Rate-Diversity Tradeoff of Space-Time Codes with Fixed Alphabet and Optimal Constructions for PSK Modulation

Hsiao-feng Lu and P. Vijay Kumar

Abstract—In this correspondence, we show that for any \((Q \times M)\) space-time code \(S\) having a fixed, finite signal constellation, there is a tradeoff between the transmission rate \(R\) and the transmit diversity gain \(\nu\) achieved by the code. The tradeoff is characterized by \(R \leq Q - \nu + 1\), where \(Q\) is the number of transmit antennas. When either BPSK or QPSK is used as the signal constellation, a systematic construction is presented to achieve the maximum possible rate for every possible value of transmit diversity gain.

Keywords—Space-time codes, rate-diversity tradeoff.

I. INTRODUCTION

Consider a space-time coded system with \(Q\) transmit and \(P\) receive antennas. Under the quasi-static Rayleigh fading assumption, the channel is fixed for a duration of \(M\) symbol transmissions. In general, we will assume \(Q \leq M\). Let \(\mathcal{A}\) denote the signal alphabet (constellation) and \(\mathcal{S} \subset \mathcal{A}^{QM}\) be a space-time code. Each codeword in the space-time code is thus a \((Q \times M)\) matrix.

Given the signal constellation \(\mathcal{A}\), we follow [7] and define the rate \(R\) of a \((Q \times M)\) space-time code \(S\) by

\[
R := \frac{1}{M} \log_{|\mathcal{A}|} |\mathcal{S}|.
\]

Under this definition, a rate-one code corresponds to a space-time code of size \(|\mathcal{A}|^M\), i.e., to a code which transmits on the average, one symbol from the signal constellation \(\mathcal{A}\) per time slot. We say that a space-time code \(S\) achieves diversity gain \(P\nu\) if the power-series expansion of the maximum pairwise-error probability \(\text{PEP}\) can be expressed as [4], [7]

\[
\text{PEP} = c \rho^{-P\nu} + o(\rho^{-P\nu-1}),
\]

where \(c\) is some constant independent of the SNR \(\rho\). The quantity \(\nu\) is termed the transmit diversity gain [1], [7]. It is shown in [7], that from the point of view of PEP, a space-time code \(S\) achieves transmit diversity gain \(\nu\) if and only if for every \(S_1 \neq S_2 \in \mathcal{S}\), the difference matrix \(\Delta S = S_1 - S_2\) has rank at least \(\nu\) over the field of complex numbers. In [4], Lu et al. showed that the transmit diversity gain equals \(\nu\) even when one replaces the PEP criterion by either the codeword-error probability or else the symbol-error probability.

In this correspondence, we first show that for a fixed, finite signal constellation \(\mathcal{A}\), there is a tradeoff between the rate \(R\) and the transmit diversity gain \(\nu\) of a space-time code \(S\). More specifically, given transmit diversity gain \(\nu\), the rate \(R\) is upper bounded by

\[
R \leq Q - \nu + 1.
\]

If either BPSK or QPSK is used as the signal constellation, i.e., \(\mathcal{A} = \{\pm 1\}\) or \(\mathcal{A} = \{\pm 1, \pm \sqrt{-1}\}\), we give a systematic code construction having rate \(R\) that achieves the upper bound \(R = Q - \nu + 1\) for every \(1 \leq \nu \leq Q\) and for any \(Q\) and \(M\) with \(Q \leq M < \infty\).

II. RATE-DIVERSITY TRADEOFF

We first show that when the signal constellation set \(\mathcal{A}\) is finite, there is a tradeoff between the rate and transmit diversity gain of the space-time code.

Theorem 1: Given desired transmit diversity gain \(\nu_0\) and signal constellation \(\mathcal{A}\) with \(|\mathcal{A}| = a < \infty\), the size of the space-time code \(S\) is upper bounded by

\[
|\mathcal{S}| \leq a^{|\mathcal{A}|(Q - \nu_0 + 1)}.
\]

Hence the rate \(R\) has the upper bound

\[
R \leq Q - \nu_0 + 1.
\]

Proof: The difference matrix \(\Delta S = S_1 - S_2\) between two distinct matrices \(S_1, S_2\) drawn from \(\mathcal{S}\) cannot have rank at least \(\nu\) if the first \(Q - \nu_0 + 1\) rows of the two matrices \(S_1, S_2\) are identical. It follows that the set \(\mathcal{S}\) cannot have size larger than \(|\mathcal{A}|^{|\mathcal{A}|(Q - \nu_0 + 1)}\). The result follows.

Remark 1: It can be seen from (4) that:
1. The tradeoff between rate $R$ and maximum transmit diversity gain $\nu$ is independent of the number of receive antennas $P$.
2. For $Q \leq M$, the tradeoff is independent of $M$.
3. Borrowing terminology from [9], we set $d^*(R)$ to be the maximum achievable diversity gain given rate $R$. In terms of $d^*(R)$, using the fact that the diversity gain $\nu$ must be an integer, we have from (4) that

$$d^*(R) \leq P\lfloor Q - R + 1 \rfloor,$$

where $\lfloor \cdot \rfloor$ is the floor function (Fig. 1).

![Fig. 1. Upper bound on the tradeoff between rate $R$ and maximum achievable diversity gain $d^*(R)$ when $Q = 4$ and $P = 1$.](image)

III. MAXIMAL-RATE BPSK CODES WITH FLEXIBLE TRANSMIT-DIVERSITY GAIN

In this section, we consider the case of BPSK modulation, i.e., the case when the signal alphabet $\mathcal{A} = \{1, -1\}$.

**Definition 1:** Let $\zeta : \mathbb{F}_2^{QM} \to \mathbb{R}^{QM}$ be the map given by

$$\zeta(C) = \zeta([C_{qm}]) = [(-1)^{C_{qm}}] = S.$$

We will often use the notation $(-1)^C$ to denote the matrix $S = \zeta(C)$. Let $\mathcal{C}$ be the collection of $\{0, 1\}$ matrices associated to the $\{\pm 1\}$ code matrices in $\mathcal{S}$. We extend notation in a natural way and write $\mathcal{S} = (-1)^\mathcal{C}$. Given a space-time code $\mathcal{S}$, its binary equivalent code $\mathcal{C}$ is defined by $\mathcal{C} = \zeta^{-1}(\mathcal{S})$.

Theorem 1 suggests that there exists a tradeoff between the rate $R$ and the transmit diversity gain $\nu$ and thus maximum diversity gain can only be achieved at the expense of the rate $R$.

In [2], Hammons and ElGamal present a sufficient criterion on the binary equivalent code $\mathcal{C}$ such that the corresponding space-time code $\mathcal{S} = (-1)^\mathcal{C}$ achieves maximal transmit-diversity gain. This criterion simplifies in the case when $\mathcal{C}$ is a linear code. A sufficient condition for a $(Q \times M)$ space-time code $\mathcal{S} = (-1)^\mathcal{C}$ to have transmit diversity gain at least $\nu$ is given below.

**Lemma 2:** If $\mathcal{C}$ is linear over the binary field $\mathbb{F}_2$ and if for every $[0] \neq C \in \mathcal{C}$ has binary rank at least $\nu$, then the space-time code $\mathcal{S} = (-1)^\mathcal{C}$ achieves transmit-diversity gain at least $\nu$.

**Proof:** The proof is a straightforward generalization of the results in [2] (in the proof by Hammons and ElGamal, we replace the $(Q \times M)$ code matrix $C$ by a $(\nu \times M)$ submatrix of rank $\nu$).

It turns out that one can construct codes that achieve the maximal possible rate $R$ given in Theorem 1 for any given transmit diversity gain $\nu$, $1 \leq \nu \leq Q$. Such a construction appears in the next theorem.

Theorem 3: For any $Q \leq M < \infty$ and $1 \leq \nu \leq Q$, let $R = Q - \nu + 1$ and define the set of code polynomials by

$$\mathcal{F} = \left\{ f(x) : f(x) = \sum_{i=0}^{R-1} f_i x^i, f_i \in \mathbb{F}_2 \right\}.$$

Associate to every code polynomial $f$ in $\mathcal{F}$ the vector

$$\mathcal{L}_f = \left[ f(1) f(\alpha) \ldots f(\alpha^{Q-1}) \right]^T,$$

where $\alpha$ is a primitive element of $\mathbb{F}_{2^M}$. We associate with every code vector $\mathcal{L}_f$, the $(Q \times M)$ code matrix

$$C_f = \left[ f(1) f(\alpha) \ldots f(\alpha^{Q-1}) \right]^T,$$

where by $f(\alpha^i)$ we mean the representation of the element $f(\alpha^i)$ as a binary $(M \times 1)$ column vector. Then the $(Q \times M)$ space-time code

$$\mathcal{S} = \left\{ (-1)^{C_f} : f \in \mathcal{F} \right\}$$

has transmit diversity gain exactly $\nu$.

**Proof:** If $\mathcal{S}$ has transmit diversity gain less than $\nu$, then there exists a vector $\mathcal{L}_f \neq 0$, for some $f \in \mathcal{F}$, such that the corresponding binary matrix $C_f$ has binary rank less than $\nu$ by Lemma 2. So, there exists a binary vector space $\mathcal{B} \subseteq \mathbb{F}_{2^2}$ of dimension $D \geq Q - \nu + 1$, such that for every $b \in \mathcal{B}$

$$b^TC_f = 0 \iff b^T\mathcal{L}_f = 0.$$

But

$$b^T\mathcal{L}_f = \sum_{i=0}^{Q-1} b_i f(\alpha^i) = f \left( \sum_{i=0}^{Q-1} b_i \alpha^i \right),$$

where we have used the fact that every code polynomial $f$ is an additive polynomial, i.e., $f(x)$ satisfies

$$f(x + y) = f(x) + f(y)$$

for every $x, y \in \mathbb{F}_{2^M}$.

Thus, for every $b \in \mathcal{B}$, the element $\sum_{i=0}^{Q-1} b_i \alpha^i$ is a zero of $f(x)$. Moreover, we have

$$\sum_{i=0}^{Q-1} b_i \alpha^i \neq \sum_{i=0}^{Q-1} a_i \alpha^i$$

for any $a_i$.
for \( a \neq b \in \mathcal{B} \) since \( M \geq Q \) and \( \{1, \alpha, \ldots, \alpha^{Q-1}\} \) is a subset of a basis \( \{1, \alpha, \ldots, \alpha^{M-1}\} \) of the field \( \mathbb{F}_{2^M} \) over \( \mathbb{F}_2 \). Thus the code polynomial \( f \) has at least \( |\mathcal{B}| = 2^D \) zeros in \( \mathbb{F}_{2^M} \). However, since \( f \) is a polynomial of degree \( 2^{R-1} \), it follows that \( R \geq D + 1 \) which together with \( D \geq Q - \nu + 1 \) is in contradiction to our assumption that \( R = Q - \nu + 1 \). Thus, every nonzero codeword in \( C \) has binary rank at least \( \nu \) and hence \( \mathcal{S} \) achieves transmit diversity gain at least \( \nu \) by Lemma 2. But from Theorem 1, \( \mathcal{S} \) cannot have transmit diversity gain larger than \( \nu \) since

\[
|\mathcal{S}| = |\mathcal{F}| = 2^{MR}.
\]

We conclude that \( \mathcal{S} \) achieves transmit diversity gain precisely equal to \( \nu \).

One means of implementing the encoder of the \((Q \times M)\) BPSK space-time code described in Theorem 3, is to recognize that the set of vectors \( \xi_f \) form a \([Q, R, \nu] \) linear block code \( D \) over \( \mathbb{F}_{2^M} \) given by

\[
D = \{ \xi_f : f \in \mathcal{F} \},
\]

where \( \xi_f \) and \( \mathcal{F} \) are defined as in Theorem 3. The code \( D \) has generator matrix

\[
G = \begin{bmatrix}
1 & \alpha & \alpha^2 & \ldots & \alpha^{Q-1} \\
1 & \alpha(2) & \alpha(2^2) & \ldots & \alpha(2^{Q-1})(2^1) \\
1 & \alpha(2^2) & \alpha(2^2)^2 & \ldots & \alpha(2^{Q-1})(2^2) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha(2^{R-1}) & \alpha(2^{R-1})^2 & \ldots & \alpha(2^{Q-1})(2^{R-1})
\end{bmatrix}.
\] (5)

This code is not surprisingly, a maximum-distance-separable (MDS) code since it is in fact, a punctured generalized Reed-Solomon code of a special kind.

We next provide an example that illustrates the construction technique.

Example 1: Here we provide an example of a \((3 \times 4)\) BPSK space-time code \( \mathcal{S} \) with desired transmit diversity gain two. Thus \( Q = 3, M = 4, \nu = 2 \). The maximal possible rate \( R \) in this case is \( R = Q - \nu + 1 = 2 \) and such a space-time code \( \mathcal{S} \) can not have more than \( 2^{MR} = 256 \) codewords.

To construct the code, let \( \alpha \) be a zero of the primitive polynomial \( f(x) = x^4 + x + 1 \) over \( \mathbb{F}_2 \). Then \( \alpha \) is a primitive element of the finite field \( \mathbb{F}_{16} \). Thus, by (5) the linear block code \( D \) over \( \mathbb{F}_{16} \) has the following generator matrix:

\[
G = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \end{bmatrix}.
\]

One can use \( \{1, \alpha, \alpha^2, \alpha^3\} \) as a vector-space basis of \( \mathbb{F}_{16} \) over \( \mathbb{F}_2 \) and then \( \{\alpha^{14}, \alpha^2, \alpha, 1\} \) can be verified to be its trace-dual basis [5]. If \( m_{11} = [\alpha \alpha^2]^T \) is the input message vector, then the corresponding codeword \( \xi_1 \) is

\[
\xi_1^T = [\alpha \alpha^2] G = [\alpha^5 \alpha^{10} \alpha^2]
\]

and represents \( \xi_1 \) as a binary matrix \( C_1 \) with respect to the basis \( \{1, \alpha, \alpha^2, \alpha^3\} \), i.e.,

\[
C_1 = \begin{bmatrix} \text{Tr}(\alpha^5 \alpha^{14}) & \text{Tr}(\alpha^5 \alpha^2) & \text{Tr}(\alpha^5 \alpha) & \text{Tr}(\alpha^5) \\
\text{Tr}(\alpha^{10} \alpha^{14}) & \text{Tr}(\alpha^{10} \alpha^2) & \text{Tr}(\alpha^{10} \alpha) & \text{Tr}(\alpha^{10}) \\
\text{Tr}(\alpha^2 \alpha^{14}) & \text{Tr}(\alpha^2 \alpha^2) & \text{Tr}(\alpha^2 \alpha) & \text{Tr}(\alpha^2) \\
0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0
\end{bmatrix}.
\]

Thus, the codeword \((-1)^{C_1}\) is the space-time codeword corresponding to the message vector \( m_{11} \). Suppose we have a second message vector \( m_{21} = [\alpha^2 \alpha^5]^T \). Then this message vector in similar fashion, leads to code matrix:

\[
C_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1
\end{bmatrix}.
\]

The difference matrix

\[
(-1)^{C_1} - (-1)^{C_2} = \begin{bmatrix} 0 & 0 & -2 & 0 \\
0 & 0 & -2 & 0 \\
2 & 0 & -2 & 2
\end{bmatrix}
\]

has rank 2. It can be verified that the code

\[
C = \{ C : \xi_f^T = m^T G, \ m \in \mathbb{F}_{16}^2 \}
\]

is a linear, binary block code of size 256 and that the space-time code given by \((-1)^C\) achieves transmit diversity gain equal to two.

The proof of Theorem 3 relies on the fact that the polynomial \( f(x) \) is additive, and that it cannot have more than \( 2^{R-1} \) zeros. The theorem below, provided without proof, notes that other forms of \( f(x) \) having these two properties would also work.

Theorem 4: For any \( Q \leq M < \infty \) and \( 1 \leq \nu \leq Q \), let \( R = Q - \nu + 1 \). Define the set of code polynomials by

\[
\mathcal{F} = \left\{ f(x) : f(x) = \sum_{i=0}^{R-1} f_i x^{2^i}, \ f_i \in \mathbb{F}_{2^M} \right\}
\]

for some \( 0 \leq e_0 < e_1 < \cdots < e_{R-1} < M \) satisfying the property that every \( f \in \mathcal{F} \) has at most \( 2^{R-1} \) zeros in \( \mathbb{F}_{2^M} \). Let \( \{\beta_m, 0 \leq m < M\} \) be a basis of \( \mathbb{F}_{2^M} \) over \( \mathbb{F}_2 \). Associate to every code polynomial \( f \) in \( \mathcal{F} \) the vector

\[
\xi_f = [f(\beta_0) f(\beta_1) \cdots f(\beta_{Q-1})]^T.
\]

We associate with every code vector \( \xi_f \), the \((Q \times M)\) code matrix

\[
C_f = [f(\beta_0)f(\beta_1)\cdots f(\beta_{Q-1})]^T,
\]

where by \( f(\beta_i) \) we mean the representation of the element \( f(\beta_i) \) as a binary \((M \times 1)\) column vector. Then the \((Q \times M)\) space-time code

\[
\mathcal{S} = \{ (-1)^{C_f} : f \in \mathcal{F} \}
\]

achieves transmit diversity gain exactly \( \nu \).
IV. MAXIMUM RATE QPSK CODES FOR ANY DESIRED TRANSMIT DIVERSITY GAIN

In the QPSK case, it is convenient to work over the integer residue ring \( \mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, \pm1, 2\} \). We first re-define the map \( \zeta \) to relate the codes over \( \mathbb{Z}_4 \) to the codes over the complex field \( \mathbb{C} \).

**Definition 2:** Let \( \zeta : \mathbb{Z}_4^{QM} \rightarrow \mathbb{C}^{QM} \) be the map given by
\[
\zeta(C) = \zeta([C_{qm}]) = [\theta^{C_{qm}}] = S,
\]
where \( \theta = \sqrt{-1} \). We use the notation \( \theta^C \) to denote the matrix \( S = \zeta(C) \). Let \( \mathcal{C} \) be the collection of \( \{0, 1, 2, -1\} \) matrices associated to \( \{1, \theta, \theta^2, \theta^3\} \) code matrices in \( S \). We extend notation in a natural way and write \( S = \theta^S \). Given a space-time code \( S \), its quaternary equivalent code \( \mathcal{C} \) is defined by \( \mathcal{C} = \zeta^{-1}(S) \).

For any \((Q \times M)\) matrix \( C \) over \( \mathbb{Z}_4 \), Hammons and El Gamal [2] defined the binary-valued row-based indicant projection \( \Xi(C) \) and column-based indicant projection \( \Psi(C) \). Furthermore, a sufficient criterion for constructing QPSK space-time codes with full transmit diversity gain is provided in [2].

As in the binary case, one can generalize the results in [2] to obtain a design criterion for the quaternary codes even in the case when the desired rank, i.e., transmit diversity gain, is less than the maximum possible.

**Lemma 5:** If \( \mathcal{C} \) is a linear code over \( \mathbb{Z}_4 \) and if for every \( 0 \neq C \in \mathcal{C} \), either \( \Xi(C) \) or \( \Psi(C) \) has binary rank at least \( \nu \), then the space-time code \( S = \theta^S \) achieves transmit diversity gain at least \( \nu \).

**Proof:** Follows from a straightforward generalization of the results in [2]. One uses the fact that \( \mathcal{C} \) is a linear code and applies the criterion in [2] to an appropriate submatrix of size \( \nu \times M \).

Our construction in the QPSK case will parallel that in the BPSK case. In place of finite fields, we work this time over an appropriate Galois ring. To construct a \((Q \times M)\) QPSK space-time code, we work over the Galois ring \( \mathcal{R} := GR(4, M) \), of characteristics 4 having \( 4^M \) elements. For more details on Galois rings, we refer the readers to [3], [6], and [8].

Every such ring \( \mathcal{R} \) is isomorphic to the residue class ring \( \mathbb{Z}_4[x]/(f(x)) \), where \( f(x) \) is a monic basic irreducible polynomial of degree \( M \) over \( \mathbb{Z}_4 \). It can be shown that \( \mathcal{R} \) is a local ring whose unique maximal ideal is the ideal generated by 2. The quotient is isomorphic to a finite field of characteristic 2, i.e., \( \mathcal{R}/(2) \cong \mathbb{F}_{2^M} \). The units of \( \mathcal{R} \) form a multiplicative group \( \mathcal{R}^* \) having the following group structure:
\[
\mathcal{R}^* \cong \mathbb{Z}_{2^M-1} \bigoplus_{i=1}^M \mathbb{Z}_2.
\]
Let \( \xi \in \mathcal{R}^* \) be a generator of the cyclic subgroup \( \mathbb{Z}_{2^M-1} \) of \( \mathcal{R}^* \) and define the set
\[
\mathcal{T} = \left\{0, 1, \xi, \cdots, \xi^{2^M-2}\right\}.
\]
It turns out that every element \( r \in \mathcal{R} \) has a unique \( 2\)-adic expression, i.e., \( r \) can be uniquely expressed as
\[
r = a + 2b
\]
for some \( a, b \in \mathcal{T} \). On the other hand, the set \( \{1, \xi, \xi^2, \cdots, \xi^{M-1}\} \) is linearly independent over \( \mathbb{Z}_4 \) and the ring \( \mathcal{R} \) can be expressed as a \( \mathbb{Z}_4 \)-module, i.e., every element \( r \in \mathcal{R} \) can be uniquely expressed as
\[
r = \sum_{i=0}^{M-1} r_i \xi^i
\]
for some \( r_i \in \mathbb{Z}_4 \).

We summarize below some other facts that will be used shortly.

**Proposition 6** ([8]) Let \( \phi \) denote the residue map \( \phi : \mathcal{R} \rightarrow \mathcal{R}/(2) \) and extend \( \phi \) to the polynomial ring in a natural way.

(i) Let \( f(x) \) be a basic primitive polynomial i.e., a polynomial over \( \mathbb{Z}_4 \) whose reduction modulo 2 is a primitive binary polynomial. If \( \xi \) is a zero of \( f(x) \) of degree \( M \) over \( \mathbb{Z}_4 \), then \( \xi \) is the generator of the cyclic subgroup of \( \mathcal{R}^* \) isomorphic to \( \mathbb{Z}_{2^M-1} \), if and only if \( f(x) \) is a basic primitive polynomial.

(ii) \( \phi(\xi) \) is a primitive element in the finite field \( \mathbb{F}_{2^M} \) and
\[
\phi(\mathcal{R}) \cong \mathbb{F}_{2^M}.
\]

We will now show that for any \( \nu \leq Q \leq M < \infty \) it is possible to construct a \((Q \times M)\) QPSK space-time code that achieves transmit diversity \( \nu \) and maximum possible rate \( R \) given by \( R = Q - \nu + 1 \).

**Theorem 7:** For any \( Q \leq M < \infty \) and \( 1 \leq \nu \leq Q \), let \( R = Q - \nu + 1 \) and let \( \mathcal{R} \) and \( \xi \) be defined as before. Define the set of code polynomials by
\[
\mathcal{F} = \left\{ f(x) : f(x) = \sum_{i=0}^{R-1} f_i x^{2^i} : f_i \in \mathcal{R} \right\}.
\]
Associate to every code polynomial \( f(x) \) in \( \mathcal{F} \) the code vector
\[
\mathcal{L}_f = \left[ f(1) \ f(\xi) \ \cdots \ f(\xi^{Q-1}) \right]^T.
\]
We associate with every code vector \( \mathcal{L}_f \), the \( Q \times M \) code matrix
\[
\mathcal{C}_f = \left[ f(1) \ f(\xi) \ \cdots \ f(\xi^{Q-1}) \right]^T,
\]
where by \( f(a^i) \) we mean the representation of the element \( f(a^i) \) as a quaternary \((M \times 1)\) column vector, i.e., an element of \( \mathbb{Z}_4^M \). Then the \((Q \times M)\) space-time code
\[
\mathcal{S} = \{\theta^{C_f} : f \in \mathcal{F}\}
\]
has transmit diversity gain exactly \( \nu \).

**Proof:** Define the sets
\[
\mathcal{L} = \{C_f : f \in \mathcal{F}\} \quad \text{and} \quad \mathcal{C} = \{C_f : f \in \mathcal{F}\}
\]
where
\[ F' = \left\{ f(x) : f(x) = \sum_{i=0}^{R-1} f_i x^i, f_i \in \mathcal{T} \right\}. \]

From the 2-adic representation of \( \{f_i\} \) in \( \mathcal{R} \) it follows that
\[ \mathcal{F} = \mathcal{F}' \oplus 2\mathcal{F}' \quad \text{and} \quad \mathcal{C} = \mathcal{L} \oplus 2\mathcal{L}. \]

From Proposition 6 and Theorem 3 we have that for any \( C \in \mathcal{C} \setminus 2\mathcal{L} \), the matrix \( \phi(C) \) has binary rank at least \( \nu \). With regard to binary rank we have
\[ \text{rank}(\phi(C)) \leq \text{rank}(\Xi(C)) \]
and hence \( \Xi(C) \) has binary rank at least \( \nu \). Similarly, for \( [0] \neq C \in 2\mathcal{L} \), the code \( \phi(C/2) \) also has binary at least \( \nu \) so that \( \Xi(C) \) has binary rank at least \( \nu \). It follows from Theorem 1 and Lemma 5 that the code \( \mathcal{S} = \theta^C \) achieves transmit diversity precisely \( \nu \).

Similar to the binary case, the set \( \mathcal{D} \) defined by
\[ \mathcal{D} = \{ \xi f : f \in \mathcal{F} \}, \]
where \( \xi f \) and \( \mathcal{F} \) are defined as in Theorem 7, is in fact an MDS \( [Q, R, \nu] \) linear block code over the Galois ring \( \mathcal{R} \) having generator matrix
\[ G = \begin{bmatrix} 1 & \xi & \xi^2 & \ldots & \xi^{Q-1} \\ 1 & \xi^2 & \xi^{2^2} & \ldots & \xi^{(Q-1)(2^1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{(2^{R-1}-1)} & \xi^{2(2^{R-1}-2)} & \ldots & \xi^{(Q-1)(2^{R-1})} \end{bmatrix}. \quad (6) \]

Example 2: We want to construct a \((3 \times 4)\) QPSK space-time code \( \mathcal{S} \) with desired transmit diversity gain two. The maximal possible rate \( \mathcal{R} \) in this case is \( \mathcal{R} = 4 - \nu + 1 = 2 \) and such a space-time code \( \mathcal{S} \) can not have more than \( 4^{MR} = 65536 \) codewords.

Earlier, in Example 1 we chose \( f(x) = x^4 + x + 1 \) to be the primitive polynomial for \( \mathbb{F}_{16} \). By making use of Hensel’s lift \([6]\) on \( f(x) \) we can obtain a basic primitive polynomial \( g(x) \) for the Galois ring \( \mathcal{R} = GR(4, 4) \). To be more specific, we have
\[ g(x^2) = f(x) f(-x) \equiv x^8 + 2x^4 - x^2 + 1 \pmod{4} \]
and hence \( g(x) = x^4 + 2x^2 - x + 1 \).

To construct the code, let \( \xi \) be a zero of the basic primitive polynomial \( g(x) \) specified above. As in Example 1, we form the MDS linear block code \( \mathcal{D} \) over the ring \( \mathcal{R} \) having generator matrix:
\[ G = \begin{bmatrix} 1 & \xi & \xi^2 & \xi^3 \\ 1 & 1 & \xi^2 & \xi^4 \end{bmatrix}. \]

We use \( \{1, \xi, \xi^2, \xi^3\} \) as a basis of \( \mathcal{R} \) over \( \mathbb{Z}_4 \) and \( \{\xi^{14} + 2, \xi^2 + 2\xi^8, -\xi, -1\} \) is its trace-dual basis. If \( m_1 = [\xi \xi^2]^T \) is the input message vector, then the corresponding codeword \( \xi_1 \) is
\[ \xi_1^T = [\xi \xi^2]G = [\xi^2 + \xi \xi^2 + \xi^4 \xi^3 + \xi^6] = [\xi^3 + 2\xi^6 \xi^{10} + 2\xi^4 \xi^2 + 2\xi^{12}]. \]

Representing \( \xi_1 \) as a quaternary matrix \( C_1 \) with respect to the basis \( \{1, \xi, \xi^2, \xi^3\} \) results in
\[ C_1 = \begin{bmatrix} 0 & -1 & 1 & 2 \\ -1 & 1 & -1 & 2 \\ 0 & 0 & 1 & 0 \end{bmatrix} + 2 \begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ -1 & 1 & -1 & 0 \\ 2 & 2 & -1 & 2 \end{bmatrix}. \]

Thus, the codeword \( \theta^{C_1} \) is the space-time codeword corresponding to the message vector \( m_1 = [\xi^2 \xi^3]^T \) and the corresponding codeword \( \xi_2 \) is
\[ \xi_2 = [\xi + 2\xi^{11} \xi^4 + 2\xi^5 \xi^{14} + 2\xi^{14}]. \]

Representing \( \xi_2 \) as a quaternary matrix gives
\[ C_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix} + 2 \begin{bmatrix} 2 & 1 & 1 & -1 \\ 0 & -1 & 1 & 2 \\ 1 & 2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 2 & 2 \\ -1 & -1 & 0 & 0 \\ -1 & 2 & 0 & 1 \end{bmatrix}. \]

Now the difference matrix
\[ \theta^{C_1} - \theta^{C_2} = \begin{bmatrix} 0 & 2\theta & 1 & \theta & 2 \\ 0 & 2\theta & -1 & -\theta & 0 \\ -1 + \theta & 0 & -1 & -\theta & -1 - \theta \end{bmatrix} \]
has rank 3. It can be verified that the code
\[ C = \{ C : \xi^T G = m^T G, m \in \mathcal{R}^2 \} \]
is a quaternary linear block code of size 65536 and the space-time code given by \( \theta^C \) will achieve transmit diversity gain exactly two.

We note moreover, that
\[ \phi(C_1) = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad \phi(C_2) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \]
which are exactly the codewords generated in Example 1. □

Using the same argument in the binary case, we state without proof, the following generalization of the above construction.

**Theorem 8:** For any \( Q \leq M < \infty \) and \( 1 \leq \nu \leq Q \), let \( R = Q - \nu + 1 \) and let \( \mathcal{R} \) and \( \xi \) be defined as before. Define the set of code polynomials by
\[ \mathcal{F} = \left\{ f(x) : f(x) = \sum_{i=0}^{R-1} f_i x^{2^i}, f_i \in \mathcal{R} \right\} \]
for some $0 \leq e_0 < e_1 < \cdots < e_{R-1} < M$ satisfying the property that for every $f \in \mathcal{F}$, the polynomial $\phi(f)$ has at most $2^{R-1}$ zeros in $\mathbb{F}_2^M$. Let $\{\beta_m, \ 0 \leq m < M\} \subset \mathcal{R}$ be a linear independent set over $\mathbb{Z}_4$. Associate to every code polynomial $f$ in $\mathcal{F}$, the $(Q \times M)$ code matrix

$$C_f = \begin{bmatrix} f(\beta_0) & f(\beta_1) & \cdots & f(\beta_{Q-1}) \end{bmatrix}^T,$$

where by $f(\beta_i)$ we mean the representation of the element $f(\beta_i)$ as a quaternary $(M \times 1)$ column vector. Then the $(Q \times M)$ space-time code

$$S = \{\theta^{C_f} : f(x) \in \mathcal{F}\}$$

has transmit diversity gain exactly $\nu$. □

REFERENCES


