha')^{-1} \in F_{\sigma}, \\
y & := \tau^{-1}(\gamma') \cdots \tau(\gamma') \sigma(\beta') \beta'^{-1} \in F_{\tau}.
\end{align*}

3. Solve the norm equation $N_{K/F}(c) = N_{F_{\tau}/F}(x)^{-1}$ for $c \in K$ and set $\gamma := c\gamma'$.

4. Choose an element $a \in F_{\sigma}$ with $\frac{\sigma(a)}{\tau(a)} = N_{K/F_a}(c)x$ and set $\alpha := aa'$.

5. Choose an element $b \in F_{\tau}$ with $\frac{b}{\pi(b)} = N_{K/F_{\tau}}(c)y$ and set $\beta := b\beta'$.

**Remark 4** ([11, Remark 2.5]).

1. Steps 1, 4 and 5 in the algorithm are just solutions to systems of linear equations. Step 3 is a single norm equation in a field extension. Over number fields methods from computational algebraic number theory can be applied here. The computer algebra software KASH has implemented an algorithm for solving relative norm equations (see, e.g., [2]). Provided that the degrees $n_1, n_2$ and the base field $F$ are small enough, this software can be used to carry out the algorithm.

2. Any solution $\alpha, \beta, \gamma \in D^{*}$ to the conditions (i) – (v) can be obtained by the algorithm. Moreover, the element $\gamma$ is uniquely determined up to multiplication by elements $c \in K^{*}$ with $N_{K/F}(c) = 1.$ If $\gamma$ is fixed, then $\alpha$ and $\beta$ are determined up to multiplication by elements from $F^{*}$.

3. The existence of a solution $\alpha, \beta, \gamma \in D^{*}$ to the conditions (i) – (v) does not depend on the choice of the extensions $\sigma$ and $\tau$ of $\sigma$ and $\tau$, respectively. To see this, it can be verified that if $\tilde{\sigma}$ and $\tilde{\tau}$ are replaced by $\text{Im}(\eta)\tilde{\sigma}$ and $\text{Im}(\xi)\tilde{\tau}$, respectively, where $\eta, \xi \in D^{*}$, then we can replace $\alpha, \beta, \gamma$ by
   \[
   \eta \tilde{\sigma}(\eta) \cdots \tilde{\sigma}^{-1}(\eta) \alpha, \quad \xi \tilde{\tau}(\xi) \cdots \tilde{\tau}^{-1}(\xi) \beta, \quad \xi \tilde{\tau}(\eta) \gamma \tilde{\sigma}(\xi)^{-1} \eta^{-1},
   \]
   respectively.

4. For different choices of $\gamma$ the resulting division rings $D(x, y; \tilde{\sigma}, \tilde{\tau}, \gamma)$ are not isomorphic, in general.

5.1.2. Automorphisms of quaternion algebras. In the construction of the twisted function field $D(x; \tilde{\sigma})$, we started with the automorphism $\tilde{\sigma}$ of $K$ and assumed that it extends to an automorphism $\tilde{\sigma}$ of $D$. Proposition 1 below settles this question when it is possible to extend $\sigma$ and how an extension can be found for a special case of quaternion algebras that will be sufficient for our purposes.

Let $K$ be any field and let $a, b \in K^{*}$. The quaternion algebra $(a, b)_{K}$ is the $K$-space with basis $1, i, j, ij$ and multiplication $i^2 = a, j^2 = b, ij = -ji$. By [22], it is a simple algebra with center $K$.

**Lemma 5.7** ([11, Lemma 3.1]). Let $\sigma$ be an automorphism of $K$. Then $\sigma$ extends to an automorphism $\tilde{\sigma}$ of $(a, b)_{K}$ if and only if $(a, b)_{K} \cong (\sigma(a), \sigma(b))_{K}$.

In the case $\sigma(b) = b$, we get:

**Proposition 1** ([11, Proposition 3.2]). Let $\sigma$ be an automorphism of $K$ with $\sigma(b) = b$. Then $\sigma$ extends to an automorphism $\tilde{\sigma}$ of $(a, b)_{K}$ if and only if there exists $\lambda \in K(j)$ with
\[
N_{K(j)/K}(\lambda) = \frac{\sigma(a)}{a}.
\]
For any such $\lambda$, an extension $\tilde{\sigma}$ of $\sigma$ is defined by
\[
\tilde{\sigma}(i) := \lambda i, \quad \tilde{\sigma}(j) := j.
\]
5.2. AN EXPLICIT EXAMPLE OF A NONCROSSED PRODUCT DIVISION ALGEBRA.

Here, we construct an explicit example of an iterated twisted function field following step by step the general construction from Subsection 5.1.1. This example discussed in greater details in [11].

Let \( p = 3 \) and \( q = 7 \) and let \( K \) be the biquadratic extension \( K = \mathbb{Q}(\sqrt{3}, \sqrt{-7}) \) of \( \mathbb{Q} \) with \( \text{Gal}(K/\mathbb{Q}) = \langle \sigma > \oplus < \tau > \), where
\[
\sigma(\sqrt{3}) = -\sqrt{3}, \quad \sigma(\sqrt{-7}) = \sqrt{-7},
\]
\[
\tau(\sqrt{3}) = \sqrt{3}, \quad \tau(\sqrt{-7}) = -\sqrt{-7}.
\]
Set \( K_1 = \mathbb{Q}(\sqrt{3}) \), \( K_2 = \mathbb{Q}(\sqrt{-7}) \). Let \( a_0 = 1 + \sqrt{3} \in \mathbb{K}_1 \) and \( b_0 = \frac{1 + \sqrt{-7}}{2} \in \mathbb{K}_2 \).

Note that
\[
\mathcal{N}_{K_1/\mathbb{Q}}(a_0) = a_0 \sigma(a_0) = -2, \quad \mathcal{N}_{K_2/\mathbb{Q}}(b_0) = b_0 \tau(b_0) = 2.
\]

Define the quaternion division algebra \( \mathbb{D} = (a,b)_{\mathbb{K}} \) by
\[
a = a_0 \sqrt{3} := 3 + \sqrt{3}, \quad b = b_0 \sqrt{-7} := \frac{-7 + \sqrt{-7}}{2}.
\]
The elements \( a, b \in \mathbb{K} \) were specially chosen such that \( a \in \mathbb{K}_1 \) and \( b \in \mathbb{K}_2 \).

Therefore, we can use Proposition 1 to find extensions of \( \sigma \) and \( \tau \) to \( \mathbb{D} \). Let \( \lambda_0 = \sigma(a_0)(-1 + i) \in \mathbb{K}_1(i) \) and \( \mu_0 = \mu_0 = b_0 + j \in \mathbb{K}_2(j) \). Note that
\[
\mathcal{N}_{K_1(i)/\mathbb{K}_1}(\lambda_0) = -2, \quad \mathcal{N}_{K_2(j)/\mathbb{K}_2}(\mu_0) = 2.
\]

Define \( \lambda := \frac{\lambda_0 \mu_0}{a_0} \in \mathbb{K}(i) \) and \( \mu := \frac{\mu_0 a_0}{a_0} \in \mathbb{K}(j) \). By using (24) and (25), we get
\[
\mathcal{N}_{\mathbb{K}(i)/\mathbb{K}}(\lambda) = \frac{\sigma(a_0)}{a_0} \quad \text{and} \quad \mathcal{N}_{\mathbb{K}(j)/\mathbb{K}}(\lambda) = \frac{\sigma(a_0)}{a_0}.
\]

Therefore, by Proposition 1, extensions \( \tilde{\sigma}, \tilde{\tau} \) of \( \sigma, \tau \) to \( \mathbb{D} \) are defined by
\[
\tilde{\sigma}(i) = \mu i, \quad \tilde{\sigma}(j) = j,
\]
\[
\tilde{\tau}(i) = i, \quad \tilde{\tau}(j) = \lambda j.
\]

To define an iterated twisted function field \( \mathbb{D}(x,y; \tilde{\sigma}, \tilde{\tau}, \gamma) \) over \( \mathbb{D} \), we now give elements \( \alpha, \beta, \gamma \in \mathbb{D}^* \) satisfying \((i) - (v)\) of Theorem 5.6. These are
\[
\alpha := \frac{1}{b_0} \mu_0 j, \quad \beta := \sqrt{3} \lambda_0 i, \quad \gamma := \frac{1}{2\sigma(a_0)}(\lambda_0 \mu_0 - 2).
\]

Note that \( \alpha \in \mathbb{K}(j) \) and \( \beta \in \mathbb{K}(i) \). By Theorem 5.6, \( Z(\mathbb{D}(x,y; \tilde{\sigma}, \tilde{\tau}, \gamma)) = \mathbb{Q}(s)(t) \), where \( s = \alpha^{-1} x^2, t = \beta^{-1} y^2 \), and \( \text{Ind}(\mathbb{D}(x,y; \tilde{\sigma}, \tilde{\tau}, \gamma)) = 8 \). This completes the example and the process of constructing \( \mathbb{D}(x,y; \tilde{\sigma}, \tilde{\tau}, \gamma) \).

The given elements \( \alpha, \beta, \gamma \) were found by Algorithm 5.1. Solutions to each step of the algorithm, can be found in [11]. We use the notation \( \lambda_0 \) for the conjugate of \( \lambda_0 \) in \( \mathbb{K}_1(i)/\mathbb{K}_1 \) and \( \mu_0 \) for the conjugate of \( \mu_0 \) in \( \mathbb{K}_2(j)/\mathbb{K}_2 \), i.e., \( \lambda_0 = \sigma(a_0)(-1 - i) \)
and \( \mu_0 = b_0 - j \). The following relations, as well as (24), will be used throughout:
\[
\begin{align*}
\lambda_0 \lambda_0 & = -2, \quad \tilde{\sigma}(\mu_0) = \mu_0, \quad \tilde{\tau}(\lambda_0) = \lambda_0, \quad i \lambda_0 = \lambda_0 i, \quad j \lambda_0 = \lambda_0 j, \\
\mu_0 \mu_0 & = 2, \quad \tilde{\sigma}(\mu_0) = \mu_0, \quad \tilde{\tau}(\lambda_0) = \lambda_0, \quad i \mu_0 = \mu_0 i, \quad j \mu_0 = \mu_0 j.
\end{align*}
\]

Also note that \( n_1 = n_2 = 2 \) and \( x = -4b_0^2 = -8\frac{b_0}{\pi(b_0)}, y = -4\sigma(a_0)^2 = 8\frac{\sigma(a_0)^2}{a_0} \).

**Remark 5.** The whole used parameters in this section, must be applied to obtain the representation of each element over \( \mathcal{F}(s)(t) \). However, we introduce \( s \) and \( t \) in the process of constructing \( \mathbb{D}(x,y; \tilde{\sigma}, \tilde{\tau}, \gamma) \), in the construction of STBC in the next section, we will replace them, in the entries of matrices, with two algebraically independent elements like \( \alpha_1 = e^{\sqrt{-2}} \) and \( \alpha_2 = e^{\sqrt{-3}} \). The reason of doing this is explained in the next theorem.
Theorem 5.8. Let $D' = D(x, y; \sigma, \tilde{\sigma}, \gamma)$ be the $F(s)(t)$-division algebra that is constructed in this section and let $B = \{v_1, \ldots, v_{n^2}\}$ be the basis of $D'$ over $F(s)(t)$. Consider $\Lambda : D' \rightarrow M_{n^2}(F(s)(t))$ to be the map which sends each $d \in D'$ to its representation over $F(s)(t)$ with respect to $B$. Also, if $\Psi : M_{n^2}(F(s)(t)) \rightarrow \Lambda$ be the map such that for all $A \in M_{n^2}(F(s)(t))$, $\Psi(A)$ is obtained by replacing $s$ and $t$ with $\alpha_1$ and $\alpha_2$, respectively, in the entries of $A$, then $D'' = \Psi(\Lambda(D')) \subset M_{n^2}(C)$ is a noncrossed product division ring.

Proof. Obviously, $\Lambda$ is an isomorphism between $D'$ and $\text{Im}(\Lambda)$. It is enough to show that $\Psi$ is also an isomorphism. Since $\alpha_1$ and $\alpha_2$ are algebraically independent over any number field, $\Psi$ is a one-to-one map and clearly onto. It can be easily verified that for all $A_1, A_2 \in M_{n^2}(F(s)(t))$, $\Psi(A_1 + A_2) = \Psi(A_1) + \Psi(A_2)$ and $\Psi(A_1 A_2) = \Psi(A_1) \Psi(A_2)$. So, $\Psi$ is an isomorphism and its restriction to $\text{Im}(\Lambda)$ is also an isomorphism. Since $D'$ is a noncrossed product division ring and $D'' \cong \Psi(\text{Im}(\Lambda))$, $D''$ is also a noncrossed product division ring.

Note that if we replace $D(x, y; \sigma, \tilde{\sigma}, \gamma)$ with $D((x, y; \sigma, \tilde{\sigma}, \gamma))$, then Theorem 5.8 is not valid. Because in this case, the map $\Psi$ is no longer an isomorphism and the algebraically independency of $\alpha_1$ and $\alpha_2$ is not sufficient for our purpose.

5.3. Construction of STBCs from iterated twisted function fields and Laurent series rings. Now we are going to construct an STBC from the introduced division algebra of Subsection 5.2. First, we need the basis of $D(x, y; \sigma, \tilde{\sigma}, \gamma)$ over $Q(s)(t)$. Also, we need to replace $Q$ with $Q(S)$, where $S$ is a preforment defined signal set. By the assumptions of Subsection 5.2, $S$ can be the $M - \text{PSK}$ signal set, where $4 \mid M$. In this case, we have $\text{Gal}(K(S)/F(S)) \cong \text{Gal}(K/F)$. If we extend $\tilde{\sigma}$ and $\tilde{\tau}$, in a natural way, from $K_1$ and $K_2$ to $K_1(S)$ and $K_2(S)$, respectively, then the whole construction of $D(x, y; \sigma, \tilde{\sigma}, \gamma)$ will remain unchanged. So, we can replace $F$ and $K$ with $Q(S)$ and $K(S)$, respectively, in all notations.

To simplify our notations, let $\theta = \sqrt{3} + \sqrt{-7}$. Then, we have $Q(\theta) = Q(\sqrt{3}, \sqrt{-7})$. Because, $\sqrt{-7} = \frac{\theta^2 - 10}{29} = \frac{9}{10} \theta + \frac{19}{20} \theta^3$ and $\sqrt{3} = \frac{\theta^2 + 10}{29} = \frac{1}{10} \theta - \frac{19}{20} \theta^3$. We use minimal polynomial of $\theta$ which is $P(z) = z^4 + 8z^2 + 100$, to write fractions of the form $f(\theta) / g(\theta)$ as a polynomial in terms of $\theta$ with degree less than $4$. Now, it can be seen that $\{1, \theta, \theta^2, \theta^3\}$ is the basis of $K = Q(\sqrt{3}, \sqrt{-7})$ over $Q$ (or equivalently, $K(S)$ over $Q(S)$).

By Theorem 5.6, we can see that the set

$$B = \{\theta^i x^m y^n, \theta^i x^m y^n, \theta^j x^m y^n, \theta^i j x^m y^n \mid l = 0, 1, 2, 3 and m, n = 0, 1\}$$

is the basis of $D(x, y; \sigma, \tilde{\sigma}, \gamma)$ over $F(s)(t)$, where $\{1, i, j, i j\}$ is the basis of $D$ over $K$. So, the degree of $D(x, y; \sigma, \tilde{\sigma}, \gamma)$ over $F(s)(t)$ is 64. Thus, a full-rank STBC for 64 transmit antennas can be constructed from this basis. Hereby, we need to find the representation of elements of $D(x, y; \sigma, \tilde{\sigma}, \gamma)$ with respect to the basis $B$, which requires finding the operation of automorphisms $\sigma$ and $\tau$ on $\theta^i$ for $i = 0, 1, 2, 3$. We have

$$\sigma(\theta) = -\sqrt{3} + \sqrt{-7} = -\frac{1}{10} \theta + \frac{1}{20} \theta^3 + \frac{9}{10} \theta + \frac{1}{20} \theta^3$$

$$\tilde{\sigma}(\theta^2) = -\theta^2 - 8$$

$$\tilde{\sigma}(\theta^3) = -24\sqrt{3} + 2\sqrt{-7} = \frac{13}{10} \theta^3 - \frac{6}{10} \theta.$$
The operation of $\tilde{\tau}$ on $\theta^i$, for $i = 0, 1, 2, 3$, can be computed analogously. Now we are ready to complete the process of constructing STBC from the constructed iterated twisted function field. We represent this procedure in following example.

**Example 5.1.** In this example, we use the basis $\mathcal{B}$, which is obtained in previous paragraph. Due to the big size of the matrices, which are $(64 \times 64)$ matrices, we can not present the complete representation of the codewords, here. So, we need to decrease the number of elements in $\mathcal{B}$ by using the introduced technique of Subsection 4.2. Here, we expose two subsets which are appropriate for our purpose. First one is $\mathcal{B}' = \{1, \theta, \theta^2, \theta^3, x, \theta x, \theta^2 x, \theta^3 x\}$. Let $V_1$ be the $F(t)$-space generated by $\mathcal{B}'$. If we consider elements of the form $e = f_0 + f_1 \theta + f_2 \theta^2 + f_3 \theta^3$ in $D(x, y; \tilde{\sigma}, \tilde{\tau}, \gamma)$, where $f_0, \ldots, f_3 \in F(s)(t)$, then the linear transformation $\lambda_e$ preserves $V_1$ invariant, i.e., $\lambda_e(V_1) \subseteq V_1$. Thus, we can write the matrix representation of $\lambda_e$ with respect to $\mathcal{B}'$. Also, it can be seen that the set of these matrices has this property that the subtraction of any two of them is a full-rank matrix. So, by Theorem 5.8, we can consider them as an STBC with codewords of the form

$$
\begin{bmatrix}
F_1 & 0 \\
0 & F_2
\end{bmatrix},
$$

where $F_1$ and $F_2$ are $(4 \times 4)$ matrices

$$
F_1 = \begin{bmatrix}
f_0 & -100f_3 & -100f_2 & 800f_3 - 100f_1 \\
f_1 & f_0 & -100f_3 & -100f_2 \\
f_2 & f_1 - 8f_3 & f_0 - 8f_2 & -8f_1 - 36f_3 \\
f_3 & f_2 & f_1 - 8f_3 & f_0 - 8f_2
\end{bmatrix},
$$

$$
F_2 = \begin{bmatrix}
f_0 - 8f_2 & -10f_1 & 13f_3 & 100f_2 \\
f_1 - \frac{8}{10}f_3 & f_0 - 8f_2 & -10f_1 & 13f_3 \\
-\frac{8}{10}f_3 & -11f_3 & f_0 & -75f_3 - 10f_1 \\
-\frac{1}{10}f_3 & -\frac{11}{10}f_3 & f_0 & -11f_3
\end{bmatrix},
$$

where $f_0, f_1, f_2, f_3$ are polynomials in terms of two variables $s = \alpha^{-1}x^2$ and $t = \beta^{-1}y^2$ with coefficients in $F$. As mentioned in Theorem 5.8, we can replace $s$ and $t$ with $\alpha_1 = e^{\sqrt{-7}}$ and $\alpha_2 = e^{\sqrt{-20}}$, respectively.

Another example of this type can be constructed by considering elements of the form $e = f_0 + f_1 \theta + f_2 \theta^2 + f_3 \theta^3 + f_4 j + f_5 \theta j + f_6 \theta^2 j + f_7 \theta^3 j$ and the subspace $V_2$, which is generated by the basis

$$
\mathcal{B}'' = \{1, \theta, \theta^2, \theta^3, x, \theta x, \theta^2 x, \theta^3 x, j, \theta j, \theta^2 j, \theta^3 j, jx, \theta jx, \theta^2 jx, \theta^3 jx\}.
$$

This STBC can be used for 16 transmit antennas. We compute only one of its columns. We use from $j^2 = b = -\frac{7}{2} + \frac{1}{2}\sqrt{-7} = -\frac{7}{2} + \frac{9}{20}\theta + \frac{9}{20}\theta^3$ and the fact that $\tilde{\sigma}(j) = j$, which implies that $jx = xj$, wherever is needed in the computations. Also, we can see that $j\theta = j\theta$. By these considerations, we have

$$
\lambda_e(jx) = jx \cdot e = \tilde{\sigma}(e)jx = \sum_{r=0}^{3} f_r \tilde{\sigma}(\theta^r)jx + \sum_{r=0}^{3} f_{r+4} \tilde{\sigma}(\theta^r)j^2x
$$

$$
= \left(-\frac{7}{2} f_4 + 28f_6 + \frac{9}{20} f_4 - \frac{72}{20} f_6\right)\theta - \left(\frac{1}{40} f_4 - \frac{1}{5} f_6\right)\theta^3
$$

$$
+ \left(-2 f_5 + \frac{60}{40} f_7 + \frac{10}{4} f_6 - \frac{25}{10} f_5 - \frac{325}{20} f_7 x + \frac{5}{20} f_5 - \frac{42}{20} f_7 \theta x\right)\theta^2 x
$$

$$
+ \left(\frac{8}{40} f_5 + \frac{6}{40} f_7 + \frac{42}{10} f_6 - \frac{18}{40} f_5 - \frac{117}{20} f_7 \theta^2 x + \frac{9}{20} f_5 - \frac{7}{20} f_7 - \frac{91}{20} f_7 \theta^3 x\right)\theta^3 x
$$

$$
+ (f_0 - 8f_2)jx + \left(\frac{8}{10} f_1 - \frac{6}{10} f_3\right)jx + (f_2 \theta^2 jx + (\frac{1}{10} f_1 + \frac{13}{10} f_3 \theta^3 jx).
$$
So, the 13th column of the codewords is
\[
\begin{align*}
\frac{-7}{2}f_4 + 28f_6, & \quad \frac{9}{20}f_1 - \frac{72}{20}f_6, 0, \quad \frac{1}{40}f_4 - \frac{1}{5}f_5, \\
-2f_5 + \frac{60}{40}f_7 + \frac{10}{4}f_6 - \frac{25}{10}f_7 - \frac{325}{10}f_5 + \frac{42}{20}f_7, \\
\frac{8}{40}f_5 + \frac{-6}{40}f_7 + \frac{42}{10}f_6 - \frac{18}{40}f_5 - \frac{117}{20}f_7, \\
-\frac{9}{20}f_6 - \frac{7}{20}f_5 - \frac{91}{20}f_7, 0, 0, 0, f_6 - 8f_2, \quad \frac{8}{10}f_1 - \frac{6}{10}f_3, -f_2, \quad \frac{1}{10}f_1 + \frac{13}{10}f_4, \quad f_0 - 8f_2.
\end{align*}
\]

All the division algebras which are used in this section, are examples of noncrossed product algebras (see, e.g., [11]). However, using them involves some heavy computations to construct the STBC, their basis has a simple form and all computations can be carried out by a simple computer algorithm. Another noncrossed product example over \( \mathbb{Q}((t)) \) and \( \mathbb{Q}(t) \), can be found in [12]. This construction is of the form \( D(x; \sigma) \) and of index and exponent 9, where \( D \) is a cubic cyclic division algebra over the maximal real subfield of the 7th cyclotomic field. The process of constructing the STBC from this division algebra, is similar to the followed process during this section.

6. Decoding and simulation results

The method which is used for decoding our STBCs is as the same as the one which is used in [29]. Maximum-likelihood (ML) decoding of our STBCs, in general, involves exhaustive search which increases exponentially with the number of transmit antennas. In [34] and [7], a sphere decoder was proposed, which uses an efficient algorithm to find the closest lattice point to a given point. This algorithm uses the fact that the column rank of the generator matrix of the lattice is at least the number of dimensions in the lattice. Damen et al., in [4], have shown that a sphere decoder can be applied for multiple-antenna systems if the perfect channel state information (CSI) is known at the receiver. If \( \mathbf{f} \) is the transmitted vector from \( n \) antennas and \( r \) is the number of receive antennas, then we have

\[
\mathbf{x} = \sqrt{\frac{\rho}{n}} \mathbf{H} \mathbf{f} + \mathbf{w},
\]

where \( \mathbf{x} \) is the received \( (r \times 1) \) vector, \( \mathbf{H} \) is the \( (n \times r) \) channel matrix, and \( \mathbf{w} \) is the additive white Gaussian noise (AWGN). By these assumptions, the lattice representation of the system model is given by

\[
\mathbf{x}' = \sqrt{\frac{\rho}{n}} \mathbf{H}' \mathbf{f}' + \mathbf{w}',
\]

where

\[
\begin{align*}
\mathbf{x}' &= \begin{bmatrix} \text{Re}(\mathbf{x}^T) & \text{Im}(\mathbf{x}^T) \end{bmatrix}^T, \\
\mathbf{f}' &= \begin{bmatrix} \text{Re}(\mathbf{f}^T) & \text{Im}(\mathbf{f}^T) \end{bmatrix}^T, \\
\mathbf{H}' &= \begin{bmatrix} \text{Re}(\mathbf{H}) & -\text{Im}(\mathbf{H}) \\
\text{Im}(\mathbf{H}) & \text{Re}(\mathbf{H}) \end{bmatrix}, \\
\mathbf{w}' &= \begin{bmatrix} \text{Re}(\mathbf{w}^T) & \text{Im}(\mathbf{w}^T) \end{bmatrix}^T.
\end{align*}
\]
Since the channel matrix $H$ is of full rank almost surely, the equivalent channel matrix, $H'$, is also of full rank. Hence, the sphere decoder can be applied whenever $f$ is from a constellation which is a subset of a lattice. Hence, sphere detector achieves ML performance with a significantly reduced complexity, which is roughly cubic in $n$ at high SNRs (see, e.g., [14]). Though phase-shift keying (PSK) constellations are not subsets of any lattice, we can still use the sphere decoder, known as complex sphere decoder, as shown by Hochwald and Ten Brink in [16]. The algorithm for the case of a PSK constellation searches through the phase angles of the constellation points instead of the lattice-point coordinates and since the phase angles of the constellation points are integer multiples of $2\pi/M$ (for M-PSK), the search is over a finite set. The complexity of complex sphere decoder is less than the complexity of the sphere decoder for lattice constellations. This is because we search for points in the case of complex sphere decoder, while we search for $2n$ points in the case of lattice sphere decoder. In our case, the equivalent channel model is

$$\hat{x} = \sqrt{\frac{\rho}{n}} \frac{1}{\sqrt{P}} H\Phi f + \hat{w}.$$ 

Since the rank of the matrix $H$ is $\min(nr, n^2)$ and the matrix $\Phi$ is invertible, the rank of the matrix $\hat{H}$ is also $\min(nr, n^2)$. Now, since the rate of our STBCs are arbitrary, say $R$, we can use the sphere decoder efficiently if $\min(nr, n^2) \geq R^2$,..
which implies that $R$ must be less than $n$. If the number of receive antennas is less than the number of transmit antennas and we need rate $n$, then we can use the generalized sphere decoder proposed in [3], which involves more computational complexity. However, we can still use the sphere decoder if we decrease the rate of our STBC.

6.1. Simulation results. Now, we present simulation results for 4 transmit antennas with 1, 2 and 4 receive antennas, respectively, over 4-PSK signal sets. Figure 1 shows the plots for 4 transmit and different numbers of receive antennas. We used the STBC of Example 4.1 in the simulation.

Acknowledgements

The research of the second author was in part supported by a grant from IPM (No. 93050220). The authors are grateful to the referees for their very meticulous reading of this manuscript. Their suggestions were very helpful in creating the improved final version.

References

[1] P. M. Cohn, *Introduction to Ring Theory*, Springer-Verlag, London, 2000.
[2] M. Daberkow, C. Fieker, J. Kl"uners, M. Pohst, K. Roegner and K. Wildanger, *KANT V4*, J. Symbolic Comp., 24 (1997), 267–283.
[3] M. O. Damen, K. Abed-Merriam and J. C. Belfiore, Generalized sphere decoder for asymmetrical space-time communication architecture, *IEEE Electron. Lett.*, 36 (2000), 16–20.
[4] M. O. Damen, A. Chkeif and J. C. Belfiore, Lattice code decoder for space-time codes, *IEEE Commun. Lett.*, 4 (2000), 161–163.
[5] M. O. Damen, A. Tewfik and J. C. Belfiore, A construction of a space-time code based on number theory, *IEEE Trans. Inf. Theory*, 48 (2002), 753–760.
[6] P. K. Draxl, *Skew Fields*, Cambridge Univ. Press, Cambridge, 1983.
[7] U. Fincke and M. Pohst, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, *Math. Comput.*, 44 (1985), 463–471.
[8] G. J. Foschini, Layered space-time architecture for wireless communications in a fading environment when using multi-element antennas, *Bell Labs. Tech. J.*, 1 (1996), 41–59.
[9] G. J. Foschini and M. Gans, On the limits of wireless communication in a fading environment when using multiple antennas, *Wireless Personal Commun.*, 6 (1998), 311–335.
[10] J. C. Guey, M. P. Fitz, M. R. Bell and W. Y. Kuo, Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels, *IEEE Trans. Commun.*, 47 (1999), 527–537.
[11] T. Hanke, An explicit example of a noncrossed product division algebra, *Math. Nachr.*, 271 (2004), 51–68.
[12] T. Hanke, A twisted Laurent series ring that is a noncrossed product, *Israel J. Math.*, 150 (2005), 199–204.
[13] B. Hassibi and B. Hochwald, High-rate codes that are linear in space and time, *IEEE Trans. Inf. Theory*, 48 (2002), 1804–1824.
[14] B. Hassibi and H. Vikalo, On the expected complexity of sphere decoding, in 35th Asilomar Conf. Sign. Syst. Comp., Pacific Grove, 2001, 1051–1055.
[15] I. N. Herstein, *Non-Commutative Rings*, Math. Assoc. Amer., Washington, 1968.
[16] B. M. Hochwald and S. T. Brink, Achieving near-capacity on a multiple-antenna channel, *IEEE Trans. Commun.*, 51 (2003), 389–399.
[17] T. W. Hungerford, *Algebra*, 3 edition, Springer-Verlag, Washington, 1980.
[18] N. Jacobson, *Basic Algebra I*, 2nd edition, Freeman, New York, 1985.
[19] T. Y. Lam, *A First Course in Noncommutative Rings*, Springer-Verlag, New York, 1991.
[20] P. J. McCarthy, *Algebraic Extensions of Fields*, Dover Publications Inc., New York.
[21] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992.
[22] R. S. Pierce, *Associative Algebras*, Springer-Verlag, Berlin, 1982.
B. A. Sethuraman and B. S. Rajan, An algebraic description of orthogonal designs and the uniqueness of the Alamouti code, in Proc. IEEE GLOBECOM (2002), Taipai, 2002, 1088–1092.

B. A. Sethuraman and B. S. Rajan, Optimal STBC over PSK signal sets from cyclotomic field extensions, in Proc. IEEE Int. Conf. Commun. (ICC 2002), New York, 2002, 1783–1787.

B. A. Sethuraman and B. S. Rajan, STBC from field extensions of the rational field, in Proc. IEEE Int. Symp. Inf. Theory (ISIT 2002), Lausanne, 2002, p. 274.

B. A. Sethuraman, B. S. Rajan and V. Shashidhar, Full-diversity, high-rate space-time block codes from division algebras, IEEE Trans. Inf. Theory, 49 (2003), 2596–2616.

V. Shashidhar, High-Rate and Information-Lossless Space-Time Block Codes from Crossed-Product Algebras, Ph.D thesis, Indian Institute of Science, Bangalore, 2004.

V. Shashidhar, B. S. Rajan and B. A. Sethuraman, STBCs using capacity achieving designs from cyclic division Algebras, in Proc. IEEE GLOBECOM (2003), San Francisco, 2003, 1957–1962.

V. Shashidhar, B. S. Rajan and B. A. Sethuraman, Information lossless STBCs from crossed-product algebras, IEEE Trans. Inf. Theory, 52 (2006), 3913–3935.

V. Shashidhar, K. Subrahmanyam, R. Chandrasekharan, B. S. Rajan and B. A. Sethuraman, High-rate, full-diversity STBCs from field extensions, in Proc. IEEE Int. Symp. Inf. Theory (ISIT 2003), Yokohama, 2003, p. 126.

V. Tarokh, N. Seshadri and A. R. Calderbank, Space-time codes for high data rate wireless communication: Performance criterion and code construction, IEEE Trans. Inf. Theory, 44 (1998), 744–765.

E. Telatar, Capacity of multi-antenna Gaussian channels, Europ. Trans. Telecommun., 10 (1999), 585–595.

J. P. Tignol, Generalized crossed products, in Séminaire Mathématique (nouvelle série), Université Catholique de Louvain, Belgium, 1987.

E. Viterbo and J. Boutros, A universal lattice code decoder for fading channel, IEEE Trans. Inf. Theory, 45 (1999), 1639–1642.

Received December 2011; revised February 2015.

E-mail address: dkiani@aut.ac.ir
dkiani7@gmail.com
E-mail address: h.khodaiemehr@aut.ac.ir
hassankhodaiemehr@gmail.com