RANK CODES OVER GAUSSIAN INTEGERS AND SPACE TIME BLOCK CODES

Hafiz M.Asif, Ernst Gabidulin, Bahram Honary

Abstract: *Maximum rank distance (MRD) codes have been used for the construction of space time block code (STBC) using a matrix method. Like orthogonal STBC's in most popular cases, MRD-STBC's can also achieve full diversity. Though an OSTBC is known to yield the best BER performance, a unique case is described where MRD-STBC performs better than Alamouti code (OSTBC). Moreover, the viability of Gabidulin's decoding algorithm has been established by decoding complex symbols generated from MRD-STBC's. Under this decoding scheme, MRD-STBC's have been shown to be preferred candidate for higher antenna configuration as the decoding complexity of Gabidulin's algorithm is far less than that of maximum likelihood (ML) decoding algorithm.*

Keywords: *Rank codes, Gaussian integers, space time block codes, orthogonal space time block codes.*

MSC*: 12E20*

Introduction

The design of error-correcting codes for two dimensional signal spaces has been widely considered. Different authors have constructed new error-correcting codes over quotient rings of Gaussian integers by using the Mannheim measure as it was introduced in [Huber, 1994]. Complex constellations based on graphs allow to construct rank codes over Gaussian integers. In turn, such codes can be used as space time block codes.

The idea of exploiting transmit diversity was introduced by Vahid Tarokh et al. [Tarokh et al., 1998] and it was later on adopted for much simpler structure by Alamouti [Alamouti, 1998]. His work was later on extended and formally developed to originate space time block codes (STBC) [Tarokh et al., 1999]. In addition, for 2×1 scenario, Alamouti code achieves full diversity gain. In [Lusina et al., 2003], the application of rank codes for forming STBC was introduced. Rank codes [Gabidulin, 1985], due to rank distance property, make themselves useful candidate for STBC's. The construction of rank codes is presented based on direct matrix method as MRD-STBC's. MRD-STBC codes performs better than orthogonal STBC (OSTBC) under certain criteria. Moreover, little work was found on decoding MRD-STBC except ML scheme which is extremely complex for higher antenna configuration. Therefore, first, the idea of using interleaved MRD codes ($\mathcal{I}$) is introduced to construct MRD-STBC's for $N_{tx} > 4$. Second, a decoding algorithm has been described that can effectively decode MRD-STBC.

The Gaussian integers

The set $\mathbb{Z}[i]$ of *Gaussian integers* is the subset of the complex numbers $\mathbb{C}$ with integer real and imaginary parts, i.e.,

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}.$$

If $0 \neq \pi = u + vi \in \mathbb{Z}[i]$, then we denote, $\mathbb{Z}[i]_\pi$, the ring of the classes of $\mathbb{Z}[i]$ modulo the ideal (π) generated by π. Therefore, we write $\beta \equiv \beta' \pmod{\pi}$ if β and β' belong to the same class modulo (π). It is well known that the cardinality $\mathcal{N}$ of $\mathbb{Z}[i]_\pi$ equals $\mathcal{N} = u^2 + v^2$. From now on, we consider the case when $0 < u < v$ and $u^2 + v^2 = p \equiv 1 \pmod{4}$, p is a prime. $\mathcal{Z}_\pi$ is a set of representatives of the residue classes $\mathbb{Z}[i]_\pi$. These constellations have been previously modeled by quotient rings of Gaussian integers, [Huber, 1994], [Costa et al., 2004], [Nóbrega et al., 2001]. Constellations and the metric based on associated graphs were introduced in [Martínez et al., 2005]. We denote by $\mathcal{MZ}_\pi$ the constellation defined by K.Huber [Huber, 1994] and by $\mathcal{GZ}_\pi$ the constellation based on graphs. In general, for a given π they are different as well as associated metrics.

The Mannheim constellation $\mathcal{MZ}_\pi$

For a given π and any Gauss integer $\alpha = a + bi$, define the projection α on $\mathcal{MZ}_\pi$ as $\rho_\alpha := \alpha - q_\alpha \pi$ where,

$$q_\alpha := \left[\frac{\alpha\overline{\pi}}{p}\right].$$

The operation $[c + di]$ denotes rounding in Gaussian integers and is defined by $[c + di] = [c] + [d]i$ with $[c]$ denoting rounding to the closest integer.
Next statements are evident.

1. $\rho_\alpha(\rho_\alpha) = \rho_\alpha$.

2. The Mannheim set $\mathcal{MZ}_\pi$ is the image of the set $\{0, 1, \ldots, p-1\}$ under the projection ρ_*.

3. For any $\alpha \in \mathcal{MZ}_\pi$, $\rho_\alpha = \alpha$.

For $\alpha = a + bi \in \mathcal{MZ}_\pi$, the Mannheim weight is defined by $w_M(\alpha) = |a| + |b|$. For any $\alpha = a + bi$, the Mannheim weight is defined by $w_M(\alpha) = w_M(\rho_\alpha)$. The Mannheim distance between two elements α and β in $\mathbb{Z}[i]_\pi$ is defined as $d_M(\alpha, \beta) = w_M(\alpha - \beta)$. In fact, the Mannheim distance is not true distance as it was shown first by example in [Martínez et al., 2005]. We give more general explanations.
Let $\pi = u + vi,\ 0 < u < v,\ u^2 + v^2 = p$. Introduce

$$r = \frac{v+u-1}{2},\ \ m = v - r = \frac{v-u+1}{2},\ \ \&\ \ s = \left\lfloor \frac{v(u-1)-u^2}{2v} \right\rfloor.$$

Lemma 1. *Let p be a prime such that $u = 1$, or, $u = v - 1$. Then the Mannheim distance is a true distance.*

Proof. In this case the sets $\mathcal{MZ}_\pi$ and $\mathcal{GZ}_\pi$ associated metrics coincide. The proof for the graph based metric can be used (see, [Martínez et al., 2005]). □

Theorem 1. *Let p be a prime such that $u \neq 1$ and $u \neq v - 1$. Then the Mannheim distance is* ***not*** *a true distance. More precisely, it does not fulfil the triangular inequality.*

Proof. First show that $v(u-1) > u^2$. Since $u \neq v - 1$, it follows that $u \leq v - 2$. It is impossible that $u = v - 2$ since the left and the right parts must have the different parity. Hence $u \leq v - 3,\ v \geq u + 3$. If we assume that $v(u-1) < u^2$, we obtain $v < u + 1 + 1/(u-1)$, or, $v \leq u + 1$ with contradiction to $v \geq u + 3$. Therefore the integer s introduced above is non negative.
For a true distance function and any three elements x, y, z must be $d(x, z) \leq d(x, y) + d(y, z)$ (the triangular inequality). We present three elements $x, y, z \in \mathcal{MZ}_\pi$ such that $d_M(x, z) > d_M(x, y) + d_M(y, z)$. Namely, let $x = u + (m+s)i,\ y = -i,\ z = 0$. By direct calculation, one can show that $\rho_x = x$. Hence all three x, y, z are in $\mathcal{MZ}_\pi$. We have $d_M(x, z) = w_M(x - z) = w_M(x) = u + m + s$ and $d_M(y, z) = w_M(y - z) = w_M(-i) = 1$. Also we have $x - y = u + (m + s + 1)i$ and by direct calculation $\rho_{x-y} = x - y - \pi = -(v - m - s - 1)i$. Thus $d_M(x, y) = w_M(x - y) = w_M(\rho_{x-y}) = w_M(-(v - m - s - 1)i) = v - m - s - 1$. Finally, $d_M(x, z) - d_M(x, y) - d_M(y, z) = u + m + s - v + m + s = 1 + 2s > 0$. The triangular inequality fails. □

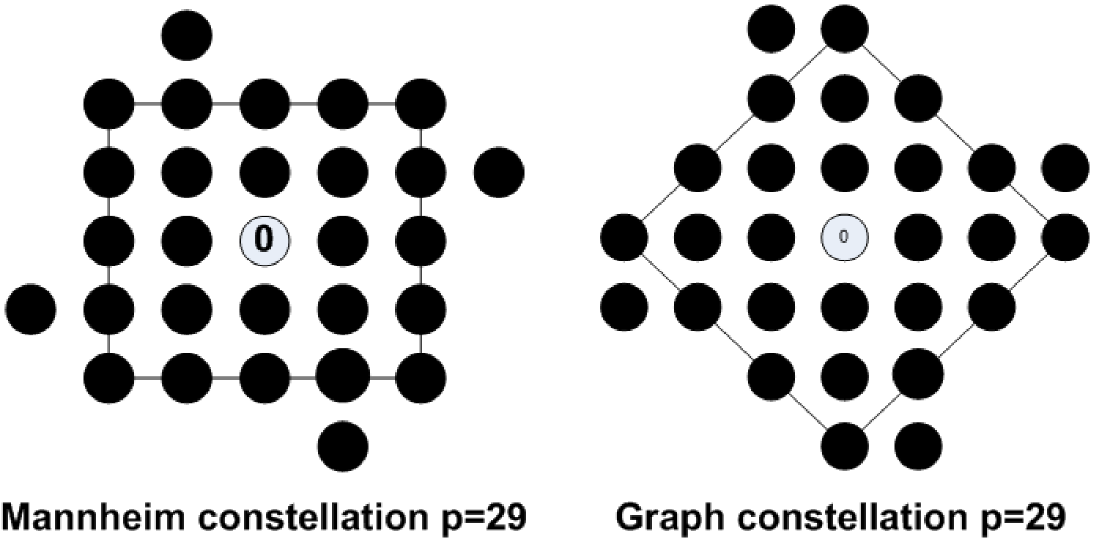

Figure 1: Constellations $\mathcal{Z}_{2+5i}, p = 29$.

The graph constellation $\mathcal{GZ}_\pi$

For $\beta, \gamma \in \mathbb{Z}[i]_\pi$, consider $x + yi$ in the class of $\beta - \gamma$ with $|x| + |y|$ minimum. The distance D_π between β and γ is $D_\pi(\beta, \gamma) = |x| + |y|$. This distance function is called the graph distance since it coincides with the distance function of the following graph.

Given $\pi = u + vi \in \mathbb{Z}[i]$ we define the graph $G_\pi = (V, E)$ where:

1. $V = \mathbb{Z}[i]_\pi$ is the node set, and
2. $E = \{(\beta, \gamma) \in V \times V \mid D_\pi(\beta, \gamma) = 1\}$ is the edge set.

We call G_π the Gaussian Graph generated by π.

The constellation $\mathcal{GZ}_\pi$ consists of Gaussian integers in the square with vertices $(ri, r, -ri, -r)$ and in four triangles with vertices $(r+i, r+(m-1)i, r-m+2+(m-1)i)$, $(-r-i, -r-(m-1)i, -(r-m+2)-(m-1)i)$, $(ri-1, ri-m+1, (r-m+2)i-m+1)$, $(-ri+1, -ri+m-1, -(r-m+2)i+m-1)$. Constellations $\mathcal{MZ}_\pi$ and $\mathcal{GZ}_\pi$ are presented below for $\pi = 2 + 5i, p = 2^2 + 5^2 = 29$.

Rank codes over Gaussian integers

The constellation $\mathcal{GZ}_\pi$ can be considered as a representation of the finite field $GF(p)$. Extension fields of degree n over Gaussian integers can be represented as n-tuples of $\mathcal{GZ}_\pi^n$. Also they can be defined in the matrix representation. Let $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ be a primitive polynomial over $GF(p)$. Then the companion matrix

$$M_n = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & 1 \\ -f_0 & -f_1 & -f_2 & \ldots & -f_{n-2} & -f_{n-1} \end{bmatrix} \tag{1}$$

represents a primitive element of the extension field $GF(p^n)$. Matrices $M_n^i,\ i = 1, \ldots, p^n - 1$, represent all non zero elements of the extension field. To obtain an extension field over $\mathcal{GZ}_\pi$, one can replace each entry by corresponding value of $\mathcal{GZ}_\pi$. Afterwards all matrix operations should be fulfilled modulo π.

Example. Let $\pi = 1 + 2i,\ p = 5$. Then $\mathcal{GZ}_\pi$ consists of $\{0, \pm 1, \pm i\}$. Let $f(x) = x^2 + x + 2$ be the primitive polynomial over $GF(5)$. We have,

$$M_2 = \begin{bmatrix} 0 & 1 \\ -2 & -1 \end{bmatrix},\ M_2^2 = \begin{bmatrix} -2 & -1 \\ 2 & -1 \end{bmatrix}, \ldots, M_2^{23} = \begin{bmatrix} 2 & 2 \\ 1 & 0 \end{bmatrix},\ M_2^{24} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The corresponding matrices over $\mathcal{GZ}_\pi$ are as follows:

$$\widetilde{M_2} = \begin{bmatrix} 0 & 1 \\ -i & -1 \end{bmatrix},\ \widetilde{M_2^2} = \begin{bmatrix} -i & -1 \\ i & -1 \end{bmatrix}, \ldots, \widetilde{M_2^{23}} = \begin{bmatrix} i & i \\ 1 & 0 \end{bmatrix},\ \widetilde{M_2^{24}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

A rank code with rank distance d is a set of $n \times n$ matrices over $GF(p)$ such that the difference of two code matrices has rank not less than d. This property holds true, if elements of $GF(p)$ are replaced by elements of $\mathcal{GZ}_\pi$.

Rank codes as space time codes

Code construction

It was investigated that if a linear code of block size 4 is formed in such a way that the absolute value of the determinant of each pairwise difference is equal to 4 then rank code (and all its coset codes) performs better than Alamouti code. The construction of such is described as follows.

Let $x^2 + x + 1$ be a primitive irreducible polynomial over GF(2), then the elements of $GF(2^2)$ form an MRD code of block size 4. The direct matrix construction (using Eq.(1)) is obtained as follows: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Having mapped 0 to 1 and 1 to -1 (BPSK), the code becomes $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$, $\begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}$, $\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}$.

Two important observations can be made on the above MRD; (1) The sum of square modules in each is equal to 4 and (2) The absolute value of the determinant of each pairwise difference is equal to 4. From physical point of view, the first condition is a transmitting power for a matrix while the second condition is a measure of difference between code matrices.

Next we consider orthogonal STBC (OSTBC) construction and select four such codes which fulfil the above mentioned two properties.

Let $G = \{0, 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{14}\}$ be an additive group of 16 elements. Let $G_S = \{0, 1, \alpha, \alpha^2\}$ be a subgroup of G comprising 4 elements. The first coset of G_S is equal to G_S, i.e., addition of 0 to G_S which in turn yields G_S. Now, 16 different Alamouti codes (16 blocks) can be constructed out of which the following four are selected: $\begin{bmatrix} 0 & -0^* \\ 0 & 0^* \end{bmatrix}$, $\begin{bmatrix} 0 & -\alpha^* \\ \alpha & 0^* \end{bmatrix}$, $\begin{bmatrix} \alpha^2 & -1^* \\ 1 & \alpha^{2^*} \end{bmatrix}$, $\begin{bmatrix} 1 & -1^* \\ 1 & 1^* \end{bmatrix}$.

The symbol $\{.\}^*$ indicates conjugate of the element. It can easily be verified that the blocks are orthogonal blocks (i.e., the determinant is identity matrix). After modulation or the mapping $(0, 1, \alpha, \alpha^2)$ to $(1, j, -1, -j)$, which has been selected by exhaustive search approach, we obtain: $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$, $\begin{bmatrix} -j & j \\ j & j \end{bmatrix}$, $\begin{bmatrix} j & j \\ j & -j \end{bmatrix}$.

It can be checked the above four OSTBC blocks satisfy the above mentioned two conditions. Hence, the two sets, each of 4 different 2×2 block, can be compared.

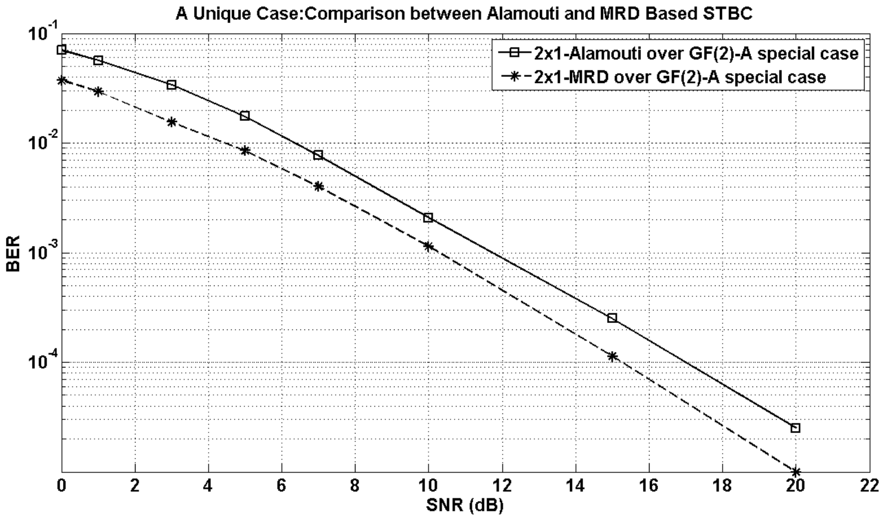

Figure 2: Orthogonal codes vs. MRD over GF(2^2) for 2×1 scenario

Simulation analysis

Simulation was carried out for comparing all described configurations of MRD with the corresponding OSTBC's described in the previous section. 2×10^5 symbols per SNR value were transmitted in each case.

The channel matrix H_C was calculated based on Rayleigh fading. The received signal y is calculated as $y = H_C c + n$, where c is the transmitted block code (2×2) and n is $AWGN$. Maximum likelihood decoding was used to decode the transmitted symbols in both cases (MRD and orthogonal). Each received signal is compared against all possible blocks ($q^{N_{tx}}$) to select the block with minimum error, i.e., with minimum Euclidean distance.

Fig.2 shows BER performance comparison of 2×1 OSTBC and 2×1 MRD-STBC which were designed based on the construction given in Section . First, it is important to note that MRD-STBC achieves full rate diversity because its slope is parallel to that of OSTBC. Second, there is a coding gain of about 1.8 dB over OSTBC which can further be multiplied by using different primitive polynomial or so. It is to be noted that OSTBC performs better than MRD-STBC for general case, i.e., if the above two conditions are not fulfilled.

Rank codes, when used as complex symbols, may lose the rank of the code block if traditional modulation schemes, such as $n - PSK$, are applied. As mentioned earlier, Gaussian integers can be used to map rank codes to corresponding complex constellations. In what next follows we describe how Gaussian integers can improve MRD-STBC's performance to some extent, especially in low SNR region, in two systems, i.e., 3×3 and 5×5 systems over GF(5^3) and GF(5^5) respectively.

3 MRD-STBC over GF(5^3)

Let $x^3 + 3x + 2$ be the primitive polynomial of degree 3, where the coefficients of the polynomial are from GF(5). Then the first non-zero companion matrix, with extension degree 3, can be written as follows (i.e., the elements of GF(5^3):

$$C = \begin{bmatrix} 0 & 0 & 3 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix}$$

Let β be a root of the above polynomial then the above companion matrix, in vector form, is as follows:

$$C_{vec} = G = \begin{bmatrix} \beta & \beta^2 & \beta^3 \end{bmatrix} \tag{2}$$

where,

$\beta^3 = 2x + 3$ and note that it is our generator matrix, G, as well. We can calculate the corresponding parity check matrix, H, by using the relationship $GH^T = 0$. The corresponding calculated H is as follows:

$$H = \begin{bmatrix} h_1 & h_2 & h_3 \\ h_1^5 & h_2^5 & h_3^5 \end{bmatrix} = \begin{bmatrix} 1 & \beta^{103} & \beta^{98} \\ 1 & \beta^{19} & \beta^{118} \end{bmatrix} \tag{3}$$

Afterwards, MRD-STBC symbols are mapped to complex domain using Gaussian integers, and finally Gabidulin's decoding was applied on the received signal which will be discussed shortly.

5 MRD-STBC over GF(5^5)

Let $x^5 + 2x^4 + 2x^2 + x + 2$ be the primitive polynomial of degree 5, where the coefficients of the polynomial are from GF(5). Then the first non-zero companion matrix, with extension degree 5, can be written as follows (i.e., the elements of GF(5^5)):

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 \end{bmatrix}$$

Let β be a root of the above polynomial then the above companion matrix, in vector form, is as follows:

$$C_{vec} = G = \begin{bmatrix} \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 \end{bmatrix} \tag{4}$$

where,

$\beta^5 = 3x^4 + 3x^2 + 4x + 3$ and note that it is our generator matrix, G, as well. The corresponding parity check matrix (H) is as follows:

$$H = \begin{bmatrix} h_1 & h_2 & h_3 & h_4 & h_5 \\ h_1^5 & h_2^5 & h_3^5 & h_4^5 & h_5^5 \\ h_1^{25} & h_2^{25} & h_3^{25} & h_4^{25} & h_5^{25} \\ h_1^{125} & h_2^{125} & h_3^{125} & h_4^{125} & h_5^{125} \end{bmatrix} = \begin{bmatrix} 1 & \beta^{3011} & \beta^{1464} & \beta^{1459} & \beta^{2348} \\ 1 & \beta^{2559} & \beta^{1072} & \beta^{1047} & \beta^{2368} \\ 1 & \beta^{299} & \beta^{2236} & \beta^{2111} & \beta^{2468} \\ 1 & \beta^{1495} & \beta^{1808} & \beta^{1183} & \beta^{2968} \end{bmatrix} \tag{5}$$

Interleaved MRD

A 4×1 MRD-STBC code can easily be constructed for 4 transmit antennas, i.e., $N_{tx} = 4$. In order to increase the code length N_{tx} to certain extent, we can use a direct concatenation of consecutive M matrices such that the concatenated code is also a unique MRD [Sidorenko and Bossert, 2010], i.e.,

$$\mathcal{I} = \left[M^{(1)}\, M^{(2)}\, M^{(3)} \ldots M^{(i)} \right], \;\; M^i \in \mathcal{M}, \tag{6}$$

Algorithm 1 Decoding MRD-STBC $(q^m; n, k, d)$

```
1: Input: Received y ∈ GF$(q^m)^{N_{tx}}$
2: Demodulate received signal, $y$, use Eq.(7) to nullify channel effect and then write the result in vector form.
3: Compute syndrome $s = yH^T$ where $H$ is parity check matrix.
4: Compute matrix $M_i$ using Eq.(8) such that $M_i \neq 0$ starting with $i = t, t-1, ...$. The value of $i$ determines rank of the error vector, $m$.
5: Solve Eq.(9) to find $\sigma_i \; \forall \; i = 0, 1, \ldots, m-1$, where $m$ =rank of the error vector. Also, write $\sigma(x)$ as shown by Eq.(10).
6: Solve Eq.(10) using Berlekamp-Massey type algorithm [Berlekamp, 1968] in order to find $m$ number of roots of this equation. Represent these roots as $z_1, z_2, \ldots, z_m$.
7: Solve Eq.(11) for any value of $i$ to find $E_i$, where $i = 1, 2, \ldots, m$.
8: Solve Eq.(12) using again Berlekamp-Massey algorithm to find $Y$.
9: Calculate error vector, $e$, using Eq.(13).
10: Codeword $c = y - e$ or decoding failure
11: If success, write $c$ again in matrix form to find BER etc.
```

where M is defined by Eq.(1) and $i = 1, 2, 3 \ldots, i$ is the *interleaving order*. The matrix $\mathcal{I}$ is known as interleaved MRD code [Sidorenko and Bossert, 2010]. Based on this definition, three MRD-STBC's were constructed for $N_{tx} = 4, 8,$ and 12 respectively. Finally, the advantage of using $\mathcal{I}$ codes is to increase the error-correction ability of the algorithm while the time complexity of the algorithm becomes $\mathcal{O}(id_r^2)$ (i is the interleaving order) which is still better than ML decoding. If d_r be the rank distance, then number of errors that can be corrected (t) in $\mathcal{I}$ code, for i interleaving order, is $i(i+1)/(d_r-1)$ [Sidorenko and Bossert, 2010]:

Decoding 4×1 MRD-STBC using Gabidulin's algorithm

In this section, it is presented how Gabidulin's algorithm [Gabidulin, 1995] can be used to decode MRD-STBC which is symbolically written as MRD$(q^m; n, k, d)$. The complete steps of the algorithm to decode STBC blocks have been shown in Algorithm I.

Followings are the equations which have been referred to in Algorithm 1:

$$y_{rec} = H^\top(c+n) = c + H^\top n \quad H \; is \; parity \; check \; matrix. \tag{7}$$

$$M_i = \begin{bmatrix} s_0 & s_1^{2^{-1}} & \ldots & s_{i-1}^{2^{-i+1}} \\ s_1 & s_2^{2^{-1}} & \ldots & s_i^{2^{-i+1}} \\ \vdots & \vdots & \vdots & \vdots \\ s_{i-1} & s_i^{2^{-1}} & \ldots & s_{2i-2}^{2^{-i+1}} \end{bmatrix}. \tag{8}$$

$$(\sigma_0, \sigma_1, ..., \sigma_{m-1})M_m = -\left[s_m, s_{m+1}^{2^{-1}}, ...s_{2m-1}^{2^{-m+1}}\right]. \tag{9}$$

$$\sigma(x) = \sum_{i=0}^{m} \sigma_i x^{2^i}, \; \sigma_m = 1. \tag{10}$$

$$\sum_{j=1}^{m} E_j z_j^{2^i} = s_i, \quad i = 0, 1, ..., d-2. \tag{11}$$

$$Z^t = YH^t. \tag{12}$$

$$e = EY. \tag{13}$$

The complexity of this decoding algorithm is $\mathcal{O}(d_r^2)$ where $d_r = n - k + 1 = 4$ is the rank distance of the code. It guarantees to correct all errors with rank $\leq \lfloor \frac{d_r - 1}{2} \rfloor$ [Sidorenko and Bossert, 2010]. It can easily be seen that the decoding complexity is far less than that of ML decoding which runs full search and compares all possible

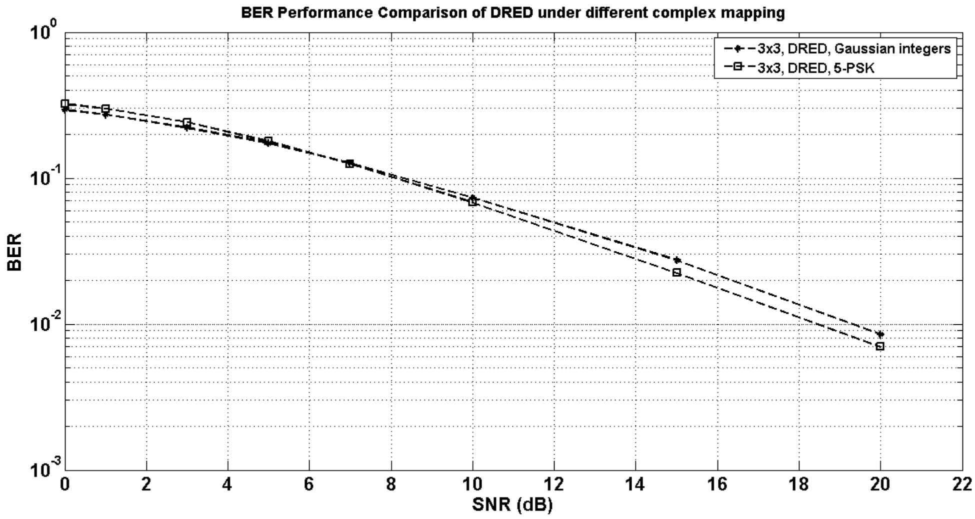

Figure 3: Gaussian integers vs 5-PSK for mapping 3×3 MRD-STBC.

combinations, i.e., $\mathcal{O}(q^{N_{tx}})$ where N_{tx} is the number of transmitting antennas. Furthermore, Interleaved MRD codes ($\mathcal{I}$) that have been used to construct $N_{tx} > 4$ STBC's are based on MRD-STBC for $N_{tx} = 4$, i.e., for $N_{tx} = 8$, and $N_{tx} = 12$.

First, simulation was run to analyze the performance of 3×3 and 5×5 mentioned above. Gaussian integers were used to map the blocks to complex symbols. At the receiver, Gabidulin's decoding algorithm was used to decode the symbols. 2×10^5 symbols per SNR value were transmitted in each case. The noise was AWGN and Rayleigh fading was used to model channel response of the system. Fig.3 shows performance curves for 3×3 MRD-STBCs that were constructed according to the above described procedure. The system was first modulated by $5 - PSK$ followed by Gaussian integers mapping. The figure shows the comparison of MRD-STBCs under two complex mapping schemes. It is evident from the figure that slight performance gain can be obtained in low SNR region by the use of Gaussian integers. The rank conservation property is better maintained by these integers in low SNR region. Furthermore, it is also clear from the graph that the gain reduces with the increase in SNR and Gaussian integers do not perform well for high SNR values. More or less, the same can be said for 5×5 system as depicted in Fig.4. Further experiments are required to investigate these integers for modulation. For instance, Gaussian integers over different fields (GF(7), GF(11) etc.) may produce better results. These investigations are left for future work.

Second, simulation was carried out to assess the viability of Gabidulin's decoding scheme for MRD-STBC especially under higher antenna configuration due to its low complexity. Because Gabidulin's decoding scheme requires vector form to function, 4×4 MRD-STBC has been constructed to exhibit 4-transmit antenna configuration. The 4-receiving antennas increase the rank of the channel matrix and thus help to nullify channel effect and convert received symbols in a vector for the decoding scheme. In a similar fashion, 8×4, and 12×4 MRD-STBC's were constructed using interleaved MRD codes represented by Eq.6.

Fig.5 shows BER comparison of 4×4, 8×4, and 12×4 MIMO systems. In each case, Gabidulin's algorithm was used to decode recovered received symbols. We can see a gradual performance improvement due to $\mathcal{I}$ codes with incremental increase in interleaving order. From the curves in Fig.5, we can see that almost over 1.5dB gain of 12×4 system is observed over 8×4 system. Similarly, there is a gain of 4dB of 12×4 over 4×4 system. The performance will be much better if the same system is decoded using ML scheme but decoding complexity increases significantly. Asymptotically, Gabidulin's algorithm is far better than ML decoder because its complexity is $\mathcal{O}\left(d_r^2\right)$ whereas that of ML is $\mathcal{O}\left(q^{N_{tx}}\right)$. This implies that (1) ML is not suitable to delay sensitive applications or the applications which cannot afford high computational complexity and (2) ML-decoder is almost impractical for higher antenna configuration ($N_{tx} \geq 4$) as its complexity grows exponentially with increase in N_{tx}. Hence, it

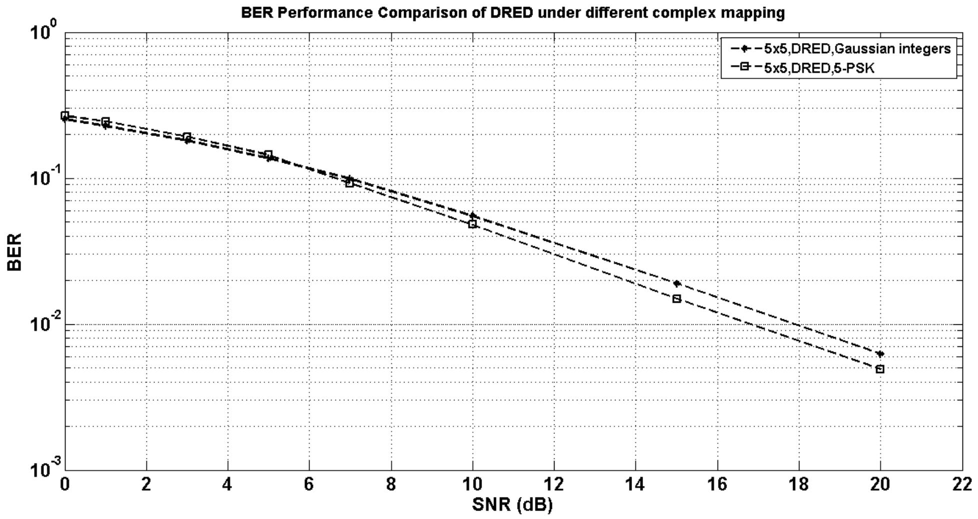

Figure 4: Gaussian integers vs 5-PSK for mapping 5×5 MRD-STBC.

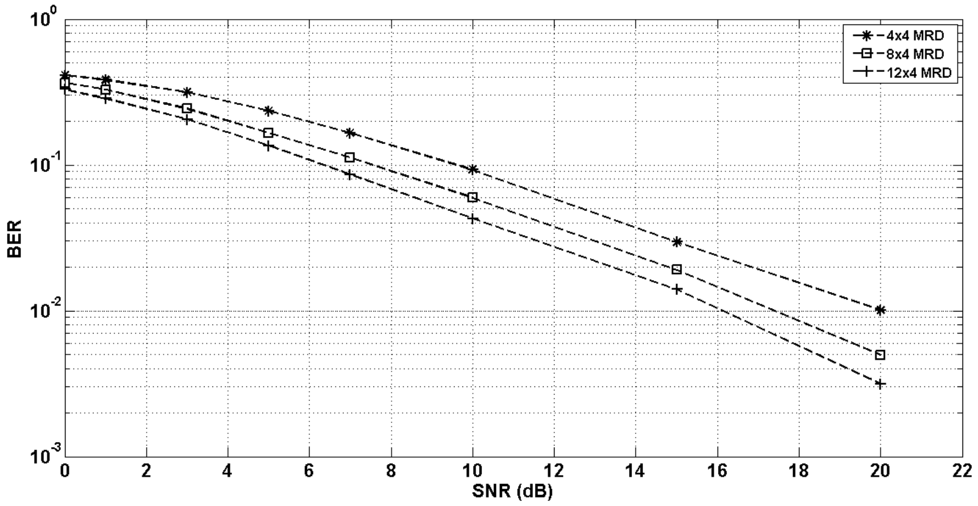

Figure 5: BER Performance Comparison of Gabidulin's Decoding Scheme for $N_{tx} = 4$, $N_{tx} = 8$, and $N_{tx} = 12$.

is reasonable to say that depending upon the trade-off between computational complexity and antennas number (N_{tx}), $\mathcal{I}$ with Gabidulin's decoding may be an elegant replacement to traditional ML-decoder for STBC's. We observe that Gabidulin's algorithm is approximately 5 times faster than ML-decoder.

Concluding Remarks

In this paper, the direct matrix construction of MRD-STBC has been presented and it was shown that the rank codes can achieve full diversity gain much like OSTBC's. Though, the performance of OSTBC is generally better than MRD-STBC yet it does outperform OSTBC provided the absolute value of the determinant of each pairwise difference is equal to 4 for both types of block code. The role of Gaussian integers has been highlighted especially low SNR region by exhibiting two STBC cases. Furthermore, we have also evaluated the viability of Gabidulin's decoding algorithm to decode MRD-STBC. The algorithm is well-suited to higher transmit antenna codes which have been constructed using interleaved MRD-STBC's and which output reasonable BER performance at the cost of low complexity.

Acknowledgements

The first and third authors would like to thank HW Communications Ltd. and COMSATS Institute of Information Technology for their support.

The paper is published with financial support by the project ITHEA XXI of the Institute of Information Theories and Applications FOI ITHEA (www.ithea.org) and the Association of Developers and Users of Intelligent Systems ADUIS Ukraine (www.aduis.com.ua).

Bibliography

[Huber, 1994] K. Huber. “Codes Over Gaussian Integers". *IEEE Transactions on Information Theory*, Vol. 40, No. 1, pp. 207-216, 1994.

[Costa et al., 2004] S.I.R. Costa, M. Muniz, E. Agustini and R. Palazzo. "Graphs, Tessellations, and Perfect Codes on Flat Tori". IEEE Transactions on Information Theory, Vol. 50, No. 10, pp. 2363-2377, October 2004.

[Nóbrega et al., 2001] T. P. da Nóbrega, J. C. Interlando, O. Milaré, M. Eliaand R. Palazzo. "Lattice Constellations and Codes from Quadratic Number Fields". IEEE Transactions on Information Theory, Vol 47, No 4, May 2001, pp. 1514-1527.

[Martínez et al., 2005] C. Martínez, R. Beivide, J. Gutierrez and E. Gabidulin. "On the Perfect t-Dominating Set Problem in Circulant Graphs and Codes over Gaussian Integers". Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT’05). Adelaide, Australia. September, 2005.

[Tarokh et al., 1998] V. Tarokh, N. Seshadri, and A. R. Calderbank, ŞSpace-time codes for high data rate wireless communication: Performance criteria and code construction,Ť IEEE Transactions on Information Theory, March 1998.

[Alamouti, 1998] S. M. Alamouti, ŞA simple transmit diversity technique for wireless communications,Ť IEEE JOURNAL ON SELECT AREAS IN COMMUNICATIONS, vol. 16, no. 8, pp. 1451Ű1458, October 1998.

[Tarokh et al., 1999] V. Tarokh, H. Jafarkhani, and A. Calderbank, ŞSpace-time block codes from orthogonal designs,Ť IEEE Transactions on Information Theory, vol. 45, no. 5, pp. 1456Ű1467, July 1999.

[Lusina et al., 2003] P. Lusina, E. Gabidulin, and M. Bossert, ŞMaximum rank distance codes as space-time codes,Ť IEEE Transactions on Information Theory, vol. 49, no. 10, pp. 2757Ű 2760, October 2003.

[Gabidulin, 1985] E. Gabidulin, ŞTheory of codes with maximum rank distance,ŤProblemy Peredachi Informatsii, vol. 21, no. 1, pp. 1Ű12, 1985.

[Gabidulin, 1995] E. Gabidulin, ŞPublic-key cryptosystems based on linear codes,Ť Technische Universiteit Delft Delft University of Technology, Tech. Rep., 1995.

[Berlekamp, 1968] E. Berlekamp, Algebraic coding theory. New York: McGraw-Hill, 1968.

[Sidorenko and Bossert, 2010] V. Sidorenko and M. Bossert, ŞDecoding interleaved gabidulin codes and multisequence linearized shift-register synthesis,Ť in IEEE International Symposium on Information Theory Proceedings (ISIT), 2010, pp. 1148Ű1152.

Authors' Information

Hafiz M.Asif *- PhD student, School of Computing & Communication Systems, Lancaster University, UK; e-mail: h.asif1@lancaster.ac.uk*

Major Fields of Scientific Research: Space time block coding, Rank codes, Wireless communication systems

Ernst Gabidulin *- Professor, Department of Radio Engineering and Telecommunications, Moscow Institute of Physics and Technology, Russia; email: ernst_gabidulin@yahoo.com*

Major Fields of Scientific Research: Information theory, rank codes, cryptography, network coding

Bahram Honary *- Professor, School of Computing & Communication Systems, Lancaster University, UK; e-mail: b.honary@lancaster.ac.uk*

Major Fields of Scientific Research: Channel coding/decoding, Low-density parity-check codes, Ultra wide band technology