Space-Time Code Design Using Quaternions, Octonions and Other Non-Associative Structures

Abstract – There are several non-associative finite dimensional division algebras over different number fields. Their representations in the corresponding matrix algebras preserve additive structure. However, the embedding does not preserve multiplication as matrix multiplication is associative. As such, it gives a generalized matrix representation. Indeed, a non-associative structure provides different platforms for more effective and useful space-time coding satisfying rank criteria, and coding gain criteria for multiple antenna wireless communication. Associative division algebras have dimension restrictions, whereas non-associative division algebras over suitable fields exist in infinitely many dimensions. We illustrate the above program by using octonion algebras.

Keywords – multiple antenna wireless communication, unitary space-time modulation, group codes, octonion constellations

1. INTRODUCTION

The main issue in space-time coding is to develop a space-time code which minimizes the probability of error $P_e$ that a receiver antenna decodes. Several models have been discussed in detail and proposed for the purpose of using different structures such as unitary spaces [1, 4, 5], quaternionic spaces [6, 7, 8], and representation theory models [8, 9, 10, 11] for wireless communication in multiple unknown channels, where ingredients of several transmitters and receiver antennas such as fading coefficients of channels are difficult to be measured or may be indeterminate. In this paper, we propose and initiate space-time modulation using non-associative structures like a Moufang loop of octonions and other non-associative structures, and minimize the probability of error by enlarging a diversity product further. We shall discuss constellations associated to these structures via suitable representations in unitary space and study their performance. In unitary space-time modulation [1], for a multiple antenna-based wireless communication system with $M$ transmitter and $N$ receiver antennas through a Rayleigh flat fading channel, we consider a set $X$ consisting of $L$ unitary matrices $A_0, A_1, A_2, \cdots, A_{L-1}$. The set $X$ is called a signal constellation. For high SNR $\rho$, the pairwise error probability $P_e$ that a receiver antenna decodes an error from $A_i$ to $A_j$ can be estimated [2, 3] as follows:

$$P_e \leq \frac{1}{2} \left( \frac{2\alpha}{\rho} \right)^{MN} \frac{1}{\text{Det}(A_i - A_j)^{2N}}, \tag{1}$$

where $\alpha = 1$ for known channels and $\alpha = 2$ unknown channels. Thus, to minimize the probability of error, one has to search for a unitary constellation $X$ for which the diversity product $\xi_X$ given by

$$\xi_X = \frac{1}{2} \min_{0 \leq i < j \leq L-1} \left| \text{Det}(A_i - A_j)^H \right|^N, \quad 0 \leq \xi_X \leq 1 \tag{2}$$

is as large as possible. A unitary constellation $X$ is said to be with full diversity if $\xi_X > 0$. As mentioned above, several constellations with full diversity products using different associative algebraic structures have been proposed and studied [4, 5]. In [5, 7], a full diversity unitary space-time constellation has been designed by using complex 2x2 matrix representations.
of the quaternion algebra \( \{a_0 + a_1i + a_2j + a_3k \mid a_i \in \mathbb{R} \} \) over \( \mathbb{R} \). In this paper, another type of a unitary space-time constellation has been designed using representations of \( \mathcal{H} \) as a subalgebra of the algebra of the real 4x4 matrices.

The octonion algebra \( \mathcal{O} \), also called the Cayley algebra, is a non-associative alternative division algebra of dimension 8 over the field \( \mathbb{R} \) of real numbers.

Since a matrix algebra is always associative, the algebra \( \mathcal{O} \) cannot be embedded in the matrix algebra over \( \mathbb{R} \). However, \( \mathcal{O} \) can be embedded as a subspace \( \tilde{\mathcal{O}} \) of the space \( \mathcal{M}(\cdot) \) of the 8x8 real matrices, and then looking at some compatible identities between the operation on \( \tilde{\mathcal{O}} \) induced by a multiplication on \( \mathcal{O} \) and matrix multiplication, we design a constellation with a full diversity product.

Further, by using an \((L, n)\) cyclic code to get the maximum equidistant points on the sphere \( S^2 = \{x \in \mathbb{R}^4 \mid ||x|| = 1\} \), we get a constellation with a large diversity product. Apart from a real division normed algebra \( \mathcal{C}, \mathcal{H} \) and \( \mathcal{O} \) giving unitary constellations, there are several other non-associative division algebras over certain number fields which give rise to space-time block codes with full diversity.

2. QUATERNION ALGEBRA AND ITS REAL MATRIX REPRESENTATION

The real quaternion algebra is an associative algebra \( \mathcal{H} \) which is a 4-dimensional vector space over \( \mathbb{R} \) with the basis \( \{1, i, j, k\} \) and in which multiplication is subject to the relations \( 1.q = q, \) for all \( q \) in \( \mathcal{H} \), \( i^2 = j^2 = k^2 = -1, i = k \) and \( jk = 1 \) (and so \( j = -k \)). Clearly, \( \mathcal{H} \) is non-commutative. An arbitrary element \( q \) in \( \mathcal{H} \) is uniquely expressible as \( q = a_0 + a_1i + a_2j + a_3k \), \( a_i \in \mathbb{R} \). The conjugate \( \bar{q} \) of \( q \) is given by \( \bar{q} = a_0 - a_1i - a_2j - a_3k \). Clearly, \( \bar{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2 = ||q||^2 \) and the inverse \( q^{-1} \) of \( q \) is given by \( q^{-1} = \bar{q}/||q||^2 \). The left multiplication map \( f_q \) by \( q \) defined by \( f_q(h) = qh \) is a linear transformation from \( \mathcal{H} \) to \( \mathcal{H} \) which is invertible and the inverse is given by \( f_{\bar{q}} \). The matrix representation \( M(q) \) of \( f_q \) with respect to the basis \( \{1, i, j, k\} \) is given by

\[
M(q) = \begin{bmatrix}
  a_0 & -a_1 & -a_2 & -a_3 \\
  a_1 & a_0 & a_3 & -a_2 \\
  a_2 & -a_3 & a_0 & a_1 \\
  a_3 & a_2 & -a_1 & a_0 \\
\end{bmatrix}
\]

Since \( \mathcal{H} \) is an associative algebra, \( M \) defines an injective algebra homomorphism from \( \mathcal{H} \) to the full matrix algebra \( M_4(\mathbb{R}) \) of the 4x4 matrices with entries in \( \mathbb{R} \). Thus, \( \mathcal{H} \) is isomorphic to the subalgebra \( \{M(q) \mid q \in \mathcal{H}\} \) of \( M(\mathbb{R}) \). Another way to represent \( M(q) \) is as follows:

\[
M(q) = Q\text{Diag}(q, q, q, q)Q',
\]

where \( Q = \frac{1}{2} \begin{bmatrix} 1 & i & j & k \\ -i & 1 & k & -j \\ -j & -k & 1 & i \\ -k & j & -i & 1 \end{bmatrix} \)

The transpose conjugate of \( Q \) is a unitary 4x4 matrix over \( \mathcal{H} \). We also note that

\[
|\text{Det}(M(q))| = |q|^4 = (a_0^2 + a_1^2 + a_2^2 + a_3^2)^2
\]

It follows that every matrix \( M(q) \) is unitarily similar to a scalar matrix \( qI \) over \( \mathcal{H} \), and consequently, \( M(q) \) is unitary if and only if \( |q|=1 \).

3. QUATERNIONIC CONSTELLATION DESIGN

Consider \( \{M(q) \in \mathcal{H} : 0\} \). For all \( q \in \mathcal{H} : 0 \),

\[
|\text{Det}(M(q) - M(q'))| = |\text{Det} M(q - q')| = |q - q'|^4 > 0
\]

In turn, it follows that \( \{M(q) : q \in \mathcal{H} : 0\} \) is a constellation with a full diversity product. As a consequence, to construct a signal constellation \( X \) consisting of \( L \) 4x4 unitary matrices with the diversity product \( \xi_X \) as large as possible, we need to construct \( L \) points \( q_0, q_1, \ldots, q_{L-1} \) on the unit sphere \( S^3 \) in \( \mathbb{R}^4 \) so that

\[
\xi_X = \frac{1}{2} \min_{0<i<j\leq L-1} |\text{Det}(M(q_i) - M(q_j))|^{1/M} = \frac{1}{2} \min_{0<i<j\leq L-1} |q_i - q_j|^{4/M}
\]

is as large as possible. For that purpose, let us start with a point \( q_0 = (a_0, a_1, a_2, a_3) \) in \( S^3 \). For each \( k \) in \( Z_L = \{0, 1, 2, \ldots, L-1\} \), and for each \( i \) in \( Z_q \), consider the matrix

\[
A(i,k) = \begin{bmatrix}
  \cos\frac{2\pi i k}{L} & \sin\frac{2\pi i k}{L} & 0 & 0 \\
  -\sin\frac{2\pi i k}{L} & \cos\frac{2\pi i k}{L} & 0 & 0 \\
  0 & 0 & \cos\frac{2\pi k}{L} & \sin\frac{2\pi k}{L} \\
  0 & 0 & -\sin\frac{2\pi k}{L} & \cos\frac{2\pi k}{L} \\
\end{bmatrix}
\]

and the set \( X = \{q_iq_A(k, k) \mid i \in Z_q\} \) of \( L \) points in \( S^3 \). Then, since \( A(k,k) \) is orthogonal, we have

\[
|q_i - q_j|^2 = |q_0A_i(k, k) - q_0A_j(k, k)|^2
= |q_0 - q_0A_i(k, k)A_j(k, k)^{-1}|^2|^2
= |q_0 - q_0A_j(k, k)A_i(k, k)^{-1}|^2 = |q_i - q_j|^2 = 2(a_i^2 + a_j^2)\cos^2\frac{(j-i)\pi k}{L} + (a_i^2 + a_j^2)\cos^2\frac{(j-i)\pi k}{L}
\]

Thus,
\[ \min_{0 \leq i < j \leq l} |q_i - q_j|^2 = \min_{0 \leq i < j \leq l} |q_0 - q_i|^2 = \min_{0 \leq i < j \leq l} \left[ 2 - 2(a_1^2 + a_2^2) \cos \frac{\pi k_i}{L} + (a_3^2 + a_4^2) \cos \frac{\pi k_j}{L} \right] \]

(9)

It follows that the diversity product depends only on \(a_1^2 + a_2^2\) and \(a_3^2 + a_4^2\), where \(q_0 = (a_1, a_2, a_3, a_4)\), \(a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1\). Thus, we can conveniently start with \(q_0 = (b_1, 0, b_2, 0)\) with \(b_1^2 + b_2^2 = 1\), and then the points \(q_i\) in \(Z_L\) are given by

\[ q_i = (b_1 \cos \frac{2\pi k_i}{L}, -b_1 \sin \frac{2\pi k_i}{L}, b_2 \cos \frac{2\pi k_i}{L}, -b_2 \sin \frac{2\pi k_i}{L}) \]

and by (9),

\[ \min_{0 \leq i < j \leq l} |q_i - q_j|^2 = \min_{0 \leq i < j \leq l} [b_1^2 \sin^2 \frac{\pi k_i}{L} + b_2^2 \sin^2 \frac{\pi k_j}{L}] \]

(10)

Hence, by (6) and (10), the diversity product \(\xi_X\) of the constellation \(X = \{M(q_i) | i \in Z_L\}\) is given by

\[ \xi_X = 2 \min_{0 \leq i < j \leq l} |q_i - q_j|^2 \]

(11)

Thus, the diversity product

\[ \xi_X = 2 \min_{0 \leq i < j \leq l} \left[ a_1^2 \sin^2 \frac{\pi k_i}{L} + a_2^2 \sin^2 \frac{\pi k_j}{L} \right] \]

(12)

where \(a_1 = b_1^2, a_2 = b_2^2\) can be maximized subject to the condition \(a_1 + a_2 = 1, a_1, a_2 \geq 0\) and \(k_1, k_2\) in \(Z_L\), and corresponding \(a_1, a_2\) and \(k_1, k_2\) can be found.

Remark: Although the distance between any two points on unit spheres in any dimension is at most 2, we can find equidistant points with distances greater than 1. As such, the diversity product of the constellation described in this paper is larger than those other constellations based on quaternions [4, 5, 6].

4. OCTONIONS AND GENERALIZED MATRIX REPRESENTATION

The octonion algebra \(\mathcal{O}\) (also called the Cayley algebra) over \(\mathbb{R}\) is an 8-dimensional non-associative normed division algebra obtained by doubling a quaternion division algebra using the Cayley-Dickson process. Thus,

\[ \mathcal{O} = \mathcal{H} \oplus \mathcal{H} e = \{a + be | a, b \in \mathcal{H}\} \]

(13)

Here, \(a + be = 0 + 0e\) if and only if \(a = 0\) and \(b = 0\). Addition + and multiplication \(\cdot\) in \(\mathcal{O}\) is defined by

\[ (a + be) + (c + de) = (a + c) + (b + d)e \]

(14)

\[ (a + be) \cdot (c + de) = (ac - \bar{d}b) + (da + bc)e \]

(15)

Obviously, \(\mathcal{H}\) is embedded through \(a \rightarrow a + 0e\) as a subalgebra of \(\mathcal{O}\). Denote \(i, j, k, e, f, g, h\) respectively. Then \(B = \{1, i, j, k, e, f, g, h\}\) is a basis of \(\mathcal{O}\) and an arbitrary element \(u \in \mathcal{O}\) has a unique representation as follows:

\[ u = a_0 1 + a_1 i + a_2 j + a_3 k + a_4 e + a_5 f + a_6 g + a_7 h \]

Further, 1 acts as a multiplicative identity; the square of each element of \(\mathcal{O}\) is -1. Indeed, the product of any two elements of \(\mathcal{O}\) is given by the following multiplicity Table 1.

Table 1: Multiplication

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>i</td>
<td>j</td>
<td>k</td>
<td>e</td>
<td>f</td>
<td>g</td>
<td>h</td>
</tr>
<tr>
<td>i</td>
<td>i</td>
<td>-1</td>
<td>k</td>
<td>-j</td>
<td>f</td>
<td>-e</td>
<td>-h</td>
<td>g</td>
</tr>
<tr>
<td>j</td>
<td>j</td>
<td>-k</td>
<td>i</td>
<td>g</td>
<td>h</td>
<td>-e</td>
<td>f</td>
<td>-j</td>
</tr>
<tr>
<td>k</td>
<td>k</td>
<td>j</td>
<td>-i</td>
<td>-1</td>
<td>h</td>
<td>g</td>
<td>-e</td>
<td>f</td>
</tr>
<tr>
<td>e</td>
<td>e</td>
<td>-f</td>
<td>-g</td>
<td>-h</td>
<td>-i</td>
<td>j</td>
<td>k</td>
<td>1</td>
</tr>
<tr>
<td>f</td>
<td>f</td>
<td>e</td>
<td>-h</td>
<td>g</td>
<td>-i</td>
<td>-k</td>
<td>j</td>
<td>1</td>
</tr>
<tr>
<td>g</td>
<td>g</td>
<td>h</td>
<td>E</td>
<td>-f</td>
<td>-j</td>
<td>k</td>
<td>-1</td>
<td>-i</td>
</tr>
<tr>
<td>h</td>
<td>h</td>
<td>-g</td>
<td>F</td>
<td>e</td>
<td>-k</td>
<td>j</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

For all \(a, b \in \mathcal{O}\). It is also \(|a|\) normed algebra in the sense that

\[ |ab| = |a||b| \]

(16)

for all \(a, b \in \mathcal{O}\), where \(|a|\) denotes the Euclidean norm

\[ a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2 \]

of \(a\). For \(a \in \mathcal{O}\), left multiplication \(f_a\) from \(\mathcal{O}\) to \(\mathcal{O}\) defined by \(f_a(x) = ax\) is a linear transformation from \((\cong \mathbb{R}^8)\) to and since \(\mathcal{O}\) is a normed algebra,

\[ |f_a(x)| = |a||x| \]

for all \(x\). Thus, for a in the 7-sphere \(S_7\), \(f_a\) preserves length and so it is an orthogonal transformation. Let us denote matrix representation of \(f_a\) with respect to the basis \(B\) (which is an orthonormal basis) by \(M(a)\). Then,
Since $f_a$ is an orthogonal transformation, $M(a)$ is an orthogonal matrix for all $a$ in $S^7$. The map $M$ is clearly an injective map from $O$ to the set $M(\cdot)$ of $8 \times 8$ matrices, which takes $S^7$ to the orthogonal group $O(8)$. Also, since multiplication in $O$ distributes over addition, multiplication in $S$ unit sphere which takes $S$ to the orthogonal group $O(8)$. The identity

$$M(ab) = M(a) M(b)$$

is immediate, and it follows from (16). A straightforward computation establishes the following:

$$M(aba) = M(a) M(b) M(a)$$

(20)

and non-associative

$$\det M(a) = |a|^8$$

(21)

for all $a, b$ in $O$. In particular, $M(a)$ is an orthogonal matrix if and only if $a$ is in the $7$-sphere $S^7$.

5. OCTONION CONSTELLATION DESIGN

As in Section 3, it follows from equations (18), (19) and (21) that the set $\{M(a) \mid a \in O\}$ is a constellation with a full diversity product. Further, as in Section 3, starting from a point $u_0 = (b_0, 0, b_0, 0, b_0, 0, b_0, 0)$ in the unit sphere $S^7 \subseteq O$ and $k_i, k_j, k_k, k_l$ in $Z_2$, the points

$$u_i = b_0 \cos \frac{2\pi k_i}{L}, -b_1 \sin \frac{2\pi k_1}{L}, b_2 \cos \frac{2\pi k_2}{L},$$

$$-b_2 \sin \frac{2\pi k_2}{L}, b_3 \cos \frac{2\pi k_3}{L}, -b_3 \sin \frac{2\pi k_3}{L}, b_4 \cos \frac{2\pi k_4}{L},$$

$$-b_4 \sin \frac{2\pi k_4}{L} - b_4 \sin \frac{2\pi k_4}{L}$$

determine the constellation $X = (M(u) \mid l \in Z_2$ with the diversity product:

$$\xi_X = 2 \min_{a \in O(8)} \left[ a_1^2 + a_2^2 \sin \frac{\pi k_2}{L} + a_3^2 \sin \frac{\pi k_3}{L} + a_4^2 \sin \frac{\pi k_4}{L} \right] / M, \quad a_i = b_i^2.$$

Further, it can be maximized subject to the condition $a_i + a_j + a_k + a_l = 1, a_i \geq 0$, and the corresponding $a_i$ and $k_i$ can be found to yield a constellation with a large diversity product compared to the one given by equation (12).

6. FULL DIVERSITY CONSTELLATION USING OTHER NON-ASSOCIATIVE STRUCTURES

Let $F$ be a field of characteristic different from 2 and let $K$ be a quadratic field extension of $F$. More explicitly, $K = \mathbb{Q}(\sqrt{2}) = \{u + v\sqrt{2} \mid u, v \in F\}$ for some $a_i$ in $F$ such that the polynomial $X^2 - a_i$ is irreducible in $F[X]$. Evidently, $K$ is a Galois extension of $F$. The map $\alpha$ from $K$ to $K$ given by $\alpha(u + v\sqrt{2}) = u - \sqrt{2} \alpha(v)$ is a unique nontrivial non-associative $K$-automorphism of $K$. Let $b_0 = u_0 + \sqrt{2} v_0$ be a nonzero element of $K\{0\}$ different from $\sqrt{2}$. Let $A$ denote the 4-dimensional vector space $K \times X$ over the field $F$. Using the Cayley-Dickson process, define the multiplication $\cdot$ in $A$ by

$$(k_1, k_2) \cdot (k_3, k_4) = (k_1 k_3 + b_0 k_4 \sigma(k_2), \sigma(k_1 k_4 + k_3 k_2)), \quad (23)$$

where $k_i, k_j, k_k, k_l$ belong to $K$. It can be easily shown that $A$ is a 4-dimensional algebra over $F$ which is a division (not necessarily associative) over $F$ if and only if $b_0$ cannot be expressed as $u^2 - \sigma(v)^2, u, v \in F$. It is associative provided that $b_0$ is in $F$ and non-associative otherwise. Note that

$$(k_1, k_2) \cdot (k_1, 0) \cdot (0, k_2) = (k_1, 0) \cdot (0, k_2).$$

The correspondence $k \mapsto (k, 0)$ is an injective embedding of $K$ as a subfield of the algebra $A$ and if we identify $k$ with $(k, 0)$ and put $j = (0, 1)$, then any element $(k_i, k_j)$ of $A$ has a unique representation as $k_i + k_j k$. Further, for the sake of simplicity, if we put $i = 0$ for $a_i$, then any element $k$ of $K$ can be written uniquely as $u + iv$, where $u, v \in F$. Again, as in the case of a classical quaternion algebra, if we put $ij = k$, any element $a$ of $A$ has a unique representation: $a = a_0 + a_1 i + a_2 j + a_3 k$.

Thus, $A$ is a 4-dimensional division algebra with the basis $(1, i, j, k)$ over $F$ subject to the relation $i^2 = a_0 j^2 = b_0 = u_0 + v_0 \sqrt{2}$, $ij = ji$ and, of course, 1 acting as an identity. It is associative if and only if $b_0 \in F$. Matrix representation $M(a)$ of right multiplication $f_a$ determined by a with respect to the basis $(1, i, j, k)$ can be seen as:

$$M(a) = \begin{bmatrix}
    a_0 & a_1 & a_0 + a_1 i & -a_0 - a_1 i \\
    a_1 & a_0 & a_0 + a_1 i & -a_0 - a_1 i \\
    a_2 & a_3 & a_2 + a_3 j & a_2 - a_3 j \\
    a_3 & a_2 & a_2 + a_3 j & a_2 - a_3 j
\end{bmatrix} \quad (24)$$
It follows that the matrix representation map $M$ is an injective vector space homomorphism from $\mathcal{A}$ to the vector space $M(\mathcal{F})$ of the 4x4 matrices with entries in $\mathcal{F}$. Thus, $M(a-b) = M(a) - M(b)$. Further, since $\mathcal{A}$ is a division algebra, the map $f_a$ is a vector space automorphism of $\mathcal{A}$ for all nonzero $a$ in $\mathcal{A}$. Hence, $M(a)$ has a nonzero determinant for all nonzero $a$ in $\mathcal{A}$. This shows that the constellation $\{M(a) | a \in \mathcal{A} - \{0\}\}$ is with the full diversity code. Starting from a suitable number field and a suitable choice of elements $a_0, u_0$ and $v_0$ in the number field and restricting to lie in $O_K \times O_K \subseteq A$, where $O_K$ denotes the ring of integers of $\mathcal{K}$, we can get constellations with good diversity products.

7. RESULT

The choice of non-associative structure increases the diversity product and thereby minimizes the probability of error. The coding used is more efficient. We have several choices of the non-associative structure as given above which can be used for this purpose.

8. CONCLUSION

The purpose of this paper is to initiate and develop space-time codes satisfying rank criteria and coding gain criteria for a multiple antenna-based wireless communication using generalized matrix representations of a non-associative group like structures for secured transmission. In future, more and more non-associative algebraic structures can be used to have more effective and useful space-time coding in different dimensions.

9. REFERENCES


