Space-Time Constellation-Rotating Codes Maximizing Diversity and Coding Gains*

Yan Xin, Zhengdao Wang, and Georgios B. Giannakis

Dept. of ECE, Univ. of Minnesota; 200 Union Str. SE, Minneapolis, MN 55455, USA

Abstract— **We apply algebraic number theoretic tools to design linear space-time constellation-rotating (ST-CR) block codes. With an arbitrary number of M transmit- and N receive-antennas, our ST-CR designs achieve 1 symbol/second rate and enjoy maximum diversity gains MN over quasi-static fading channels. When M is an Euler number $\phi(P)$ for $P \not\equiv 0 \pmod 4$, or, when $M = 2^m$ for some positive integer m, the designed ST-CR precoders also maximize coding gains over QAM constellations. When M takes other integer values, we construct a method to design precoders with large coding gains that can be computed explicitly. Simulations corroborate our theoretical findings.**

I. Introduction

Spatial diversity is implemented by deploying multiple transmit and/or receive antennas at base stations and/or at mobile units. Because of size and power limitations at mobile units, multi-antenna receive diversity is more appropriate for the uplink rather than the downlink. As a result, transmit diversity schemes have attracted considerable interest recently (see e.g., [1, 6] and references therein).

Space-time (ST) trellis codes enjoy maximum diversity and large coding gains but decoding complexity grows exponentially in the transmission rate [7], which does not encourage usage of large size constellations. On the other hand, ST orthogonal designs (ST-OD) [1, 6] offer maximum transmit diversity and afford linear decoding with remarkably low complexity. Unfortunately, ST-OD codes come with reduced transmission rates when complex constellations are used and the number of transmit antennas M is greater than two. Constellation Rotating (CR) codes on the other hand do not sacrifice rate for single-antenna [2], or ST multi-antenna diversity systems [3, 9, 10].

This paper builds on [9, 10] and derives important methodologies for constructing ST-CR precoders using algebraic number theoretic tools. The design of linear unitary precoders based on parameterizations of unitary matrices is carried out through computer search [3, 9]. Such designs are infeasible when either the number of transmit antennas or the constellation size is large. Algebraic number theoretic approaches are possible for designing linear precoders with reasonably good coding gains [2, 4], even when M and/or the constellation size is large. Without computer search, the systematic construction of linear unitary precoders which can achieve maximum diversity gains is restricted to cases where $M = 2^m$ for $m \in \mathbb{N}$ [4].

Based on the analysis in [9, 10] on diversity and coding gains, we first construct both unitary and non-unitary linear ST-CR precoders for any M that can achieve maximum diversity gain MN and a lower-bounded coding gain. We also find a tight upper bound on the coding gain. When M is an Euler number [1] $\phi(P)$, for $P \not\equiv 0 \pmod 4$, or, when $M = 2^m$ for a positive integer m, we construct linear precoders that achieve maximum coding gains. When M is an odd integer, we can still construct linear precoders with large coding gains that can be computed explicitly although they can not achieve the upper bound of coding gains.

Notation: Bold lower (upper) case letters are used to denote vectors (matrices). T and $\mathcal{H}$ represent transpose and conjugate transpose of a matrix, respectively. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are used to denote the positive integer set, the integer ring, the rational number field, the real number field, and the complex number field, respectively. diag$\{\cdot\}$ denotes a diagonal matrix.

II. Design Criteria of ST-CR Precoders

In this section, we describe the system model of ST-CR codes and review briefly performance analysis results and pertinent design criteria detailed in [9, 10].

A. ST-CR Precoding Scheme

With reference to Figure 1, let us consider a wireless link with M transmit and N receive antennas over Rayleigh flat fading channels. The symbol stream $\sqrt{\mathcal{E}_s}s_i$ from the constellation set $\mathcal{C}$ is first parsed into $T_0 \times 1$ signal vectors $\mathbf{s}$, and then it is linearly precoded by a $T_0 \times T_0$ matrix $\mathbf{\Theta}$, where $\mathcal{E}_s$ denotes the average symbol energy. The precoded block $\sqrt{\mathcal{E}_s}\mathbf{\Theta s}$ is fed to an ST encoder. The ST encoder maps $\sqrt{\mathcal{E}_s}\mathbf{\Theta s}$ to an $M \times T_0$ code matrix $\bar{\mathbf{S}}$ that is sent over the M antennas during T_0 time intervals. Specifically, the (m, i)th entry $\bar{s}_{mi} := \sqrt{\mathcal{E}_s}u_{mi}\boldsymbol{\theta}_i^T\mathbf{s}$, is transmitted through the mth antenna at the ith time interval, where u_{mi} denotes the (m, i)th entry of a unitary matrix $\mathbf{U}$, i.e., $[\mathbf{U}]_{mi} := u_{mi}$, vector $\boldsymbol{\theta}_i^T$ denotes the ith row of $\mathbf{\Theta}$, and T_0 is chosen equal to M. Defining $\mathbf{D_s} := \sqrt{\mathcal{E}_s}\text{diag}\{\boldsymbol{\theta}_1^T\mathbf{s}, \ldots, \boldsymbol{\theta}_M^T\mathbf{s}\}$, we can thus write the $M \times M$ transmitted ST-CR code matrix as $\bar{\mathbf{S}} = \mathbf{UD_s}$. The signal x_{ni} received by antenna n at the ith time interval after receive-filtering and symbol rate sampling is given by:

$$x_{ni} = \sqrt{\mathcal{E}_s}\sum_{m=1}^{M} h_{nm}u_{mi}\boldsymbol{\theta}_i^T\mathbf{s} + w_{ni}, \tag{1}$$

where h_{nm} denotes the fading coefficient between the mth transmitter and nth receiver antenna. We assume that i) h_{nm}'s are i.i.d. zero mean complex Gaussian with variance 0.5 per dimension; ii) h_{nm}'s are known to the receiver and invariant over T_0 time intervals (*quasi-static flat fading*); iii) w_{ni}

*Supported by the NSF Wireless Initiative grant no. 99-79443

[1] *Euler number* $\phi(P)$ is defined as the number of positive integers $< P$ which are relatively prime to P.

is zero-mean complex Gaussian noise with variance $\sigma^2/2$ per dimension.

Let $\mathbf{X}$ be the $N \times M$ received signal matrix with (n,i)th entry $[\mathbf{X}]_{ni} = x_{ni}$; $\mathbf{H}_o$ the $N \times M$ channel matrix with $[\mathbf{H}_o]_{nm} = h_{nm}$; and $\bar{\mathbf{W}}$ the $N \times M$ noise matrix with $[\bar{\mathbf{W}}]_{ni} = w_{ni}$. Applying these notational conventions, under the quasi-static fading assumption ii), we can re-write (1) in matrix form as follows:

$$\mathbf{X} = \bar{\mathbf{H}}_o \mathbf{S} + \bar{\mathbf{W}} = \mathbf{H}_o \mathbf{D}_{\mathbf{s}} + \bar{\mathbf{W}}. \tag{2}$$

B. Performance analysis and design criteria

Optimality criteria for selecting $\boldsymbol{\Theta}$ have been derived in [9,10] based on maximum likelihood (ML) detection and pairwise error probability analysis. Briefly, defining the matrix error event $\{\mathbf{D}_{\mathbf{s}} \to \mathbf{D}_{\tilde{\mathbf{s}}}\}$ as the event that the receiver decodes $\mathbf{D}_{\tilde{\mathbf{s}}} := \sqrt{\mathcal{E}_s}\text{diag}\{\boldsymbol{\theta}_1^T\tilde{\mathbf{s}}, \ldots, \boldsymbol{\theta}_M^T\tilde{\mathbf{s}}\}$ erroneously, when $\mathbf{D}_{\mathbf{s}}$ is actually sent, we have at high SNR

$$P(\mathbf{D}_{\mathbf{s}} \to \mathbf{D}_{\tilde{\mathbf{s}}}) \approx \frac{C_\Theta \left(\frac{\bar{\gamma}}{4}\right)^{-|\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}|N}}{\left(\prod_{m\in\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}} |\boldsymbol{\theta}_m^T(\mathbf{s}-\tilde{\mathbf{s}})|^2\right)^N}, \tag{3}$$

where $C_\Theta := \frac{(2N-1)!!}{(2N)!!}(1/2)^{M-|\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}|}$, and !! stands for odd (or even) order factorial, $\bar{\gamma} := E(|h_{nm}|^2)\mathcal{E}_s/N_0 = \mathcal{E}_s/N_0$ and $N_0 := \sigma^2$, where E denotes expectation, and $\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}} := \{m : |\boldsymbol{\theta}_m^T(\mathbf{s}-\tilde{\mathbf{s}})|^2 \neq 0\}$, whose cardinality is $|\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}|$. Based on (3), the following design criteria for linear precoders $\boldsymbol{\Theta}$ are proposed in [9,10] for ST-CR precoders:

i) Diversity Gain. Define $\mu := \min_{\{\mathbf{s}\neq\tilde{\mathbf{s}}\}}|\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}|$ over all distinct pairs of $\{\mathbf{s},\tilde{\mathbf{s}}\}$. The negative slope μN of the BER vs. SNR curve is defined as the *diversity gain* achieved by $\boldsymbol{\Theta}$ with N receive-antennas. Recalling the definition of $\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}$, we infer that the maximum $\mu = M$ is achieved when the following *maximum transmit-diversity condition* holds true:

$$|\boldsymbol{\theta}_m^T(\mathbf{s}-\tilde{\mathbf{s}})| \neq 0, \quad \forall\, m \in [1, M], \forall\, \mathbf{s} \neq \tilde{\mathbf{s}} \in \mathcal{C}^M. \tag{4}$$

ii) Coding Gain. For a given diversity gain μ, the *coding gain* ν_μ is defined as follows:

$$\nu_\mu = \min_{\mathbf{s}\neq\tilde{\mathbf{s}}} \left[C_\Theta^{-\frac{1}{N}} \prod_{m\in\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}} |\boldsymbol{\theta}_m^T(\mathbf{s}-\tilde{\mathbf{s}})|^2 \right]^{\frac{1}{\mu}}. \tag{5}$$

When $\mu = M$, the coding gain becomes: $\nu_M = C_\Theta^{-\frac{1}{MN}}\delta^{\frac{2}{M}}$, where we have defined the *minimum product distance* to be $\delta := \min_{\mathbf{s}\neq\tilde{\mathbf{s}}}\prod_{m=1}^M |\boldsymbol{\theta}_m^T(\mathbf{s}-\tilde{\mathbf{s}})|$. Note that (4) is equivalent to having $\delta \neq 0$.

When the diversity gain is μN, the coding gain ν_μ measures the savings in SNR of the linear precoded system as compared to an ideal benchmark system with BER $\approx (\bar{\gamma}/4)^{-\mu N}$ at high SNR. Certainly, the diversity gain μN, the coding gain ν_μ, and the kissing number κ all depend on the choice of the precoder $\boldsymbol{\Theta}$. For *high* SNR, it is reasonable to maximize the diversity gain first because it determines the slope of the BER-SNR curve. Within the class of $\boldsymbol{\Theta}$'s that achieve diversity gain μ, the coding gain ν_μ should be maximized afterwards.

III. Algebraic ST-CR Constructions

The existence of diversity-maximizing linear precoders was established in [4,9]. Ensured by this result, we are now motivated to look for a linear precoder $\boldsymbol{\Theta}$ that maximizes the coding gains within the class of diversity-maximizing precoders. For precoders that achieve the maximum diversity gain MN, the parameter $C_{\boldsymbol{\Theta}}$ in (3) becomes independent of $\boldsymbol{\Theta}$ because $|\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}| = M$. Subject to the power constraint: $E(\|\boldsymbol{\Theta}\mathbf{s}\|^2) = E(\|\mathbf{s}\|^2) = M$, the resulting optimization problem can thus be formulated as follows [c.f. (5)]:

$$\boldsymbol{\Theta}_{\text{opt}} = \underset{\substack{E(\|\boldsymbol{\Theta}\mathbf{s}\|^2)=E(\|\mathbf{s}\|^2)\\ =M}}{\arg\max} \; \min_{\mathbf{s}\neq\tilde{\mathbf{s}}} \prod_{m=1}^M |\boldsymbol{\theta}_m^T(\mathbf{s}-\tilde{\mathbf{s}})|^2. \tag{6}$$

In other words, the optimum precoder $\boldsymbol{\Theta}_{\texttt{opt}}$ in (6) which maximizes the coding gains maximizes the minimum product distance δ when $|\mathcal{M}_{\mathbf{s},\tilde{\mathbf{s}}}| = M$. In the sequel, we will focus on the minimum product distance which can be easily related to the coding gain according to (5).

A. Algebraic number theory preliminaries

We start by briefly introducing some necessary definitions and results from [4] for the completeness of the exposition.

Definition 1 *(Cyclotomic Polynomials)* : If $P \in \mathbb{N}$, the Pth cyclotomic polynomial is defined as $\Phi_P(x) = \prod_{\text{gcd}(i,P)=1}(x - \alpha^i)$ $(1 \leq i \leq P)$, where $\alpha := e^{j2\pi/P}$ with $j := \sqrt{-1}$. The degree of $\Phi_P(x)$ is $\phi(P)$, where $\phi(P)$ is an Euler number.

Definition 2 *(Extension of an embedding)* : An embedding η is a ring monomorphism of $\mathbb{Q}(j)(\alpha)$ in $\mathbb{C}$, and if η is an embedding of $\mathbb{Q}(j)(\alpha)$ in $\mathbb{C}$ such that $\eta(z) = z\ \forall z \in \mathbb{Q}(j)$, then η is called an $\mathbb{Q}(j)$-isomorphism of $\mathbb{Q}(j)(\alpha)$.

Definition 3 *(Relative norm of a field)* : Let $\alpha := \alpha_0, \ldots, \alpha_{M-1}$ denote the complex roots of the minimal polynomial of α; and let $\eta_m(\alpha) := \alpha_m$ for $m = 0, 1, \ldots, M-1$ be M distinct $\mathbb{Q}(j)$-isomorphisms of $\mathbb{Q}(j)(\alpha)$. Consider $\beta \in \mathbb{Q}(j)(\alpha)$, and define the relative norm of β from the field $\mathbb{Q}(j)(\alpha)$ as $\mathcal{N}(\beta) := \mathcal{N}_{\mathbb{Q}(j)(\alpha)/\mathbb{Q}(j)}(\beta) := \prod_{m=0}^{M-1}\eta_m(\beta)$.

Definition 4 *(Integral over $\mathbb{Z}[j]$)* : An element β of $\mathbb{Q}(j)(\alpha)$ is said to be an integral over $\mathbb{Z}[j]$ if β is a root of a monic polynomial with coefficients in $\mathbb{Z}[j]$. Clearly, every element in $\mathbb{Z}[j]$ is an integral over $\mathbb{Z}[j]$.

Result 1: The $\Phi_P(x)$ polynomial is the minimal polynomial of α over $\mathbb{Q}$ and $\Phi_P(\alpha^i) = 0\ \forall\, i \in \mathbb{Z}$ such that $\text{gcd}(i,n) = 1$.

Result 2: If $M = 2^m$ with $m \in \mathbb{N}$, then the minimal polynomial of $\alpha := \exp(2j\pi/4M)$ over $\mathbb{Q}(j)$ is $x^M - j$ with all distinct roots $\alpha_m := \alpha e^{j2\pi m/M}$, $m \in [0, M-1]$.

Result 3: If $\mathbb{Q}(j)(\alpha)$ is a finite extension of the field $\mathbb{Q}(j)$ with degree denoted by $[\mathbb{Q}(j)(\alpha) : \mathbb{Q}(j)] = M$, then $\{1, \alpha, \ldots, \alpha^{M-1}\}$ forms a basis of $\mathbb{Q}(j)(\alpha)$ over $\mathbb{Q}(j)$.

Result 4: The set of elements of $\mathbb{Q}(j)(\alpha)$ which are integral over $\mathbb{Z}[j]$ is a subring of $\mathbb{Q}(j)(\alpha)$ containing $\mathbb{Z}[j]$.

Result 5: If $\beta \in \mathbb{Q}(j)(\alpha)$ is integral over $\mathbb{Z}[j]$, then the relative norm of β from $\mathbb{Q}(j)(\alpha) \in \mathbb{Z}[j]$.

B. ST-CR constructions and coding gain bounds

Before presenting our constructions that are based on the algebraic results of the previous subsection, we first state without proof the following lemmas:

Lemma 1: *If $\phi(P) = 4n+2$ for $n \in \mathbb{N}$, then $P \not\equiv 0 \pmod 4$.*

Lemma 2: *If $P \not\equiv 0 \pmod 4$, then the minimal polynomial of $\alpha := e^{j2\pi/P}$ over $\mathbb{Q}(j)$ is $\Phi_P(x)$ and its degree is $\phi(P)$.*

Lemma 3: *All roots of the minimal polynomial of $\alpha := e^{j2\pi/P}$ for some $P \in \mathbb{N}$ over $\mathbb{Q}(j)$ have modulus 1.*

We propose two construction rules for constructing linear precoders. Construction A develops linear precoders for any $M \in \mathbb{N}$. However, only when $M = 2^m$ ($m \in \mathbb{N}$), the construction yields unitary precoders. As unitary precoders preserve the energy and the Euclidean distance among constellation points, unitary precoders do not alter the system performance when the channel is AWGN and are thus desirable whenever possible. Therefore, we propose construction B specially for constructing *unitary* precoders for any $M \neq 2^m$.

- *Construction A*: Let α be integral over $\mathbb{Z}[j]$. We construct the following linear precoder (see also [2, 4, 10]):

$$\mathbf{\Theta}_M = \frac{1}{\psi}\begin{pmatrix} 1 & \alpha_0 & \dots & \alpha_0^{M-1} \\ 1 & \alpha_1 & \dots & \alpha_1^{M-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_{M-1} & \dots & \alpha_{M-1}^{M-1} \end{pmatrix}, \qquad (7)$$

where $[\mathbb{Q}(j)(\alpha) : \mathbb{Q}(j)] = M$, α_m ($m \in [0, M-1]$) are roots of the minimal polynomial of α over $\mathbb{Q}(j)$, $\alpha_0 := \alpha$, and $1/\psi$ is the normalizing factor that enforces the power constraint: $E(\|\mathbf{\Theta}_M \mathbf{s}\|^2) = E(\|\mathbf{s}\|^2) = M$.

- *Construction B*: We consider *unitary* precoding matrices in the form $\mathbf{\Theta}_M := \mathbf{F}_M \text{diag}\{1, \alpha, \dots, \alpha^{M-1}\}$, where $\alpha := e^{j2\pi/P}$ for $M, P \in \mathbb{N}$ and $\mathbf{F}_M$ is the M-point inverse fast Fourier transform (IFFT) matrix.

The relative norm of a field is closely related to the product distance of $\mathbf{\Theta s}$, when $\mathbf{\Theta}$ is constructed based on the algebraic design (7). For all constellations carved from the cubic lattice $\mathbb{Z}[j]$, that is, $\mathbf{s} \in (\mathbb{Z}[j])^M$, $\boldsymbol{\theta}_m^T \mathbf{s}$ ($m \in [0, M-1]$) are integral over $\mathbb{Z}[j]$ according to Construction A. As the absolute value of the norm of β from the field $\mathbb{Q}(j)(\alpha)$ is always ≥ 1 when $\beta \neq 0$ is integral over $\mathbb{Z}[j]$, the minimum product distance will be lower bounded for these constellations. We rely on the following two lemmas to find values of M that achieve the maximum coding gains by Construction A.

Lemma 4: *If α in (7) is integral over $\mathbb{Z}[j]$, then $1/\psi \leq 1/\sqrt{M}$, and the equality holds if only if all roots α_m ($m \in [0, M-1]$) have modulus 1.*

Lemma 5: *If $M > 1$ is an odd integer, α is integral over $\mathbb{Z}[j]$, and $[\mathbb{Q}(j)(\alpha) : \mathbb{Q}(j)] = M$, then not all roots of the minimal polynomial of α over $\mathbb{Q}(j)$ have modulus 1. In other words, we have $1/\psi < 1/\sqrt{M}$ in (7).*

Let us define the set $\mathcal{S}_M := \{M : M$ is the degree of the minimal polynomial of $\alpha := e^{j2\pi/P}$ over $\mathbb{Q}(j)$ for some $P \in \mathbb{N}\}$. Values in this set are special to our goal of maximizing the coding gain, as we will see soon. By Lemma 2 and Result 2, we know $M = \phi(P)$ for $P \not\equiv 0 \pmod 4$ or $M = 2^m$ for $m \in \mathbb{N}$ belong to $\mathcal{S}_M$. On the other hand, according to Lemmas 3 and 5, odd integers $M > 1$ do not belong to $\mathcal{S}_M$.

We study next properties of our Construction A, and establish the following theorems on their coding gains:

Theorem 1 *(Lower bound on coding gains) If one applies $\mathbf{\Theta}_M$ in (7) to rotate the constellation curved from $\mathbb{Z}[j]$ and normalized by $\sqrt{\mathcal{E}_s}$, then $\delta^{2/M} \geq (\psi^2 \mathcal{E}_s)^{-1}$.*

Proof: For any distinct $\mathbf{s}$ and $\tilde{\mathbf{s}}$, we define $f(\alpha) := \sum_{k=0}^{M-1} \sqrt{\mathcal{E}_s}(s_k - \tilde{s}_k)\alpha^k$. As M is the degree of the minimal polynomial of α over $\mathbb{Q}(j)$, $\{1, \alpha, \dots, \alpha^{M-1}\}$ are linearly independent by Result 3. We infer that $f(\alpha) \neq 0$; so, $\mathcal{N}(f(\alpha)) := \prod_{m=0}^{M-1} \eta_m(f(\alpha)) = \prod_{m=0}^{M-1} f(\alpha_m) \neq 0$.

Moreover, from Definition 4 and Result 4, it follows that $f(\alpha)$ is integral over $\mathbb{Z}[j]$. But using Result 5, we have that $\mathcal{N}(f(\alpha)) \in \mathbb{Z}[j] \setminus 0$, which implies that $|\mathcal{N}(f(\alpha))| \geq 1$. Hence, we have

$$\prod_{m=0}^{M-1} |\boldsymbol{\theta}_m^T \sqrt{\mathcal{E}_s}(\mathbf{s} - \tilde{\mathbf{s}})| = \frac{1}{\psi^M} \prod_{m=0}^{M-1} \left| \sum_{k=0}^{M-1} \sqrt{\mathcal{E}_s}(s_k - \tilde{s}_k)\alpha_m^k \right|$$

$$= \frac{1}{\psi^M} \left| \prod_{m=0}^{M-1} f(\alpha_m) \right| = \frac{1}{\psi^M} |\mathcal{N}(f(\alpha))| \geq \frac{1}{\psi^M} \qquad (8)$$

Therefore, by the definition of δ, we infer that

$$\mathcal{E}_s \delta^{2/M} = \left(\prod_{m=0}^{M-1} |\boldsymbol{\theta}_m^T \sqrt{\mathcal{E}_s}(\mathbf{s} - \tilde{\mathbf{s}})| \right)^{\frac{2}{M}} \geq \frac{1}{\psi^2}. \quad \square$$

Theorem 2 *(Upper bound on coding gains for QAM) Consider a QAM constellation $\mathcal{C}$ with signal points from $(2k-1-Q)d + j(2l-1-Q)d$ where $k,l \in [1,Q]$ and $d \in \mathbb{N}$, and is normalized by $\sqrt{\mathcal{E}_s}$. Among all linear precoders which are subject to the power constraint $E(\|\mathbf{\Theta s}\|^2) = E(\|\mathbf{s}\|^2) = M$, the maximum minimum product distance is given by*

$$\delta_{\max} \leq 4\left[d^2/(M\mathcal{E}_s) \right]^{M/2}. \qquad (9)$$

In particular, for the linear precoders of (7), we have

$$\delta \leq \left[4d^2/(\psi^2 \mathcal{E}_s) \right]^{M/2}. \qquad (10)$$

Proof: For any $\mathbf{\Theta}$ that satisfies the power constraint: $E(\|\mathbf{\Theta s}\|^2) = E(\|\mathbf{s}\|^2) = M$, the trace of $\mathbf{\Theta}^{\mathcal{H}}\mathbf{\Theta}$ is equal to M. By the definition of the trace of a matrix and the non-negativity of the diagonal entries of $\mathbf{\Theta}^{\mathcal{H}}\mathbf{\Theta}$, there exists at least one column of $\mathbf{\Theta}$ with Euclidean norm ≤ 1. Without loss of generality, assume that the Euclidean norm of the pth column is ≤ 1, and let $\{\mathbf{s}, \tilde{\mathbf{s}}\}$ be a particular pair with $\mathbf{s} - \tilde{\mathbf{s}} = 2d\mathbf{e}_p/\sqrt{\mathcal{E}_s}$, where $\mathbf{e}_p$ is the pth column of the identity matrix. Using that $\|\boldsymbol{\theta}_p\|^2 = \sum_{m=1}^{M} |\theta_{mp}|^2 \leq 1$ with $\theta_{mp} := (\mathbf{\Theta})_{mp}$ and the arithmetic-geometric mean inequality, the square of the product distance of $\mathbf{s}-\tilde{\mathbf{s}}$ is as follows:

$$\delta^2 \le \prod_{m=1}^{M} |\boldsymbol{\theta}_m^T(\mathbf{s}-\tilde{\mathbf{s}})|^2 = \left(\frac{4d^2}{\mathcal{E}_s}\right)^M \prod_{m=1}^{M} |\theta_{mp}|^2$$

$$\le \left(\frac{4d^2}{\mathcal{E}_s}\right)^M \left(\frac{\sum_{m=1}^{M}|\theta_{mp}|^2}{M}\right)^M \le \left(\frac{4d^2}{M\mathcal{E}_s}\right)^M . \qquad (11)$$

Because $\boldsymbol{\Theta}$ is chosen arbitrarily and the right hand side of (11) is independent of the choice of $\boldsymbol{\Theta}$, we have that $\delta_{\max} \le \left[4d^2/(M\mathcal{E}_s)\right]^{M/2}$. By considering a particular pair $\mathbf{s}-\tilde{\mathbf{s}} = 2d\mathbf{e}_1/\sqrt{\mathcal{E}_s}$, with $\boldsymbol{\Theta}_M$ from (7), we have

$$\delta^2 \le \left(\frac{4d^2}{\mathcal{E}_s}\right)^M \prod_{m=1}^{M} |\theta_{m1}|^2 = \left(\frac{4d^2}{\psi^2\mathcal{E}_s}\right)^M . \ \square$$

The following theorem shows that the coding gains can be computed explicitly if one applies Construction A.

Theorem 3 *(Coding gains for QAM) For $M \in \mathbb{N}$ and the linear precoder $\boldsymbol{\Theta}_M$ of* (7)*, the minimum product distance over QAM is given by*

$$\delta = \left[4d^2/(\psi^2\mathcal{E}_s)\right]^{M/2} . \qquad (12)$$

Proof: For the QAM constellation points $(2k-1-Q)d+j(2l-1-Q)d$ with $k,l \in [1,Q]$ and $d \in \mathbb{N}$, we have $\sqrt{\mathcal{E}_s}(s_k - \tilde{s}_k) := 2d\zeta_k$ with $\zeta_k \in \mathbb{Z}[j]\backslash 0$. From (8) and the fact that $\sum_{k=0}^{M-1}\zeta_k\alpha^k$ is integral over $\mathbb{Z}[j]$, we can obtain

$$\mathcal{E}_s\delta^{2/M} = \frac{1}{\psi^2}\left|(2d)^M\mathcal{N}\left(\sum_{k=0}^{M-1}\zeta_k\alpha^k\right)\right|^{\frac{2}{M}} \ge \frac{4d^2}{\psi^2}.$$

Hence, the minimum product distance δ is lower bounded by $\left(4d^2/(\psi^2\mathcal{E}_s)\right)^{M/2}$. This, together with the upper bound given in Theorem 2, establishes that the minimum product distance of Construction A is exactly $\delta = \left(4d^2/(\psi^2\mathcal{E}_s)\right)^{M/2}$. $\square$

The following theorem establishes the values of M, for which Construction A can or can not achieve the upper bound (9) over QAM constellations.

Theorem 4 *(Maximum coding gains for QAM) For $M \in \mathcal{S}_M$, Construction A achieves maximum coding gain when using QAM constellations: $\delta_{\max} = \left[4d^2/(M\mathcal{E}_s)\right]^{M/2}$. For $M \notin \mathcal{S}_M$, Construction A can not achieve the upper bound* (9) *of coding gains over QAM constellations.*

Proof: When $M \in \mathcal{S}_M$, we have $1/\psi = 1/\sqrt{M}$ by Lemma 4. When $M \notin \mathcal{S}_M$, not all roots of α have modulus 1 as α is integral over $\mathbb{Z}[j]$ by Lemma 1.6 in [8]. Hence, we have $1/\psi < 1/\sqrt{M}$ by Lemma 5. Therefore, the upper bound (9) can not be achieved by (12) in Theorem 3. $\square$

Next, we state without proof a theorem which provides lower bounds on coding gains of Construction B.

M	4	5	6	7	8	9	10
$\delta_{\mathrm{NU}}^{2/M}$	–	0.297	0.333	0.208	–	0.160	0.2
$\delta_{\mathrm{U}}^{2/M}$	0.5	0.125	0.139	0.051	0.25	–	–

TABLE I

$\delta^{2/M}$ OF ST-CR CODES FOR $M = 4, 5, 6, 7, 8, 9, 10$ OVER 4-QAM.

Theorem 5 *(Lower bounds of coding gains of unitary precoders) For Construction B, let I denote the number of distinct minimal polynomials $p_i(x)$ of $\{\beta_m := \alpha e^{j2\pi m/M}\}_{m=0}^{M-1}$ over $\mathbb{Q}(j)$, where $\mathcal{B} := \{\beta_m : m = 0,\ldots,M-1\}$, and suppose D_i's are their degrees, for $i = 0,1,\ldots,I-1$. If $D_i \ge M$, then we have $\delta^{2/M} \ge (1/HM)^{2(\chi-1)}/(M\mathcal{E}_s)$, where $\chi := (\sum_{i=0}^{I-1}D_i)/M$ and $H := \max_{\{s,\tilde{s}\in\mathcal{C}\}}\left|\sqrt{\mathcal{E}_s}(s-\tilde{s})\right|$.*

In particular, if $M = 2^m$ for $m \in \mathbb{N}$, then M is the degree of the minimal polynomial $x^M - j$ of $\alpha := e^{j2\pi/4M}$ over $\mathbb{Q}(j)$ by Result 2. The linear precoders constructed in [4] for $M = 2^m$ are special cases of (7) which maximize the coding gain over the QAM constellations. Especially, when $M = 2^m$, the linear precoders of (7) are unitary [4], and when $M = \phi(P)$ for some $P \not\equiv 0 \pmod 4$, e.g., $M = 6, 10, 12, 18, \cdots$, then M is the degree of the minimal polynomial $\Phi_P(x)$ of $\alpha := e^{j2\pi/P}$ over $\mathbb{Q}(j)$ by Lemma 2. We provide special cases to corroborate Theorems 3 and 4.

Example 1 *If $d = 1$ and $\mathcal{E}_s = 2$, then $\delta_{\max}^{2/M} = 2/M$. Table I verifies the maximum $\delta^{2/M}$ for $M = 4, 6, 8, 10$ and* (12) *for $M = 5, 7, 9$ over 4-QAM constellations with $d = 1$ and $\mathcal{E}_s = 2$, where δ_{NU} and δ_{U} denote the minimum product distance of the non-unitary and unitary precoders, respectively. We apply the polynomials $\Phi_P(x)$ and $x^M - (1+j)$ to construct* (7) *for $M = 4, 6, 8, 10$ and for $M = 5, 7, 9$, respectively. Table I also shows that the linear precoders for $M = 5, 7, 9$ provide quite large coding gains even when the construction of* (7) *can not achieve the upper bound* (9)*.*

To design *unitary* precoders with large coding gains, Theorem 5 suggests choosing $\alpha := e^{j2\pi/P}$ such that the number of distinct minimal polynomials of $\{\beta_m := \alpha e^{j2\pi m/M}\}_{m=0}^{M-1}$ in Theorem 5 is small and their degrees are as low as possible, in order to make χ small.
Heuristic rules for unitary precoders: For any given M odd, choose $P = lM \in \mathcal{S}_M$ for some $l \in \mathbb{N}$ such that most of α_m's are roots of the minimal polynomial of α to make χ small, and $D_i \ge M$ for $i \in [0, I-1]$.

Example 2 *If $M = 5$ and we choose $P = 35$, then $\alpha_k := e^{j2\pi q_k/35}$ with $q_k := 1, 8, 15, 22, 29$ for $k \in [0,4]$, has all α_k's except α_2 as roots of the minimal polynomial $\Phi_{35}(x)$ of α_0 with $D_0 = 24$, while α_2 is a root of $\Phi_7(x)$ with $D_1 = 6$. In this construction, we have $\chi = 6$. Based on simulations, we find that $\delta^{2/M} = 0.1247$ for 4-QAM constellations.*

IV. Simulated Performance

To test the performance of our ST-CR codes, we simulated QAM constellations of size $|\mathcal{C}|$ with symbol energy $\mathcal{E}_s =$

$2(|\mathcal{C}|-1)/3$. The AWGN has variance $\sigma^2 = 1/(2\mathcal{E}_s\text{SNR})$ per real dimension. The average symbol error rate (SER) of ST-CR precoders is obtained through Monte-Carlo simulations using the decoders presented in [10], while the average SER of ST-OD block codes is obtained by evaluating numerically the integrals in [5, Eq. (9.21)] .

Figure 2 shows the performance comparisons between ST-CR with 64-QAM constellations and rate $3/4$ ST-OD codes with 256-QAM constellations. ST-CR codes outperform ST-OD codes by about 3 dB at BER $= 10^{-3}$ in this case. Figures 3 and 4 compare performance of ST-CR with 4-QAM signals against ST-OD with 16-QAM signals and $M = 5,6$, $7,8$ transmit antennas. It can be seen that at BER $= 10^{-3}$ ST-CR codes outperform ST-OD codes by about $2-3$ dB. Our simulations also illustrate that the linear precoder built from (7) outperforms the real precoder of [2] for $M \neq$ by about 1 dB.

V. Conclusions

In this paper, we developed an algebraic approach to designing ST-CR precoders. The linear precoders we constructed maximize not only diversity gains but also coding gains for $M = \phi(P)$ or $M = 2^m$, where $P \not\equiv 0 \pmod 4$ and $m \in \mathbb{N}$ over QAM constellations. Moreover, for any $M \in \mathbb{N}$, we designed the linear precoders possessing large coding gains over QAM constellations. We also developed a method to build unitary precoders for any $M \in \mathbb{N}$ and proved that the constructed unitary precoders have lower bounded coding gains. Finally, we have illustrated through simulations that ST-CR codes can achieve better performance than ST-OD codes when M, N and/or the spectral efficiency increase.

References

[1] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications," *IEEE Journal Selected Areas on Communications*, vol. 16, pp. 1451-1458, Oct. 1998.

[2] J. Boutros and E. Viterbo, "Signal Space Diversity: A Power and Bandwidth Efficient Diversity Technique for the Rayleigh Fading Channel," *IEEE Trans. on Info. Theory*, vol. 44, pp. 1453-1467, July 1998.

[3] V. M. DaSilva and E. S. Sousa, "Fading-Resistant Modulation Using Several Transmitter Antennas," *IEEE Trans. on Comm.*, pp. 1236-1244, Oct. 1997.

[4] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic Tools to Build Modulation Schemes for Fading Channels," *IEEE Trans. on Info. Theory*, vol. 43, pp. 938-952, May 1997.

[5] M. K. Simon and M.-S. Alouini, *Digital Communications over Generalized Fading Channels: A Unified Approach to Performance Analysis*, New York: Wiley, 2000.

[6] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-Time Block Codes from Orthogonal Designs," *IEEE Trans. on Info. Theory*, 45, pp. 1456-1466, July 1999.

[7] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction," *IEEE Trans. on Info. Theory*, vol. 44, pp. 744–765, March 1998.

[8] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math.83, Second edition, Springer-Verlag, 1997.

[9] Y. Xin, Z. Wang, and G. B. Giannakis, "Linear Unitary Precoders for Maximum Diversity Gains with Multiple Transmit and Receive Antennas," in *Proc. of 34th Asilomar Conf. on Signals, Systems, and Computers*, pp. 1553-1557, Pacific Grove, CA, Oct. 29-Nov. 1, 2000.

[10] Y. Xin, Z. Wang, and G. B. Giannakis, "Space-Time Diversity Systems based on Unitary Constellation-Rotating Precoders," in *Proc. of Intl. Conf. on ASSP*, Salt Lake, Utah, May 7-11, 2001. (available at http://www.ece.umn.edu/users/zhengdao/research.html)

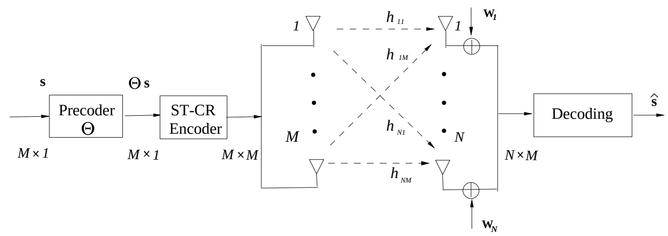

Fig. 1. Discrete-Time Baseband Equivalent Model

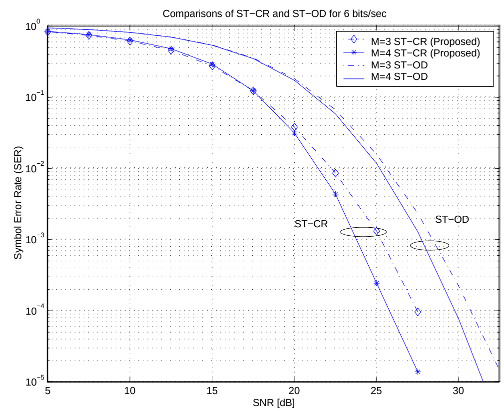

Fig. 2. $M = 3, 4$, $N = 2$, and rate $= 6$ bits/sec

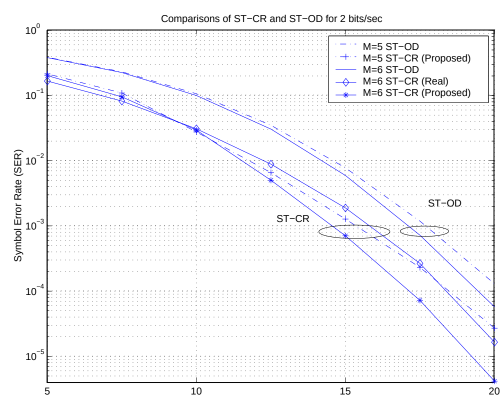

Fig. 3. $M = 5, 6$, $N = 1$ and rate $= 2$ bits/sec

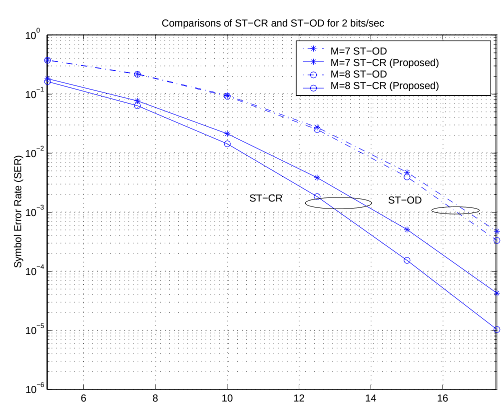

Fig. 4. $M = 7, 8$, $N = 1$ and rate $= 2$ bits/sec