

Maximal Diversity Algebraic Space–Time Codes With Low Peak-to-Mean Power Ratio

Pranav Dayal, *Student Member, IEEE*, and Mahesh K. Varanasi, *Senior Member, IEEE*

Abstract—The design requirements for space–time coding typically involves achieving the goals of good performance, high rates, and low decoding complexity. In this paper, we introduce a further constraint on space–time code design in that the code should also lead to low values of the peak-to-mean envelope power ratio (PMEPR) for each antenna. Towards that end, we propose a new class of space–time codes called the “low PMEPR space–time” (LPST) codes. The LPST codes are obtained using the properties of certain cyclotomic number fields. The LPST codes achieve a performance identical to that of the threaded algebraic space–time (TAST) codes but at a much smaller PMEPR. With M antennas and a rate of one symbol per channel use, the LPST codes lead to a decrease in PMEPR by at least a factor of M relative to a Hadamard spread version of the TAST code. For rates beyond one symbol per channel use and up to a guaranteed amount, the LPST codes have provably smaller PMEPR than the corresponding TAST codes. Additionally, with the concept of punctured LPST codes proposed in this paper, significant performance improvement is obtained over the full diversity TAST schemes of comparable complexity. Numerical examples are provided to illustrate the advantage of the proposed codes in terms of PMEPR reduction and performance improvement for very high rate wireless communications.

Index Terms—Algebraic number theory, diversity methods, peak-to-mean power ratio, Rayleigh fading, space–time codes, space–time modulation, sphere decoding.

I. INTRODUCTION

SPACE–time coding is a signaling strategy for multiple-input multiple-output (MIMO) wireless systems. Consider a MIMO channel with M transmit and N receive antennas with independent Rayleigh fading between each transmit–receive antenna pair and additive white gaussian noise (AWGN) at the receiver. The quasi-static fading model is assumed so that the fading remains constant over the entire duration of a codeword. The design of space–time codes for the wireless channel has traditionally been treated as a problem of minimization of the probability of error for a fixed rate and signal-to-noise ratio (SNR). It is conveniently presumed that the transmit antennas do not impose a limitation on the possible characteristics of the signals that comprise the space–time code. In practice, however,

hardware restrictions present an additional factor for the selection of good space–time codes. For example, the peak-to-mean envelope power ratio (PMEPR) of the signals transmitted is an important parameter to be considered during hardware design. High values of PMEPR pose difficulty in the design of amplifier operating characteristics and raise the cost of the transmitter. Additionally, the antennas designed for a signaling scheme with a smaller PMEPR exhibit a larger transmission efficiency; thereby, resulting in a higher average received SNR with the same power consumption at the transmitter.

The aim of this paper is to design high-rate space–time codes that simultaneously achieve both good performance and low PMEPR and yet are efficiently decodable. For good performance, the code must satisfy the full diversity rank criterion and have high coding gain. For low PMEPR, the amplitude variation of the actual signal transmitted by the code must be as small as possible. For efficient decoding, the space–time code should have sufficient structure. A quick review of the existing space–time coding schemes is presented in this paper which shows that they all meet a few but not all of these desirable properties.

In this paper, we propose a new class of codes called the low PMEPR space–time (LPST) codes. These codes are shown to satisfy all the requirements of space–time code design mentioned above. The LPST codes belong to the family of linear dispersion codes based on information symbols drawn from a finite constellation on the complex plane such as the quadrature amplitude modulation (QAM) or the hexagonal constellation. The LPST codes can be designed for any rate of L symbols per channel use with $1 \leq L \leq M$ and are shown to possess full diversity. The performance of the LPST codes is identical to that of the high-performance threaded algebraic space–time (TAST) codes [1]. However, the PMEPR of the LPST codes is much lower than that of the TAST codes. In fact, for a rate of $L = 1$ symbols per channel use, it is proved that the LPST codes actually exhibit the least possible PMEPR among all linear dispersion codes based on the same input constellation. For the case of $L = 1$ and M being a power of 2, the LPST code only transmits QAM information symbols in each position of the space–time codeword, thus becoming an attractive readily implementable code with existing hardware structures. For $L > 1$, the PMEPR with the LPST code is no greater than L times the PMEPR of the input constellation. Several interesting properties regarding the relative behavior of PMEPR for each antenna with the LPST codes are presented here. The LPST codes can also be decoded efficiently using the sphere-decoding algorithm [2]. The LPST codes are obtained by exploiting the algebraic

Manuscript received May 30, 2003; revised December 21, 2004. This work was supported in part by the National Science Foundation under Grants CCR-0112977 and CCF-0434410. The material in this paper was presented in part at the IEEE Global Telecommunications Conference, San Francisco, CA, December 2003.

The authors are with the Department of Electrical and Computer Engineering, University of Colorado, Boulder, CO 80309-0425 USA (e-mail: dayalp@dsp.colorado.edu; varanasi@dsp.colorado.edu).

Communicated by G. Caire, Associate Editor for Communications.
Digital Object Identifier 10.1109/TIT.2005.846398

properties of certain algebraic number fields which were first introduced for coding on fading channels in [3].

The proposed LPST codes also lend themselves to the process of puncturing so that an increase in rate is obtained with a small sacrifice in transmit diversity. The increase in rate is shown to offer a significant performance improvement over the original LPST scheme for moderate/reasonable range of the SNR and high spectral efficiencies. The punctured LPST codes also inherit the low PMEPR advantage of the parent LPST codes.

This paper is organized as follows. The system model and the associated definitions, such as diversity and PMEPR, are presented in Section II-A. A brief review of existing space-time designs is presented in Section II-B. A detailed summary of the contributions of this paper is provided in Section II-C. An introduction to the required tools of algebraic number theory is provided in Section II-D. The cyclotomic number fields used in this paper are described in Section III. The rate one LPST codes are introduced in Section IV. The general LPST codes of higher rates are introduced in Section V. The merits of the puncturing process are presented in Section VI. Numerical comparison of the proposed LPST codes with TAST for specific examples are described in detail in Section VII. The conclusions are summarized in Section VIII.

II. PRELIMINARIES

A. Definitions

In the complex baseband model, let \mathcal{C} be the space-time codebook of $M \times T$ sized matrices. Each row of the codeword $\mathbf{X} \in \mathcal{C}$ corresponds to the signals transmitted on a particular antenna. Let \mathbf{H} be the $N \times M$ matrix of fading coefficients with independent and identically distributed (i.i.d.) $CN(0, 1)$ entries, where $CN(m, \sigma^2)$ denotes the complex normal distribution with mean m and variance σ^2 . With the quasi-static assumption, the fading matrix remains constant for the entire duration of the codeword and changes independently across codewords. Let \mathbf{N} be the $N \times T$ matrix of noise samples with i.i.d. $CN(0, N_0)$ entries. If $\mathbf{X} \in \mathcal{C}$ is transmitted, then the received statistics \mathbf{Y} are given by

$$\mathbf{Y} = \sqrt{\rho} \mathbf{H} \mathbf{X} + \mathbf{N} \quad (1)$$

and the average received SNR is $\frac{\rho E[\text{tr}(\mathbf{X} \mathbf{X}^\dagger)]}{T N_0}$. The spectral efficiency R of the transmission scheme in context is $\frac{1}{T} \log_2(|\mathcal{C}|)$ bits per channel use (bpcu). It is assumed that the channel state information, i.e., the matrix \mathbf{H} , is available at the receiver so that the optimum decoding rule is

$$\hat{\mathbf{X}}(\mathbf{Y}) = \arg \min_{\mathbf{X}' \in \mathcal{C}} \|\mathbf{Y} - \sqrt{\rho} \mathbf{H} \mathbf{X}'\|^2. \quad (2)$$

The diversity order for any decoding rule is defined as

$$\lim_{\text{SNR} \rightarrow \infty} \frac{-\log(P_e(\mathcal{C}))}{\log(\text{SNR})}$$

where $P_e(\mathcal{C})$ is the corresponding codeword error probability. It was shown in [4] that the diversity order for the decoding rule in (2) is N times the transmit diversity, defined as the minimum rank among the differences of any two distinct codewords in \mathcal{C} . Thus, with an $M \times T$ sized space-time codebook, the maximum achievable diversity order is $N \min(M, T)$.

With any space-time code \mathcal{C} , the PMEPR for the r th transmit antenna, denoted by ϵ_r , is given by

$$\epsilon_r = \frac{\max_{\substack{\mathbf{X} \in \mathcal{C} \\ 1 \leq t \leq T}} |\mathbf{X}_{r,t}|^2}{\mathbb{E}_{\mathbf{X}} \left[\frac{1}{T} \sum_{t=1}^T |\mathbf{X}_{r,t}|^2 \right]}, \quad 1 \leq r \leq M. \quad (3)$$

where $\mathbb{E}_{\mathbf{X}}[\cdot]$ denotes the expectation over all codewords $\mathbf{X} \in \mathcal{C}$. All the codewords are assumed to be equally likely. The definition of ϵ_r remains the same irrespective of the fading model and the extent of channel state information known at the receiver. Note that ϵ_r , as defined above, is invariant to a scaling of the codebook \mathcal{C} by a constant. Hence, the PMEPR is independent of SNR. Also, the formulation of PMEPR in this manner is more meaningful than in [5] as we address the PMEPR for each antenna separately.

It will be useful to also define the PMEPR of any multidimensional complex vector valued constellation. For an M -dimensional constellation \mathcal{S} , the PMEPR of the r th coordinate is given by

$$\zeta_r = \frac{\max_{\mathbf{s} \in \mathcal{S}} |\mathbf{s}_r|^2}{\mathbb{E}_{\mathbf{s}} [|\mathbf{s}_r|^2]}, \quad 1 \leq r \leq M \quad (4)$$

where $\mathbb{E}_{\mathbf{s}}[\cdot]$ denotes the expectation over all constellation points $\mathbf{s} \in \mathcal{S}$.

A multidimensional constellation is said to exhibit full modulation diversity (FMD) if any pair of distinct constellation points differ in all the coordinates. The space-time codes considered in this paper employ FMD complex constellations obtained from a unitary transformation (i.e., rotation) of a vector of input information symbols. Such special rotations were constructed using the tools of algebraic number theory in [3], [6], [7]. A description of the relevant results of algebraic number theory used in this paper will be summarized in Section II-D.

The symbol \mathcal{I} denotes a finite constellation of q points in the complex plane and will be one of two types, \mathcal{I}_i or \mathcal{I}_j , in this paper. Let $i = \sqrt{-1}$ and $j = e^{i\frac{2\pi}{3}}$. The constellations \mathcal{I}_i and \mathcal{I}_j are obtained as

$$\mathcal{I}_i = \{a + ib : a, b \text{ odd integers}, -\sqrt{q} + 1 \leq a, b \leq \sqrt{q} - 1\}$$

$$\mathcal{I}_j = \{a + jb : a, b \text{ odd integers}, -\sqrt{q} + 1 \leq a, b \leq \sqrt{q} - 1\}$$

where the size q is an even power of 2. The constellation \mathcal{I}_i is just the standard q -QAM constellation and \mathcal{I}_j is the hexagonal constellation carved out of the A_2 lattice [8]. The average energy of \mathcal{I} is denoted by E_{av} and the constellation point in \mathcal{I} with the maximum envelope by z_{max} . The PMEPR of \mathcal{I} is given by $\epsilon_{\mathcal{I}} = \frac{|z_{\text{max}}|^2}{E_{\text{av}}}$. In particular

$$\epsilon_{\mathcal{I}_i} = 3 \left(\frac{\sqrt{q} - 1}{\sqrt{q} + 1} \right) \quad \text{and} \quad \epsilon_{\mathcal{I}_j} = \frac{9}{2} \left(\frac{\sqrt{q} - 1}{\sqrt{q} + 1} \right).$$

The operator \otimes refers to the Kronecker product of two matrices [9]. The K -dimensional identity matrix is denoted by \mathbf{I}_K . The symbol $\lfloor \cdot \rfloor$ represents the floor function and the symbol $\lfloor \cdot \rfloor_M$ represents modulo operation of an integer with respect to the integer M . An $M \times M$ matrix \mathcal{H}_M is a Hadamard matrix if it consists of ± 1 only and if $\mathcal{H}_M^T \mathcal{H}_M = M \mathbf{I}_M$.

B. Existing Space–Time Designs

The design of space–time code should simultaneously account for several desirable properties. For good performance, the space–time code should possess maximum diversity and should also support high rates. For implementation advantage, the space–time code should minimize the PMEPR for each antenna. For decoding simplicity, the space–time codes should have enough structure to enable the maximum-likelihood decoding without performing an exhaustive search. In the following, we mention some earlier works on space–time code design and conclude that none of the existing codes meet all the above mentioned criteria.

Early works on space–time coding schemes considered coding over a long block length using the concepts of trellis-coded modulation over finite alphabets such as QAM and phase-shift keying (PSK) [4]. Even though good performance and low values of PMEPR can be obtained with these codes, such designs lead to very low rates and also incur large decoding delays.

Short-length space–time codes were proposed in the form of orthogonal designs in [10]. These space–time codes provide full diversity and also low values of PMEPR because the code consists only of the symbols of the input constellation and their conjugates. However, beyond $M = 2$, these codes suffer a loss in rate in terms of the number of independent information symbols sent by the codeword and, consequently, do not lead to good performance.

The class of linear dispersion space–time codes proposed in [11], [12] support much higher rates than the orthogonal designs and are also efficiently decodable using the sphere-decoding algorithm. In a linear dispersion code, the codewords are linear combinations of K matrices of size $M \times T$. The K matrices are referred to as the dispersion matrices. The coefficients of the linear combination, also referred to as symbols, are drawn from a finite constellation in the complex plane. The rate of the code is defined to be $\frac{K}{T}$ symbols per channel use. The choice of dispersion matrices for good performance was made in [11], [12] using a numerical search and did not provide any guarantee on the diversity order or the resulting PMEPR.

The class of diagonal algebraic space–time (DAST) codes [13] or equivalently the space–time linear constellation precoding (ST-LCP) scheme [14] are a special case of linear dispersion codes where the effective dispersion matrices are obtained from algebraic means. These codes are obtained by rotating a multidimensional QAM constellation using an FMD generator matrix and transmitting the coordinates of the resulting lattice point along the diagonal of the codeword. With M QAM information symbols on the diagonal, the DAST codes achieve a rate of one symbol per channel use. The DAST codes satisfy the full transmit diversity rank criterion [4] and also provide a lower bound with respect to the minimum determinant criterion [4]. However, the design of DAST codes disregards the required constraints of low PMEPR.

The generalization of DAST codes for higher rates in terms of symbols per channel use are presented in [1], [15]. The resulting

codes are referred to as the TAST codes. The TAST codes were an extension of DAST in the sense that, to achieve a rate of L symbols per channel use, L independent and nonoverlapping layers of multidimensional FMD lattice points were threaded in a matrix and scaled appropriately to ensure full transmit diversity. Since the TAST codes essentially consist of several layers of DAST codes, the TAST codes inherit the high PMEPR disadvantage of the DAST codes.

When M is 2 or a multiple of 4, it was suggested in [13] to spread the DAST codewords using a Hadamard transform to reduce the PMEPR without affecting the system performance. For the TAST code corresponding to the special case of $M = 4$, $L = 2$, an example of Hadamard spreading to reduce the PMEPR was provided in [1]. Nevertheless, the PMEPR even with the Hadamard transform remains as high as that of the rotated QAM constellation. Implicitly, a further reduction in the PMEPR of the DAST or TAST codes was thought to be unavoidable. In this paper, however, a class of algebraic codes is proposed that exhibits a performance as good as that of the TAST codes and yet does not suffer from the high values of PMEPR.

C. LPST Code Design Summary

In this work, we propose a new class of space–time codes called the LPST codes. These LPST codes are an improvement over the existing codes summarized above because they possess all the desirable properties for a space–time code. The LPST codes exhibit full transmit diversity and can be designed for high rates in terms of symbols per channel use. The LPST codes are also designed with the PMEPR constraints in mind. The PMEPR obtained with the LPST codes is much lower than that of competing codes with similar performance. The LPST codes are also efficiently decodable using the sphere-decoding algorithm. Several properties of the proposed LPST codes are investigated in this paper and the key results are summarized as follows.

1. For a rate of one symbol per channel use, the LPST codes only transmit information symbols from the QAM constellation whenever M is a power of 2.
2. It is proved that the PMEPR obtained for each antenna with the LPST codes of rate one symbol per channel use is the least possible among all possible linear dispersion codes based on the same input constellation.
3. The performance of LPST codes is identical to that of the TAST codes at any rate and for any given set of code parameters.
4. We propose a generalization of the Hadamard spreading to reduce the PMEPR of the TAST codes. In spite of this improvement for the TAST codes, we prove that there exists a guaranteed rate of number of symbols per channel use up to which the LPST codes exhibit a smaller PMEPR compared to the TAST codes spread in the Hadamard fashion.
5. For a rate of L symbols per channel use, the PMEPR for each antenna with the LPST code is no more than L times the PMEPR of the input constellation.

6. With the LPST codes, the transmit antennas can be divided into certain groups such that each antenna in a particular group exhibits the same PMEPR behavior with respect to the code parameters.
7. The proposed LPST codes lend themselves to the process of puncturing that leads to an increase in rate by sacrificing the full transmit diversity of the code. The punctured LPST codes are still decodable using the efficient sphere-decoding algorithm and preserve the PMEPR advantage of the original LPST code.

While this paper was under review, a modified construction of the TAST codes appeared in [5]. The codes in [5] are obtained by modifying the TAST scheme so that for any $L < M$, all the M layers in the code are filled but with only L information symbols in each layer. Although aiming to achieve similar objectives, the codes proposed in [5] are different from the LPST codes proposed in this paper in several aspects. The following points compare and contrast some of the key results of this paper and those of [5] and further reinforce the contribution of this work.

1. For the case of one symbol per channel use, both the LPST codes and the modified TAST codes of [5] exhibit identical performance. Moreover, both achieve the least possible PMEPR among all linear codes. However, unlike the code of [5], all the symbols transmitted by the LPST code in this case are from the QAM constellation whenever M is a power of 2, thereby avoiding any constellation expansion.
2. As opposed to [5], the proof of optimality of PMEPR at one symbol per channel use presented in this paper is among general linear space-time codes irrespective of any symmetry among the one-dimensional constellation transmitted across space and time. Our formal proof shows the need for assuming a certain structure on the input information constellation, namely, if z_{\max} is the maximum envelope point of the input constellation, then $-z_{\max}$ is also a valid constellation point. Without enforcing this constraint on the input constellation, the claim of optimality of PMEPR among linear space-time codes presented in [5] is incorrect. We note that this constraint on the input constellation is indeed satisfied by the QAM and hexagonal constellations carved from the A_2 lattice. Our derivation is therefore not only more general but also more rigorous than the argument given in [5]. Also, the PMEPR with a space-time code is defined in this paper with respect to each transmit antenna and therefore provides a more detailed and practically meaningful view compared to [5].
3. For rates beyond one symbol per channel use, the modified TAST scheme of [5] is obtained by using a smaller number of input information symbols linearly combining at any position as compared to the original TAST construction of [1]. This is argued to be beneficial in reducing the PMEPR but, except for some special cases, no formal proof of this fact is provided in [5]. In this paper, we explicitly prove that with our construction of LPST codes,

there exists a guaranteed number of layers up to which the PMEPR of LPST codes is necessarily smaller than that of the TAST codes.

4. The modification of the TAST scheme in [5] does not preserve the performance of the original TAST code. This poorer performance of the modified TAST scheme is also indicated by our numerical results in Section VII. The PMEPR reduction in [5], therefore, occurs at the expense of a loss in performance. On the other hand, the performance of the LPST codes presented in this paper is identical to that of the original TAST codes. Hence, the PMEPR improvement is obtained without a loss in performance using the LPST codes. An example comparing the PMEPR and performance with the LPST and the modified TAST scheme of [5] is provided in Section VII.
5. For the tradeoff of diversity versus complexity presented in [5], it is suggested that complexity reduction for a rectangular space-time code should be achieved by nulling out some layers. However, this method increases the PMEPR of the space-time code due to presence of zero positions and an unnecessarily larger number of information symbols combining in the remaining positions. We show in this paper that the diversity versus complexity tradeoff can be achieved without any significant increase in PMEPR using *punctured* LPST codes.

D. Algebraic Number Theory

The essential facts of number theory required in this paper are summarized here for the sake of reference. For the proofs of the following results and a detailed study of algebraic number theory, the reader is referred to [16], [17].

Let Q , R , and C be the field of rationals, reals, and complex numbers, respectively. Let Z be the ring of rational integers and Z^+ the set of natural numbers. Let K_1 and K_2 be subfields of C such that $K_1 \subseteq K_2$. For any field K , let $K[x]$ denote the ring of polynomials in x with coefficients in K .

- A number $\alpha \in C$ is said to be algebraic over K_1 if it is a root of some polynomial in $K_1[x]$. Every number α algebraic over K_1 is a root of a unique monic irreducible polynomial called the minimal polynomial $\mu_{K_1, \alpha}(x) \in K_1[x]$. The degree of $\mu_{K_1, \alpha}(x)$ is said to be the degree of α over K_1 . If $K_1 = Q$, then α is simply called an algebraic number. An algebraic number α is said to be an algebraic integer if the coefficients of $\mu_{Q, \alpha}(x)$ belong to Z . The set of all algebraic integers in C forms a ring \mathcal{A} .
- If all elements of K_2 are algebraic over K_1 , then K_2 is called an algebraic extension of K_1 . If the extension is finite-dimensional, then the dimension, denoted by $[K_2 : K_1]$ is called the degree of K_2 over K_1 . A finite-dimensional algebraic extension of Q is known as an algebraic number field.
- If $K_1 \subseteq K_2 \subseteq K_3$ is a tower of finite-dimensional algebraic extensions, then $[K_3 : K_1] = [K_3 : K_2] \times [K_2 : K_1]$.
- If $\alpha \in C$ is algebraic over K_1 , then the smallest algebraic extension of K_1 containing α is denoted by $K_1(\alpha)$. The extension $K_1(\alpha)$ is finite-dimensional with degree

$[K_1(\alpha) : K_1] = \deg(\mu_{K_1, \alpha}(x)) = n$, say. A basis for the extension $K_1(\alpha)/K_1$ is $(1, \alpha, \dots, \alpha^{n-1})$.

- Let K_2 be an algebraic extension of K_1 . A field isomorphism from K_2 to a subfield L of C is said to be an automorphism if $L = K_2$. The set of all automorphisms of K_2 that keep the elements of K_1 fixed, forms a group called the Galois group $G = \text{Gal}(K_2/K_1)$. The extension K_2 of K_1 is said to be Galois if the set of all elements in K_2 that remain invariant with respect to all the automorphisms in $\text{Gal}(K_2/K_1)$ is K_1 itself.
- The algebraic extension $K_2 = K_1(\alpha)$ is normal if all roots of $\mu_{K_1, \alpha}(x)$ are elements in K_2 . In this case, each automorphism of $G = \text{Gal}(K_2/K_1)$ is obtained by mapping α to one of the roots of $\mu_{K_1, \alpha}(x)$. For instance, let $\deg(\mu_{K_1, \alpha}(x)) = n$ and $(\alpha^{(1)} = \alpha, \alpha^{(2)}, \dots, \alpha^{(n)})$ be the n roots of $\mu_{K_1, \alpha}(x)$. Any element $\beta \in K_2$ has the unique representation $\beta = \sum_{l=1}^n c_l \alpha^{l-1}$, where $c_l \in K_1$, $1 \leq l \leq n$. The image of β under the k th automorphism of G is given by

$$\beta^{(k)} = \sum_{l=1}^n c_l (\alpha^{(k)})^{l-1}.$$

The number $\beta^{(k)}$ will be referred to as the k th conjugate of β .

- The algebraic number field $\xi_n = Q(e^{i\frac{2\pi}{n}})$ is known as the n th cyclotomic number field. The degree of ξ_n over Q is $\varphi(n)$, where $\varphi(n)$, known as the Euler function of n , is the number of natural numbers smaller than n that are coprime to n . For instance, the fields $Q(j)$ and $Q(i)$ are the cyclotomic fields ξ_3 and ξ_4 , respectively.
- If n is even, then the only roots of unity in ξ_n are the n th roots of unity. If n is odd, then the only roots of unity in ξ_n are the $2n$ th roots of unity. This result implies that $Q(i)$ is a subfield of ξ_n if and only if n is a multiple of 4 and $Q(j)$ is a subfield of ξ_n if and only if n is a multiple of 3. Moreover, for n odd, $\xi_n = \xi_{2n}$.
- If K is an algebraic number field of degree n , then the set $O_K = \mathcal{A} \cap K$ is the ring of algebraic integers in K . There exists a basis $(\omega_1, \omega_2, \dots, \omega_n) \in O_K^n$ called the integral basis such that any element of $\beta \in O_K$ has a unique representation $\beta = Z_1\omega_1 + Z_2\omega_2 + \dots + Z_n\omega_n$ with $Z_i \in Z$, $1 \leq i \leq n$. As an example, the algebraic number fields $Q(i)$ and $Q(j)$ are of degree 2 over Q . The ring of Gaussian integers $Z[i] = \{z_1 + iz_2 : z_1, z_2 \in Z\}$ is the ring of algebraic integers in $Q(i)$. The set $Z[j] = \{z_1 + jz_2 : z_1, z_2 \in Z\}$ is the ring of algebraic integers in $Q(j)$.
- Let $Q \subset F \subseteq K = Q(\alpha)$, where F is an algebraic field extension of Q and α is an algebraic integer. If $[K : F] = n$, then the elements $(1, \alpha, \dots, \alpha^{n-1})$ are linearly independent in K over F . Let D be generated as

$$D = \left\{ \beta : \beta = \sum_{l=1}^n z_l \alpha^{l-1}, z_l \in O_F, 1 \leq l \leq n \right\}.$$

Then, the set D forms a subring of O_K .

III. SPECIAL ALGEBRAIC FIELDS

In this section, we introduce the notation for certain number-theoretic tools that we use later for the development of the proposed LPST codes. Consider the following two disjoint sets of integers:

$$\mathcal{M}_1 = \{m | m = 2^\kappa, \kappa \in Z^+\} \quad (5)$$

$$\mathcal{M}_2 = \{m | m = 3^{\kappa_1} 2^{\kappa_2}, \kappa_1 \in Z^+, \kappa_2 \in Z^+ \cup \{0\}\}. \quad (6)$$

The algebraic number fields needed in this paper will depend on whether $M \in \mathcal{M}_1$ or $M \in \mathcal{M}_2$. However, to simplify the presentation, a common notation will be followed for the two cases described next.

1. $M \in \mathcal{M}_1$: Define the element $\theta = e^{\frac{j2\pi}{M}}$ so that the algebraic number field $Q(\theta)$ contains $Q(i)$ as a subfield. The degree

$$[Q(\theta) : Q(i)] = \frac{\varphi(4M)}{2} = M$$

and the minimal polynomial of θ over $Q(i)$ is $\mu_{Q(i), \theta}(x) = x^M - e$, where the constant $e = i$. Moreover, $Q(\theta)$ is a Galois extension of $Q(i)$. Set $F = Q(i)$, $O_F = Z[i]$, and the finite constellation $\mathcal{I} = \mathcal{I}_i$.

2. $M \in \mathcal{M}_2$: In this case, define the element $\theta = e^{\frac{j2\pi}{6M}}$ so that the algebraic number field $Q(\theta)$ contains $Q(j)$ as a subfield. The degree

$$[Q(\theta) : Q(j)] = \frac{\varphi(6M)}{2} = M$$

and the minimal polynomial of θ over $Q(j)$ is $\mu_{Q(j), \theta}(x) = x^M - e$, where the constant $e = -j^2 = 1 + j$. Once again, $Q(\theta)$ is a Galois extension of $Q(j)$. Set $F = Q(j)$, $O_F = Z[j]$, and the finite constellation $\mathcal{I} = \mathcal{I}_j$.

The M conjugates of θ in both cases above are given by $\theta^{(k)} = \omega_M^{k-1} \theta$, $1 \leq k \leq M$, where $\omega_M = \exp(\frac{2j\pi}{M})$. The set $(1, \theta, \theta^2, \dots, \theta^{M-1})$ forms a basis of the extension $Q(\theta)/F$. For the set of M numbers $(z_1, \dots, z_M) \in O_F^M$, the element $\alpha = \sum_{l=1}^M z_l \theta^{l-1}$ is an algebraic integer in $Q(\theta)$. Let each information symbol z_l be chosen from the finite subset \mathcal{I} of O_F . Let $(\alpha^{(1)}, \dots, \alpha^{(M)})$ be the conjugates of α obtained by application of the M automorphisms of $\text{Gal}(Q(\theta)/F)$ to α . We then have that

$$\alpha^{(k)} = \sum_{l=1}^M z_l \theta^{l-1} \omega_M^{(k-1)(l-1)}, \quad 1 \leq k \leq M. \quad (7)$$

One can view the conjugates of α as the coordinates of an M -dimensional complex constellation \mathcal{S} . This constellation is, in fact, a rotation of the input \mathcal{I}^M constellation and exhibits full modulation diversity [3]. The generator matrix of the rotated constellation is $\mathbf{G} = \mathbf{S}_M \mathbf{D}_\theta$, where

$$\mathbf{D}_\theta = \text{diag}(1, \theta, \dots, \theta^{M-1})$$

and \mathbf{S}_M is the $M \times M$ inverse discrete Fourier transform (IDFT) matrix given by

$$[\mathbf{S}_M]_{kl} = \omega_M^{(k-1)(l-1)}.$$

Thus, $\mathcal{S} = \{\mathbf{G}\mathbf{u} | \mathbf{u} \in \mathcal{I}^M\}$. Let ζ_s be the PMEPR for the s th coordinate of the rotated constellation \mathcal{S} .

IV. RATE ONE LOW PMEPR SPACE-TIME CODE

In this section, we consider space-time codes of rate one symbol per channel use. The design of a new full diversity space-time code that transmits information symbols from \mathcal{I} is presented and the optimality of the resulting PMEPR is proved.

We begin by introducing an algebraic description of a particular DAST code obtained from the number fields chosen in Section III. Let $\mathbf{E}_M(z_1, \dots, z_M)$ be the code that consists of codewords of the form $\text{diag}(\alpha^{(1)}, \dots, \alpha^{(M)})$. This algebraic representation of the DAST code is more useful for our purpose as opposed to the generic construction in [13]. We now consider space-time codes of the form

$$\mathbf{U}\mathbf{E}_M(z_1, \dots, z_M)\mathbf{V} \quad (8)$$

where \mathbf{U} and \mathbf{V} are fixed full-rank matrices normalized so that the transmitted power is the same as that with $\mathbf{U} = \mathbf{I}_M$ and $\mathbf{V} = \mathbf{I}_M$. If the matrices \mathbf{U} and \mathbf{V} are unitary then the performance of the code is exactly the same as that with $\mathbf{U} = \mathbf{I}_M$ and $\mathbf{V} = \mathbf{I}_M$ [18], [19]. When \mathbf{U} and \mathbf{V} are identity matrices, the PMEPR of the transmit antennas is given by (3) and (4) to be $\epsilon_r = M\zeta_r$, $1 \leq r \leq M$. The factor of M in ϵ_r appears due to the absence of signal on the off-diagonal positions of the codeword. This factor can be avoided if M is a Hadamard dimension, i. e., 2 or a multiple of 4, by choosing $\mathbf{V} = \mathbf{I}_M$ and \mathbf{U} to be the normalized Hadamard matrix $\frac{1}{\sqrt{M}}\mathcal{H}_M$ [13]. The effect of the Hadamard transform is to repeat a scaled version of the $\alpha^{(j)}$ in the j th column. The PMEPR of the DAST code with the Hadamard transform is

$$\epsilon_r = \max_{1 \leq s \leq M} \zeta_s, \quad 1 \leq r \leq M.$$

A closed-form expression for ζ_s was obtained in [20] for $M \in \mathcal{M}_1$ and is given by

$$\zeta_s = \epsilon_{\mathcal{I}_i} \times \frac{1}{2M \sin^2(\frac{\pi}{4M})} \triangleq \zeta, \quad 1 \leq s \leq M. \quad (9)$$

Now, $\epsilon_r = \max_{1 \leq s \leq M} \zeta_s = \zeta$, $1 \leq r \leq M$.¹ Thus, even with the Hadamard transform, the PMEPR of all transmit antennas is $w = \frac{1}{2M \sin^2(\frac{\pi}{4M})}$ times more than the PMEPR of the QAM constellation \mathcal{I}_i , a factor that grows almost linearly for large M . For $M \in \mathcal{M}_2$, the ζ_s are not even the same for each s but one can set $z_l = z_{\max}$, $1 \leq l \leq M$ to get that

$$\zeta_1 \geq \epsilon_{\mathcal{I}_j} \times \frac{1}{4M \sin^2(\frac{\pi}{6M})}.$$

Hence,

$$\max_{1 \leq s \leq M} \zeta_s \geq w\epsilon_{\mathcal{I}_j}$$

where

$$w = \frac{1}{4M \sin^2(\frac{\pi}{6M})}.$$

Therefore, if $M \in \mathcal{M}_2$ and M is a multiple of 4, then the PMEPR ϵ_r with the Hadamard transform is at least a factor of w times the PMEPR of the input constellation \mathcal{I}_j . If $M \in \mathcal{M}_2$ and

¹In fact, setting $z_l = z_{\max}$, $1 \leq l \leq M$, shows that ζ_1 has to be at least ζ as defined in (9).

M is not a multiple of 4, then a Hadamard spread is not even possible for the original DAST code.

A. A New Rate One Space-Time Code

In this subsection, a unitary spreading matrix $\mathbf{\Theta}_M$ is presented for $M \in \mathcal{M}_1 \cup \mathcal{M}_2$ such that by setting $\mathbf{U} = \mathbf{\Theta}_M$ and $\mathbf{V} = \mathbf{\Theta}_M^{-1}$, the PMEPR for each transmit antenna becomes exactly equal to the PMEPR of the input constellation \mathcal{I} , thereby outperforming the Hadamard transform in this objective by at least the factor w mentioned earlier.

It is first noted that multiplication of $\alpha^{(1)} = \alpha$ by θ^j , $1 \leq j \leq M-1$, leads to an algebraic integer whose representation in the basis $(1, \theta, \dots, \theta^{M-1})$ is given by

$$(ez_{M-j+1}, ez_{M-j+2}, \dots, ez_M, z_1, \dots, z_{M-j}).$$

Such a cyclic shift of the representation of α and multiplication by e in the first j positions is due to the special structure of $\mu_{F,\theta}(x)$ so that $\theta^{M-1+j} = e\theta^{j-1}$. Thus,

$$\begin{bmatrix} 1 \\ \theta \\ \vdots \\ \theta^{M-1} \end{bmatrix} \alpha^{(1)} = \mathbf{Z}(z_1, z_2, \dots, z_M) \begin{bmatrix} 1 \\ \theta \\ \vdots \\ \theta^{M-1} \end{bmatrix} \quad (10)$$

where the matrix formatting function \mathbf{Z} is given by

$$\mathbf{Z}(z_1, z_2, \dots, z_M) = \begin{bmatrix} z_1 & z_2 & z_3 & \cdots & z_M \\ ez_M & z_1 & z_2 & \cdots & z_{M-1} \\ ez_{M-1} & ez_M & z_1 & \cdots & z_{M-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ ez_2 & ez_3 & \cdots & ez_M & z_1 \end{bmatrix}. \quad (11)$$

The matrix representation of α , as in (10), is an instance of a well-known linear map of a number field to itself (see [16, Ch. 2, Problem 17]). Applying the M automorphisms of $Q(\theta)$ to (10) and compiling all the M equations into a matrix notation, we get that

$$\mathbf{D}_\theta \mathbf{S}_M \text{diag}(\alpha^{(1)}, \dots, \alpha^{(M)}) = \mathbf{Z}(z_1, z_2, \dots, z_M) \mathbf{D}_\theta \mathbf{S}_M. \quad (12)$$

If $\mathbf{\Theta}_M \triangleq \frac{1}{\sqrt{M}} \mathbf{D}_\theta \mathbf{S}_M$, then $\mathbf{\Theta}_M^\dagger \mathbf{\Theta}_M = \mathbf{I}_M$ and we get from (12) that

$$\mathbf{Z}(z_1, z_2, \dots, z_M) = \mathbf{\Theta}_M \text{diag}(\alpha^{(1)}, \dots, \alpha^{(M)}) \mathbf{\Theta}_M^{-1}. \quad (13)$$

Thus, the conjugates $(\alpha^{(1)}, \dots, \alpha^{(M)})$ are, in fact, the eigenvalues of the matrix $\mathbf{Z}(z_1, \dots, z_M)$. It can now be seen from (13) and (8) that setting $\mathbf{U} = \mathbf{\Theta}_M$ and $\mathbf{V} = \mathbf{\Theta}_M^{-1}$ leads to the new space-time code $\mathbf{Z}(z_1, \dots, z_M)$ which will be referred to as the rate one LPST code.

For $M \in \mathcal{M}_1$, all the entries of $\mathbf{Z}(z_1, \dots, z_M)$ are elements of the input q -QAM constellation as multiplication of any point in the square QAM constellation \mathcal{I}_i by $e = i$ leads to another point in the same constellation \mathcal{I}_i . Hence, the proposed spread for $M \in \mathcal{M}_1$ results in a space-time code that transmits only QAM information symbols at the rate of one symbol per channel use and the PMEPR for each antenna becomes equal to the PMEPR of \mathcal{I}_i . This is an advantage over the modified TAST scheme of [5] because there is no constellation expansion with the proposed LPST code. For $M \in \mathcal{M}_2$, multiplication of a constellation point in \mathcal{I}_j by $e = -j^2$ does not necessarily lead to another constellation point in \mathcal{I}_j . Nevertheless, since $|e| = 1$,

the PMEPR for each antenna with the proposed spread is equal to the PMEPR of \mathcal{I}_j . Therefore, there is no increase in PMEPR of the new space-time code with respect to the input constellation \mathcal{I} for any $M \in \mathcal{M}_1 \cup \mathcal{M}_2$. Moreover, this has been achieved without any change in the performance of the code since the matrix Θ_M is unitary.

B. PMEPR Optimality of $\mathbf{Z}(z_1, \dots, z_m)$

It is shown now that a space-time code that transmits only information symbols from \mathcal{I} , as in $\mathbf{Z}(z_1, \dots, z_M)$, has the smallest PMEPR for each transmit antenna among all codes that transmit a linear combination of independent information symbols from \mathcal{I} . The following proposition is valid for all linear space-time codes, irrespective of their rate and transmit diversity. For the definition of PMEPR to make sense, it is assumed that each row of the codeword has at least one position with not all coefficients of the linear combination being zero. Each entry of the space-time code is a linear combination of independent information symbols but the same information symbol can occur in any number of entries.

Proposition 1: Let \mathcal{I} be a complex constellation with the maximum envelope point z_{\max} satisfying $-z_{\max} \in \mathcal{I}$. Then, for all $M \times T$ space-time codes that transmit linear combination of independent information symbols from \mathcal{I} in every position, the PMEPR of any transmit antenna is lower-bounded by the PMEPR of \mathcal{I} .

Proof: Consider the r th transmit antenna with the $M \times T$ space-time code \mathcal{C} . For $\mathbf{X} \in \mathcal{C}$, let the signal $X_{r,j}$, $1 \leq j \leq T$, be a linear combination of $n_{r,j}$ independent information symbols from \mathcal{I} . Thus, we have

$$\mathbf{X}_{r,j} = \sum_{l=1}^{n_{r,j}} \phi_{r,j,l} z_{r,j,l} \quad (14)$$

for nonzero complex numbers $\phi_{r,j,l}$, $1 \leq l \leq n_{r,j}$. For the r th antenna, let the maximum of $\max_{1 \leq j \leq T} |\mathbf{X}_{r,j}|^2$ among all codewords \mathbf{X} be obtained for some codeword $\mathbf{E} \in \mathcal{C}$ and let the maximum be attained in the $\mathbf{E}_{r,t}$ position for some $1 \leq t \leq T$. Let $\mathbf{E}_{r,t}$ correspond to

$$(z_{r,t,1}, \dots, z_{r,t,n_{r,t}}) = (\chi_1 z_{\max}, \dots, \chi_{n_{r,t}} z_{\max})$$

where χ_s , for each $1 \leq s \leq n_{r,t}$, is a complex number describing the position of the maximizing symbol $z_{r,t,s}$ relative to z_{\max} on the complex plane. We then have that

$$|\mathbf{E}_{r,t}|^2 = |\phi_{r,t,1}\chi_1 + \dots + \phi_{r,t,n_{r,t}}\chi_{n_{r,t}}|^2 |z_{\max}|^2. \quad (15)$$

We also have that

$$E_{\mathbf{X}}[|\mathbf{X}_{r,j}|^2] = \left(\sum_{l=1}^{n_{r,j}} |\phi_{r,j,l}|^2 \right) E_{\text{av}}, \quad 1 \leq j \leq T. \quad (16)$$

By the definition of \mathbf{E} and t , we get that the PMEPR ϵ_r is

$$\begin{aligned} \epsilon_r &= \frac{|\mathbf{E}_{r,t}|^2}{\frac{1}{T} \sum_{j=1}^T E[|\mathbf{X}_{r,j}|^2]} \\ &= \frac{T \left| \sum_{l=1}^{n_{r,t}} \phi_{r,t,l} \chi_l \right|^2}{\left(\sum_{l=1}^{n_{r,1}} |\phi_{r,1,l}|^2 \right) + \dots + \left(\sum_{l=1}^{n_{r,T}} |\phi_{r,T,l}|^2 \right)} \frac{|z_{\max}|^2}{E_{\text{av}}} \\ &= P \frac{|z_{\max}|^2}{E_{\text{av}}}. \end{aligned} \quad (17)$$

We now show that the quantity P implicitly defined in (17) is greater than or equal to 1.

By definition of χ_s , $1 \leq s \leq n_{r,t}$, and the fact that $\pm z_{\max} \in \mathcal{I}$, we can conclude that the quantity $\left| \sum_{l=1}^{n_{r,t}} \phi_{r,t,l} \chi_l \right|^2$ is greater than $\left| \sum_{l=1}^{n_{r,j}} \phi_{r,j,l} w_l \right|^2$ for all $1 \leq j \leq T$ and any choice of the variables $w_l \in W_c = \{1, -1\}$, $1 \leq l \leq n_{r,j}$. Now fix a j between 1 and T . The average of $\left| \sum_{l=1}^{n_{r,j}} \phi_{r,j,l} w_l \right|^2$ over all $w_l \in W_c$, $1 \leq l \leq n_{r,j}$, is smaller than $\left| \sum_{l=1}^{n_{r,t}} \phi_{r,t,l} \chi_l \right|^2$ because the expected value of a positive random variable is always smaller than an upper bound for the random variable. Hence,

$$\sum_{l=1}^{n_{r,j}} |\phi_{r,j,l}|^2 \leq \left| \sum_{l=1}^{n_{r,t}} \phi_{r,t,l} \chi_l \right|^2, \quad 1 \leq j \leq T \quad (18)$$

using the fact that the first and second moments of the symbols in W_c are 0 and 1, respectively. By adding the inequalities in (18) for all j , we get that P is at least 1. Thus, $\epsilon_r \geq \frac{|z_{\max}|^2}{E_{\text{av}}}$ and we conclude the proof. \square

Corollary 1: The proposed code $\mathbf{Z}(z_1, \dots, z_M)$ is optimal with respect to PMEPR among all linear space-time codes over \mathcal{I} .

Proof: The input information constellation of the linear code $\mathbf{Z}(z_1, \dots, z_M)$ is either \mathcal{I}_i or \mathcal{I}_j and hence satisfies the condition of Proposition 1. Furthermore, the PMEPR for each antenna with the $\mathbf{Z}(z_1, \dots, z_M)$ code meets the lower bound of Proposition 1. \square

Proposition 1 and Corollary 1 provide a rigorous proof of the fact that the PMEPR with any general linear space-time code is lower-bounded by the PMEPR of the input information constellation and therefore the $\mathbf{Z}(z_1, \dots, z_M)$ code is optimal with respect to PMEPR. The proof makes explicit use of the fact that the maximum envelope point z_{\max} in the input information constellation \mathcal{I} is such that $-z_{\max} \in \mathcal{I}$. This fact is conveniently satisfied by both \mathcal{I}_i and \mathcal{I}_j constellations. It can be shown easily that there exists an input constellation and an associated linear space-time code such that the PMEPR of the linear code is smaller than that of the input constellation. However, such an input constellation must necessarily satisfy $-z_{\max} \notin \mathcal{I}$.

V. HIGH-RATE LOW PMEPR SPACE-TIME CODES

In this section, we consider the design of higher rate LPST codes and study their properties. The proposed LPST codes are shown to achieve full diversity, high number of symbols per channel use, low values of PMEPR, and also admit efficient decoding. The development of LPST codes in this section is organized as follows. We first introduce a compact and analytically useful representation of the TAST codes which aids the algebraic development of the LPST codes. A generalization of the Hadamard spreading scheme to reduce the PMEPR of the TAST codes is proposed. Subsequently, the construction of high-rate LPST codes is presented and the PMEPR advantage over the Hadamard spread of the TAST codes is proved. Several properties of the PMEPR with the LPST codes are then explored. Finally, the performance of the LPST codes is discussed and the decoding strategy at the receiver is presented.

The L -layer TAST code, denoted by $\mathcal{T}_{M,L,N}$, consists of L independent DAST codes arranged in nonoverlapping layers. However, we present here a more useful representation of the

L -layer TAST code as a sum of permuted DAST codes. Let $\mathbf{z} = [z_{1,1}, \dots, z_{1,M}, \dots, z_{L,1}, \dots, z_{L,M}]^T$ be the vector of LM information symbols from the input constellation \mathcal{I} , where $M \in \mathcal{M}_1 \cup \mathcal{M}_2$. The algebraic integer α_l corresponding to the information symbols of the l th layer is given by

$$\alpha_l = \sum_{k=1}^M z_{l,k} \theta^{k-1}, \quad 1 \leq l \leq L. \quad (19)$$

We introduce the following representation of the L -layer TAST code:

$$\mathcal{T}_{M,L,N}(\mathbf{z}) = \sum_{l=1}^L \phi_l \mathbf{P}^{l-1} \text{diag}(\alpha_l^{(1)}, \dots, \alpha_l^{(M)}) \quad (20)$$

where the M -dimensional permutation matrix \mathbf{P} is given by

$$\mathbf{P} = \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{I}_{M-1} & \mathbf{0} \end{bmatrix}$$

and $\mathbf{P}^0 = \mathbf{I}_M$. The constants $(\phi_1, \dots, \phi_L) \in C^L$, known as the Diophantine numbers for the L layers, are critical in ensuring full transmit diversity of the TAST code and their choice will be discussed at the end of this subsection. However, for the sake of PMEPR computation in general, no restrictions are imposed on the ϕ_l .

The PMEPR of the r th antenna with the L -layer TAST code is given by

$$\epsilon_r = \frac{\max_{1 \leq l \leq L} (|\phi_l|^2 \zeta_{\lfloor r-l \rfloor_{M+1}})}{\frac{1}{M} \sum_{l=1}^L |\phi_l|^2}, \quad 1 \leq r \leq M \quad (21)$$

where we have used the fact that $E_{\mathbf{x} \in \mathcal{S}}[|\mathbf{x}_s|^2]$ is the same for all $1 \leq s \leq M$.

Consider first the case for $M \in \mathcal{M}_1$. In this case, the expression for ϵ_r simplifies to

$$\epsilon_r = \zeta \left(\frac{\max_{1 \leq l \leq L} |\phi_l|^2}{\frac{1}{M} \sum_{l=1}^L |\phi_l|^2} \right), \quad 1 \leq r \leq M \quad (22)$$

where the constant ζ is the PMEPR of the rotated constellation \mathcal{S} , as defined in (9). The quantity in brackets in (22) is always greater than $\frac{M}{L}$ thus providing a lower bound on ϵ_r . If $L = M$ and $|\phi_l| = 1$, $1 \leq l \leq M$, then $\epsilon_r = \zeta$, $1 \leq r \leq M$.

We now propose a simple modification of the TAST code based on Hadamard transform to provide a baseline for comparison of the LPST codes to be constructed later. When $M \in \mathcal{M}_1$, it is possible to spread the TAST code for $L < M$ layers by Hadamard sequences, while preserving the performance, so that the PMEPR is reduced. Specifically, this is achieved by using the modified codebook

$$\sqrt{\frac{L'}{M}} (\mathcal{H}_{\frac{M}{L'}} \otimes \mathbf{I}_{L'}) \mathcal{T}_{M,L,N}(\mathbf{z}) \quad (23)$$

where L' is the smallest integer greater than or equal to L such that M/L' is a Hadamard dimension. The PMEPR of the TAST code spread in the Hadamard fashion is smaller than the expression in (22) by a factor of M/L' . Clearly, the Hadamard spread is not possible if $L > M/2$, thereby exposing the limitation of this spreading scheme (we set $L' = M$ if $L > M/2$). The

smallest value of PMEPR is obtained when M/L itself is equal to 2 or a multiple of 4. A particular example of such a spread was provided in [1] where for $M = 4$, $L = 2$, the $\mathcal{T}'_{4,2,2}$ code results in $\epsilon_r = \zeta$. In any case, we have the following lower bounds on the PMEPR of the TAST code with the Hadamard spread of (23) for $M \in \mathcal{M}_1$:

$$\epsilon_r \geq \zeta \frac{L'}{L} \geq \zeta, \quad 1 \leq r \leq M. \quad (24)$$

When $M \in \mathcal{M}_2$, knowledge of the magnitudes of ϕ_l is required to separate the terms in the maximization in (21) because ζ_l varies with l . Consequently, we will resort to numerical evaluation of the ϵ_r for $M \in \mathcal{M}_2$ later on. Again, the spread of the TAST code by Hadamard sequences is possible for $L < M \in \mathcal{M}_2$ if $\lfloor M \rfloor_4 = 0$.

For a rate greater than $\log_2(q)$ bpcu, it is not possible to obtain a full diversity spreaded version of the TAST code that transmits only q -QAM information symbols [4, Corollary 3.3.1]. We can, however, find a code equivalent to $\mathcal{T}_{M,L,N}$ that has a PMEPR smaller than ζ when $L < M$ and $M \in \mathcal{M}_1 \cup \mathcal{M}_2$. Moreover, this reduction in PMEPR is possible for more values of L than $M/2$, as in the Hadamard spread.

A. Low PMEPR Space-Time Code Construction

The main idea is to apply the spreading Θ_M as in (13) to the TAST code in (20) so that the performance remains unaffected. First, the product $\Theta_M \mathbf{P}^{l-1}$ is expressed in a convenient form using the structure of the IDFT matrix \mathbf{S}_M . We have that

$$\begin{aligned} [\mathbf{S}_M \mathbf{P}^{l-1}]_{j,k} &= [\mathbf{S}_M]_{j, \lfloor k+l-1 \rfloor_M} \\ &= \exp\left(\frac{i2\pi}{M}(j-1)(k+l-2)\right) \end{aligned}$$

and so, if we set

$$\Psi_l = \text{diag}\left(1, \omega_M^{l-1}, \omega_M^{2(l-1)}, \dots, \omega_M^{(M-1)(l-1)}\right)$$

then

$$\mathbf{S}_M \mathbf{P}^{l-1} = \Psi_l \mathbf{S}_M \quad (25)$$

$$\Rightarrow \Theta_M \mathbf{P}^{l-1} = \Psi_l \Theta_M. \quad (26)$$

Hence, applying the spreading Θ_M to the TAST codeword in (20), we get from (26) and (13) that

$$\begin{aligned} \Theta_M \mathcal{T}_{M,L,N}(\mathbf{z}) \Theta_M^{-1} & \\ &= \sum_{l=1}^L \phi_l \Psi_l \Theta_M \text{diag}(\alpha_l^{(1)}, \dots, \alpha_l^{(M)}) \Theta_M^{-1} \\ &= \sum_{l=1}^L \phi_l \Psi_l \mathbf{Z}(z_{l,1}, z_{l,2}, \dots, z_{l,M}) \\ &\triangleq \mathcal{L}_{M,L,N}(\mathbf{z}) \end{aligned} \quad (27)$$

where the formatter \mathbf{Z} is the same as that in (11). The new code $\mathcal{L}_{M,L,N}$ given by (28) is the general rate L symbols per channel use LPST code. The justification for the low PMEPR part of the nomenclature will be provided in Section V-B. As an example, the LPST code for $M = 4$ and $L = 2$ is given by the equation

at the bottom of the page, where the Diophantine numbers are $(\phi_1, \phi_2) = (1, \phi^{\frac{1}{4}})$.

In general, the (r, c) element of $\mathcal{L}_{M,L,N}(\mathbf{z})$ is given by

$$\mathcal{L}_{M,L,N}(r, c) = \sum_{l=1}^L \phi_l \omega_M^{(r-1)(l-1)} \gamma_{r,c} z_{l, M - \lfloor r-c-1 \rfloor_M} \quad (29)$$

where the term $\gamma_{r,c} = e$ if $c < r$ and $\gamma_{r,c} = 1$ if $c \geq r$. Thus, every antenna transmits a linear combination of L independent information symbols from \mathcal{I} in each time slot.

B. PMEPR Properties of LPST Codes

The improved PMEPR properties of the $\mathcal{L}_{M,L,N}$ code are shown next. As before, the average energy of \mathcal{I} is E_{av} and $z_{\max} \in \mathcal{I}$ is one of the points in \mathcal{I} with the maximum envelope. The average power of the signal on any transmit antenna is $P_{av} = (\sum_{l=1}^L |\phi_l|^2) E_{av}$. The PMEPR for the r th antenna with the $\mathcal{L}_{M,L,N}$ code is obtained from (29) as

$$\epsilon_r = \frac{1}{P_{av}} \max_{z_{l,k} \in \mathcal{I}, 1 \leq l \leq L, 1 \leq k \leq M} |\mathcal{L}_{M,L,N}(r, c)|^2 \quad (30)$$

$$= \frac{1}{P_{av}} \max_{z'_l \in \mathcal{I}} \left| \sum_{l=1}^L \phi_l e^{\frac{i2\pi(r-1)(l-1)}{M}} z'_l \right|^2 \quad (31)$$

where we have simplified with the fact that for a fixed r , the maximum of $|\mathcal{L}(r, c)|^2$ among all codewords is independent of c . Also, the set of L information symbols z'_l are independently chosen from \mathcal{I} .

Proposition 2: The PMEPR ϵ_r with the $\mathcal{L}_{M,L,N}$ space-time code for $M \in \mathcal{M}_1 \cup \mathcal{M}_2$ is upper-bounded as

$$\epsilon_r \leq L\epsilon_{\mathcal{I}}, \quad 1 \leq r \leq M. \quad (32)$$

Proof: For any (r, c) position in the code, application of the Cauchy-Schwartz inequality in (29) gives

$$\begin{aligned} |\mathcal{L}_{M,L,N}(r, c)|^2 &\leq \left(\sum_{l=1}^L |z_{l, M - \lfloor r-c-1 \rfloor_M}|^2 \right) \left(\sum_{l=1}^L |\phi_l|^2 \right) \\ &\leq L |z_{\max}|^2 \left(\sum_{l=1}^L |\phi_l|^2 \right). \end{aligned}$$

Hence, we have an upper bound, independent of (r, c) , for the peak envelope power for any transmit antenna. The PMEPR for the new code is now upper-bounded by the ratio of the upper bound on the peak power to the average power P_{av} . Hence,

$$\epsilon_r \leq L \frac{|z_{\max}|^2}{E_{av}} = L\epsilon_{\mathcal{I}}, \quad 1 \leq r \leq M. \quad (33)$$

□

For a given q , the upper bound of Proposition 2 on the PMEPR of all transmit antennas depends only on L . Thus, with the choice of L so that the upper bound to the PMEPR

TABLE I
VALUES OF L_M^g

| M | L_M^g |
|-----|---------|
| 2 | 1 |
| 4 | 3 |
| 8 | 7 |
| 16 | 14 |
| 32 | 28 |

of the LPST code is less than a lower bound on the PMEPR of the TAST code, our construction will necessarily result in a reduction of PMEPR for all the transmit antennas. Such a guarantee on the number of layers is obtained for $M \in \mathcal{M}_1$ from the lower bound on the PMEPR of the TAST code in (24) and is presented in the next proposition.

Proposition 3: For $M \in \mathcal{M}_1$ and a fixed q , the L -layer LPST code $\mathcal{L}_{M,L,N}$ necessarily has a smaller PMEPR than that obtained with a Hadamard spread of the TAST code $\mathcal{T}_{M,L,N}$ if

$$1 \leq L \leq \left\lfloor \frac{1}{\sqrt{2} \sin\left(\frac{\pi}{4M}\right)} \right\rfloor \triangleq L_M^g. \quad (34)$$

Proof: See Appendix A. □

The values of L_M^g for a few values of $M \in \mathcal{M}_1$ are shown in Table I. It is seen from Table I that the reduction of PMEPR can be obtained for large values of L . The new code $\mathcal{L}_{M,L,N}$ actually exploits the absence of some layers to make the PMEPR smaller than that of the rotation \mathcal{S} . This is because the LPST code transmits a linear combination of only L information symbols as opposed to M symbols in the original TAST code. This is unlike the spreading by Hadamard sequences, as in $\mathcal{T}'_{4,2,2}$, where the spreaded code continues to transmit a linear combination of M information symbols even if $L < M$. For $M = 4$, it can be seen from Table I that our construction leads to PMEPR reduction for $L = 3$ also, whereas a spread of $\mathcal{T}_{4,3,N}$ by Hadamard sequences is not possible. Note that the condition $L < M$ would be necessary, for instance, when $N < M$, in which case one has to use $L = N < M$ layers to employ the efficient sphere decoding algorithm.

The PMEPR of the modified TAST scheme in [5] was also shown to be upper-bounded by L times the PMEPR of the input constellation. However, it was not proved therein whether the actual PMEPR is indeed smaller than that of the original TAST construction of [1]. On the other hand, Proposition 3 here explicitly proves the advantage of using fewer information symbols for the linear combination at each position of the LPST code. Furthermore, the LPST codes achieve the upper bound on the PMEPR without affecting the performance of the TAST code. This is unlike the modified TAST scheme of [5] which actually pays a price in terms of performance as shown in Sections V-C and VII.

$$\mathcal{L}_{4,2,N}(\mathbf{z}) = \begin{bmatrix} z_{1,1} + \phi^{\frac{1}{4}} z_{2,1} & z_{1,2} + \phi^{\frac{1}{4}} z_{2,2} & z_{1,3} + \phi^{\frac{1}{4}} z_{2,3} & z_{1,4} + \phi^{\frac{1}{4}} z_{2,4} \\ iz_{1,4} - \phi^{\frac{1}{4}} z_{2,4} & z_{1,1} + \phi^{\frac{1}{4}} iz_{2,1} & z_{1,2} + \phi^{\frac{1}{4}} iz_{2,2} & z_{1,3} + \phi^{\frac{1}{4}} iz_{2,3} \\ i(z_{1,3} - \phi^{\frac{1}{4}} z_{2,3}) & i(z_{1,4} - \phi^{\frac{1}{4}} z_{2,4}) & z_{1,1} - \phi^{\frac{1}{4}} z_{2,1} & z_{1,2} - \phi^{\frac{1}{4}} z_{2,2} \\ iz_{1,2} + \phi^{\frac{1}{4}} z_{2,2} & iz_{1,3} + \phi^{\frac{1}{4}} z_{2,3} & iz_{1,4} + \phi^{\frac{1}{4}} z_{2,4} & z_{1,1} - \phi^{\frac{1}{4}} iz_{2,1} \end{bmatrix}$$

Note that for $L = 1$, the $\mathcal{L}_{M,1,N}$ code is the same as the rate one LPST code $\mathcal{Z}(z_1, \dots, z_M)$ of Section IV leading to a PMEPR equal to that of \mathcal{I} for all antennas. If $L > 1$, the PMEPR of the transmit antennas depends on the Diophantine numbers and can also vary across the transmit antennas. In order to compute the exact value of PMEPR given by (31), one needs to compute the maximum amplitude of a linear combination of symbols from \mathcal{I} . The computation of the PMEPR is greatly simplified due to the following lemma which implies that finding the maximum amplitude of a linear combination of K information symbols from the \mathcal{I}_i or \mathcal{I}_j constellation only requires 4^K hypothesis tests rather than q^K tests required by an exhaustive search.

Lemma 1: Let (ϕ_1, \dots, ϕ_n) be arbitrary nonzero complex numbers. Define the functions f_i and f_j by

$$f_i(z_1, \dots, z_n) = \left| \sum_{l=1}^n \phi_l z_l \right|^2, \quad z_l \in \mathcal{I}_i, \quad 1 \leq l \leq n \quad (35)$$

$$f_j(z_1, \dots, z_n) = \left| \sum_{l=1}^n \phi_l z_l \right|^2, \quad z_l \in \mathcal{I}_j, \quad 1 \leq l \leq n. \quad (36)$$

Then, $f_i(z_1, \dots, z_n)$ is maximized only when

$$z_l \in W_i = \{z_{\max}, -z_{\max}, iz_{\max}, -iz_{\max}\}, \quad 1 \leq l \leq n$$

where z_{\max} is the maximum envelope point in \mathcal{I}_i . Also, $f_j(z_1, \dots, z_n)$ is maximized only when

$$z_l \in W_j = \left\{ z_{\max}, -z_{\max}, \frac{i}{\sqrt{3}}z_{\max}, \frac{-i}{\sqrt{3}}z_{\max} \right\}, \quad 1 \leq l \leq n$$

where z_{\max} is the maximum envelope constellation point in \mathcal{I}_j .

Proof: For any point z in \mathcal{I}_i or \mathcal{I}_j , let $a(z)$ and $b(z)$ be the odd integers such that $z = a(z) + ib(z)$ if $z \in \mathcal{I}_i$ and $z = a(z) + jb(z)$ if $z \in \mathcal{I}_j$. The functions $f_i(z_1, \dots, z_n)$ and $f_j(z_1, \dots, z_n)$ are positive quadratics in each of the variables $a(z_l)$ and $b(z_l)$, $1 \leq l \leq n$. The maxima of f_i and f_j are attained only when each of $a(z_l)$ and $b(z_l)$, $1 \leq l \leq n$, assume either of their extremum values. The result of the proposition follows since all possible choices of the extremum values of $a(z_l)$ and $b(z_l)$ give rise to valid constellation points enumerated in W_i and W_j for \mathcal{I}_i and \mathcal{I}_j , respectively. \square

Further simplification in the computation of PMEPR can be obtained using the following lemma which notes that multiplication of the coefficients of a linear combination of information symbols from \mathcal{I}_i does not change the resulting maximum amplitude.

Lemma 2: Let (ϕ_1, \dots, ϕ_n) be arbitrary nonzero complex numbers. Define the function g by

$$g(\phi_1, \dots, \phi_n) = \max_{\substack{z_l \in \mathcal{I}_i \\ 1 \leq l \leq n}} \left| \sum_{l=1}^n \phi_l z_l \right|^2. \quad (37)$$

Then, for $\chi_l \in \{\pm 1, \pm i\}$, $1 \leq l \leq n$, $g(\phi_1, \dots, \phi_n) = g(\phi_1 \chi_1, \dots, \phi_n \chi_n)$.

Proof: Let $(w_1, \dots, w_n) \in \mathcal{I}_i^n$ and $(w'_1, \dots, w'_n) \in \mathcal{I}_i^n$ correspond to the maximum in the objective functions for $g(\phi_1, \dots, \phi_n)$ and $g(\phi_1 \chi_1, \dots, \phi_n \chi_n)$, respectively. Note that

$(w'_1 \chi_1, \dots, w'_n \chi_n) \in \mathcal{I}_i^n$ and $(\frac{w_1}{\chi_1}, \dots, \frac{w_n}{\chi_n}) \in \mathcal{I}_i^n$. Thus, we get that

$$g(\phi_1 \chi_1, \dots, \phi_n \chi_n) \geq \left| \sum_{l=1}^n \phi_l \chi_l \frac{w_l}{\chi_l} \right|^2 = g(\phi_1, \dots, \phi_n). \quad (38)$$

Similarly

$$g(\phi_1, \dots, \phi_n) \geq \left| \sum_{l=1}^n \phi_l (w'_l \chi_l) \right|^2 = g(\phi_1 \chi_1, \dots, \phi_n \chi_n). \quad (39)$$

From (38) and (39), we get that $g(\phi_1, \dots, \phi_n) = g(\phi_1 \chi_1, \dots, \phi_n \chi_n)$. \square

For a fixed set of Diophantine numbers and $M \in \mathcal{M}_1$, Lemma 2 leads to the the following proposition which states that some of the antennas exhibit the same PMEPR with the LPST code.

Proposition 4: For any $M \in \mathcal{M}_1 \setminus \{2\}$ and $L > 1$, the transmit antennas can be partitioned into $M/4$ disjoint groups so that every antenna in the same group exhibits the same PMEPR with the LPST code. For $M = 2$, both the transmit antennas have the same PMEPR.

Proof: If the index of a particular antenna is r , then the antenna with the index $\lfloor r + (M/4) \rfloor_M$ for $M \geq 4$ and with the index $\lfloor r + 1 \rfloor_M$ for $M = 2$ also gives the same maximum absolute value of $\mathcal{L}_{M,L,N}(r, c)$ in (29) due to Lemma 2. The average power for all transmit antennas is the same. Thus, for $M \geq 4$ there are four antennas in the same group with the same PMEPR and there are $M/4$ such groups. Similarly, for $M = 2$, both the antennas have the same PMEPR. \square

It is proved next that the PMEPR of a particular transmit antenna with the LPST codes strictly increases with the number of layers in the code if the size q of the constellation \mathcal{I} is kept fixed.

Proposition 5: For a fixed $M \in \mathcal{M}_1$, constellation size q and $|\phi_l| = 1, \forall l$, the PMEPR for each antenna with LPST codes is a strictly increasing function of L .

Proof: See Appendix B. \square

In Section V-C, we shall consider the restriction of the Diophantine numbers to the form

$$(\phi_1, \dots, \phi_L) = (1, \phi^{\frac{1}{M}}, \dots, \phi^{\frac{L-1}{M}})$$

for a given complex number ϕ . This parameterization simplifies the problem of coding gain maximization with the TAST and LPST codes. If $|\phi| \neq 1$, then the PMEPR of the TAST code, as in (22), is necessarily greater than the PMEPR of the inherent rotation. For the purpose of illustration, we constrain $\phi = e^{i\lambda}$, for $\lambda \in \mathbb{R}$. In this case, the PMEPR ϵ_r of the original TAST code is independent of λ . However, with the LPST code, the ϵ_r depends on λ and this warrants an optimum selection of λ that leads to the least PMEPR, while preserving the diversity advantage of the code. Henceforth, we use $\epsilon_r(\lambda)$ to denote the PMEPR of the r th antenna for a particular choice of λ . The behavior of the PMEPR with respect to λ is generalized in the following proposition.

Proposition 6: For any $M \in \mathcal{M}_1$, $\epsilon_r(\lambda) = \epsilon_r(\lambda + M\frac{\pi}{2})$ with the LPST code.

Proof: Replacing λ by $\lambda + M\frac{\pi}{2}$ leads to a multiplication by i for the coefficients of the linear combination in (29). Hence, by Lemma 2, the maximum of $|\mathcal{L}_{M,L,L}(r, c)|^2$ remains unchanged. Since $|i| = 1$, the average power for any transmitter also remains unchanged and thus the result of the proposition follows. \square

C. Performance of LPST Codes

The performance of the LPST codes and the TAST codes are identical for a given rate and a given set of Diophantine numbers. The advantage of the LPST codes is that for $1 \leq L \leq L_M^g$, $M \in \mathcal{M}_1$ and the choice of $\{\phi_l\}_{l=1}^L$ that optimizes the coding gain of $\mathcal{T}_{M,L,N}$, the corresponding LPST code $\mathcal{L}_{M,L,N}$ also enjoys the same performance but at a lower PMEPR for the transmit antennas. Numerical computation for $M = 3 \in \mathcal{M}_2$ in Section VII also leads to a similar conclusion for the PMEPR with the LPST code. In this subsection, we draw comparisons of the performance of the LPST codes with those of the modified TAST codes of [5]. By computing the exponents of a lower bound on the coding gain, we argue that the modified TAST codes actually reduce the PMEPR at the expense of a loss in performance compared to the original TAST code. The LPST codes, on the other hand, achieve both low values of PMEPR and good performance simultaneously.

The selection of ϕ_l to guarantee full transmit diversity of the TAST codes is nontrivial in general with no imposed constraints on the Diophantine numbers. Hence, it was suggested in [1] to parameterize all the Diophantine numbers with a single Diophantine number as $(\phi_1, \dots, \phi_L) = (1, \phi^{\frac{1}{M}}, \dots, \phi^{\frac{L-1}{M}})$. With this structure, full transmit diversity is readily obtained by choosing ϕ such that the set $(1, \phi, \dots, \phi^{L-1})$ is algebraically independent over the number field containing the elements of the rotation for each layer (see [1, Theorems 1 and 2]). The effective degree of the number field containing ϕ and the rotation elements is $2ML$. The exponent of the lower bound² in [1, Theorem 3] becomes proportional to $(2ML-1)(L-1)$. In the modified TAST scheme of [5], there exist M layers each containing L independent information symbols. Therefore, the code in [5] requires M Diophantine numbers, namely, $(\phi_1, \dots, \phi_M) = (1, \phi^{\frac{1}{M}}, \dots, \phi^{\frac{M-1}{M}})$. Full diversity is now obtained by choosing $(1, \phi, \dots, \phi^{M-1})$ to be independent over the new rotated elements of each layer. The exponent of a lower bound similar to the one given by [1, Theorem 3] now becomes proportional to $(2M^2-1)(M-1)$ if L does not divide M or $(2ML-1)(M-1)$ if L divides M . In any case, this exponent is larger than that for the original TAST code, thereby suggesting a reduction in coding gain with the modified TAST scheme of [5]. The LPST codes, on the other hand, are obtained from unitary transformations of the original TAST codes and, therefore, preserve the exact performance of these codes.

We also highlight another difference between the LPST codes and the modified TAST codes for the special case of $L = 2$ symbols per channel use. It was shown in [1] that full diversity of the TAST code with $L = 2$ can be guaranteed by choosing

²The factor m in [1, Theorem 3] should actually be $m - 1$ as can be checked using [1, Theorem 8].

the Diophantine number to have degree just 2 over the complex rationals. This leads to an improvement in the coding gain compared to the general guideline for choosing the Diophantine number. Thus, the LPST code having a performance identical to that of the TAST code can also benefit from this simplification. However, this simplification is no longer possible with the modified TAST scheme of [5].

D. Decoding of LPST Codes

The decoding of the LPST codes is discussed now. The rate one code of Section IV is a special case of the LPST codes introduced in this section and, hence, its decoding is similar. The received statistic \mathbf{Y} for the $\mathcal{L}_{M,L,N}$ code is given by

$$\begin{aligned} \mathbf{Y} &= \sqrt{\rho} \mathbf{H} \Theta_M \mathcal{T}_{M,L,N}(\mathbf{z}) \Theta_M^{-1} + \mathbf{N} \\ \Rightarrow \tilde{\mathbf{Y}} &= \mathbf{Y} \Theta_M = \sqrt{\rho} \mathbf{H} \Theta_M \mathcal{T}_{M,L,N}(\mathbf{z}) + \tilde{\mathbf{N}} \end{aligned} \quad (40)$$

where the entries of $\tilde{\mathbf{N}}$ are also i.i.d. $CN(0, N_0)$. Equation (40) serves to demonstrate that the performance of the spreaded code is exactly the same as that of $\mathcal{T}_{M,L,N}$ because the modified fading coefficients $\mathbf{H} \Theta_M$ are also i.i.d. and $CN(0, 1)$ [19]. One may argue that the LPST code can be decoded as in [1] with \mathbf{H} replaced by $\mathbf{H} \Theta_M$ and the received signal matrix by $\tilde{\mathbf{Y}}$. However, the multiplication by Θ_M is not necessary and only a rearrangement of the columns of \mathbf{H} is required for the equivalent channel matrix seen by the decoder. Referring to (28) we see that

$$\begin{aligned} \mathbf{Y} &= \sqrt{\rho} \mathbf{H} \sum_{l=1}^L \phi_l \Psi_l \mathbf{Z}(z_{l,1}, \dots, z_{l,M}) + \mathbf{N} \\ &= \sqrt{\rho} \sum_{l=1}^L \bar{\mathbf{H}}_l \mathbf{Z}(z_{l,1}, \dots, z_{l,M}) + \mathbf{N}, \quad \text{say.} \end{aligned}$$

Denote the j th column of $\bar{\mathbf{H}}_l$ by $\bar{\mathbf{H}}_l^j$ and define the effective channel matrix $\hat{\bar{\mathbf{H}}}_l$ seen by the information symbols of the l th layer by

$$\hat{\bar{\mathbf{H}}}_l = \begin{bmatrix} \bar{\mathbf{H}}_l^1 & e \bar{\mathbf{H}}_l^M & \dots & e \bar{\mathbf{H}}_l^2 \\ \bar{\mathbf{H}}_l^2 & \bar{\mathbf{H}}_l^1 & \dots & e \bar{\mathbf{H}}_l^3 \\ \vdots & \vdots & \ddots & \vdots \\ \bar{\mathbf{H}}_l^M & \bar{\mathbf{H}}_l^{M-1} & \dots & \bar{\mathbf{H}}_l^1 \end{bmatrix}. \quad (41)$$

Let the $\text{vec}(\cdot)$ operator stack the columns of a matrix one below the other so that

$$\text{vec}(\mathbf{Y}) = \sqrt{\rho} [\hat{\bar{\mathbf{H}}}_1, \dots, \hat{\bar{\mathbf{H}}}_L] \mathbf{z} + \text{vec}(\mathbf{N}) = \bar{\mathcal{H}} \mathbf{z} + \text{vec}(\mathbf{N}). \quad (42)$$

The $LM \times 1$ information symbol vector \mathbf{z} can now be decoded using the sphere decoder [2], with $\bar{\mathcal{H}}$ being the effective $NM \times LM$ size channel.³ For $L \leq N$, the sphere decoder is of polynomial complexity in the number of information symbols.

³For $M \in \mathcal{M}_2$, the effective generator matrix in the real representation of the sphere decoder should be multiplied by

$$\begin{bmatrix} \mathbf{I} & \frac{-1}{2} \mathbf{I} \\ \mathbf{0} & \frac{\sqrt{3}}{2} \mathbf{I} \end{bmatrix}$$

for both TAST and LPST codes.

If $L > N$, then the generalized sphere-decoding algorithm [21] can be employed which has a complexity roughly exponential in $M(L - N)$.

We note that the average complexity of the sphere decoder being polynomial in the number of information symbols has been explicitly proved only for the special case of the vector model $\mathbf{r} = \mathbf{G}\mathbf{z} + \mathbf{n}$, where \mathbf{G} is an $N_e \times N_v$ matrix ($N_e \geq N_v$) of i.i.d. Gaussian elements and \mathbf{n} consists of i.i.d. Gaussian noise elements [22]. In practice, however, the expected complexity of the sphere decoder is much smaller than an exhaustive search for several other scenarios as well, such as the space-time model described above, and appears to be polynomial in the number of information symbols [1], [2], [23], [24] (whenever $N_e \geq N_v$). In this paper, polynomial complexity of the sphere decoder essentially means that the number of information symbols is not more than the number of available equations and that the effective channel matrix has full rank with probability one. The maximum-likelihood decoding in such cases using the sphere decoder is far more efficient than performing an exhaustive search.

VI. PUNCTURED LPST CODES

In addition to the reduced PMEPR property, we show that punctured LPST codes can significantly improve upon the *performance* of the corresponding L -layer TAST codes (for $L < M$) for moderate/reasonable SNRs by sacrificing diversity for rate.

Proposition 7: For the L -layer LPST code $\mathcal{L}_{M,L,N}$ with $N \geq M$, consider the punctured space-time code of size $M \times D$, $L \leq D \leq M$, obtained by deleting any $M - D$ columns of all codewords in $\mathcal{L}_{M,L,N}$ and denoted by $\mathcal{L}_{M,L,N}^D$. Then, the punctured code $\mathcal{L}_{M,L,N}^D$

- has a transmit diversity of D ,
- a rate of $\frac{ML}{D}$ symbols per channel use,
- the r th antenna PMEPR ϵ_r equal to that of the original $\mathcal{L}_{M,L,N}$ code for each $1 \leq r \leq M$,
- and is decodable with polynomial complexity using the sphere decoder.

Proof: The columns in the difference of any two codewords in the full transmit diversity code $\mathcal{L}_{M,L,N}$ are linearly independent. Therefore, the columns in the difference of any two codewords in $\mathcal{L}_{M,L,N}^D$ are linearly independent, leading to a transmit diversity of D . The first column of $\mathcal{L}_{M,L,N}^D$ consists of ML independent information symbols from \mathcal{I} that fix the entire codeword. Hence, the rate is $\frac{ML}{D}$ information symbols per channel use. Moreover, the maximum value of $|\mathcal{L}_{M,L,N}(r, c)|^2$ for any r is independent of c , as seen from (29). Hence, the PMEPR ϵ_r remains the same as that of $\mathcal{L}_{M,L,N}$ irrespective of the number of columns deleted from $\mathcal{L}_{M,L,N}$. Finally, $\mathcal{L}_{M,L,N}^D$ lends itself to polynomial-time sphere decoding since $D \geq L$ and $N \geq M$ and the size of the effective channel in the linear model is $ND \times ML$ (note that the received statistics for the $\mathcal{L}_{M,L,N}^D$ code are simply the first ND entries in (42)).⁴ \square

⁴The original TAST code does not lead to polynomial-time sphere decoding by the puncturing mechanism for any value of L .

In the special case $D = L$, the puncturing process leads to a code with the full rate of M symbols per channel use. As an example, the punctured $\mathcal{L}_{3,2,3}^2$ code is obtained from (28) as

$$\mathcal{L}_{3,2,3}^2(\mathbf{z}) = \begin{bmatrix} z_{1,1} + \phi^{\frac{1}{3}}z_{2,1} & z_{1,2} + \phi^{\frac{1}{3}}z_{2,2} \\ ez_{1,3} + \phi^{\frac{1}{3}}jez_{2,3} & z_{1,1} + \phi^{\frac{1}{3}}jz_{2,1} \\ ez_{1,2} + \phi^{\frac{1}{3}}j^2ez_{2,2} & ez_{1,3} + \phi^{\frac{1}{3}}j^2ez_{2,3} \end{bmatrix} \quad (43)$$

where $e = -j^2$, $z_{l,k} \in \mathcal{I}_j$, $1 \leq l \leq 2$, $1 \leq k \leq 3$.

In comparing the L -layer TAST code with the punctured, full-rate LPST code $\mathcal{L}_{M,L,N}^L$ at a given spectral efficiency, the information symbol constellation for the latter would be smaller than that for the L -layer TAST code. As shown in Section VII, this manifests a significant improvement in the performance of the punctured LPST code compared to the L -layer TAST code at moderate values of SNR.

The punctured LPST code with $D = L$ offers an attractive scheme for transmission of M information symbols from \mathcal{I} in every channel use. The simple uncoded Bell Labs layered space-time (BLAST) scheme [25] transmits at the full rate of M symbols per channel use but exhibits a transmit diversity of only 1. The full layer ($L = M$) TAST code transmits at the rate of M symbols per channel use and exhibits a transmit diversity of M but requires the extreme complexity of the M^2 sized sphere decoder. The punctured LPST codes offer everything in between; higher transmit diversity relative to the uncoded BLAST scheme and reduced complexity relative to the full-layer TAST scheme.

We next compare the proposed punctured LPST codes with the reduced diversity space-time constellations in [5]. Suppose a transmit diversity order of T ($T < M$) is required with a sphere decoder complexity of L_c complex dimensions. If $L_c \leq T \min(M, N)$, then one writes $TM = L_c + n_1T + n_2$, where $n_1 \geq 0$ and $0 \leq n_2 < T$. It was suggested in [5] to delete the last n_1 threads and n_2 information symbols from another thread in the modified TAST scheme to achieve the required diversity order with the imposed restriction on complexity. However, deleting some threads in the code leads to an increase in PMEPR due to the zero symbols in the code matrix and an unnecessarily large number T of symbols that combine linearly at some of the nonzero positions. Now, if L_c is a multiple of M , then the proposed punctured LPST code with the values $D = T$, $L = \frac{L_c}{M}$ also meets the required diversity order and complexity constraints but there are no zero symbols in the resulting code matrix and the number of symbols that combine linearly at the nonzero positions is $L \leq \frac{T \min(N, M)}{M} \leq T$. Hence, we see that complexity reduction at reduced diversity orders can also be achieved in a manner that simultaneously reduces the PMEPR for each antenna.

VII. NUMERICAL RESULTS

The LPST codes constructed in the previous sections were shown to be promising in terms of PMEPR reduction and rate enhancement by puncturing. In this section, specific examples of the LPST codes are discussed. The Diophantine numbers in all the examples are chosen to be $\phi_l = \phi^{\frac{l-1}{M}}$, $1 \leq l \leq L$, with $\phi = e^{i\lambda}$, $\lambda \in \mathcal{R}$. Thus, the PMEPR will be denoted by $\epsilon_r(\lambda)$ to explicitly represent the dependence on λ .

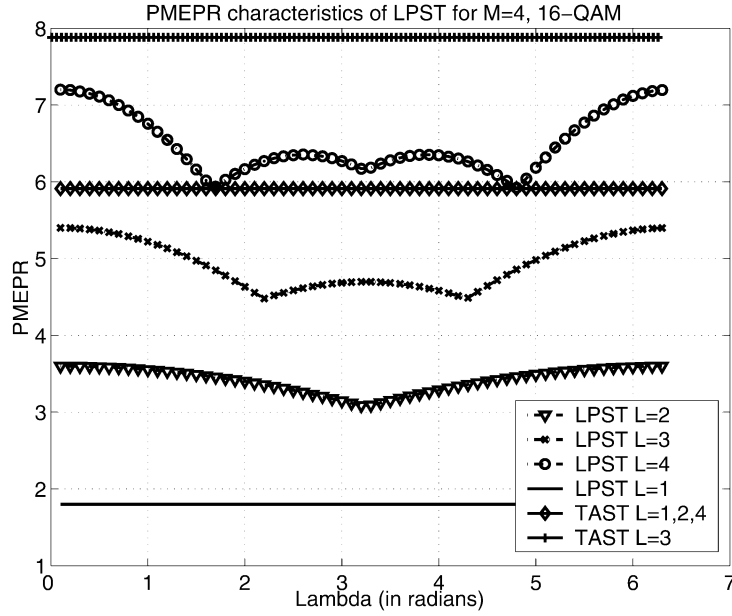


Fig. 1. PMEPR reduction for $M = 4$.

A. PMEPR Comparisons

The examples in this section demonstrate the PMEPR reduction obtained with the full diversity LPST codes compared to the Hadamard spread of the TAST codes. The reader is referred to (31) for the exact expression of PMEPR of the r th transmit antenna with the LPST code.

1) $M = 4, 1 \leq L \leq 4$: In this example, we get from (31) and Lemma 2 that for $1 \leq r \leq 4$

$$\epsilon_r(\lambda) = \frac{1}{LE_{av}} \max_{z'_l \in \mathcal{I}_i} \left| \sum_{l=1}^L \exp\left(i \frac{\lambda(l-1)}{4}\right) z'_l \right|^2. \quad (44)$$

Since the expression for $\epsilon_r(\lambda)$ does not depend on r , all transmit antennas have the same PMEPR. The PMEPR is also periodic in λ with a period of 2π . For this range of λ , a plot of the variability of the PMEPR of all transmit antennas with respect to λ for $1 \leq L \leq 4$ is shown in Fig. 1 for 16-QAM information symbols. The PMEPR of the original TAST code for $M = 4$ spread with the Hadamard sequence for $L = 1, 2, 4$ is also shown in the figure. Since a Hadamard spread of this TAST code with $L = 3$ is not possible, the corresponding PMEPR is $4/3$ times higher as shown in the figure.

Notice the significant reduction in PMEPR for the L -layer LPST code with respect to the L -layer TAST code at the same information symbol constellation size. With a single layer ($L = 1$), $\mathcal{L}_{4,1,N}$ results in a PMEPR saving of 5.2 dB. For $L = 2$, the LPST code can result in PMEPR savings from 2.2 to 2.8 dB, depending on the choice of λ , compared to $T'_{4,2,2}$. For $L = 3$, the PMEPR savings range from 1.6 to 2.5 dB depending on the choice of λ .

The coding gain of the TAST code depends on the choice of λ . Even so, for $1 \leq L \leq 3$ and the λ that minimizes the error probability, the LPST code will exhibit a much smaller PMEPR and will also enjoy the same performance as the corresponding TAST code.

Note that the constellation size q is fixed in Fig. 1. As proved in Proposition 5, the PMEPR shown in Fig. 1 does strictly increase with L . The PMEPR $\epsilon'_r(\lambda)$ with any other square QAM constellation of size q' can be obtained by multiplying $\epsilon_r(\lambda)$ with the ratio of the PMEPR of the QAM constellation of size q' to the PMEPR of the QAM constellation of size q . This is useful for comparing the PMEPR of the LPST or the TAST codes with different number of layers at the same spectral efficiency.

2) $M = 8, 1 \leq L \leq 7$: The PMEPR of the r th transmit antenna, $1 \leq r \leq 8$, in this case, is given by (31)

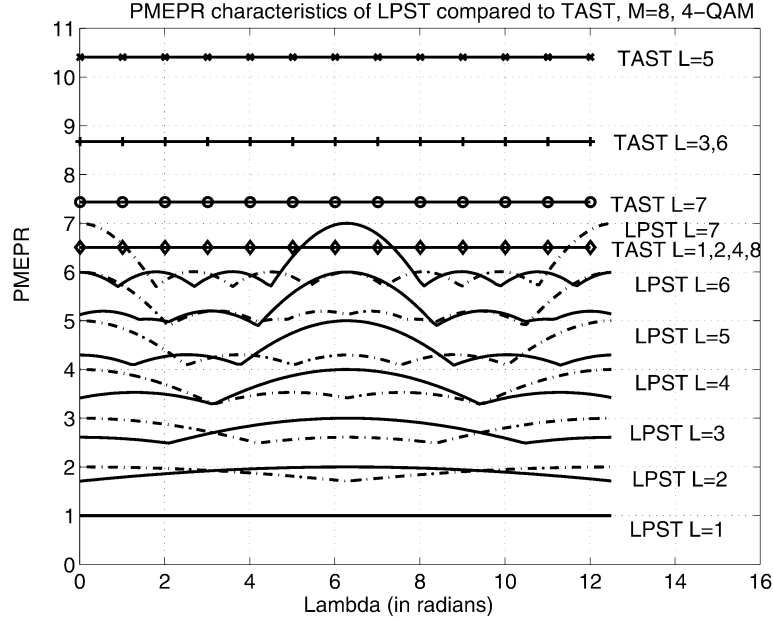
$$\epsilon_r(\lambda) = \frac{1}{LE_{av}} \max_{z'_l \in \mathcal{I}_i} \left| \sum_{l=1}^L \exp\left(i \frac{\lambda + 2\pi(r-1)}{8}(l-1)\right) z'_l \right|^2. \quad (45)$$

Thus, for a fixed r , $\epsilon_r(\lambda)$ has a period of 4π with respect to λ . Also, there are two disjoint groups of antennas that exhibit the same PMEPR as a function of λ . The two groups of antennas correspond to the odd and even values of r . A plot of the PMEPR of the spreaded code for $1 \leq L \leq 7$ and 4-QAM is shown in Fig. 2. The set of increasing solid lines correspond to one of the two groups of antennas for increasing L as shown. The set of increasing dotted lines corresponds to the other group for increasing $L (> 1)$.

For a given L , we refer to the maximum of the solid and dotted curves corresponding to the two groups of antennas as the ϵ_L^{\max} curve. Using ϵ_L^{\max} , one can determine the range for λ so that the PMEPR for all the transmit antennas is less than a required threshold.

The minima of ϵ_L^{\max} curve occurring at a certain $\lambda_{L,\min}$ reflects the potential savings in PMEPR achievable with the LPST code compared to the TAST code with the Hadamard spread as shown in the figure. The corresponding PMEPR gains with the LPST code at $\lambda_{L,\min}$ are tabulated in Table II for $1 \leq L \leq 7$.

For $L = 1$, the LPST code has a PMEPR of 1 for all transmit antennas since the 4-QAM constellation results in a constant envelope space-time code in this case.

Fig. 2. PMEPR reduction for $M = 8$.TABLE II
POTENTIAL PMEPR SAVINGS WITH $\mathcal{L}_{8,L,N}$

| L | Gain(dB) |
|-----|----------|
| 1 | 8.2 |
| 2 | 5.2 |
| 3 | 5.2 |
| 4 | 2.9 |
| 5 | 3.4 |
| 6 | 2.4 |
| 7 | 0.97 |

3) $M = 3, 1 \leq L \leq 3$: The three-dimensional complex rotated constellation has different values of PMEPR for each coordinate. For the input constellation \mathcal{I}_j with $q = 4$ symbols, we perform an exhaustive search to get that $\zeta_1 = 4.1454$, $\zeta_2 = 3.2057$, and $\zeta_3 = 3.2435$. Consequently, we have the following expressions for PMEPR of all the transmit antennas in the original TAST code

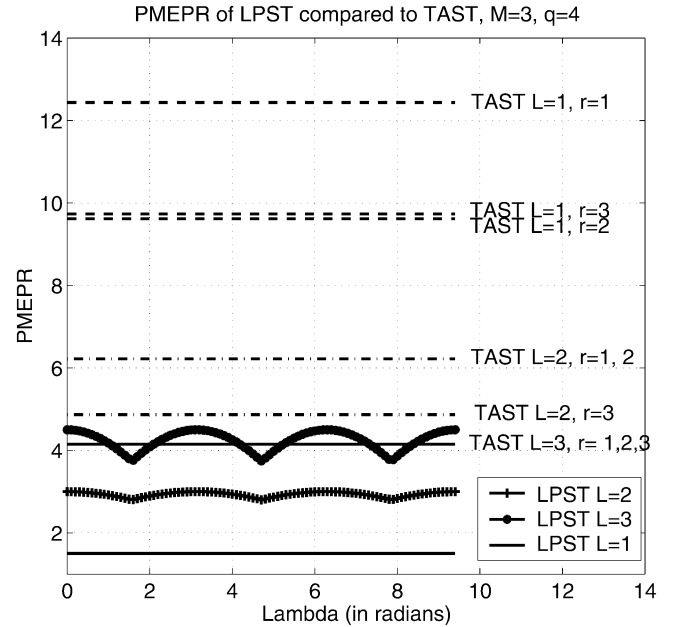
$$\begin{aligned} L = 1 : \epsilon_r &= 3\zeta_r, & 1 \leq r \leq 3 \\ L = 2 : \epsilon_1 = \epsilon_2 &= \frac{3}{2}\zeta_1, & \epsilon_3 = \frac{3}{2}\zeta_3 \\ L = 3 : \epsilon_r &= \zeta_1, & 1 \leq r \leq 3. \end{aligned}$$

The PMEPR with the LPST code for $L = 1$ is equal to $\epsilon_{\mathcal{I}_j}$ for all transmit antennas. For $L = 2$ and $L = 3$, the expression

$$\epsilon_r(\lambda) = \frac{1}{LE_{av}} \max_{z'_l \in \mathcal{I}_j} \left| \sum_{l=1}^L \exp\left(i \frac{\lambda + 2\pi(r-1)(l-1)}{3}\right) z'_l \right|^2 \quad (46)$$

gives the PMEPR of the LPST code.

In Fig. 3, only the curve for $\epsilon_L^{\max}(\lambda) = \max_{1 \leq r \leq 3}(\epsilon_r(\lambda))$, $1 \leq L \leq 3$, is shown for the LPST code. The range for λ is chosen to be $[0, 3\pi]$ as one can verify, with the help of proof of Lemma 2, that the PMEPR of the LPST code is periodic in λ with a period of at most 3π . The figure also shows the PMEPR of the original TAST code for comparison.

Fig. 3. PMEPR reduction for $M = 3$.

It is clear from the figure that for all values of λ , the PMEPR with the LPST code is smaller than that of TAST for $L = 1$ and $L = 2$. Interestingly, even for $L = 3$, there exists a range for λ wherein the PMEPR of the LPST code is smaller than that of the corresponding TAST code.

B. Performance Comparisons

The $\mathcal{L}_{M,L,N}$ code and the L -layer TAST code have identical performance. We show here that at high spectral efficiencies, the punctured LPST code $\mathcal{L}_{M,L,N}^D$ outperforms the L -layer TAST code for $L < M \leq N$ and moderate values of SNR. However, we also show that, at low spectral efficiencies, the reduced diversity $\mathcal{L}_{M,L,N}^D$ code suffers a loss in performance compared to the full diversity $\mathcal{L}_{M,L,N}$ code.

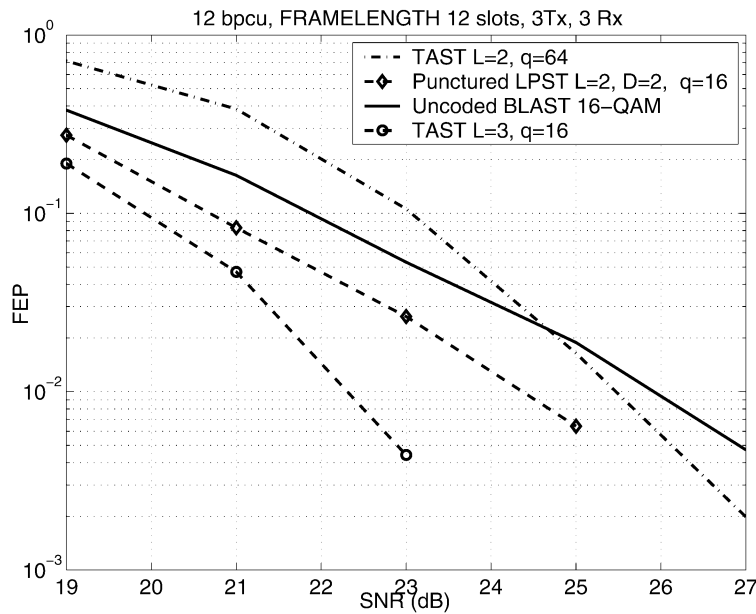


Fig. 4. Performance comparison for $M = N = 3$, $R = 12$ bpcu.

For the following examples, the fading channel is assumed to be fixed for a frame length of F time slots and each such frame is formed by concatenation of independent smaller space-time block codes that have been discussed in this paper. The performance is measured with respect to the frame error probability. The Diophantine number is chosen to be $\phi = e^{\frac{1}{2}}$ unless stated otherwise.

1) $M = N = 3$, $F = 12$, $R = 12$ bpcu: In this example, the two TAST codes for $L = 2$ and $L = 3$ provide a transmit diversity of 3. The punctured LPST code $\mathcal{L}_{3,2,3}^2$ given in (43) provides a transmit diversity of 2 whereas the uncoded BLAST scheme exhibits a transmit diversity of 1. The performance of these schemes are shown in Fig. 4.

While the diversity advantage of the two-layer TAST code compared to BLAST appears only at the end of the SNR region shown in Fig. 4, the reduced diversity punctured LPST code offers an improvement over the BLAST scheme for all values of SNR shown. Note the effect of the two superior properties of the punctured LPST code—a higher rate compared to the two-layer TAST code and a higher diversity compared to the BLAST scheme. The punctured LPST code, therefore, offers a better alternative to reducing the complexity of the three-layer TAST code than reducing the number of layers to two.

2) $M = N = 4$, $F = 12$, $R = 24$ bpcu: In Fig. 5, the performance of the TAST codes for $L = 2, 3$ and 4 are compared with the BLAST scheme, all at the same spectral efficiency of $R = 24$ bpcu. In spite of the high transmit diversity, the reduced-layer TAST codes perform poorly compared to the full-rate BLAST scheme. Therefore, the corresponding LPST codes $\mathcal{L}_{4,2,4}$ and $\mathcal{L}_{4,3,4}$ are not particularly useful either. For such high spectral efficiencies, the punctured LPST codes $\mathcal{L}_{4,2,4}^2$ and $\mathcal{L}_{4,3,4}^3$ serve the purpose of increasing the rate compared to the reduced layer TAST codes and their performance is also shown in Fig. 5. The $\mathcal{L}_{4,2,4}^2$ code is obtained by puncturing the second and fourth columns of $\mathcal{L}_{4,2,4}$ and the $\mathcal{L}_{4,3,4}^3$ code is obtained by puncturing the fourth column of $\mathcal{L}_{4,3,4}$. Both the

punctured schemes outperform the BLAST scheme in the range of SNR shown.

The PMEPR for each antenna with BLAST, $\mathcal{L}_{4,2,4}^2$, $\mathcal{L}_{4,3,4}^3$, and the full-layer TAST schemes are 3.6736, 6.6731, 8.4057, and 8.8442 dB, respectively. The size of the sphere decoder required for these schemes are 4, 8, 12, and 16, respectively. Both the PMEPR and the decoding complexities increase with a decrease in error probability. However, note the almost similar performance of the $\mathcal{L}_{4,2,4}^2$ and the $\mathcal{L}_{4,3,4}^3$ codes. The $\mathcal{L}_{4,2,4}^2$ code is, therefore, a better choice than the $\mathcal{L}_{4,3,4}^3$ code due to both lower PMEPR and lower complexity.

3) $M = 4$, $N = 2$, $F = 4$, $R = 4$ bpcu: In this example, we compare the construction of the modified TAST scheme with the LPST code. For the modified TAST scheme, we use the code $\mathcal{D}_{4,4,2}$ presented in [5] wherein the Diophantine number $\phi = e^{i2\pi/7}$ was found to achieve a local optimum of the coding gain with the 4-QAM constellation. The LPST code $\mathcal{L}_{4,2,2}$ is used for comparison with this code with the Diophantine number $\phi = e^{i2\pi/6}$.

The performance of these two codes are shown in Fig. 6. The LPST code has the same performance as the original TAST scheme of [1]. However, the modified TAST scheme $\mathcal{D}_{4,4,2}$ is almost 0.5 dB worse in performance at the highest SNR shown. The PMEPR with the $\mathcal{D}_{4,4,2}$ and the $\mathcal{L}_{4,2,2}$ codes are 2.32 and 2.99 dB, respectively. Thus, even though the $\mathcal{D}_{4,4,2}$ has a slightly smaller PMEPR than $\mathcal{L}_{4,2,2}$, its performance is poorer compared to the $\mathcal{L}_{4,2,2}$ code. Interestingly, by examining Fig. 5, we see that the PMEPR of the $\mathcal{L}_{4,2,2}$ code can be made smaller by choosing ϕ to be $e^{3.2i}$, for instance. With this value of ϕ , the PMEPR of $\mathcal{L}_{4,2,2}$ becomes 2.35 dB and its performance, also shown in Fig. 6, is actually slightly better than with $\phi = e^{i\pi/6}$. Thus, the LPST framework provides both good performance and low PMEPR in this example simultaneously.

4) $M = N = 4$, $F = 480$, $R = 4$ bpcu: This example shows that the reduced diversity of the punctured LPST codes can be disadvantageous at low spectral efficiencies. In Fig. 7,

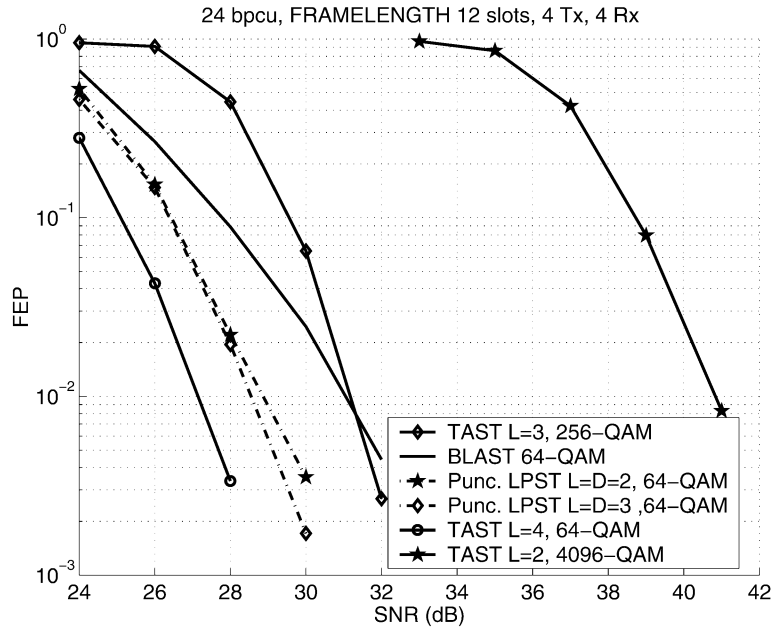


Fig. 5. Performance comparison for $M = N = 4$, $R = 24$ bpcu.

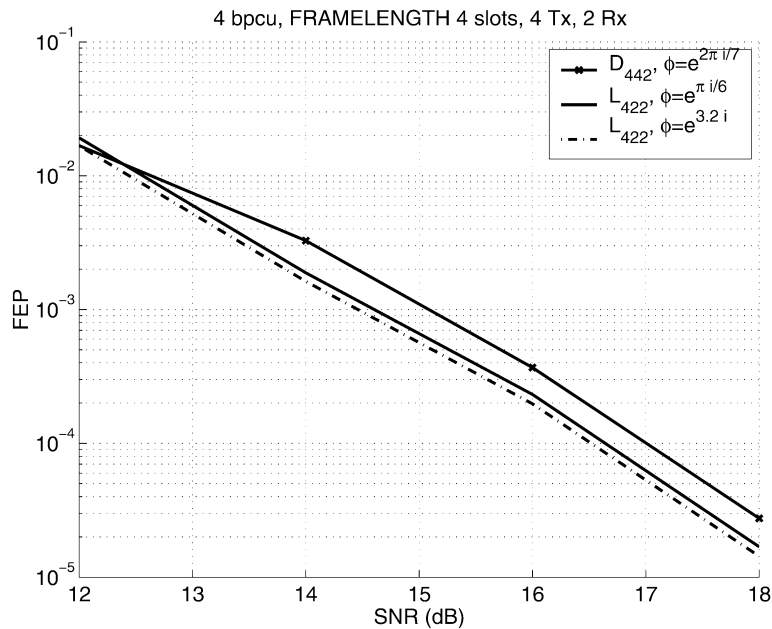


Fig. 6. Performance comparison for $M = 4$, $N = 2$, $R = 4$ bpcu.

the performance of the $\mathcal{L}_{4,2,4}$ code is compared with the $\mathcal{L}_{4,2,4}^2$ code. The lower diversity of the $\mathcal{L}_{4,2,4}^2$ code compared to the $\mathcal{L}_{4,2,4}$ code causes a significant loss in performance.

Interestingly, the performances of the $\mathcal{L}_{4,2,4}$ code and the full-layer TAST code are similar. The size of the sphere decoder in the equivalent real representation is the same for these two codes because the full-layer TAST code employs the real binary phase-shift keying (BPSK) constellation. Since the BPSK signal set is not a square QAM constellation, the PMEPR with the full-layer TAST has to be explicitly evaluated and is equal to 5.1644 dB for each antenna. The PMEPR with the $\mathcal{L}_{4,2,4}$ code is only 2.99 dB. Thus, the smaller PMEPR of the $\mathcal{L}_{4,2,4}$ code makes it a better choice than the full-layer TAST code in this example.

VIII. CONCLUSION

The problem of designing high-rate and maximal diversity space-time codes with low PMEPR was addressed. The principal means of obtaining the LPST codes proposed in this paper is premultiplication and postmultiplication of a high-performance space-time code by suitable unitary matrices of appropriate sizes. Without sacrificing the performance of the original code, the PMEPR was proved to be necessarily reduced in most cases. The proposed spreading schemes were presented for both DAST and TAST codes.

It was shown that the DAST codes that employ the optimal complex rotation obtained from cyclotomic number fields, as in [3], can be spread so that every antenna exhibits a PMEPR equal

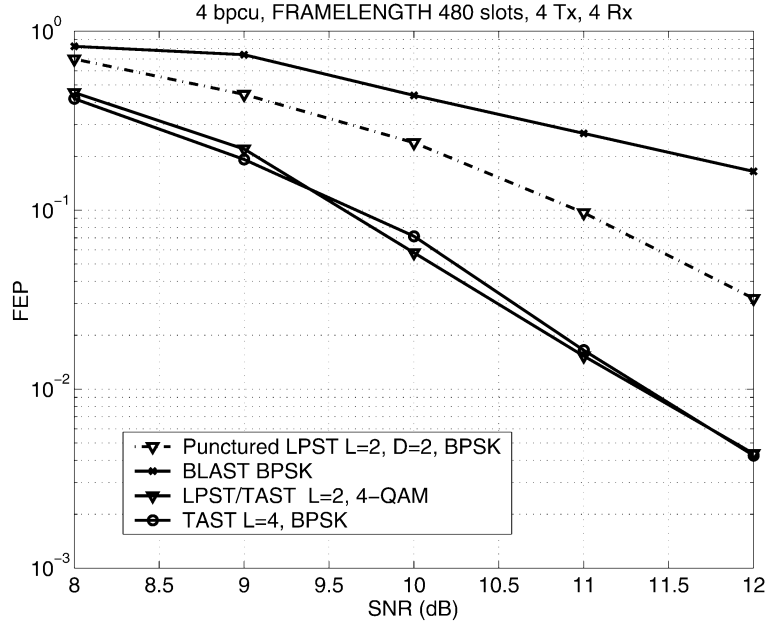


Fig. 7. Performance comparison for $M = N = 4$, $R = 4$ bpcu.

to the PMEPR of the input constellation, namely, a finite subset of either the Gaussian integers or the A_2 lattice. The spreading matrix for DAST can also be applied to the TAST code for the quasi-static channel, wherein the PMEPR becomes smaller than that of the inherent rotation for several possible numbers of layers of the code.

It was noted that the PMEPR of the proposed LPST codes depends on the Diophantine number required in the construction of TAST codes. Nevertheless, there exists a guarantee on the number of layers for which any choice of the Diophantine number will result in a smaller PMEPR of the LPST codes compared to the TAST codes. Hence, an independent search for the Diophantine number that maximizes the coding gain of the TAST code will also lead to an equally good performance of the LPST code and at a smaller PMEPR.

The spreading scheme proposed in this paper is the key to obtaining punctured LPST codes that provide higher rate at the cost of reduced transmit diversity. The polynomial-time sphere decoding algorithm remains applicable even for the decoding of the punctured LPST codes. For high spectral efficiencies, the higher rate of the punctured LPST code leads to a smaller input information constellation compared to the corresponding TAST code, thereby, causing both a reduction in PMEPR and an improvement in performance.

APPENDIX A PROOF OF PROPOSITION 3

When the upper bound on the PMEPR of LPST codes as in Proposition 2 is set to be smaller than the weaker lower bound on the PMEPR of TAST code given in (24), we get

$$L \leq \left\lfloor \frac{1}{2M \sin^2(\frac{\pi}{4M})} \right\rfloor = L_M^{g^1}. \quad (47)$$

Since $\sin(x) < x$, $\forall x > 0$, we have that $L_M^{g^1} \geq \frac{M}{2}$ and thus the number of layers for the guaranteed reduction of PMEPR is

at least $\frac{M}{2}$. For $L > \frac{M}{2}$, $L' = M$ and comparison of the tighter lower bound in (24) with the upper bound on the PMEPR of the LPST code gives

$$L \leq \left\lfloor \frac{1}{\sqrt{2} \sin(\frac{\pi}{4M})} \right\rfloor = L_M^{g^2} \quad (48)$$

for the LPST codes to have a smaller PMEPR than TAST. The ratio of the argument of the floor function in (48) to that in (47) is $\frac{\sin(\frac{\pi}{4M})}{\frac{1}{\sqrt{2}\pi}}$, where

$$\text{sinc}(x) = \frac{\sin(\pi x)}{\pi x}.$$

By the monotonicity of the sinc function in the interval $[0, 1]$, the ratio under consideration is greater than 1 for $M \geq 2$. Therefore, $L_M^{g^2} \geq L_M^{g^1}$ and up to $L_M^{g^2}$ layers lead to smaller PMEPR for the LPST code compared to the TAST code.

APPENDIX B PROOF OF PROPOSITION 5

For $1 \leq L \leq M$, let the function $f(L)$ be given by

$$f(L) = \frac{1}{L} \max_{\substack{z_l \in \mathcal{L}_l \\ 1 \leq l \leq L}} \left| \sum_{l=1}^L \phi_l z_l \right|^2. \quad (49)$$

We must show that $f(L+1) > f(L)$, $1 \leq L \leq M-1$. Fix an L between 1 and $M-1$. From Lemma 1, let the maxima of $f(L)$ be obtained by $(z_1, \dots, z_L) = (\chi_1 z_{\max}, \chi_2 z_{\max}, \dots, \chi_L z_{\max})$, where each $\chi_l \in \{\pm 1, \pm i\}$.

Then, $f(L) = \frac{1}{L} |z_{\max}|^2 |g|^2$, where

$$g \triangleq \sum_{l=1}^L \phi_l \chi_l. \quad (50)$$

Now, a lower bound on $f(L+1)$ will be found and shown to be greater than $f(L)$. Let $\chi_{L+1} \in \{\pm 1, \pm i\}$. Then

$$\begin{aligned} f(L+1) &= \frac{1}{L+1} \max_{\substack{z_l \in \mathcal{L}_l \\ 1 \leq l \leq L+1}} \left| \sum_{l=1}^{L+1} \phi_l z_l \right|^2 \\ &\geq \frac{1}{L+1} \left| \left(\sum_{l=1}^L \phi_l \chi_l z_{\max} \right) + \phi_{L+1} \chi_{L+1} z_{\max} \right|^2 \\ &= \frac{|z_{\max}|^2}{L+1} \left[|g|^2 + 1 + 2\Re(\phi_{L+1}^* g \chi_{L+1}^*) \right]. \end{aligned}$$

The inequality is obtained by substituting the particular values of $(z_1, \dots, z_{L+1}) = (\chi_1 z_{\max}, \dots, \chi_{L+1} z_{\max})$. It is now noted that a certain χ_{L+1} can always be chosen such that the real part of $\phi_{L+1}^* g \chi_{L+1}^*$ is greater than $|g| \cos(\frac{\pi}{4})$. This is because the angle of the nonzero complex number $\phi_{L+1}^* g$ can be changed by $0, \frac{\pi}{2}, \pi$ or $\frac{3\pi}{2}$ by an appropriate choice of χ_{L+1} . Hence, we get that

$$f(L+1) \geq \frac{|z_{\max}|^2}{L+1} \left[|g|^2 + 1 + \sqrt{2}|g| \right]. \quad (51)$$

If we take the difference of the lower bound on $f(L+1)$ in (51) and $f(L)$, we get

$$|z_{\max}|^2 \left(\frac{|g|^2 + 1 + \sqrt{2}|g|}{L+1} - \frac{|g|^2}{L} \right) \quad (52)$$

$$= \frac{|z_{\max}|^2}{L(L+1)} \left[|g|^2 - \sqrt{2}L|g| - L \right]. \quad (53)$$

Application of the triangle inequality in (50) shows that $|g| \leq L$ and, thus, $|g|$ always lies between the roots of quadratic in (53). Hence, the term in (53) is positive and we get that $f(L+1) > f(L)$. Hence, $f(L)$ is an increasing function in L .

REFERENCES

- [1] H. El Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1097–1119, May 2003.
- [2] M. O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice code decoder for space-time codes," *IEEE Commun. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.
- [3] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 938–952, May 1997.
- [4] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communications: Performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744–765, Mar. 1998.
- [5] M. O. Damen, H. El Gamal, and N. C. Beaulieu, "Linear threaded algebraic space-time constellations," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2372–2388, Oct. 2003.
- [6] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 502–518, Mar. 1996.
- [7] J. Boutros and E. Viterbo, "Signal space diversity: A power- and bandwidth-efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1453–1467, Jul. 1998.
- [8] J. Conway and N. J. Sloane, *Sphere Packings, Lattices and Groups*. New York: Springer-Verlag, 1988.
- [9] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1993.
- [10] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1456–1467, Jul. 1999.
- [11] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804–1824, Jul. 2002.
- [12] R. W. Heath Jr and A. J. Paulraj, "Linear dispersion codes for MIMO systems based on frame theory," *IEEE Trans. Signal Process.*, vol. 50, no. 10, pp. 2429–2441, Oct. 2002.
- [13] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 628–636, Mar. 2002.
- [14] Y. Xin, Z. Wang, and G. B. Giannakis, "Space-time diversity systems based on linear constellation precoding," *IEEE Trans. Wireless Commun.*, vol. 2, no. 2, pp. 294–309, Mar. 2003.
- [15] X. Ma and G. B. Giannakis, "Full-diversity full-rate complex-field space-time coding," *IEEE Trans. Signal Process.*, vol. 51, no. 11, pp. 2917–2930, Nov. 2003.
- [16] D. A. Marcus, *Number Fields*. New York: Springer-Verlag, 1977.
- [17] P. Morandi, *Field and Galois Theory*. New York: Springer-Verlag, 1996.
- [18] M. O. Damen and N. C. Beaulieu, "On diagonal algebraic space-time block codes," *IEEE Trans. Commun.*, submitted for publication.
- [19] İ.E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, Nov. 1999.
- [20] M. O. Damen and N. C. Beaulieu, "On diagonal space-time codes using algebraic rotations," in *Proc. Europ. Wireless*, Feb. 2002.
- [21] P. Dayal and M. K. Varanasi, "A fast generalized sphere decoder for optimum decoding of under-determined MIMO systems," in *Proc. Allerton Conf. Communications, Control, and Computing*, Monticello, IL, Oct. 2003, pp. 1216–1225.
- [22] B. Hassibi and H. Vikalo, "On sphere decoding algorithm: Parts I and II," *IEEE Trans. Signal Process.*, to be published.
- [23] M. O. Damen, K. Abed-Meriam, and M. S. Lemdani, "Further results on the sphere decoder," in *Proc. IEEE Int. Symp. Information Theory*, Washington, DC, Jun. 2001, p. 333.
- [24] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, pp. 463–471, Apr. 1985.
- [25] G. J. Foschini, "Layered space-time architecture for wireless communication in fading environments when using multiple antennas," *AT&T Bell Labs Tech. J.*, vol. 1, no. 2, pp. 41–59, Autumn 1996.