Unitary Space-Time Constellation designs from Group Codes

Terasan Niyomsataya[1], Ali Miri[1] and Monica Nevins[2]

School of Information Technology and Engineering[1], Department of Mathematics and Statistics[2]

University of Ottawa, Ottawa, Canada K1N 6N5

tniyomsa,samiri@site.uottawa.ca, mnevins@uottawa.ca

October 27, 2003

Abstract

We propose new unitary space-time constellation designs with high diversity products. Our Hamiltonian and product constellations are based on Slepian's group codes, and can be used for any number of transmitter antennas M and any data rate R. Our Hamiltonian constellations achieve the theoretical upper bound of diversity product in the case where M is even and the cardinality of the signal constellation is less than or equal to 5. Many of our Hamiltonian and product constellations outperform, and have higher diversity products, than the best known designs in the literature. These include orthogonal designs, dicyclic groups, cyclic groups, parametric codes, numerical approaches, nongroup designs, cayley codes, TAST codes and some constellations obtained from fixed-point free groups.

Index terms-wireless communications, multiple-antenna systems, differential unitary space-time modulation, group codes, Hamiltonian constellation, product constellation.

1 Introduction

The use of multiple antenna systems is a technique for increasing the data rate of wireless communications in a fading environment [4, 21]. Space-time coding was developed for use in multiple-antenna wireless communications to achieve high data rate and reliability, using a combination of techniques in error control coding and transmit diversity. The design of a good space-time constellation with high coding gain and simple encoding-decoding algorithm is still an open problem. The construction of full diversity constellations for any number of transmitter antennas and for any data rate poses a particular challenge.

Space-time trellis codes [20] and space-time block codes from orthogonal designs for two transmitter antennas [1] and for any M transmitter antennas [19] were introduced for use in a known channel, when the transmitter/receiver antennas know the fading coefficient of the channel. In practical applications, the fading coefficient of the channel is generally not known to the receiver antenna. In [8, 14], unitary space-time modulation techniques, in which all transmitted signal matrices are unitary, were proposed for use in the case of unknown channels. These techniques can work well for a piecewise-constant fading model. Differential unitary space-time modulation [9, 10] was also proposed for use in unknown continuous fading channels. In [18] and [12], the space-time block codes of [1] and [19], respectively, are modified for differential transmission.

Let $\mathcal{V} = \{V_l\}_{l=0}^{L-1}$ be a signal constellation, where $|\mathcal{V}| = L$ and V_l is an $M \times M$ unitary matrix. The data rate is $R = \log_2 L/M$. The design problem of differential unitary space-time constellations is to maximize the diversity product, $\zeta_{\mathcal{V}}$, which is computed from a constellation $\mathcal{V}$ as

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{0 \le l < l' \le L-1} |\det(V_l - V_{l'})|^{\frac{1}{M}} \tag{1}$$

Our goal in this paper is to find a set $\mathcal{V}$ of $M \times M$ unitary matrices which has $\zeta_{\mathcal{V}}$ as large as possible. The problem of constructing a full diversity constellation with high diversity product has been studied in many prior works. For example, some of the group structures proposed to represent constellations are cyclic and dicyclic groups [9, 10, 11], fixed-point free groups [16] and the compact symplectic group $Sp(2)$ [23]. Some examples of nongroup constellations include products of fixed-point free groups [16], parametric codes [13] and numerical methods [6]. Many of these designs still have some limitations in performance, the number of transmitters used, and the data rate achieved.

In this paper, we propose new unitary space-time constellation designs: Hamiltonian and product constellations. These constellations can be used for any number of transmitter antennas and for any data rate. Furthermore, they achieve full diversity and can be used for both known and unknown channels with differential unitary space-time modulation. We begin with a 2×2 unitary constellation which is constructed from 2×2 Hamiltonian matrices. The diversity product of a 2×2 Hamiltonian constellation equals one half of the Euclidean distance between two points in $\mathbb{C}^2$. By considering the transformation from $\mathbb{R}^4$ to $\mathbb{C}^2$, the idea of group codes [17] is used to construct constellations for any cardinality L. We propose a new matrix form of a 2×2 Hamiltonian constellation which is built by an $(L, 4)$ cyclic group code [2]. $M \times M$ Hamiltonian constellations for any M transmitter antennas can then be constructed by using a direct sum of 2×2 Hamiltonian matrices for M even, and a direct sum of 2×2 Hamiltonian matrices with the L^{th} roots of unity for M odd. A product method is also proposed to increase the data rate and improve the diversity product. Although our Hamiltonian and product constellations do not form a group, we show that the optimization will not be computationally intensive for large L. It only requires checking $L - 1$ distinct matrices, making it comparable to those that use group constellations. This paper is organized as follows: Section 1 briefly gives some background in multiple-antenna systems for both known and unknown channel. Also the design criteria of unitary space-time constellations and a summary of prior works of high diversity product designs are reviewed in this section. Section 2 presents a 2×2 Hamiltonian matrix to be a full diverse constellation. Section 3 explains the idea of cyclic group codes. Section 4 and 5 propose the designs of constructing Hamiltonian and product constellations respectively. Section 6 gives the results of our constellations and also compare the performance of them with different designs. Section 7 is the conclusion of the work of this paper.

1.1 Multiple antenna systems

In this section, we review some background of multiple antenna systems in wireless communications [8, 9, 10, 20].

Consider multiple antennas in a Rayleigh flat-fading channel with M transmitter antennas and N receiver antennas. At time t, a fading coefficient from transmitter antenna m to receiver antenna n, h_{tmn}, and an additive noise on receiver antenna n, ω_{tn}, are independent complex Gaussian variables with zero mean and variance one, $\mathcal{CN}(0, 1)$. Let a transmitted signal at time t on transmitter antenna m be s_{tm}, $m = 1, 2, \ldots, M$. The received signal at time t on receiver antenna n is then equal to

$$x_{tn} = \sqrt{\rho} \sum_{m=1}^{M} h_{tmn} s_{tm} + \omega_{tn}, \quad t = 0, 1, \ldots \text{ and } n = 1, \ldots, N \tag{2}$$

where ρ is the signal-to-noise ratio, SNR, at each receiver antenna. At each time t, the expected value of the sum of all transmitted signal powers equals to one, that is, $\mathbf{E} \sum_{m=1}^{M} |s_{tm}|^2 = 1$. Generally the transmitted signals can be transmitted in a block of period T. Therefore from (2) a received signal

X_τ can be written in matrix form as

$$X_\tau = \sqrt{\rho} S_\tau H_\tau + W_\tau, \qquad \tau = 0, 1, \ldots \tag{3}$$

where τ is an index of a block. The size of the received signal matrix X_τ and a transmitted signal matrix S_τ are $T \times N$ and $T \times M$ respectively. W_τ is the $T \times N$ additive noise matrix. H_τ is called the $M \times N$ *channel matrix*, and we assume that h_{tmn} is constant within the block.

1.1.1 Known channels

If a receiver antenna knows the channel matrix, H_τ, the channel is called *the perfect channel state information, Perfect CSI*. Let L be the size of the alphabet. The data rate R, in bits/channel use, is computed by $R = \log_2 L/M$. A message is sent as a sequence $z_0, z_1, z_2 \ldots$ with $z_\tau \in \{0, 1, \ldots L-1\}$. The transmitted signal S_τ is chosen from a transmitted signal constellation $\mathcal{V} = \{V_l\}_{l=0}^{L-1}$ by index z_τ. Equivalently

$$S_\tau = V_{z_\tau} \tag{4}$$

where each V_l is a $T \times M$ unitary matrix which satisfies $V_l V_l^* = I_T$, where $()^*$ denotes conjugate transpose. The received signal is defined by (3). Using the maximum likelihood decoder, the receiver antenna will decode to a message $\hat{z}_\tau$ as

$$\hat{z}_\tau = \arg \min_{l=0,\ldots,L-1} \|X_\tau - V_l H_\tau\| \tag{5}$$

where $\|A\|^2 = \mathrm{Tr}(AA^*) = \mathrm{Tr}(A^*A) = \sum_{i,j} |a_{ij}|^2$.

Suppose the time period in one block equals the number of transmitter antennas, that is, $T = M$. Then the size of the signal V_l is $M \times M$. Using the Chernoff bound, the pairwise error probability that the receiver antenna decodes an error from V_l to $V_{l'}$ can be computed [8] by

$$P_e \leq \frac{1}{2} \prod_{m=1}^{M} [1 + \frac{\rho}{4} \sigma_m^2 (V_l - V_{l'})]^{-N} \tag{6}$$

where $\sigma_m(V_l - V_{l'})$ is the m^{th} singular value of the matrix $V_l - V_{l'}$. We know that the product of the squares of the singular values equals the norm squared of the determinant. Therefore, at high ρ the pairwise error probability P_e can be approximated by

$$P_e \leq \frac{1}{2} (\frac{4}{\rho})^{MN} \frac{1}{|\det(V_l - V_{l'})|^{2N}}. \tag{7}$$

1.1.2 Unknown channels

The channel is called *no CSI* when the receiver antenna does not know H_τ. Hughes [10] and Hochwald *et. al.* [9] proposed *differential unitary space-time modulation* for multiple antennas with no knowledge of channel information. The idea of differential space-time modulation is similar to that of differential phase shift keying modulation, *DPSK*, for noncoherent modulation in single antenna communications. The current transmitted signal S_τ is obtained by multiplication of the previous signal $S_{\tau-1}$ with its signal constellation index V_{z_τ}. Equivalently,

$$S_\tau = V_{z_\tau} S_{\tau-1} \tag{8}$$

with $S_0 = I_M$. In the case of unknown channels, we have to modify the received signal equation in (3), since H_τ is unknown. From [9, 10] we assume that H_τ is constant over two consecutive time periods, $H_\tau \approx H_{\tau-1} = H$. From (3), we will have

$$\begin{aligned} X_{\tau-1} &= \sqrt{\rho} S_{\tau-1} H + W_{\tau-1} && (9) \\ X_\tau &= \sqrt{\rho} S_\tau H + W_\tau && (10) \end{aligned}$$

Substituting $S_{\tau-1} = S_\tau / V_{z_\tau}$ in (9), and then adding the resulting equation to (10), gives

$$X_\tau = V_{z_\tau} X_{\tau-1} + W_\tau - V_{z_\tau} W_{\tau-1}. \tag{11}$$

Since additive noise is independent and invariant under multiplication with a unitary matrix, the received signal matrix X_τ for unknown channel is

$$X_\tau = V_{z_\tau} X_{\tau-1} + \sqrt{2} W'_\tau \tag{12}$$

where W'_τ is also $\mathcal{CN}(0,1)$. A Maximum Likelihood decoder is also used for the receiver antenna to decode a message $\hat{z}_\tau$ to be

$$\hat{z}_\tau = \arg \min_{l=0,\ldots,L-1} \|X_\tau - V_l X_{\tau-1}\| \tag{13}$$

Now suppose $T = M$. The pairwise probability that a receiver antenna decodes an error from V_l to $V_{l'}$ can be computed, using Chernoff bound, as

$$P_e \le \frac{1}{2} \prod_{m=1}^{M} [1 + \frac{\rho^2}{4(1+2\rho)} \sigma_m^2 (V_l - V_{l'})]^{-N}. \tag{14}$$

At high ρ, P_e can be also estimated by

$$P_e \le \frac{1}{2} (\frac{8}{\rho})^{MN} \frac{1}{|\det(V_l - V_{l'})|^{2N}}. \tag{15}$$

Clearly from (7) and (15), at high ρ, the unknown channel has twice the error probability, P_e, of the known channel. This implies a 3 dB penalty for differential space-time modulation for unknown channels.

1.2 Design criteria for unitary space-time constellations

Let $\mathcal{V} = \{V_l\}_{l=0}^{L-1}$ be a signal constellation, where $|\mathcal{V}| = L$, and V_l is an $M \times M$ unitary matrix. We define the *diversity product*, $\zeta_{\mathcal{V}}$, which is computed from a constellation $\mathcal{V}$ by

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{0 \leq l < l' \leq L-1} |\det(V_l - V_{l'})|^{\frac{1}{M}} \tag{16}$$

where M is the number of transmitter antennas. The term exponent $\frac{1}{M}$ represents a geometric mean of M eigenvalues, and $0 \leq \zeta_{\mathcal{V}} \leq 1$. A constellation $\mathcal{V}$ which has $\zeta_{\mathcal{V}} > 0$ is said to have *full diversity.* Clearly we need to minimize P_e in (16). Therefore a design criteria for our full diversity constellation $\mathcal{V}$ is to find a set $\mathcal{V}$ of $M \times M$ unitary matrices which has $\zeta_{\mathcal{V}}$ as large as possible.

1.3 Summary of prior works

The problem of constructing a full diversity constellation $\mathcal{V}$ with high $\zeta_{\mathcal{V}}$ has been studied in many prior works. We give a brief overview of them in this section. These constellations will be compared later to our constellation in Sections 6.

1.3.1 Orthogonal designs

A 2×2 orthogonal constellation for two transmitter antennas was first introduced by Alamouti [1]. A 2×2 signal matrix has the form

$$V_l = \frac{1}{\sqrt{2}} \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix} \tag{17}$$

where $|x|^2 = |y|^2 = 1$ is the constraint that makes this matrix unitary and can be used for differential detection in unknown channel [18]. x, y are chosen from the Q^{th} roots of unity: $x, y \in \{1, e^{2\pi j/Q}, e^{2\pi j 2/Q}, \ldots, e^{2\pi j(Q-1)/Q}\}$. The order of the constellation is given by $L = Q^2$. The diversity product can be computed as

$$\zeta_{\mathcal{V}} = \frac{\sin(\pi/Q)}{\sqrt{2}} \tag{18}$$

A differential detection of orthogonal designs [19] for multiple transmitter antennas was proposed later in [12].

1.3.2 Dicyclic and cyclic group designs

Hughes [10, 11] and Hochwald *et.al* [9] used dicyclic and cyclic group structures to represent their constellations. For $M = 2$, the dicyclic group constellation, a quaternion group Q_p is

$$Q_p = \left\langle \begin{bmatrix} e^{j2\pi/2^p} & 0 \\ 0 & e^{-j2\pi/2^p} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle. \tag{19}$$

The order of dicyclic constellation is $L = 2^{p+1}$. On the other hand, an $M \times M$ cyclic group constellation has the form $\mathcal{V} = \{V_l\}_{l=0}^{L-1}$ where

$$V_l = \mathrm{diag}(e^{j2\pi u_1 l/L}, e^{j2\pi u_2 l/L}, \ldots, e^{j2\pi u_M l/L}), \tag{20}$$

and $u_i \in \{0, 1, \ldots, L-1\}$. The diversity product is given by

$$\zeta_{\mathcal{V}} = \min_{l=1,2,\ldots,L-1} \left| \prod_{m=1}^{M} \sin \frac{\pi u_i l}{L} \right|^{\frac{1}{M}} \tag{21}$$

1.3.3 Fixed-point free group designs

Hassibi *et.al.* [16] have classified all six classes of fixed-point free groups: $G_{m,r}$, $D_{m,r,l}$, $E_{m,r}$, $F_{m,r,l}$, $J_{m,r}$ and $K_{m,r,l}$ which are induced from a cyclic group. Some of these constellations have excellent diversity product, and their diversity product are higher than constellations from [1, 9, 10, 11, 18]. But there are still some limitations in these designs. First the possible constellations are limited when M is large and odd. Second there exist only even order for 2×2 constellations.

1.3.4 Nongroup designs

There are three nongroup constellation designs for any order L and M transmitter antennas also proposed in [16]: a 2×2 Hamiltonian matrix for only $M = 2$, a nongroup $S_{m,r}$ which is a generalization of a fixed-point free group $G_{m,r}$ and a matrix product of two different representations of fixed-point free groups. It is shown that some constellations from $S_{m,r}$ and product nongroups have diversity product higher than group constellation designs.

1.3.5 Symplectic group designs

Subsets of the infinite symplectic group $Sp(2)$ are used to construct full diversity constellations for $M = 4$ transmitter antennas in [23]. $Sp(2)$ is not a fixed-point free group. The constellations produced are finite subsets of $Sp(2)$ with diversity product not equal to zero. Although $Sp(2)$ underperforms fixed-point free group designs, its significance is in its simple decoding algorithm.

1.3.6 Parametric code designs

A parametric code design [13] was proposed for only $M = 2$ transmitter antennas. A parametric code matrix is defined as a product of three 2×2 unitary matrices as:

$$V_l = \begin{bmatrix} e^{j\theta_L} & 0 \\ 0 & e^{jk_1\theta_L} \end{bmatrix}^l \begin{bmatrix} \cos(k_2\theta_L) & \sin(k_2\theta_L) \\ -\sin(k_2\theta_L) & \cos(k_2\theta_L) \end{bmatrix}^l \begin{bmatrix} e^{jk_3\theta_L} & 0 \\ 0 & e^{-jk_3\theta_L} \end{bmatrix}^l \tag{22}$$

where $\theta_L = 2\pi/L$ and $k_1, k_2, k_3 \in \{0, 1, \ldots, L-1\}$. The value of $k = (k_1, k_2, k_3)$ is found by exhaustive search to maximize $\zeta_{\mathcal{V}}$. This search is computationally intensive when L is large as it needs to consider $L(L-1)/2$ distinct values of $V_l, V_{l'}$ in (16).

1.3.7 Numerical methods

In [6], a numerical approach is used to construct large diversity product constellations for any dimension M and order L. A simulated annealing and a genetic algorithm are used to search optimized constellations from the algebraic structures: $A^kB^l, AB, A^kB^k, A^kB^lC^m, ABC$ and $A^kB^kC^k$ where A, B, C are $M \times M$ unitary matrices and k, l, m are arbitrary numbers for a given L.

2 Hamiltonian constellation designs

A 2×2 Hamiltonian matrix can be used to design a full diversity constellation for $M = 2$ transmitter antennas. This matrix is defined by

$$H = \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix} \tag{23}$$

where $x, y \in \mathbb{C}$ and $|x|^2 + |y|^2 = 1$. This differs from orthogonal design [1, 18] which requires $|x|^2 = |y|^2 = 1$. Here H is unitary. Let $\mathcal{H} = \{H_l\}_{l=0}^{L-1}$ be a Hamiltonian constellation. From (16), a diversity product $\zeta_{\mathcal{H}}$ can be computed as

$$\begin{aligned} \zeta_{\mathcal{H}} &= \frac{1}{2}|\det(H - H')|^{\frac{1}{2}} \\ &= \frac{1}{2}\det \begin{bmatrix} x - x' & -(y - y')^* \\ y - y' & (x - x')^* \end{bmatrix}^{\frac{1}{2}} \\ &= \frac{1}{2}\sqrt{|x - x'|^2 + |y - y'|^2} \end{aligned} \tag{24}$$

From (24), we can easily see that now $\zeta_{\mathcal{H}}$ equals one half of the Euclidean distance between two points (x, y) and (x', y') in $\mathbb{C}^2$. Consider a transformation from $\mathbb{R}^4$ to $\mathbb{C}^2$. If $A(a_1, a_2, a_3, a_4)$ is a point on the unit sphere in $\mathbb{R}^4$ where $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1$, then we can convert this point onto the unit sphere in $\mathbb{C}^2$ space using the mapping:

$$A(a_1, a_2, a_3, a_4)_{\mathbb{R}^4} \longmapsto A(a_1 + ja_2, a_3 + ja_4)_{\mathbb{C}^2} = A(x, y)_{\mathbb{C}^2} \tag{25}$$

where $x = a_1 + ja_2, y = a_3 + ja_4$, $j^2 = -1$ and $a_1, a_2, a_3, a_4 \in \mathbb{R}$. Consequently now the problem of constructing a 2×2 Hamiltonian constellation can be reduced to finding L points on a unit sphere in $\mathbb{R}^4$ space such that the minimum distance between two points as large as possible. A possible solution to this problem is to use *Slepian's group codes* [17] to get these maximum equidistant L points on a unit sphere in $\mathbb{R}^4$ when in the group codes these points are considered as a set of L codewords in four-dimensional space, that is, $(L, 4)$ group codes. For simplicity, we choose a cyclic group of order L to generate codewords.

3 Group codes

We review the idea of a cyclic group code as given in [2] in this section.

3.1 Definitions

An (L,n) *group code* is a set of L codewords in the Euclidean space of dimension n. Basically we can think that all L codewords are on the surface of a unit sphere in n dimensional space. Let $\{O_l\}_{l=0}^{L-1}$ be a group of $n \times n$ orthogonal matrices. Then the codewords $\{X_l\}_{l=0}^{L-1}$ can be generated by

$$X_l = O_l X \tag{26}$$

where X is called *an initial vector*. We assume all X_l are equiprobable. The distance from any codeword X_l to all nearest neighbors is thus the same as from codeword X_k to all nearest neighbors for all $l, k = 0, 1, \ldots, L-1$, or equivalently, all codewords have the same error probability. The distance, d, between an initial vector X and codeword X_l is computed using

$$d^2(X, X_l) = \|X - X_l\|^2 = 2 - 2X \cdot O_l X \tag{27}$$

The main problem of group codes is how to choose the best initial vector X in (26) to minimize the error probability, or to maximize the minimum distance of nearest codewords of (27). This is extremely difficult and a solution for the general case has not yet been found, except for special cases such as for a full homogeneous representation and the $(n-1)$-dimensional representation of the symmetric group S_n [3], for a cyclic group [2], and for a finite reflection group [15].

3.2 Cyclic group codes

The 4×4 orthogonal matrix, O_l, of an $(L, 4)$ cyclic group code [2] has the form:

$$O_l = \mathrm{diag}(A(lk_1), A(lk_2)) \tag{28}$$

where $A(k_i)$ is defined by

$$A(k_i) = \begin{bmatrix} \cos\frac{2\pi}{L}k_i & \sin\frac{2\pi}{L}k_i \\ -\sin\frac{2\pi}{L}k_i & \cos\frac{2\pi}{L}k_i \end{bmatrix} \tag{29}$$

$k_i \in \{1, 2, \ldots, L-1\}$. Let $X = (x_1, x_2, x_3, x_4)$ be an initial vector. From (27), we can compute the Euclidean distance between X and $O_l X$ by

$$d_l^2 = \|X - O_l X\|^2 = 4\sum_{i=1}^{2} \mu_i \sin^2 \frac{\pi}{L} l k_i \tag{30}$$

where $\mu_1 = x_1^2 + x_2^2$ and $\mu_2 = x_3^2 + x_4^2$.

4 Hamiltonian constellations

4.1 The case $M = 2$

From (30), we observe that the distance between X and X_l depends on the sum of squares of pair of entries. Let $X = (\sqrt{x_1}, 0, \sqrt{x_2}, 0)$ be an initial vector with

$$x_1 + x_2 = 1 \quad \text{and} \quad x_1, x_2 \geq 0. \tag{31}$$

Generate the $(L, 4)$ cyclic codewords by $\{X_l\}_{l=0}^{L-1} = O_l X$, where O_l is defined in (28). This gives

$$X_l = \left(\sqrt{x_1}\cos\frac{l2\pi k_1}{L}, -\sqrt{x_1}\sin\frac{l2\pi k_1}{L}, \sqrt{x_2}\cos\frac{l2\pi k_2}{L}, -\sqrt{x_2}\sin\frac{l2\pi k_2}{L}\right). \tag{32}$$

Transforming these codewords to the new codewords in $\mathbb{C}^2$, $X_{l\mathbb{C}^2}$, by (25) gives

$$X_{l\mathbb{C}^2} = \begin{bmatrix} \sqrt{x_1}(\cos\frac{l2\pi k_1}{L} - j\sin\frac{l2\pi k_1}{L}) \\ \sqrt{x_2}(\cos\frac{l2\pi k_2}{L} - j\sin\frac{l2\pi k_2}{L}) \end{bmatrix} = \begin{bmatrix} \sqrt{x_1}e^{-j\frac{l2\pi k_1}{L}} \\ \sqrt{x_2}e^{-j\frac{l2\pi k_2}{L}} \end{bmatrix}. \tag{33}$$

Substitute in the form of a Hamiltonian matrix in (23) to get a 2×2 Hamiltonian constellation $\mathcal{H}_{2\times 2} = \{H_l\}_{l=0}^{L-1}$ with

$$H_l = \begin{bmatrix} \sqrt{x_1}e^{-j\frac{l2\pi k_1}{L}} & -\sqrt{x_2}e^{j\frac{l2\pi k_2}{L}} \\ \sqrt{x_2}e^{-j\frac{l2\pi k_2}{L}} & \sqrt{x_1}e^{j\frac{l2\pi k_1}{L}} \end{bmatrix} \tag{34}$$

We can also write H_l in terms of $H_{l=0} = H_0$ as

$$H_l = e^{j\frac{2\pi l k_1}{L}} R_l H_0 T_l \tag{35}$$

where

$$R_l = \begin{bmatrix} e^{-j\frac{2\pi l k_1}{L}} & 0 \\ 0 & e^{-j\frac{2\pi l k_2}{L}} \end{bmatrix}, \; H_0 = \begin{bmatrix} \sqrt{x_1} & -\sqrt{x_2} \\ \sqrt{x_2} & \sqrt{x_1} \end{bmatrix} \text{ and } T_l = \begin{bmatrix} e^{-j\frac{2\pi l k_1}{L}} & 0 \\ 0 & e^{j\frac{2\pi l k_2}{L}} \end{bmatrix}$$

Both $\{R_l\}_{l=0}^{L-1}$ and $\{T_l\}_{l=0}^{L-1}$ form cyclic groups of order L. The diversity product of a 2×2 Hamiltonian constellation is computed by

$$\zeta_{\mathcal{H}} = \frac{1}{2}\min_{0\leq l<l'\leq L-1} |\det(H_l - H_{l'})|^{\frac{1}{2}}. \tag{36}$$

Even though the H_l do not form a group, we may compute $\zeta_{\mathcal{H}}$ just by taking $H_{l=0}$ and $H_{l'=l}$ (see Appendix A). Then

$$\begin{aligned}\zeta_{\mathcal{H}} &= \frac{1}{2}\min_{l=1,2,\ldots,L-1} |\det(H_0 - H_l)|^{\frac{1}{2}} \\ &= \frac{1}{2}\min_{l=1,2,\ldots,L-1} \left\{4\left(x_1 \sin^2\frac{\pi k_1 l}{L} + x_2 \sin^2\frac{\pi k_2 l}{L}\right)\right\}^{\frac{1}{2}} \end{aligned} \tag{37}$$

The values of $x = (x_1, x_2)$ of (31) and $k = (k_1, k_2)$ are chosen to maximize $\zeta_{\mathcal{H}}$ of (37).

4.2 The case M even, $M > 2$

An $M \times M$ constellation for a case where M is even can be constructed by the direct sum of 2×2 Hamiltonian matrices. $\mathcal{H}_{M\times M} = \{J_l\}_{l=0}^{L-1}$, has the block diagonal form

$$J_l = \mathrm{diag}(H_l^{1,2}, H_l^{3,4}, \ldots, H_l^{M-1,M}) \tag{38}$$

where $H_l^{m,n}$ is defined as

$$H_l^{m,n} = \begin{bmatrix} \sqrt{x_1}e^{-j\frac{l2\pi k_m}{L}} & -\sqrt{x_2}e^{j\frac{l2\pi k_n}{L}} \\ \sqrt{x_2}e^{-j\frac{l2\pi k_n}{L}} & \sqrt{x_1}e^{j\frac{l2\pi k_m}{L}} \end{bmatrix} \tag{39}$$

Using the similar derivation as above, the diversity product can be computed by

$$\zeta_{\mathcal{H}} = \frac{1}{2}\min_{l=1,2,\ldots,L-1} \left| 2^M \prod_{j=1}^{M/2} \sum_{i=1}^{2} x_i \sin^2\frac{\pi k_{2j-2+i} l}{L} \right|^{\frac{1}{M}}. \tag{40}$$

Again, the values of $x = (x_1, x_2)$ of (31) and $k = (k_1, k_2, \ldots, k_M)$ are chosen to maximize $\zeta_{\mathcal{H}}$ of (40).

4.3 The case M odd, $M \geq 3$

For a case where M is odd, an $M \times M$ constellation is constructed by using the direct sum of 2×2 Hamiltonian matrices and the L^{th} roots of unity. Thus a block diagonal matrix of $\mathcal{H}_{M\times M} = \{J_l\}_{l=0}^{L-1}$ is

$$J_l = \mathrm{diag}(e^{j2\pi k_1 l}, H_l^{2,3}, \ldots, H_l^{M-1,M}). \tag{41}$$

Using a derivation similar to the above, the diversity product can be given by

$$\zeta_{\mathcal{H}} = \frac{1}{2}\min_{l=1,2,\ldots,L-1}\left|2^M \sin\frac{\pi k_1 l}{L}\prod_{j=2}^{(M+1)/2}\sum_{i=1}^{2} x_i \sin^2\frac{\pi k_{2j-3+i} l}{L}\right|^{\frac{1}{M}} \tag{42}$$

The values of $x = (x_1, x_2)$ of (31) and $k = (k_1, k_2, \ldots, k_M)$ are found such that they maximize $\zeta_{\mathcal{H}}$ of (42).

5 Product constellations

The representation of degree M of a cyclic group of order L_C, $\mathcal{C} = \{O_k\}_{k=0}^{L_C-1}$, has the diagonal form

$$O_k = \mathrm{diag}(e^{j2\pi r_1 k/L_C}, e^{j2\pi r_2 k/L_C} \ldots, e^{j2\pi r_M k/L_C}) \tag{43}$$

We use the product of $\mathcal{H}_{M\times M} = \{J_l\}_{l=0}^{L_H-1}$ in (38) and (41) and a cyclic group $\mathcal{C}$ in (43) to get a product constellation $\mathcal{P}$ for M even and odd respectively, as follows:

$$\mathcal{P} = \mathcal{H} \times \mathcal{C} = \{J_l O_k\}_{l,k=0}^{L_H-1, L_C-1} \tag{44}$$

A product constellation $\mathcal{P}$ is unitary, and $|\mathcal{P}|$ can be at most $L_H L_C$. From (16), a diversity product of $\mathcal{P}$ can be computed by

$$\begin{aligned} \zeta_{\mathcal{P}} &= \frac{1}{2}\min_{P,P'\in\mathcal{P}} |\det(P-P')|^{\frac{1}{M}} & (45)\\ &= \frac{1}{2}\min_{\substack{0\le l,l'\le L_H-1\\ 0\le k,k'\le L_C-1\\ (l,k)\neq(l',k')}} |\det(J_l O_k - J_{l'} O_{k'})|^{\frac{1}{M}} & (46)\end{aligned}$$

It is a straightforward calculation (see the proof in Appendix B) to check that

$$|\det(J_l O_k - J_{l'} O_{k'})| = |\det(J_0 - J_{l'-l} O_{k'-k})|. \tag{47}$$

Hence to compute a diversity product it suffices to consider the case of $l = k = 0$ and l', k' are arbitrary. This will give us

$$\zeta_{\mathcal{P}} = \frac{1}{2}\min_{(l,k)\neq(0,0)} |\det(J_0 - J_l O_k)|^{\frac{1}{M}} \tag{48}$$

Thus although the product constellation $\mathcal{P}$ does not form a group, our search will require checking only of $L_H L_C - 1$ distinct values of P, P'.

Then we search for the value of $x = (x_1, x_2)$ of (31), $k = (k_1, k_2, \ldots, k_M)$ and $r = (r_1, r_2, \ldots, r_M)$ which maximizes $\zeta_{\mathcal{P}}$ in (48). A necessary condition for full diversity, $\zeta_{\mathcal{P}} > 0$, is that $\gcd(r_i, L_C) = 1$ for all i. Hence we may restrict our search to choices of r such that $r_1 = 1$ and $\gcd(r_i, L_C) = 1,\ i = 2, \ldots, M$.

Theorem 1 *A product constellation $\mathcal{P}$ will reduce to the form of Hamiltonian constellation of (38) and (41) if $r_{2i-1}+r_{2i} = L_C$ for all $i = 1, \ldots, M/2$ for M even and $r_{2i}+r_{2i+1} = L_C$ for all $i = 1, \ldots, M-1/2$ for M odd.*

Proof: The proof is shown for $\mathcal{P}_{2\times 2}$ case, where the proof for $\mathcal{P}_{M\times M}$ follows immediately. From (44), we have

$$\{J_l O_k\} = \begin{bmatrix} \sqrt{x_1} e^{-j\frac{2\pi k_1 l}{L_H}} e^{j\frac{2\pi k r_1}{L_C}} & -\sqrt{x_2} e^{j\frac{2\pi k_2 l}{L_H}} e^{j\frac{2\pi k r_2}{L_C}} \\ \sqrt{x_2} e^{-j\frac{2\pi k_2 l}{L_H}} e^{j\frac{2\pi k r_1}{L_C}} & \sqrt{x_1} e^{j\frac{2\pi k_1 l}{L_H}} e^{j\frac{2\pi k r_2}{L_C}} \end{bmatrix} \tag{49}$$

We can see that $J_l O_k$ will reduce to the form of a 2×2 J_l for all $k = 0, 1, \ldots, L_C - 1$ if $e^{j\frac{2\pi k r_1}{L_C}} = e^{-j\frac{2\pi k r_2}{L_C}}$, or equivalently $e^{j\frac{2\pi k}{L_C}(r_1+r_2)} = 1$. This gives L_c divides $r_1 + r_2$. The values of r_1 and r_2 are chosen from $\{0, 1, \ldots, L_C - 1\}$ thus the only one possible condition which satisfies L_c divides $r_1 + r_2$ is $r_1 + r_2 = L_C$.
$\square$

To get a product constellation $\mathcal{P}$ of (44) which has a diversity product higher than a Hamiltonian constellation $\mathcal{H}$, we thus omit those choices of r in Theorem 1.

Theorem 2 *For M odd, if $\gcd(L_H, L_C) > 1$ then the product constellation $\mathcal{P}$ of (44) will have $\zeta_{\mathcal{P}} = 0$. If $\gcd(L_H, L_C) = 1$, then there exist values of $k = (k_1, k_2, \ldots, k_M)$ and $r = (r_1, r_2, \ldots, r_M)$ such that $\zeta_{\mathcal{P}} > 0$, with k_1 relatively prime to L_H, and each $r_i, i = 1, 2, \ldots, M$ relatively prime to L_C.*

Proof: In (48), $\zeta_{\mathcal{P}}$ will equal 0 if $e^{j2\pi(\frac{k_1 l}{L_H} + \frac{r_1 k}{L_C})} = 1$. The first part of Theorem 2 can be proved by showing that if $\gcd(L_H, L_C) > 1$, then for any choice of k_1, r_1 there exist choices of k, l, not both zero, such that $\frac{k_1 l}{L_H} - \frac{r_1 k}{L_C}$ is an integer. There are two cases that need to be considered.

Case 1: If $\gcd(k_1, L_H) = t > 1$*, then take* $l = L_H/t$*, so that* $k_1 l = k_1 L_H/t = \text{lcm}(k_1, L_H)$*, which is an integer; and* $k = 0$*. Since* $t > 1$*,* $l \neq 0$*, and* $l < L_H$*. The case of* $\gcd(r_1, L_C) > 1$ *can be treated similarly.*

Case 2: If $\gcd(k_1, L_H) = 1$ *and* $\gcd(r_1, L_C) = 1$*, then set* $g = \gcd(L_H, L_C)$*. Then* L_H/g *and* L_C/g *are integers strictly less than* L_H *and* L_C*, respectively. Moreover, we compute*

$$\frac{L_H/g}{L_H} - \frac{L_C/g}{L_C} = \frac{1}{g} - \frac{1}{g} = 0.$$

We require the following lemma.

Lemma 1 *If* $\gcd(a, A) = 1$*, then the set* $S = \{al \mod A \mid l = 0, 1, \ldots A-1\}$ *has* A *distinct values.*

Proof of lemma: If not, then some al *must equal another* al' *modulo* A*; say* $l' < l$*. This would mean* $a(l - l') = 0 \mod A$*. Both sides are integers, so this means* A *divides* $a(l - l')$*. But this is impossible unless* $l = l'$*: since* $\gcd(a, A) = 1$*, no part of* A *can divide* a*, and since* $l - l' < A$*,* A *cannot divide* $l - l'$ *unless* $l - l' = 0$*. Thus all values are distinct, and give representatives of all residue classes. (In particular, the value* $l = 0$ *gives the zero residue class.)* $\square$

Using the Lemma, we may choose l *so that* $k_1 l \equiv L_H/g \mod L_H$ *and also choose* k *so that* $r_1 k \equiv L_C/g \mod L_C$*, proving the first part of the theorem.*

Now to prove the second part of the theorem, suppose that $\gcd(L_H, L_C) = 1$*. If* $\gcd(k_1, L_H) > 1$ *or* $\gcd(r_1, L_C) > 1$*, then a similar argument as the one made in Case 1 above shows that the diversity product will be zero. So suppose we choose* $\gcd(k_1, L_H) = 1$ *and* $\gcd(r_1, L_C) = 1$*. In this case, the lemma shows that* $e^{j2\pi(\frac{k_1 l}{L_H} + \frac{r_1 k}{L_C})} = 1$ *if and only if for some choice of* $a = 0, 1, \ldots L_H - 1$ *and* $b = 0, 1, \ldots L_C - 1$*, we have*

$$\frac{a}{L_H} - \frac{b}{L_C} = 0.$$

This is equivalent to saying that $aL_C = bL_H$ *for some* a, b*. But this product is strictly less that* $L_H L_C$*, which is the least common multiple of* L_H *and* L_C*, by the hypothesis that* $\gcd(L_H, L_C) = 1$*. Hence it must be zero, and thus* $a = 0$ *and* $b = 0$*. Consequently, the only values of* k *and* l *giving* $e^{j2\pi(\frac{k_1 l}{L_H} + \frac{r_1 k}{L_C})} = 1$ *in the original product are* $k = 0, l = 0$*. That the remaining* 2×2 *blocks will not produce a zero diversity product for all choices in the given set follows from (24) and the remarks preceding Theorem 1.* $\square$

Due to a limitation of possible product constellations for a case where M is odd (see Theorem 2), we propose another unitary product constellation, $\mathcal{P}_{\mathcal{H}}$, which is obtained by a product of two Hamiltonian constellations with the diagonal blocks in different order.

$$\mathcal{P}_{\mathcal{H}} = \mathcal{H}_1 \times \mathcal{H}_2^{\dagger} = \{J_l J_k^{\dagger}\}_{l,k=0}^{L_{H_1}-1, L_{H_2}-1} \tag{50}$$

where L_{H_1}, L_{H_2} are the order of $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, and $J_k^{\dagger}$ denotes a block diagonal matrix with different order of J_k in (41):

$$J_k^{\dagger} = \mathrm{diag}(H_k^{1,2}, H_k^{3,4}, \ldots, H_k^{M-2,M-1}, e^{j2\pi r_M k/L_{H_2}}), \tag{51}$$

To optimize a diversity product of (45) which $P_H, P_H' \in \mathcal{P}_{\mathcal{H}}$, it also suffices to consider a case of $l, k = 0$ and arbitrary l', k' because (see Appendix C)

$$|\det(J_l J_k^{\dagger} - J_{l'} J_{k'}^{\dagger})| = |\det(J_0 J_0^{\dagger} - J_{l'-l} J_{k'-k}^{\dagger})|. \tag{52}$$

Thus this gives us

$$\begin{aligned} \zeta_{\mathcal{P}_{\mathcal{H}}} &= \frac{1}{2} \min_{\substack{0 \le l, l' \le L_{H_1}-1 \\ 0 \le k, k' \le L_{H_2}-1 \\ (l,k) \ne (l',k')}} |\det(J_l J_k^{\dagger} - J_{l'} J_{k'}^{\dagger})|^{\frac{1}{M}} \qquad (53) \\ &= \frac{1}{2} \min_{\substack{0 \le l, k \le L_{H_1}-1, L_{H_2}-1 \\ (l,k) \ne (0,0)}} |\det(J_0 J_0^{\dagger} - J_l J_k^{\dagger})|^{\frac{1}{M}} \qquad (54) \end{aligned}$$

We assume that both $\mathcal{H}_1$ and $\mathcal{H}_2^{\dagger}$ have the same value of $x = (x_1, x_2)$. We choose x which satisfies (31), $k = (k_1, k_2, \ldots, k_M)$ of $\mathcal{H}_1$ and $r = (r_1, \ldots, r_M)$ of $\mathcal{H}_2^{\dagger}$ in order to maximize $\zeta_{\mathcal{P}_{\mathcal{H}}}$ in (54).

6 Results and Performance

6.1 Results

Table 2 shows some of Hamiltonian and product constellations with their best diversity product comparing with different designs: orthogonal [1, 18], dicyclic, cyclic groups in [9, 10, 11], fixed-point free groups, nongroups in [16], parametric codes [13] and numerical methods [6]. Our constellations have diversity product higher than orthogonal designs, dicyclic groups, cyclic groups, nongroups, numerical methods, parametric codes and some of those obtained from fixed-point free groups. Our Hamiltonian constellations of $L = 2$ to 5 for every M even case are optimal constellations whose diversity product achieve the upper bound [13] given by $\sqrt{\frac{L}{2(L-1)}}$.

L	2	3	4	5
$\zeta = \sqrt{\frac{L}{2(L-1)}}$	1.0000	0.8660	0.8165	0.7906

Table 1: Optimal diversity product for $L = 2$ to 5.

From Table 2, for $M = 2$, we can see that the product $\mathcal{P}_{2\times2}, L = 120$ has $\zeta = 0.3090$ which equals the excellent fixed-point free group $SL_2(\mathbb{F}_5)$ constellation. The product constellation $\mathcal{P}_{2\times2}$ at $L = 1089$ also has an excellent diversity product $= 0.1142$. For $M = 3$, we have $\mathcal{H}_{3\times3}, L = 3$ which has $\zeta = 0.8660$ is the optimal constellation. $\mathcal{P}_{\mathcal{H}_{3\times3}}$ at $L = 513$ has an excellent diversity product $= 0.2283$ which is higher than the fixed-point free group $G_{171,94}$.

6.2 Performance

We compare the performance of our Hamiltonian and product constellations with different designs as listed in Table 2. The performance is considered by plotting the block error rate, *bler*, against SNR. All plots are considered in an unknown Rayleigh flat fading channel which use the differential modulation to transmit signals as explained in Section 1.1.2. The fading coefficient and additive noise are independent $\mathcal{CN}(0,1)$ and the channel matrix is assumed to be constant within two consecutive time periods.

Figure. 1 shows the block error rate performance for $M = 2$ transmitter antennas and $N = 2$ receiver antennas at the same $R = 3.00, L = 64$ of a product $\mathcal{P}_{2\times2}$ compared with dicyclic group [10], cyclic group [9], orthogonal design [18] and parametric code [13]. Our product constellation outperforms other four designs.

Figure. 2 compares the bler performance for $M = 2$ transmitter antennas, $N = 1$ receiver antenna at the high rate $R = 6.00$ of our product constellation $\mathcal{P}_{2\times2}$ and orthogonal design [18], cayley code $Q = 4$ [7] and TAST code $\mathcal{T}_{2,2,2}$ [5]. We can see that our proposed constellation again outperforms other three designs.

Figure. 3 compares the bler performance for $M = 3$ transmitter antennas, $N = 1$ and 2 receiver antenna at the same $R = 1.06, L = 9$ of Hamiltonian $\mathcal{H}_{2\times2}$ and the fixed-point free group $G_{9,1}$ [16].

We can see that our Hamiltonian constellation outperforms the fixed-point free group.

Figure. 4 shows the bler performance for $M = 4$ transmitter antennas, $N = 1$ receiver antenna of Hamiltonian $\mathcal{H}_{4\times4}$ at $R = 2.00$, cyclic group [9] at $R = 2.00$, cayley code with $Q = 7, r = 2$ [7] at $R = 1.75$ and 4×4 orthogonal design with z_1, z_2, z_3 are chosen from 6-PSK [22] at $R = 1.94$. We can see that our Hamiltonian constellation outperforms other three designs.

Figure. 5 displays Hamiltonian constellations at the same $R = 1.00$ for $M = 2, 3, 4$ transmitter antennas and $N = 1$ receiver antenna of $\mathcal{H}_{2\times2}$, $\mathcal{H}_{3\times3}$ and $\mathcal{P}_{4\times4}$ respectively.

7 Conclusion

We have constructed new unitary space-time constellations with high diversity products, which can be used for any number of transmitter antennas and for any data rate. Our constellations have full diversity and can be used for both unknown and known channel with differential modulation. Although the Hamiltonian constellations $\mathcal{H}$ and the product constellations $\mathcal{P}, \mathcal{P}_{\mathcal{H}}$ do not form groups, the optimization of the diversity products requires checking only $L - 1$ distinct matrices in their constellations. Hamiltonian constellations for $L \leq 5$ for the case where M is even achieve the optimal theoretical bound. In addition, many of our proposed constellations have the best known diversity products in the literature, as shown in Table 2, and outperform all other constellation designs.

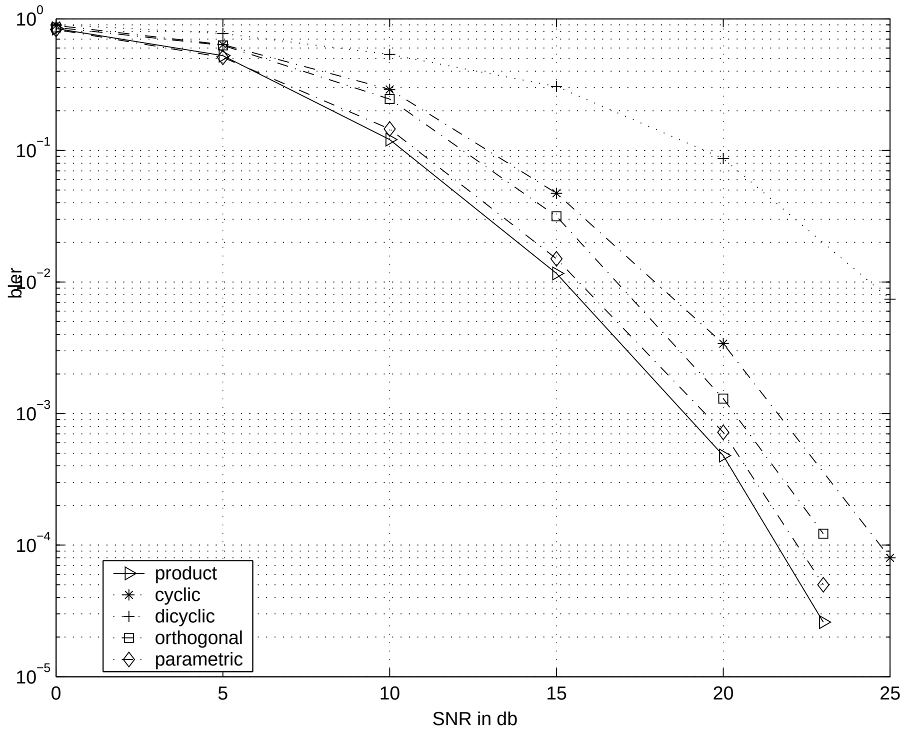

Figure 1: Block error rate performance for $M = 2, N = 2$ of the product $\mathcal{P}_{2\times 2}$, dicyclic group [10], cyclic group [9], orthogonal design [18] and parametric code [13] at $R = 3.00, L = 64$.

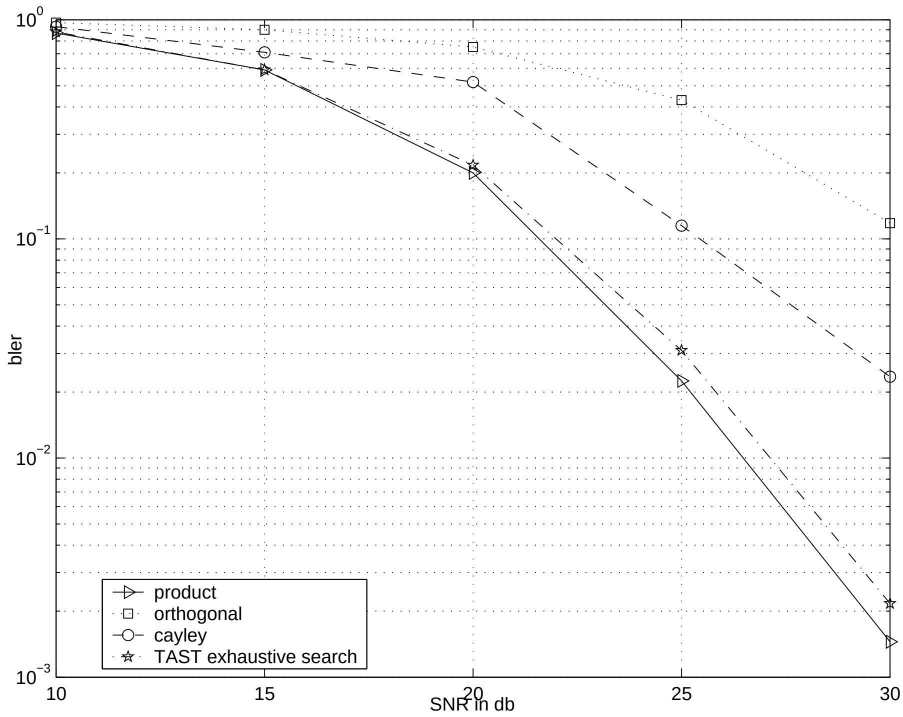

Figure 2: Block error rate performance for $M = 2$, $N = 1$ at $R = 6.00$ of product $\mathcal{P}_{2\times 2}$, orthogonal design [18], cayley code [7] and TAST code [5].

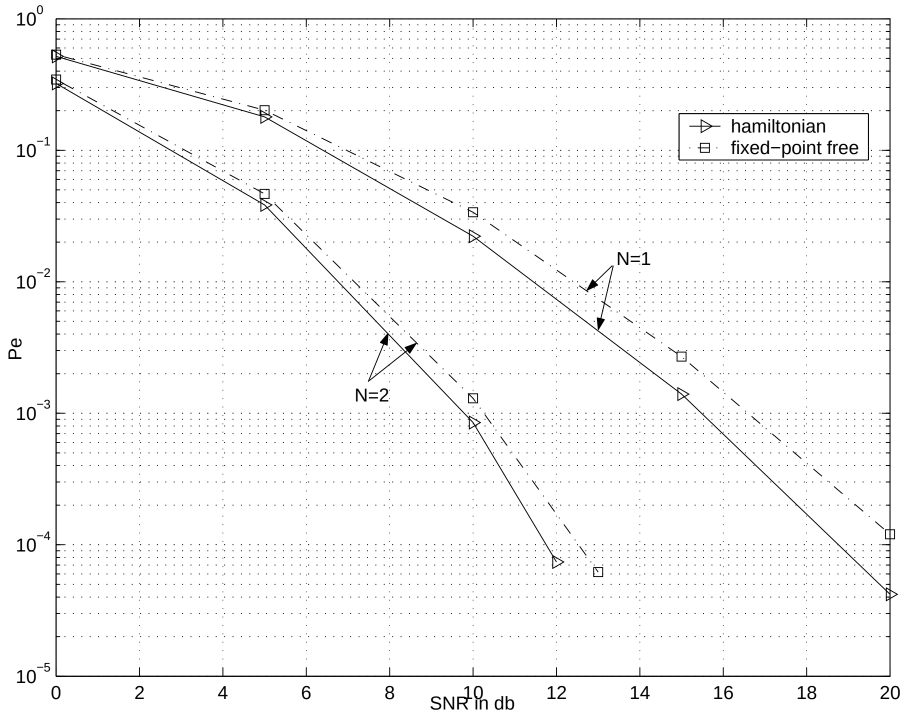

Figure 3: Block error rate performance for $M = 3, N = 1$ and 2 at $R = 1.06$ of Hamiltonian $\mathcal{H}_{3\times3}$ and the fixed-point free group [16].

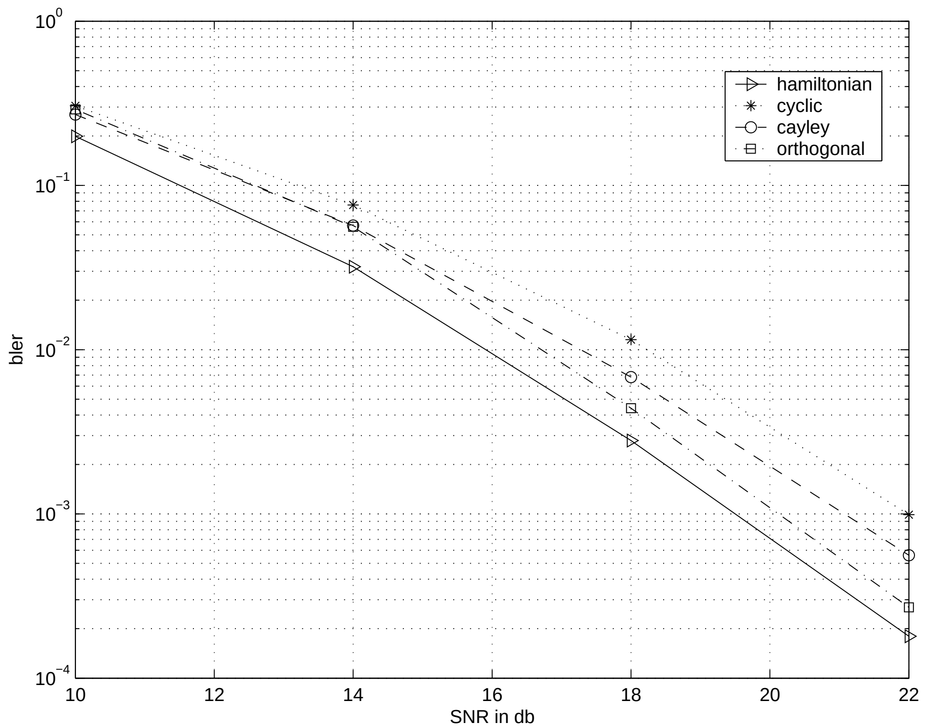

Figure 4: Block error rate performance for $M = 4, N = 1$ of Hamiltonian $\mathcal{H}_{4\times4}$ $R = 2.00$, cyclic group [9] $R = 2.00$, cayley code [7] $R = 1.75$ and orthogonal design [22] $R = 1.94$.

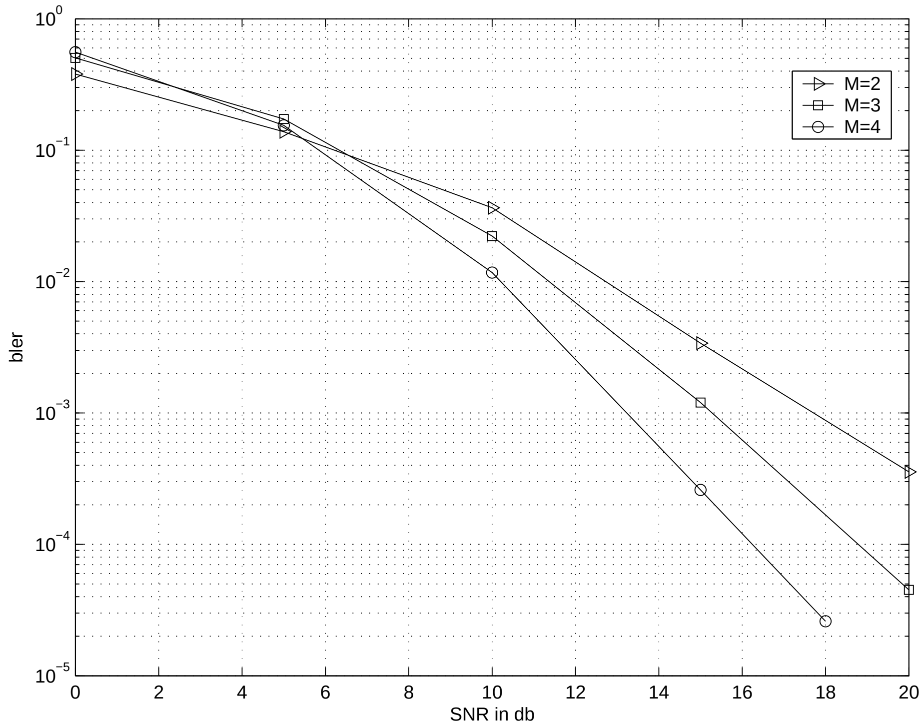

Figure 5: Block error rate performance for $M = 2, 3, 4$, and $N = 1$ at $R = 1.00$ of our proposed constellations: $\mathcal{H}_{2\times 2}, \mathcal{H}_{3\times 3}$ and $\mathcal{P}_{4\times 4}$ as described in Table 2.

Appendix A

We prove that to compute the diversity product in (36) it suffices to choose $l = 0$ for H_l and arbitrary $l' = 1, \ldots, L-1$ for $H_{l'}$. This proof can also be worked for the general $M \times M$ case. From (34), we can write H_l in terms of H_0 as $H_l = e^{j\frac{2\pi lk_1}{L}} R_l H_0 T_l$ where $R_l = \mathrm{diag}(e^{-j\frac{2\pi lk_1}{L}}, e^{-j\frac{2\pi lk_2}{L}})$ and $T_l = \mathrm{diag}(e^{-j\frac{2\pi lk_1}{L}}, e^{j\frac{2\pi lk_2}{L}})$. We show that $|\det(H_l - H_{l'})| = |\det(H_0 - H_{l'-l})|$ for $0 \le l < l' \le L-1$.

$$\begin{aligned} |\det(H_l - H_{l'})| &= |\det(e^{j\frac{2\pi lk_1}{L}} R_l H_0 T_l - e^{j\frac{2\pi l' k_1}{L}} R_{l'} H_0 T_{l'})| \\ &= |e^{j2\pi lk_1}||\det R_l||\det(H_0 - e^{j\frac{2\pi(l'-l)k_1}{L}} R_{l'-l} H_0 T_{l'-l})||\det T_l| \\ &= |\det(H_0 - H_{l'-l})| \end{aligned}$$

□

Appendix B

We prove that to compute the diversity product of $\mathcal{P}$ in (46) it suffices to choose $l = k = 0$ for

P, and arbitrary $0 \le l' \le L_H - 1,\ \ 0 \le k' \le L_C - 1$ and $(l', k') \ne (0, 0)$ for P'. The proof is shown for the 2×2 case, from which the general $M \times M$ case can follow immediately. We will show that $|\det(P - P')| = |\det(H_l O_k - H_{l'} O_{k'})| = |\det(H_0 - H_{l'-l} O_{k''})|$ for $0 \le l < l' \le L_H - 1$ and $0 \le, k, k', k'' \le L_C - 1$.

$$\begin{aligned}
|\det(H_l O_k - H_{l'} O_{k'})| &= |\det(e^{j\frac{2\pi l k_1}{L_H}} R_l H_0 T_l O_k - e^{j\frac{2\pi l' k_1}{L_H}} R_{l'} H_0 T_{l'} O_{k'})| \\
&= |\det(e^{j\frac{2\pi l k_1}{L_H}} R_l H_0 T_l - e^{j\frac{2\pi l' k_1}{L_H}} R_{l'} H_0 T_{l'} O_{k''})| \\
&= |e^{-j\frac{2\pi l k_1}{L}}||\det R_l||\det(H_0 - e^{j\frac{2\pi (l'-l) k_1}{L_H}} R_{l'-l} H_0 T_{l'-l} O_{k''})||\det T_l| \\
&= |\det(H_0 - e^{j\frac{2\pi (l'-l) k_1}{L_H}} R_{l'-l} H_0 T_{l'-l} O_{k''})| \\
&= |\det(H_0 - H_{l'-l} O_{k''})|
\end{aligned}$$

$\square$

Appendix C

We prove that to compute the diversity product of $\mathcal{P}_{\mathcal{H}}$ in (53) it suffices to choose $l = k = 0$ for $J_l J_k^\dagger$, and arbitrary $0 \le l' \le L_{H_1} - 1,\ \ 0 \le k' \le L_{H_2} - 1$ and $(l', k') \ne (0, 0)$ for $J_{l'} J_{k'}^\dagger$. The proof is shown for a 3×3 case, for a case of general M odd follows immediately. A 3×3 J_l can be written as

$$\begin{aligned}
J_l &= \begin{bmatrix} e^{j\frac{2\pi k_1 l}{L_{H_1}}} & 0 & 0 \\ 0 & e^{j\frac{2\pi k_2 l}{L_{H_1}}} & 0 \\ 0 & 0 & e^{j\frac{2\pi k_2 l}{L_{H_1}}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-j\frac{2\pi k_2 l}{L_{H_1}}} & 0 \\ 0 & 0 & e^{-j\frac{2\pi k_3 l}{L_{H_1}}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \sqrt{y_1} & -\sqrt{y_2} \\ 0 & \sqrt{y_2} & \sqrt{y_1} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-j\frac{2\pi k_2 l}{L_{H_1}}} & 0 \\ 0 & 0 & e^{j\frac{2\pi k_3 l}{L_{H_1}}} \end{bmatrix} \\
&= K_l R_l J_0 T_l
\end{aligned} \tag{55}$$

Similarly, we can also write a 3×3 $J_k^\dagger$ as

$$\begin{aligned}
J_k^\dagger &= \begin{bmatrix} e^{j\frac{2\pi r_2 k}{L_{H_2}}} & 0 & 0 \\ 0 & e^{j\frac{2\pi r_2 k}{L_{H_2}}} & 0 \\ 0 & 0 & e^{j\frac{2\pi r_3 k}{L_{H_2}}} \end{bmatrix} \begin{bmatrix} e^{-j\frac{2\pi r_1 k}{L_{H_2}}} & 0 & 0 \\ 0 & e^{-j\frac{2\pi r_2 k}{L_{H_2}}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \sqrt{y_1} & -\sqrt{y_2} & 0 \\ \sqrt{y_2} & \sqrt{y_1} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} e^{j\frac{2\pi r_1 k}{L_{H_2}}} & 0 & 0 \\ 0 & e^{-j\frac{2\pi r_2 k}{L_{H_2}}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \\
&= K_l^\dagger R_l^\dagger J_0^\dagger T_l^\dagger
\end{aligned} \tag{56}$$

Define

$$A = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}, \ D = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{bmatrix} \text{ and } E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b^{-1}c \end{bmatrix}$$

where a, b, c are arbitrary number. $A = DE$, and also $A^{-1} = D^{-1}E^{-1}$. We will use this property in our proof:

$$J_0 A J_0^\dagger = D J_0 J_0^\dagger E \tag{57}$$

We note that D, D^{-1} and E, E^{-1} can commute with J_0 and $J_0^\dagger$ (as well as any diagonal matrices) respectively.

$$\begin{aligned}
&|\det(J_l J_k^\dagger - J_{l'} J_{k'}^\dagger)| \\
&= |\det(K_l R_l J_0 T_l K_k^\dagger R_k^\dagger J_0^\dagger T_k^\dagger - K_{l'} R_{l'} J_0 T_{l'} K_{k'}^\dagger R_{k'}^\dagger J_0^\dagger T_{k'}^\dagger)| \\
&= |\det(J_0 T_l R_k^\dagger J_0^\dagger - K_{l'-l} R_{l'-l} J_0 T_{l'} R_{k'}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger)| \\
&= |\det(J_0 A J_0^\dagger - K_{l'-l} R_{l'-l} J_0 T_{l'} R_{k'}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger)|, \quad \text{where } A = T_l R_k^\dagger \\
&= |\det(D J_0 J_0^\dagger E - K_{l'-l} R_{l'-l} J_0 T_{l'} R_{k'}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger)|, \quad \text{from a property (57)} \\
&= |\det D||\det(J_0 J_0^\dagger - D^{-1} K_{l'-l} R_{l'-l} J_0 T_{l'} R_{k'}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger E^{-1})||\det E| \\
&= |\det(J_0 J_0^\dagger - K_{l'-l} R_{l'-l} J_0 T_{l'} D^{-1} E^{-1} R_{k'}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger)| \\
&= |\det(J_0 J_0^\dagger - K_{l'-l} R_{l'-l} J_0 T_{l'} A^{-1} R_{k'}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger)| \\
&= |\det(J_0 J_0^\dagger - K_{l'-l} R_{l'-l} J_0 T_{l'} T_{-l} R_{-k}^\dagger R_{k'}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger)|, \quad \text{where } A^{-1} = (T_l R_k^\dagger)^{-1} = T_{-l} R_{-k}^\dagger \\
&= |\det(J_0 J_0^\dagger - K_{l'-l} R_{l'-l} J_0 T_{l'-l} R_{k'-k}^\dagger K_{k'-k}^\dagger J_0^\dagger T_{k'-k}^\dagger)| \\
&= |\det(J_0 J_0^\dagger - J_{l'-l} J_{l'-l}^\dagger)|
\end{aligned}$$

□

References

[1] S.M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J.Sel.Area Comm*, vol.16, pp.1451-1458, Oct 1998.

[2] E. Biglieri and M. Elia, "Cyclic-group codes for the Gaussian channel," *IEEE Trans. Info. Theory*, vol.22, pp.624-629, Sept 1976.

[3] I.F. Blake, "Distance properties of group codes for the Gaussian channel," *SIAM J.Appl. Math*, vol.23, pp.312-324, Nov 1972.

[4] G. J. Foschini, " Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs. Tech. J.*, vol.1, no.2, pp.41-59, 1996

[5] H. El Gamal and M. O. Damen, "Universal space-time coding," " *IEEE Trans. Info. Theory*, vol.49, pp.1079-1119, May 2003.

[6] G. Han and J. Rosenthal, "A numerical approach for designing unitary space time codes with large diversity product and diversity Sum." *In Proceedings IEEE ISIT 2003*, Japan, pp. 178. Download available at `http://www.nd.edu/~eecoding`

[7] B. Hassibi and B. M. Hochwald, "Cayley Differential Unitary Space-time Codes," " *IEEE Trans. Info. Theory*, vol.48, pp.1485-1503, June 2002.

[8] B.M. Hochwald and T.L. Mazetta, "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat-fading," *IEEE Trans. Info. Theory*, vol.46, pp.543-564, Mar 2000.

[9] B.M. Hochwald and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Info. Theory*, vol.48, pp.2041-2052, Dec 2000.

[10] B.L. Hughes, "Differential space-time modulation", *IEEE Trans. Info. Theory*, vol.46, pp.2567-2578, Nov 2000.

[11] B.L. Hughes, "Optimal space-time constellations from groups", *IEEE Trans. Info. Theory*, vol.49, pp.401-410, Feb 2003.

[12] H. Jafarkhani and V. Tarokh, "Multiple transmit antenna differential detection from generalized orthogonal designs", *IEEE Trans. Info. Theory*, vol.47, pp.2626-2631, Sept 2001.

[13] X.B. Liang and X.G. Xia, "Unitary signal constellations for differential space-time modulation with two transmit antennas: Parametric codes, optimal designs, and bounds", *IEEE Trans. Info. Theory*, vol.48, pp.2291-2322, Aug 2002.

[14] T.L. Marzetta and B.M. Hochwald, "Capacity of a mobile multiple-antenna communication in Rayleigh flat-fading", *IEEE Trans. Info. Theory*, vol.45, pp.139-157, Jan 1999.

[15] T. Mittelhozer and J. Lathtonen, "Group codes genrated by finite reflection groups", *IEEE Trans. Info. Theory*, vol.42, pp.519-528, Mar 1996.

[16] A. Shokrollahi, B. Hassibi, B.M. Hochwald and W. Sweldens, "Representation theory for high-rate multiple-antenna code designs," *IEEE Trans. Info. Theory*, vol.47, pp.2335-2367, Sept 2001.

[17] D. Slepian, "Group codes for the Gaussian Channel," *The Bell system technical journal*, pp.575-602, April 1968.

[18] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE J.Sel.Area Comm*, vol.18, pp.1169-1174, July 2000.

[19] V. Tarokh, H. Jafarkhani and A.R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Info. Theory*, vol.45, pp.1456-1174, July 1999.

[20] V. Tarokh, N. Seshadri and A.R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans Info. Theory*, vol.44, pp.744-765, March 1998.

[21] I. E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans Telecommun.*, vol.10, pp. 585-598, Nov 1999.

[22] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space-time block codes for complex signal constellations," *IEEE Trans. Info. Theory*, vol.48, pp.384-395, Feb 2002.

[23] Y. Jing and B. Hassibi, "Design of fully-diverse multiple-antenna codes based on $Sp(2)$," *IEEE Trans Info. Theory*, submitted for publication.

M	L	R	ζ	Constellation designs
2	4	1.00	0.7071	dicyclic group Q_1
2	4	1.00	0.7071	cyclic group $u = (1, 1)$
2	4	1.00	0.7071	orthogonal with 2^{th}-roots of unity
2	4	1.00	0.8165	$\mathcal{H}$ $x_1 = 0.6667,\ k = (1, 2)$ Figure. 1
2	8	1.50	0.7071	dicyclic group Q_2
2	8	1.50	0.5946	cyclic group $u = (1, 3)$
2	8	1.50	0.7071	$\mathcal{H}$ $x_1 = 0.5000,\ k = (1, 3)$
2	16	2.00	0.3827	dicyclic group Q_3
2	16	2.00	0.3827	cyclic group $u = (1, 7)$
2	16	2.00	0.5000	orthogonal with 4^{th}-roots of unity
2	16	2.00	0.5946	parametric code, $k = (3, 4, 2)$
2	16	2.00	0.5098	$\mathcal{H}$ $x_1 = 0.5198,\ k = (1, 4)$
2	16	2.00	0.5412	$\mathcal{P}$ $L_H = 8, L_C = 2, x_1 = 0.5858, k = (1, 2), r = (1, 1)$
2	24	2.29	0.5000	fixed-point free group $E_{3,1} = SL_2(\mathbb{F}_3)$
2	24	2.29	0.5000	$\mathcal{P}$ $L_H = 8, L_C = 3, x_1 = 0.5000, k = (1, 3), r = (1, 1)$
2	27	2.38	0.4122	numerical method $A^k B^k C^k$
2	27	2.38	0.4122	$\mathcal{P}$ $L_H = 9, L_C = 3, x_1 = 0.7733, k = (1, 3), r = (1, 1)$
2	32	2.50	0.1951	dicyclic group Q_4
2	32	2.50	0.2494	cyclic group $u = (1, 7)$
2	32	2.5	0.3827	parametric code, $k = (7, 8, 2)$
2	32	2.50	0.3827	$\mathcal{H}$ $x_1 = 0.4953,\ k = (1, 7)$
2	32	2.50	0.4082	$\mathcal{P}$ $L_H = 8, L_C = 4, x_1 = 0.6667, k = (1, 2), r = (1, 1)$
2	36	2.59	0.3860	numerical method $A^k B^l$
2	36	2.59	0.4039	$\mathcal{P}$ $L_H = 9, L_C = 4, x_1 = 0.2577, k = (1, 2), r = (1, 1)$

Table 2: Comparison of different constellation designs: our constellations are highlighted in grey, orthogonal design [18], dicyclic and cyclic groups [9, 10], fixed-point free groups and nongroups [16], parametric codes [13] and numerical methods [6].

M	L	R	ζ	Constellation designs
2	48	2.79	0.3868	fixed-point free group $F_{3,1,-1}$
2	48	2.79	0.3678	$\mathcal{P}$ $L_H = 3, L_C = 16, x_1 = 0.2113, k = (1,2), r = (1,7)$
2	49	2.81	0.3781	numerical method $A^k B^l$
2	49	2.81	0.4118	$\mathcal{P}$ $L_H = 7, L_C = 7, x_1 = 0.5000, k = (1,6), r = (1,4)$
2	55	2.89	0.3874	parametric code, $k = (34, 15, 0)$
2	55	2.89	0.4074	$\mathcal{P}$ $L_H = 11, L_C = 5, x_1 = 0.5904, k = (1,2), r = (1,1)$
2	64	3.00	0.0980	dicyclic group Q_5 Figure.1
2	64	3.00	0.1985	cyclic group $u = (1, 19)$ Figure.1
2	64	3.00	0.2706	orthogonal with 8^{th}-roots of unity Figure.1
2	64	3.00	0.3070	parametric code, $k = (7, 10, 0)$ Figure.1
2	64	3.00	0.3090	numerical method $A^k B^k$
2	64	3.00	0.2816	$\mathcal{H}$ $x_1 = 0.6281,\ k = (1, 27)$
2	64	3.00	0.3678	$\mathcal{P}$ $L_H = 4, L_C = 16, x_1 = 0.6533, k = (1,2), r = (1,9)$ Figure.1
2	75	3.11	0..3535	parametric code, $k = (49, 18, 0)$
2	75	3.11	0.3535	$\mathcal{P}$ $L_H = 25, L_C = 3, x_1 = 0.5000, k = (1,7), r = (1,1)$
2	81	3.17	0.2417	nongroup, $L_A = 9, u = (1, 2)$
2	81	3.17	0.2974	$\mathcal{P}$ $L_H = 27, L_C = 3, x_1 = 0.4024, k = (1,12), r = (1,1)$
2	91	3.25	0.3451	parametric code, $k = (64, 21, 0)$
2	91	3.25	0.3451	$\mathcal{P}$ $L_H = 13, L_C = 17, x_1 = 0.5000, k = (1,5), r = (1,1)$
2	105	3.36	0.3116	parametric code, $k = (34, 42, 0)$
2	105	3.36	0.3116	$\mathcal{P}$ $L_H = 35, L_C = 3, x_1 = 0.5000, k = (1,13), r = (1,1)$
2	120	3.45	0.1353	cyclic group $u = (1, 43)$
2	120	3.45	0.3090	fixed-point free group $J_{1,1} = SL_2(\mathbb{F}_5)$
2	120	3.45	0.2377	numberical method
2	120	3.45	0.3090	$\mathcal{P}$ $L_H = 24, L_C = 5, x_1 = 0.5000, k = (1,5), r = (1,1)$
2	121	3.46	0.1922	orthogonal with 11^{th}-roots of unity
2	121	3.46	0.2106	$\mathcal{H}$ $x_1 = 0.5590,\ k = (1, 22)$
2	121	3.46	0.2795	$\mathcal{P}$ $L_H = 11, L_C = 11, x_1 = 0.3670, k = (1,6), r = (1,1)$

M	L	R	ζ	Constellation designs
2	128	3.50	0.0491	dicyclic group Q_6
2	128	3.50	0.1498	cyclic group $u = (1, 47)$
2	128	3.50	0.2606	parametric code, $k = (1, 8, 20)$
2	128	3.50	0.2031	$\mathcal{H}$ $x_1 = 0.5142,\ k = (1, 12)$
2	128	3.50	0.2793	$\mathcal{P}$ $L_H = 16, L_C = 8, x_1 = 0.6104, k = (1, 6), r = (1, 3)$
2	240	3.95	0.1045	cyclic group $u = (1, 151)$
2	240	3.95	0.2257	fixed-point free group $F_{15,1,11}$
2	240	3.95	0.1511	$\mathcal{H}$ $x_1 = 0.4173,\ k = (1, 85)$
2	240	3.95	0.2381	$\mathcal{P}$ $L_H = 10, L_C = 24, x_1 = 0.2960, k = (1, 4), r = (1, 5)$
2	256	4.00	0.0245	dicyclic group Q_7
2	256	4.00	0.0988	cyclic group $u = (1, 75)$
2	256	4.00	0.1379	orthogonal with 16^{th}-roots of unity
2	256	4.00	0.1651	numerical method $A^k B^k$
2	256	4.00	0.1477	$\mathcal{H}$ $x_1 = 0.5526,\ k = (1, 119)$
2	256	4.00	0.1981	$\mathcal{P}$ $L_H = 8, L_C = 32, x_1 = 0.3477, k = (1, 4), r = (1, 13)$
2	289	4.09	0.1625	nongroup, $L_A = 17, u = (1, 12)$
2	289	4.09	0.1838	$\mathcal{P}$ $L_H = 17, L_C = 17, x_1 = 0.6640, k = (1, 4), r = (1, 1)$
2	1089	5.04	0.0794	nongroup, $L_A = 33, u = (1, 26)$
2	1089	5.04	0.1142	$\mathcal{P}$ $L_H = 99, L_C = 11, x_1 = 0.7900, k = (1, 9), r = (1, 1)$
2	4096	6.00	0.0347	orthogonal with 64^{th}-roots of unity Figure.2
2	4096	6.00	0.0685	$\mathcal{P}$ $L_H = 64, L_C = 64, x_1 = 0.3898, k = (1, 28), r = (1, 33)$ Figure.2
2	4225	6.02	0.0436	nongroup, $L_A = 65, u = (1, 19)$
2	4225	6.02	0.0671	$\mathcal{P}$ $L_H = 65, L_C = 65, x_1 = 0.4026, k = (1, 39), r = (1, 33)$
3	3	0.53	0.8660	$\mathcal{H}$ $x_1 = 0.5000,\ k = (1, 1, 1)$
3	5	0.77	0.7183	numerical method
3	5	0.77	0.7673	$\mathcal{H}$ $x_1 = 0.2316,\ k = (1, 1, 2)$
3	8	1.00	0.5134	cyclic group $u = (1, 1, 3)$
3	8	1.00	0.6588	$\mathcal{H}$ $x_1 = 0.8089,\ k = (1, 3, 4)$ Figure. 1

M	L	R	ζ	Constellation designs
3	9	1.06	0.6004	fixed-point free group $G_{9,1}$ with $u = (1, 2, 5)$ Figure. 3
3	9	1.06	0.6632	$\mathcal{H}$ $x_1 = 0.4679,\ k = (1, 4, 3)$ Figure. 3
3	9	1.06	0.6283	$\mathcal{P}_{\mathcal{H}}$ $L_{H_1} = 3, L_{H_2} = 3, x_1 = 0.3820, k = (1, 1, 3), r = (2, 2, 1)$
3	63	1.99	0.3301	cyclic group $u = (1, 17, 26)$
3	63	1.99	0.3851	fixed-point free group $G_{21,4}$
3	63	1.99	0.3498	$\mathcal{H}$ $x_1 = 0.3758,\ k = (1, 20, 27)$
3	63	1.99	0.4023	$\mathcal{P}_{\mathcal{H}}$ $L_{H_1} = 7, L_{H_2} = 9, x_1 = 0.4603, k = (1, 1, 6), r = (5, 3, 1)$
3	64	2.00	0.2765	cyclic group $u = (1, 11, 27)$
3	64	2.00	0.3478	$\mathcal{H}$ $x_1 = 0.6994,\ k = (1, 23, 30)$
3	513	3.00	0.1353	fixed-point free group $G_{171,64}(t = 19)$
3	513	3.00	0.1664	$\mathcal{P}$ $L_H = 27, L_C = 19, x_1 = 0.4110, k = (1, 3, 11), r = (1, 18, 15)$
3	513	3.00	0.2028	$\mathcal{P}_{\mathcal{H}}$ $L_{H_1} = 9, L_{H_2} = 57, x_1 = 0.4970, k = (1, 1, 5), r = (15, 20, 1)$
3	529	3.02	0.1863	nongroup $L_A = 23, u = (1, 13, 19)$
3	529	3.02	0.2283	$\mathcal{P}_{\mathcal{H}}$ $L_{H_1} = 23, L_{H_2} = 23, x_1 = 0.3671, k = (1, 19, 1), r = (2, 20, 1)$
4	3	0.40	0.8660	$\mathcal{H}$ $x_1 = 0.5000,\ k = (1, 1, 1, 1)$
4	4	0.50	0.8165	$\mathcal{H}$ $x_1 = 0.6667,\ k = (1, 2, 1, 2)$
4	5	0.58	0.7906	$\mathcal{H}$ $x_1 = 0.5000,\ k = (1, 2, 1, 2)$
4	9	0.79	0.5904	numerical method
4	9	0.79	0.7119	$\mathcal{H}$ $x_1 = 0.4094,\ k = (1, 2, 6, 5)$
4	16	1.00	0.5453	cyclic group $u = (1, 3, 5, 7)$
4	16	1.00	0.6377	$\mathcal{H}$ $x_1 = 0.3680,\ k = (1, 3, 7, 5)$
4	16	1.00	0.6580	$\mathcal{P}$ $L_H = 4, L_C = 4, x_1 = 0.5000, k = (1, 2, 1, 4), r = (1, 3, 3, 1)$ Figure. 1
4	240	1.98	0.2145	cyclic group $u = (1, 31, 133, 197)$
4	240	1.98	0.5000	fixed-point free group $K_{1,1,-1}$
4	240	1.98	0.3614	$\mathcal{P}_{\mathcal{H}}$ $L_{H_1} = 16, L_{H_2} = 15, x_1 = 0.3614, k = (1, 2, 9, 18), r = (1, 11, 7, 2)$

M	L	R	ζ	Constellation designs
4	256	2.00	0.2208	cyclic group $u = (1, 25, 97, 107)$ Figure. 4
4	256	2.00	0.3320	$\mathcal{H}$ $x_1 = 0.4834$, $k = (1, 121, 79, 87)$ Figure. 4
4	289	2.04	0.3105	nongroup, $L_A = 17, u = (1, 3, 4, 11)$
4	289	2.04	0.3287	$\mathcal{H}$ $x_1 = 0.4646$, $k = (1, 126, 12, 67)$
5	32	1.00	0.4095	cyclic group $u = (1, 5, 7, 9, 11)$
5	32	1.00	0.5444	$\mathcal{H}$ $x_1 = 0.4500$, $k = (1, 11, 13, 15, 7)$
6	3	0.26	0.8660	$\mathcal{H}$ $x_1 = 0.5000$, $k = (1, 1, 1, 1, 1, 1)$
6	4	0.33	0.8165	$\mathcal{H}$ $x_1 = 0.6667$, $k = (1, 2, 1, 2, 1, 2)$
6	5	0.39	0.7906	$\mathcal{H}$ $x_1 = 0.5000$, $k = (1, 2, 1, 2, 1, 2)$
6	64	1.00	0.3792	cyclic group $u = (1, 7, 15, 23, 25, 31)$
6	64	1.00	0.5185	$\mathcal{H}$ $x_1 = 0.4549$ $k = (1, 19, 3, 57, 23, 31)$