Optimal Rate-Diversity Tradeoff STBCs from Codes over Arbitrary Finite Fields

Kiran .T and B. Sundar Rajan
Dept. of ECE, Indian Institute of Science
Bangalore-560012, INDIA
Email: {kirant,bsrajan}@ece.iisc.ernet.in

***Abstract*— A linear rank-distance code is a set of matrices over a finite field $\mathbf{F}_q$, with the rank over $\mathbf{F}_q$ as a distance metric. A Space-Time Block Code (STBC) is a finite set of complex matrices with the rank over the complex field as a metric. Rank-distance codes over prime fields $\mathbf{F}_p$ have found applications as space-time codes. In this paper, we extend this result to arbitrary finite fields by providing an isomorphism from $\mathbf{F}_q$ ($q = p^m$) to a subset of the ring of integers of an appropriate number field. Using this map and a maximal rank-distance code over $\mathbf{F}_q$, we construct STBCs that achieve optimal rate-diversity tradeoff for any given diversity order. Simulation results confirm the diversity gain obtained using these codes.**

I. Introduction

A quasi-static Rayleigh fading multiple input multiple output (MIMO) channel with n_t transmit and n_r receive antennas is modeled as $\mathbf{Y}_{n_r\times l} = \mathbf{H}_{n_r\times n_t}\mathbf{X}_{n_t\times l} + \mathbf{W}_{n_r\times l}$, where $\mathbf{Y}_{n_r\times l}$ is the received matrix over l channel uses, $\mathbf{X}_{n_t\times l}$ is the transmitted matrix, $\mathbf{H}_{n_r\times n_t}$ is the channel matrix and $\mathbf{W}_{n_r\times l}$ is the additive noise matrix, with the subscripts denoting the dimension of the matrices. The matrices $\mathbf{H}_{n_r\times n_t}$ and $\mathbf{W}_{n_r\times l}$ have entries which are i.i.d complex circularly symmetric Gaussian random variables with zero mean and unit variance. The collection of all possible transmit codewords $\mathbf{X}_{n_t\times l}$ forms a space-time block code (STBC) $\mathcal{C}_{ST}$. From the pair-wise error probability point of view, it is well-known that the performance of a space-time code at high SNR is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of the ranks of the difference matrices $\left(\mathbf{X}_{n_t\times l} - \mathbf{X}'_{n_t\times l}\right)$, for any $\mathbf{X}_{n_t\times l} \neq \mathbf{X}'_{n_t\times l} \in \mathcal{C}_{ST}$; also called the transmit diversity or the rank of $\mathcal{C}_{ST}$. An $n_t \times l$ STBC is said to be of full-rank if it achieves the maximum transmit diversity n_t (assuming $n_t \leq l$).

Let $\mathcal{S}$ denote a complex signal set (constellation) and $\mathcal{C}_{ST} \subset \mathcal{S}^{n_t\times l}$ be an STBC *completely over* $\mathcal{S}$ [1]. Following the convention in [2], [3], we define the rate of an $n_t \times l$ STBC completely over $\mathcal{S}$ as

$$R = \frac{\log_{|\mathcal{S}|}|\mathcal{C}_{ST}|}{l}, \tag{1}$$

where $|\mathcal{C}_{ST}|$ is the cardinality of $\mathcal{C}_{ST}$. If the code $\mathcal{C}_{ST}$ achieves transmit diversity equal to $d_{\mathbb{C}}$, there exists a rate-diversity tradeoff for space-time codes completely over $\mathcal{S}$, which is given by the relation

$$R \leq n_t - d_{\mathbb{C}} + 1. \tag{2}$$

A space-time code which achieves equality in the above tradeoff is said to be *optimal*.

A particularly interesting class of STBCs completely over a signal set is the ones obtained from rank-distance codes over finite fields: A rank-distance (RD) code over a fiite field $\mathbf{F}_q$ is a linear code $\mathcal{C}_{FF}$, where each codeword is an $n_t \times l$ matrix over $\mathbf{F}_q$. For any pair of codewords $C_1 \neq C_2$, the rank-distance $r_q(C_1 - C_2)$ is the rank over $\mathbf{F}_q$ of the difference matrix $C_1 - C_2$ [4] and the rank of $\mathcal{C}_{FF}$ (denoted by d_q) is the minimum of $r_q(C_1 - C_2)$ over all possible pairs of distinct codewords. If $k = \log_q|\mathcal{C}_{FF}|$, then the normalized rate k/l needs to satisfy a bound similar to (2), where we need to replace R with k/l and $d_{\mathbb{C}}$ with d_q. A rank d_q code achieving this bound with equality is said to be a rank-d_q *maximal rank-distance* (MRD) code. If $d_q = n_t$, then $\mathcal{C}_{FF}$ is just a full-rank RD code if $k < l$, or a full-rank MRD code if $k = l$.

Application of RD codes to space-time code construction was first proposed by Hammons and El Gamal in [5], where full-rank space-time codes over a BPSK/QPSK constellation were obtained starting from binary full-rank codes. In a related work [6], a general framework for using full-rank MRD codes as space-time codes is given by Gabidulin *et.al.*, which employs an $n_t \times n_t$ full-rank MRD code over $\mathbf{F}_q$, and a one-one map $\phi : \mathbf{F}_q \rightarrow \mathcal{S}$, to obtain an STBC, $\mathcal{C}_{ST} = \{(\phi(C_{ij})) : C = (C_{ij}) \in \mathcal{C}_{FF}\}$. The properties of the chosen signal constellation $\mathcal{S}$ and the map ϕ determine the rank of the STBC $\mathcal{C}_{ST}$. We emphasize the fact that the authors in [6] give only the framework, but fail to give a method for finding a map ϕ and $\mathcal{S}$ that would yield full-rank space-time codes starting from RD codes over arbitrary $\mathbf{F}_q$. This has been partially solved in a subsequent work by the same authors [7], where, for any prime p of the form $4k+1$, a map ϕ from $\mathbf{F}_p$ to the Gaussian integer ring is given that can be used to get full-rank STBCs from full-rank RD codes over $\mathbf{F}_p$. Only full-rank MRD codes over $\mathbf{F}_p$ are considered and it is shown that ϕ preserves full-rank, i.e., it is rank preserving if the RD code is full-rank. In a series of papers, Lu and Kumar have generalized the construction given in [5]. The most generalized version, which is the so called Generalized Unified (GU) construction [10], yields optimum STBCs over a variety of signal sets including the p^K-PAM, p^K-PSK as well as 2^K-QAM.

In summary, all prior works have only managed to construct STBCs from RD codes over a prime field $\mathbf{F}_p$. In view of these results, a natural extension would be to look for STBC

0-7803-8938-7/05/$20.00 (C) 2005 IEEE

construction from RD codes over arbitrary field $\mathbf{F}_q$, via a rank preserving map from the matrix ring $\mathbf{F}_q^{n_t \times l}$ to $\mathcal{S}^{n_t \times l} \subset \mathbb{C}^{n_t \times l}$. In this paper, we give a solution to this problem by generalizing the technique used in [7]. Algebraic number theoretic results are used to obtain rank preserving map for arbitrary values of q, which maps an element of $\mathbf{F}_q$ to an element of some suitable algebraic integer ring in a number field. We then show that the map in [7] is obtained as a special case when we specialize our technique to a prime of the form $4k+1$, thus proving that the map used in [7] is not only full-rank preserving but also preserves any arbitrary rank.

The code constructions in this paper assume knowledge of number fields and ideal factorization in their algebraic integer rings. We refer the readers to [11] for an overview on this topic. Let $\mathbb{K}$ be a number field and $\mathbb{Z}_{\mathbb{K}}$ denote the ring of algebraic integers in $\mathbb{K}$. If $\mathfrak{P}$ is a prime ideal in $\mathbb{Z}_{\mathbb{K}}$, then there is a unique rational prime p satisfying $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Our main principle for establishing a rank preserving map relies on the fact that $\mathbb{Z}_{\mathbb{K}}/\mathfrak{P}$ is isomorphic to the finite field $\mathbf{F}_{p^f}$, where $f = f(\mathfrak{P}|p)$ called the inertial degree of $\mathfrak{P}$ over p is an integer that divides the degree of $\mathbb{K}$ over $\mathbb{Q}$.

II. Main principle for STBC construction

Suppose $\mathcal{C}_{FF}$ is an $n_t \times l$ RD code over $\mathbf{F}_{p^K}$ and we want to construct an $n_t \times l$ STBC using $\mathcal{C}_{FF}$. The first step is to find a signal set $\mathcal{S}$ along with a one-one map ϕ from $\mathbf{F}_{p^K}$ to $\mathcal{S}$ as follows.

- Find a number field $\mathbb{K}$ such that the prime ideal $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$ for some prime ideal $\mathfrak{P} \subset \mathbb{Z}_{\mathbb{K}}$, with $f(\mathfrak{P}|p) = K$.
- Let ϕ denote the isomorphism $\mathbb{Z}_{\mathbb{K}}/\mathfrak{P} \rightarrow \mathbf{F}_{p^K}$, and let $\mathcal{S}$ be equal to a **complete representative set** of the quotient ring $\mathbb{Z}_{\mathbb{K}}/\mathfrak{P}$. This means, $\mathcal{S} = \left\{r_1, r_2, \ldots, r_{p^k}\right\}$ such that no two elements in $\mathcal{S}$ belong to the same coset in $\mathbb{Z}_{\mathbb{K}}/\mathfrak{P}$, and
$$\begin{aligned}(r_j + \mathfrak{P}) + (r_k + \mathfrak{P}) &= (r_l + \mathfrak{P}),\\ (r_j + \mathfrak{P})(r_k + \mathfrak{P}) &= (r_m + \mathfrak{P}),\end{aligned}$$
for some $r_l, r_m \in \mathcal{S}$ that are unique for the pair r_i, r_j. For the sake of convenience, we call the above two operations as "modulo $\mathfrak{P}$" addition and subtraction on $\mathcal{S}$. Thus, the set $\mathcal{S}$ is a field with respect to "modulo $\mathfrak{P}$" addition and subtraction.
- We use the set $\mathcal{S}$ as a signal set. The isomorphism ϕ when restricted to the set $\mathcal{S}$, is a one-one map from $\mathcal{S}$ to $\mathbf{F}_{p^K}$. The STBC $\mathcal{C}_{ST}$ over $\mathcal{S}$ is then obtained as:
$$\mathcal{C}_{ST} = \left\{\phi^{-1}(C) = \left(\phi^{-1}(C_{i,j})\right) \mid C \in \mathcal{C}_{FF}\right\}$$

Although the main principle is applicable for constructing STBCs from MRD codes over arbitrary finite fields, because of space constraints, in this paper we apply this principle to construct STBCs from MRD codes over $\mathbf{F}_p$ and $\mathbf{F}_{p^2}$ only. This principle has been used in a more general setting by considering codes over Galois rings as well [12], [13].

Theorem 1 (rate-diversity optimality): Let $\mathcal{C}_{FF}$ be an $n_t \times l$ rank-d MRD code over $\mathbf{F}_q$ and $\mathcal{C}_{ST}$ be the STBC obtained using the above principle. Then the code $\mathcal{C}_{ST}$ is optimal, with the diversity gain equal to d.

According to Theorem 1, we can always construct optimal STBCs with arbitrary transmit diversity, provided there exists MRD code construction technique for any arbitrary rank and over any finite field $\mathbf{F}_q$. Following theorem is a generalization of the binary MRD code construction [3] to arbitrary field.

Theorem 2 (MRD code construction): Let q be a power of a prime p and $R = n_t - d + 1$, for $1 \leq n_t \leq l < \infty$; $1 \leq d \leq n_t$. Let $\mathbf{F}_{q^l}$ be an extension of the finite field $\mathbf{F}_q$, with ζ as a primitive element. Consider the set of q-linearized polynomials
$$\mathcal{F} = \left\{ f(x) \mid f(x) = \sum_{j=0}^{R-1} f_j x^{q^j}, f_j \in \mathbf{F}_{q^l} \right\},$$
and associate with every linearized polynomial $f(x) \in \mathcal{F}$, an $n_t \times l$ matrix $C_f = \left[\underline{f(1)}\ \underline{f(\zeta)}\ \underline{f(\zeta^2)} \cdots \underline{f(\zeta^{n_t-1})}\right]^T$, where $\underline{f(\zeta^j)}$ denotes the representation of $f(\zeta^j)$ as an $l \times 1$ vector over $\mathbf{F}_q$, using the ordered basis $\{1, \zeta, \ldots, \zeta^{l-1}\}$. Then the collection of q^{lR} codeword matrices $\mathcal{C}_{FF} = \{C_f \mid f(x) \in \mathcal{F}\}$, is a rank-$d$ MRD code over $\mathbf{F}_q$.

Example 1: Let $q = 3^2, n_t = l = 2$ and $d = 2$. The maximal rate is then equal to $R = n_t - d + 1 = 1$. We use the primitive polynomial $\Phi(x) = x^4 + x + 2$ for constructing the field $\mathbf{F}_{3^4}$ with ζ denoting a root of $\Phi(x)$. Then the subfield $\mathbf{F}_9 = \{0, 1, \zeta^{10}, \zeta^{20}, \ldots, \zeta^{70}\}$, and $\{1, \zeta\}$ is a basis for $\mathbf{F}_{81}$ over $\mathbf{F}_9$.

When $R = 1$, the MRD code of Theorem 2 is same as the matrix representation of the extension field $\mathbf{F}_{q^l} = \mathbf{F}_q(\zeta)$ over $\mathbf{F}_q$, using the companion matrix of ζ over $\mathbf{F}_q$. In this example, the minimal polynomial of ζ over $\mathbf{F}_9$ is $\Phi_1(x) = x^2 - \zeta^{60}x + \zeta^{10}$ (divides $\Phi(x)$) and hence the companion matrix of ζ over $\mathbf{F}_9$ is
$$M_\zeta = \begin{bmatrix} 0 & 1 \\ -\zeta^{10} & \zeta^{60} \end{bmatrix}.$$
Since every element of $\mathbf{F}_{81}$ is of the form $s_0 + s_1\zeta$ with $s_0, s_1 \in \mathbf{F}_9$, the corresponding matrix representation is
$$s_0 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + s_1 M_\zeta = \begin{bmatrix} s_0 & s_1 \\ -s_1\zeta^{10} & s_0 + s_1\zeta^{60} \end{bmatrix}.$$
Clearly, all these matrices have rank equal to $n_t = l = 2$.

In the next section, we construct signal sets along with a one-one map from $\mathbf{F}_q$ to the signal set, using quadratic number fields.

III. Signal constellations from quadratic fields

A number field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ is said to be quadratic if $[\mathbb{K} : \mathbb{Q}] = 2$ and d is some non-square integer. We will only consider the case $d < 0$, in which case the corresponding fields are called imaginary quadratic fields. A quadratic field is a Galois extension with the Galois group $\{1, \sigma\}$, where $\sigma(\sqrt{d}) = -\sqrt{d}$. The ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is equal to $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \mod 4$ and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1$

$\bmod 4$. In the special case when $d = -1$ and $d = -3$, the integer ring is the Gaussian ring (square lattice) and the hexagonal lattice (equilateral triangular lattice) respectively.

If p is a rational prime number, then the ideal $p\mathbb{Z}_{\mathbb{Q}(\sqrt{d})}$ can factorize in three different ways. If it factorizes as $\mathfrak{P}_1\mathfrak{P}_2$ such that $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are co-prime, then p is said to *split* in $\mathbb{Q}(\sqrt{d})$, else if $p\mathbb{Z}_{\mathbb{Q}(\sqrt{d})} = \mathfrak{P}^2$, then p is ramified and finally, if $p\mathbb{Z}_{\mathbb{Q}(\sqrt{d})}$ remains prime, then p is a prime in $\mathbb{Q}(\sqrt{d})$. Accordingly, in the first two cases, the inertial degree is $f = 1$ and when p remains prime $f = 2$, and so the ring of integers $\mathbb{Z}_{\mathbb{Q}(\sqrt{d})}$ is suitable for constructing signal sets isomorphic to $\mathbf{F}_p$ or $\mathbf{F}_{p^2}$. We will illustrate this by considering some specific imaginary quadratic fields.

A. Space-time codes from Gaussian integer ring

Let $d = -1$ and $i = \sqrt{-1}$. The ring of integers of the quadratic field $\mathbb{Q}(i)$ is the Gaussian integer ring $\mathbb{Z}[i]$. The non-trivial automorphism of $\mathbb{Q}(i)$ is nothing but the usual complex conjugation, and the norm map is given by $n(x+iy) = (x+iy)(x-iy) = x^2+y^2$. Gaussian integer ring is a Euclidean domain with respect to the norm map (norm-Euclidean) and therefore, it is a principal ideal domain (PID).

1) $\mathcal{S}$ isomorphic to $\mathbf{F}_p$ (Lusina, Gabidulin and Bossert Construction [7]): Let p be a rational prime number of the form $4k+1$. The ideal $p\mathbb{Z}[i]$ splits into a product of two distinct prime ideals. Since $\mathbb{Z}[i]$ is a PID, the factorization is of the form $p\mathbb{Z}[i] = (\pi\mathbb{Z}[i])(\pi^*\mathbb{Z}[i])$ such that $(\pi\mathbb{Z}[i]) \cap \mathbb{Z} = (\pi^*\mathbb{Z}[i]) \cap \mathbb{Z} = p\mathbb{Z}$. The quotient ring $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is isomorphic to $\mathbf{F}_p$ and it is straight-forward to verify that the set $\{0, 1, \ldots, p-1\}$ is a complete coset representative set. The ring $\mathbb{Z}[i]$ is norm-Euclidean and so, for any $j \in \{0, 1, \ldots, p-1\}$, there exist $q_j, r_j \in \mathbb{Z}[i]$ satisfying

$$j = q_j\pi + r_j \text{ with } 0 \leq n(r_j) < n(\pi). \tag{3}$$

The element r_j belongs to the same coset as j because $j - r_j = q_j\pi \in \pi\mathbb{Z}[i]$ and so the set $\mathcal{S} = \{r_0, r_1, \ldots, r_{p-1}\}$ is also a complete representative set. According to Theorem 1, the set $\mathcal{S}$ along with the one-one map $\phi : j \longmapsto r_j$, can be used to get STBCs over $\mathcal{S}$ from RD codes over $\mathbf{F}_p$. The element q_j that appears in (3) is chosen such that, if $\frac{j}{\pi} \in \mathbb{Q}(i)$ is equal to $x_j + iy_j$ for some $x_j, y_j \in \mathbb{Q}$, and $q_j = m_j + in_j$ for some $m_j, n_j \in \mathbb{Z}[i]$, then m_j and n_j are the integers satisfying $|x_j - m_j| \leq 1/2$ and $|y_j - n_j| \leq 1/2$. This is exactly the "rounding operation (to the closest algebraic integer)", $\left\lceil \frac{j}{\pi} \right\rfloor = \left\lceil \frac{j\pi^*}{\pi\pi^*} \right\rfloor$ that was used to denote q_j in [7]. From this it is easy to see that the constellation $\mathcal{S}$ consisting of

$$\left\{ r_j = j - q_j\pi = j - \left\lceil \frac{j\pi^*}{\pi\pi^*} \right\rfloor \pi \right\}_{j=0}^{p-1}, \tag{4}$$

is the same constellation that is used in [7]. Since $\mathbb{Z}[i]$ is a PID and $\mathfrak{P} = \pi\mathbb{Z}[i]$, the "modulo $\mathfrak{P}$" operations on $\mathcal{S}$ are equivalent to the "modulo π" operations considered in [7].

While this map was used only for full-rank STBC construction in [7], Theorem 1 says that this map preserves arbitrary rank and so optimal STBCs with arbitrary rank can be obtained.

Example 2 (Full-rank STBC for $n_t = l = 2$): Let $q = p = 5$ and $n_t = l = d = 2$. We use $\Phi(x) = x^2 + x + 2$ as the primitive polynomial for extending $\mathbf{F}_5$ to $\mathbf{F}_{5^2}$. The MRD code with rank 2, obtained following the construction in Theorem 2 is

$$\mathcal{C}_{FF} = \left\{ \begin{bmatrix} s_0 & s_1 \\ 3s_1 & s_0 + 4s_1 \end{bmatrix} : s_0, s_1 \in \mathbf{F}_5 \right\}.$$

We find that $p = 5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$. If we choose $\pi = 2 + i$, then the signal set obtained is (see Fig. 1(a)) $\mathcal{S} = \{r_0 = 0, r_1 = 1, r_2 = -i, r_3 = i, r_4 = -1\}$ and the map ϕ maps $j \in \mathbf{F}_5$ to $r_j \in \mathcal{S}$. With this MRD code, using our main principle we get the STBC

$$\mathcal{C}_{ST} = \left\{ \begin{bmatrix} \phi(s_0) & \phi(s_1) \\ \phi(3s_1) & \phi(s_0 + 4s_1) \end{bmatrix} : s_0, s_1 \in \mathbf{F}_5 \right\}.$$

Using the same MRD code, the GU construction yields an STBC

$$\mathcal{C}_{ST}^{(GU)} = \left\{ \begin{bmatrix} \omega_5^{s_0} & \omega_5^{s_1} \\ \omega_5^{3s_1} & \omega_5^{s_0}\omega_5^{4s_1} \end{bmatrix} : s_0, s_1 \in \mathbf{F}_5 \right\},$$

which is a code over the 5-PSK constellation $\{1, \omega_5, \omega_5^2, \ldots, \omega_5^4\}$ (ω_m denotes primitive m-th root of unity).

Both these codes are full-rank codes, with rate $R = 1$. Our simulations of the codeword error probability performance using Maximum-Likelihood (ML) decoding show that both codes have same performance (Fig. 2). If p is chosen to be a very large prime (of the form $4k+1$), then our construction continues to use signal sets that are subsets of $\mathbb{Z}[i]$, while the GU construction uses p-PSK constellation. As p grows bigger, the distance profile of our signal sets is better than the distance profile of the p-PSK constellation and hence we expect our codes to perform better than the GU constructed codes. This is evident for $p = 17 = (4+i)(4-i)$. Using $\pi = 4 + i$, we get the signal set as shown in Fig. 1(b). For rank-2 MRD code construction over $\mathbf{F}_{17}$, we use $\Phi(x) = x^2 + x + 3$ as the irreducible polynomial for constructing F_{17^2} over F_{17^2} and the space-time codewords are of the form

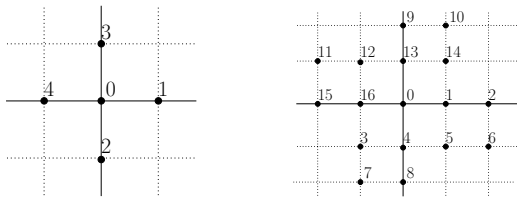
$$\begin{bmatrix} \phi(s_0) & \phi(s_1) \\ \phi(14s_1) & \phi(s_0 + 16s_1) \end{bmatrix} : s_0, s_1 \in \mathbf{F}_{17},$$

while the GU constructed STBC consists of codewords of the form

$$\begin{bmatrix} \omega_{17}^{s_0} & \omega_{17}^{s_1} \\ \omega_{17}^{14s_1} & \omega_{17}^{s_0}\omega_{17}^{16s_1} \end{bmatrix} : s_0, s_1 \in \mathbf{F}_{17}.$$

Fig. 2 shows that our code performs better than the GU constructed code for $p = 17$.

2) $\mathcal{S}$ isomorphic to $\mathbf{F}_{p^2}$: If p is a rational prime number of the form $4k+3$, then the ideal $\mathfrak{P} = p\mathbb{Z}[i]$ is prime in $\mathbb{Z}[i]$. The inertial degree $f(\mathfrak{P} \mid p\mathbb{Z}) = 2$ and hence $\mathbb{Z}[i]/\mathfrak{P}$ is isomorphic to the field $\mathbf{F}_{p^2}$. The ring $\mathbb{Z}[i]$ is a free $\mathbb{Z}$-module with basis $\{1, i\}$, and the ideal $\mathfrak{P}$ is an additive $\mathbb{Z}$-submodule of $\mathbb{Z}[i]$, with a free basis $\{p, ip\}$. Therefore, the set $\mathcal{S} = \left\{ m + in : -\frac{p-1}{2} \leq m, n \leq \frac{p-1}{2} \right\}$ is a complete coset



(a) $\mathbf{F}_5$ (b) $\mathbf{F}_{17}$

Fig. 1. Signal sets isomorphic to $\mathbf{F}_p$ from $\mathbb{Z}[i]$.

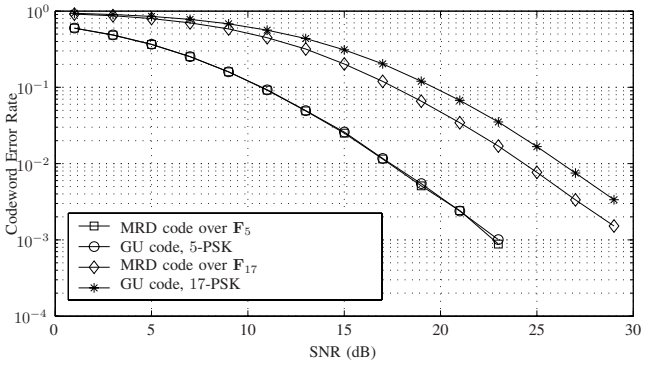


Fig. 2. Codeword error rate for $n_t = l = 2$ and $n_r = 1$ STBCs

representative set of $\mathbb{Z}[i]/\mathfrak{P}$, which can be used as the complex signal set. Since $\mathbb{Z}[i]$ is a PID, the "modulo $\mathfrak{P}$" operation is equivalent to the "component-wise modulo p" operation:

$$(m_1 + in_1) + (m_2 + in_2) \mod p = (m_1 + m_2) \bmod p + i(n_1 + n_2) \bmod p, \quad (5a)$$

$$(m_1 + in_1)(m_2 + in_2) \mod p = (m_1 m_2 - n_1 n_2) \bmod p + i(m_1 n_2 + m_2 n_1) \bmod p. \quad (5b)$$

The set $\mathcal{S}$ is a field containing p^2 elements with respect to modulo p operations defined above. An element $\zeta = m + in \in \mathcal{S}$ is a primitive element of $\mathbf{F}_{p^2}$ if the multiplicative order of $m^2 + n^2$ in $\mathbb{Z}/p\mathbb{Z}$ is equal to $p - 1$.

Example 3: Let $p = 3$, which remains a prime in $\mathbb{Z}[i]$. The quotient ring $\mathbb{Z}[i]/3\mathbb{Z}[i]$ is isomorphic to $\mathbf{F}_{3^2}$ and the corresponding signal set $\mathcal{S} = \{m + in : -1 \le m, n \le 1\}$ is shown in Fig. 3. We have labeled the points using exponential form (of a finite field) with $\gamma = 1 + i$ as the primitive element (Notice that $(1+i)(1-i) = 2$ has order equal to $2 = 3 - 1$ in $\mathbb{Z}/3\mathbb{Z}$). We get an optimal full-rank STBC for $n_t = l = 2$, by using this signal set and the 2×2 full-rank MRD code over $\mathbf{F}_9$ that we have constructed in Example 1. The codewords of this STBC are of the form $\begin{bmatrix} \phi(s_0) & \phi(s_1) \\ \phi(-s_1\zeta^{10}) & \phi(s_0 + s_1\zeta^{60}) \end{bmatrix}$, where $s_0, s_1 \in \{0, 1, \zeta^{10}, \zeta^{20}, \ldots, \zeta^{70}\}$ (notation used in Example 1) and ϕ maps 0 to 0 and the element ζ^{10k} to the complex point labeled with γ^k in Fig. 3.

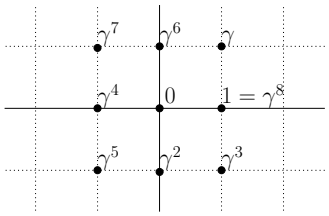


Fig. 3. Signal set isomorphic to $\mathbf{F}_9$.

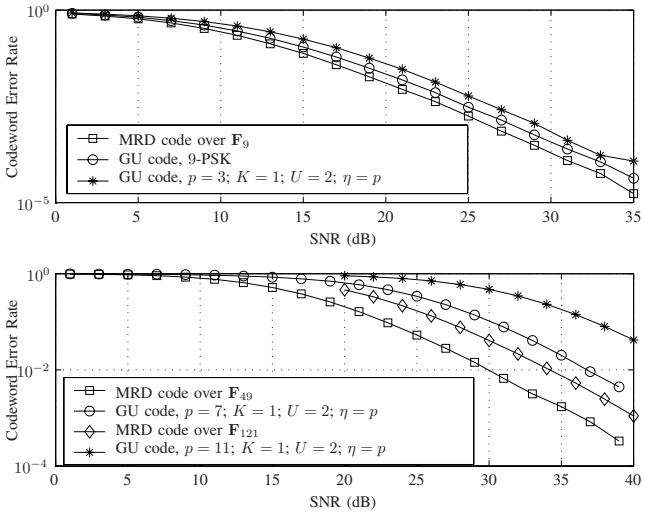


Fig. 4. Codeword error rate for $n_t = l = 2$ and $n_r = 1$ STBCs

In Fig. 4, we compare the performance of this code with the full-rank optimal STBCs obtained by the GU construction for $n_t = l = 2$ and $n_r = 1$. We consider two different codes that are constructible using GU construction: one corresponding to the parameters $p = 3, K = 2, U = 1$ uses the 9-PSK constellation and the other corresponding to the parameters $p = 3, K = 1, U = 2, \eta = 3$ and $\kappa = 1$. All these three codes consist of $9^2 = 81$ codewords. While the slope of the codeword error probability is the same for all codes, our code has better coding gain. In Fig. 4, we also compare the performance of our codes constructed using rate 1 MRD codes over $\mathbf{F}_{7^2}$ and $\mathbf{F}_{11^2}$ against the GU constructed optimal codes with parameters $p = 7, K = 1, U = 2, \eta = 7, \kappa = 1$ and $p = 11, K = 1, U = 2, \eta = 11, \kappa = 1$ respectively. Our codes outperform the corresponding GU constructed codes and the coding gain difference increases with the value of p. We also observe that our code over $\mathbf{F}_{11^2}$ which has 11^4 codewords, outperforms the GU code with $p = 7$ which consists of only 7^4 codewords.

As long as an algebraic integer ring $\mathbb{Z}_{\mathbb{Q}(\sqrt{d})}$ is norm-Euclidean, signal sets isomorphic to $\mathbf{F}_p$ or $\mathbf{F}_{p^2}$ can be constructed using the modulo π or modulo p operation depending on whether p splits or remains prime in $\mathbb{Z}_{\mathbb{Q}(\sqrt{d})}$. We will next construct signal sets using another well-known ring which belongs to this category, and in the subsequent subsection we will consider the ring corresponding to $d = -5$ which is not

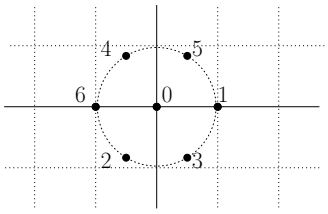


Fig. 5. Signal set isomorphic to $\mathbf{F}_7$.

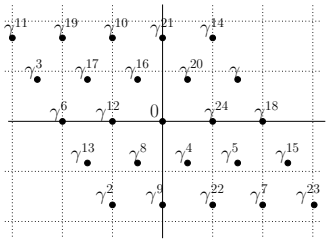


Fig. 6. Signal set isomorphic to $\mathbf{F}_{5^2}$.

a Euclidean domain.

B. Space-time codes from Eisenstein ring

Let $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. The ring of algebraic integers of this field (called the Eisenstein ring) is $\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[\omega_3]$, where $\omega_3 = (-1+\sqrt{-3})/2$ is a primitive 3rd root of unity. The non-trivial automorphism of $\mathbb{K}$ given by $\sigma(\sqrt{-3}) = -\sqrt{-3}$, maps ω_3 to ω_3^2 and the norm map is given by $n(a+b\omega_3) = (a+b\omega_3)(a+b{\omega_3}^2) = a^2 - ab + b^2$. For a rational prime p, the factorization of ideal $p\mathbb{Z}[\omega_3]$ depends on the type of prime p. The ideal $p\mathbb{Z}[\omega_3]$ splits as $(\pi\mathbb{Z}[\omega_3])(\bar{\pi}\mathbb{Z}[\omega_3])$ if $p \equiv 1 \mod 3$ and it remains prime in $\mathbb{Z}[\omega_3]$ if $p \equiv 2 \mod 3$.

Example 4: Let $p = 7$. In $\mathbb{Z}_{\mathbb{Q}(\sqrt{-3})}$, the ideal $7\mathbb{Z}_{\mathbb{Q}(\sqrt{-3})} = \langle\pi\rangle\langle\bar{\pi}\rangle$ where $\pi = 3 + \omega_3$ and $\bar{\pi} = \sigma(\pi) = 2 - \omega_3$. Since $7\mathbb{Z}_{\mathbb{Q}(\sqrt{-3})}$ is a maximal ideal, $\mathbb{Z}_{\mathbb{Q}(\sqrt{-3})}/\langle\pi\rangle$ is isomorphic to $\mathbf{F}_7$. We could use any complete representative set as a constellation (for. eg., $\{-3,-2,\ldots,2,3\}$), but since $\mathbb{Z}[\omega_3]$ is norm-Euclidean, we can use the modulo π operation to design a constellation whose average energy is smaller. We use $\{\zeta_0,\zeta_1,\ldots,\zeta_6\}$ as the signal set, where ζ_j is the element that appears in the expression $j = q_j\pi + \zeta_j$ with $0 \le n(\zeta_j) < n(\pi)$. The element $q_j = m_j + n_j\omega_3 \in \mathbb{Z}_{\mathbb{Q}(\sqrt{-3})}$ is the *closest* algebraic integer to $\frac{j}{\pi} \in \mathbb{Q}(\sqrt{-3})$ in the sense that, if $\frac{j}{\pi} = x_j + y_j\omega_3$ where $x_j, y_j \in \mathbb{Q}$, then m_j and n_j are the integers satisfying $|x_j - m_j| \le 1/2$ and $|y_j - n_j| \le 1/2$. As in [7], we use the notation $\left[\frac{j}{\pi}\right] = \left[\frac{j\bar{\pi}}{\pi\bar{\pi}}\right]$ for q_j and therefore the constellation is obtained via the map: $\zeta_j = \left(j - \left[\frac{j\bar{\pi}}{\pi\bar{\pi}}\right]\pi\right) \mod \pi$. The complete signal set is shown in Fig. 5.

Example 5: If $p = 5$, which is a prime in $\mathbb{Z}[\omega_3]$ then $\mathbb{Z}[\omega_3]/p\mathbb{Z}[\omega_3]$ is isomorphic to the field $\mathbf{F}_{5^2}$. The set $\mathcal{S} = \{m + \omega_3 n : -2 \le m, n \le 2\}$ can be used as the complex signal set, which is a field with the modulo p operations obtained by replacing i with ω_3 in (5). This signal set is labeled using $\gamma = 2 + \omega_3$ as a primitive element in Fig. 6, where the complex point corresponding to ω_3 is labeled by γ^{16}.

C. Space-time codes from $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$

The ring of integers $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$ is not a norm-Euclidean domain and it is not even a PID. Therefore, the constellations constructed using this ring will not have nice maps as in (4) or (5). Nevertheless, following our main principle, signal sets isomorphic to $\mathbf{F}_p$ or $\mathbf{F}_{p^2}$ can be constructed based on the conditions between rational prime p and $d = -5$.

Example 6: The algebraic integer ring $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ and hence this is a rectangular lattice in the complex field.

1) The ideal $7\mathbb{Z}[\sqrt{-5})] = \langle 7, 3+\sqrt{-5}\rangle\langle 7, 3-\sqrt{-5}\rangle$. If $\mathfrak{p} = \langle 7, 3+\sqrt{-5}\rangle$, then $7\mathbb{Z}[\sqrt{-5})]/\mathfrak{p}$ is isomorphic to $\mathbf{F}_7$. The set $\{0, 1, -1-\sqrt{-5}, -\sqrt{-5}, \sqrt{-5}, 1+\sqrt{-5}, -1\}$ is a compete representative set that can be used as a signal set for constructing optimal STBCs over $\mathbf{F}_7$.
2) The ideal $13\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$ remains prime in $\mathbb{Z}[\sqrt{-5})]$ and so $\mathbb{Z}[\sqrt{-5})]/\langle 13\rangle$ is isomorphic to the finite field $\mathbf{F}_{13^2}$. The set $\mathcal{S} = \{m + \sqrt{-5}n : -6 \le m, n \le 6\}$ is a complete representative set for $\mathbb{Z}[\sqrt{-5})]/\langle 13\rangle$ that can be used for constructing optimal STBCs from MRD codes over $\mathbf{F}_{13^2}$.

ACKNOWLEDGMENT

This work was supported partly by the DRDO-IISc Program on Advanced Research in Mathematical Engineering and also by the CSIR, India, through Research Grant (22(0365)/04/EMR-II) to B.S. Rajan.

REFERENCES

[1] B.A. Sethuraman, B.S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct 2003.
[2] V. Tarokh, N. Sheshadri, and A.R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, Mar 1998.
[3] H.-F. Lu and P. V. Kumar, "Rate-diversity tradeoff of space-time codes with fixed alphabet and optimal constructions for PSK modulation," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2747–2751, Oct 2003.
[4] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, Jan-Mar 1985.
[5] A. R. Hammons Jr and H. El Gamal, "On the theory of space-time codes for PSK modulation," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 524–542, Mar 2000.
[6] E. Gabidulin, M. Bossert, and P. Lusina, "Space-time codes based on rank codes," in *IEEE ISIT*, Sorrento, Italy, June 25-30 2000, p. 284.
[7] P. Lusina, E. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2757–2760, Oct 2003.
[8] U. Sripati, V. Shashidhar, and B.S. Rajan, "Full-diversity STBCs for block-fading channels from cyclic codes," in *IEEE GLOBECOM 2004*, Dallas, Texas, 29 Nov-3 Dec 2004.
[9] U. Sripati, V. Shashidhar, and B.S. Rajan, "Designs and full-rank STBCs from DFT domain description of cyclic codes," in *IEEE ISIT*, Chicago, June 27-July 2 2004, p. 340.
[10] H.-F. Lu and P. V. Kumar, "Generalized unified construction of space-time codes with optimal rate-diversity tradeoff," in *IEEE ISIT*, Chicago, June 27-July 2 2004, p. 95.
[11] P. Morandi, *Field and Galois Theory*, Springer-Verlag New York, 1996.
[12] Kiran .T and B. S. Rajan, "STBCs with optimal rate-diversity tradeoff from codes over Galois rings," submitted to IEEE Trans. Inform. Theory, Oct 2004.
[13] Kiran .T and B.S. Rajan, "Optimal STBCs from codes over Galois rings," in *IEEE ICPWC*, New Delhi, Jan 2005, pp. 120–124.