Representation Theory for High-Rate Multiple-Antenna Code Design

BABAK HASSIBI BERTRAND M. HOCHWALD AMIN SHOKROLLAHI WIM SWELDENS

Bell Laboratories, Lucent Technologies
600 Mountain Avenue, Murray Hill, NJ 07974
{hassibi,hochwald,amin,wim}@research.bell-labs.com
http://mars.bell-labs.com

March, 2000

Multiple antennas can greatly increase the data rate and reliability of a wireless communication link in a fading environment, but the practical success of using multiple antennas depends crucially on our ability to design high-rate space-time constellations with low encoding and decoding complexity. It has been shown that full transmitter diversity, where the constellation is a set of unitary matrices whose differences have nonzero determinant, is a desirable property for good performance.

We use the powerful theory of fixed-point-free groups and their representations to design high-rate constellations with full diversity. Furthermore, we thereby classify all full-diversity constellations that form a group, for all rates and numbers of transmitter antennas. The group structure makes the constellations especially suitable for differential modulation and low-complexity decoding algorithms.

The classification also reveals that the number of different group-structures with full diversity is very limited when the number of transmitter antennas is large and odd. We therefore also consider extensions of the constellation designs to nongroups. We conclude by showing that many of our designed constellations perform excellently on both simulated and real wireless channels.

Index Terms—Wireless communications, transmit diversity, receive diversity, space-time coding, fading channels

1 Introduction

It is well known that multiple-antenna wireless communication links promise very high data rates with low error probabilities, especially when the channel is known at the receiver [2, 3]. But the design of so-called space-time codes that achieve these promises is still in its early stages. In [4] some trellis-based codes for known channels are developed, and in [5] some block codes are designed. However, the assumption that the channel is known is sometimes questionable, especially in a rapidly changing mobile environment or when many transmitter antennas are employed and extensive training is required. In [6, 7], some information-theoretic and signal constellation design issues are considered for channels that are known neither to the transmitter nor the receiver. In particular, a class of signals called *unitary space-time signals* is developed where the transmitted signal matrices that form a constellation are all unitary. Further justification for using unitary space-time signals is given in [8], where it is shown that these signals can form their own channel code and achieve arbitrary reliability over a single fading coherence interval with a large number of transmitter antennas.

To help make unknown-channel multiple-antenna communication practical, a scheme using *differential unitary space-time* signals is proposed in [1] that is well-tailored for unknown continuously varying Rayleigh flat-fading channels. Differential unitary space-time signals are unitary matrix-valued signals that are a multiple-antenna generalization of the standard differential phase-shift keying (DPSK) signals commonly used with a single antenna over an unknown channel. A similar differential multiple-antenna scheme is also described in [9]. A two-antenna differential scheme based on orthogonal designs is described in [10].

Although [1] describes, in full generality, the properties that a constellation of differential matrix-valued signals should have, only so-called "diagonal" signals are analyzed in detail. Diagonal signals effectively sequentially activate the antennas, one at a time and always in the same order. If we model the fading paths from every transmitter antenna to the receiver antenna(s) as independent, then the diagonal differential space-time signals provide full transmitter diversity and can lower error probability significantly. At low rates the diagonal signals yield excellent performance. However, at higher rates it is conjectured in [1] that there exist "fuller" matrices (no longer diagonal) that have the necessary unitary and full diversity properties, but would perform even better. In this paper, we show how to design signal matrices satisfying these requirements.

As shown in [1], the design problem for unitary space time constellations is the following: let M be the number of transmitter antennas and R the desired transmission rate (in bits/channel use). Construct a set $\mathcal{V}$ of $L = 2^{RM}$ unitary $M \times M$ matrices such that for any two distinct elements A and B in $\mathcal{V}$, the quantity $|\det{(A-B)}|$ is as large as possible. Any set $\mathcal{V}$ such that $|\det{(A-B)}| > 0$ for all distinct $A, B \in \mathcal{V}$ is said to have *full diversity*. Since both the objective cost (the determinant of the pairwise differences of the elements of $\mathcal{V}$), as well as the constraint set (the set of $L = 2^{RM}$ unitary matrices) are nonconvex, finding an exact solution to the design problem appears to be computationally intractable. Further confounding the problem is the potential size of the constellation 2^{RM}.

Thus, to simplify the design problem it is necessary to introduce some structure on the constellation set $\mathcal{V}$. In this paper, we shall primarily focus on sets of unitary matrices that form a group with respect to matrix multiplication. The use of a group structure offers certain advantages. The first is its potential for good performance. If $\mathcal{V}$ is not a group, $|\det(A-B)|$ generally may take on $L(L-1)/2$ distinct values for $A \neq B \in \mathcal{V}$. The minimum value (equivalent to the minimum distance of the constellation) may therefore be quite small. But if $\mathcal{V}$ is a group, the determinant takes on at most $L-1$ distinct values given by $|\det(I-A)|$ for $I \neq A \in \mathcal{V}$, yielding a possibly larger minimum distance. We show that many of the groups indeed have large minimum distances and perform extremely well.

The second advantage is practical. Since differential space-time modulation multiplies matrices in $\mathcal{V}$ to form the transmitted signal matrix, if $\mathcal{V}$ is a group, every transmitted signal matrix is always an element of $\mathcal{V}$. Therefore, explicit matrix multiplication is replaced by the simpler group table-lookup.

Because any abstract group has a representation in unitary matrices, we restrict our search to groups that have representations with full diversity. In [1], full diversity sets $\mathcal{V}$ that form an *Abelian* (commutative) group are considered. This is equivalent to constraining $\mathcal{V}$ to be a cyclic group represented by a set of diagonal matrices. The codes thereby generated are shown experimentally to have good performance at low rates ($R < 2$, for example). Not explored in [1] are sets $\mathcal{V}$ that are noncommutative groups as potential candidates for good performance at higher rates. One of our primary goals is to find good-performing high-rate noncommutative groups.

In this paper, we completely characterize the class of unitary matrices that provide full diversity and form a group. The characterization is derived using results in the theory of fixed-point-free groups. A fixed-point-free group can be represented as a group of unitary matrices (for some M) with full diversity. An early reference for fixed-point-free groups is Burnside in [11] who shows that any group that is fixed-point-free and has order that is a power of a prime number must be either cyclic or a generalized quaternion group with a full-diversity representation for $M = 2$. These groups are used for differential modulation in [9] (there the generalized quaternion groups are also called "dicyclic"). Another pioneer is Zassenhaus, who classifies many more of these groups in [12]. However, the classification in [12] appears to be incomplete and contains errors; we complete the classification in its entirety. While many of the results in this paper are motivated with differential modulation in mind, we should note that the design problem of maximizing $|\det(A-B)|$ for distinct $A,\ B \in \mathcal{V}$ is important also when the channel is known to the receiver [4, 7]. However, when the channel is known it appears to be less important to have the group property of being able to multiply the matrices in $\mathcal{V}$ without leaving the set.

Some of the groups that emerge as good signal sets are rather surprising. We show, for example, that if M is odd, there is only a single class of possible groups. If $M = 2$ or $M = 4$, some of the signal sets that are excellent performers involve $\mathrm{SL}_2(\mathbb{F}_5)$—the special linear group in two dimensions over the field $\mathbb{F}_5$. In general, however, we find that full-diversity groups do not necessarily exist for all M and R. As a consequence, we also consider sets $\mathcal{V}$ that have some of the properties of a group, but are not themselves groups, and find that there are some simple design rules for generating nongroup constellations with good performance. These allow us to construct good signal constellations for practically all values of M and R.

The paper is organized as follows. The next section motivates and states the problem that we are solving in detail. For ease of reference, and since the paper is rather lengthy, Section 3 contains a summary of the principal results in this paper and a comparison with previous work. Section 4 introduces representation theory and gives an example of a class of non-Abelian fixed-point-free groups. Section 5 classifies all full-diversity or, equivalently, all fixed-point-free groups and gives their representations. Sections 6 and 7 give some consequences of the classification for multiple-antenna constellations. Section 8 uses the structure of the group constellations to generate some nongroup constellations. Section 9 tabulates some of the best group and nongroup constellations and includes some illustrative performance curves for various numbers of antennas and rates. Section 10 discusses fast decoding of the constellations. Section 11 provides the conclusion. Appendices A–C develop most of the mathematical machinery required for the results of this paper and prove the classification theorem.

2 Multiple antenna space-time modulation

2.1 The Rayleigh flat fading channel

Consider a communication link with M transmitter antennas and N receiver antennas operating in a Rayleigh flat-fading environment. The nth receiver antenna responds to the symbol sent on the mth transmitter antenna through a statistically independent multiplicative complex-Gaussian fading coefficient h_{mn}. The received signal at the nth antenna is corrupted at time t by additive complex-Gaussian noise w_{tn} that is statistically independent among the receiver antennas and also independent from one symbol to the next. We assume that time is discrete, $t = 0, 1, \ldots$.

It is convenient to group the symbols transmitted over the M antennas in blocks of M channel uses. We use $\tau = 0, 1, \ldots$ to index these blocks; within the τth block, $t = \tau M, \ldots, \tau M + M - 1$. The transmitted signal is written as an $M \times M$ matrix S_τ whose mth column contains the symbols transmitted on the mth antenna as a function of time; equivalently, the rows contain the symbols transmitted on the M antennas at any given time. The matrices are normalized so that the expected square Euclidean norm of each row is equal to one. Hence, the total transmitted power does not depend on the number of antennas. The fading coefficients h_{mn} are assumed to be constant over these M channel uses.

Similarly, the received signals are organized in $M \times N$ matrices X_τ. Since we have assumed that the fading coefficients are constant within the block of M symbols, the action of the channel is given by the simple matrix equation

$$X_\tau = \sqrt{\rho}\, S_\tau\, H_\tau + W_\tau \quad \text{for} \quad \tau = 0, 1, \ldots . \tag{1}$$

Here $H_\tau = \{h_{mn}\}$ and $W_\tau = \{w_{tn}\}$ are $M \times N$ matrices of independent $\mathcal{CN}(0,1)$-distributed random variables. Because of the power normalization, ρ is the expected SNR at each receiver antenna.

2.2 Known Channel Modulation

We first discuss signal encoding and decoding when the receiver knows the channel H_τ. We assume that the data to be transmitted is a sequence $z_0, z_1, \ldots$ with $z_\tau \in \{0, \ldots, L-1\}$. The data then simply dictates which matrix is transmitted:

$$S_\tau = V_{z_\tau}.$$

Each transmitted matrix occupies M time samples of the channel, implying that transmitting at a rate of R bits per channel use requires a constellation $\mathcal{V} = \{V_1, \ldots, V_L\}$ of $L = 2^{RM}$ unitary signal matrices.

The receiver knows H_τ and computes the maximum likelihood estimate of the transmitted data as[1]

$$\hat{z}_\tau = \arg \min_{\ell=0,\ldots,L-1} \|X_\tau - V_\ell H_\tau\| , \tag{2}$$

where the matrix norm is the Frobenius norm

$$\|A\|^2 = \mathrm{tr}\,(A^\dagger A) = \mathrm{tr}\,(AA^\dagger) = \sum_{i,j} |a_{ij}|^2 . \tag{3}$$

The quality of a constellation $\mathcal{V}$ is determined by the probability of error of mistaking one symbol of $\mathcal{V}$ for another. In [4, 7] it is shown that the Chernoff bound on the pairwise probability of mistaking V_ℓ for $V_{\ell'}$ with

[1] To see that the scaling factor $\sqrt{\rho}$ is not needed, collect the terms from expanding the squared-norm and use the fact that V_ℓ is unitary.

a known channel (averaged over the statistics of H) is given by

$$P_e \leqslant \frac{1}{2} \prod_{m=1}^{M} \left[1 + \frac{\rho}{4} \sigma_m^2 (V_\ell - V_{\ell'})\right]^{-N}, \tag{4}$$

where $\sigma_m(V_\ell - V_{\ell'})$ is the mth singular value of the $M \times M$ matrix $V_\ell - V_{\ell'}$.

2.3 Differential unitary space-time modulation

When the receiver does not know the channel, one can communicate using multiple-antenna differential modulation [1]. Multiple-antenna differential modulation is formally similar to standard single-antenna differential phase-shift keying. In standard DPSK, the transmitted symbol has unit-modulus and is the product of the previously transmitted symbol and the current data symbol. The data symbol typically is one of L equally-spaced points on the complex unit circle. As a generalization, M-antenna differential unitary space-time modulation differentially encodes $M \times M$ unitary matrix-valued signals. We transmit an $M \times M$ unitary matrix that is the product of the previously transmitted matrix and a unitary data matrix taken from the constellation. In other words,

$$S_\tau = V_{z_\tau} S_{\tau-1}, \qquad \tau = 1, 2, \ldots, \tag{5}$$

with $S_0 = I_M$. We immediately see why it is useful in practice to have $\mathcal{V}$ form a group under matrix multiplication: from (5), if $\mathcal{V}$ is a group then all the transmitted matrices S_τ also belong to $\mathcal{V}$. Therefore, the transmitter sends matrices S_τ from a finite set and does not need to explicitly multiply $S_\tau = V_{z_\tau} S_{\tau-1}$, but rather can use a group table-lookup.

If the fading coefficients are approximately constant over $2M$ time samples ($H_\tau \approx H_{\tau-1}$), the received matrices turn out to obey

$$X_\tau = V_{z_\tau} X_{\tau-1} + \sqrt{2}\, W'_\tau, \tag{6}$$

where W'_τ is a $M \times N$ matrix of additive independent $\mathcal{CN}(0,1)$ noise [1], uncorrelated with the signal V_{z_τ}. As shown in [1], the maximum likelihood decoder has the simple structure

$$\hat{z}_\tau = \arg \min_{\ell=0,\ldots,L-1} \| X_\tau - V_\ell X_{\tau-1} \|, \tag{7}$$

and the Chernoff bound on the pairwise probability of error with differential modulation on an unknown channel is

$$P_e \leqslant \frac{1}{2} \prod_{m=1}^{M} \left[1 + \frac{\rho^2}{4(1+2\rho)} \sigma_m^2 (V_\ell - V_{\ell'}) \right]^{-N} . \tag{8}$$

At high SNR, both bounds (4) and (8) depend primarily on the product of the singular values, which is the modulus of the determinant of $V_\ell - V_{\ell'}$. In other words, for high SNR we may write

$$P_e \lesssim \frac{1}{2} \left(\frac{4\alpha}{\rho} \right)^{MN} \cdot \frac{1}{|\det (V_\ell - V_{\ell'})|^{2N}},$$

where $\alpha = 1$ when the channel is known and $\alpha = 2$ when the channel is unknown and used differentially. Hence, there is a 3 dB advantage for knowing versus not knowing the channel, and we may measure the quality of a constellation $\mathcal{V}$ by its so-called *diversity product*

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{0 \leqslant \ell < \ell' < L} |\det (V_\ell - V_{\ell'})|^{\frac{1}{M}} . \tag{9}$$

The scaling factor $\frac{1}{2}$ guarantees that $0 \leqslant \zeta_{\mathcal{V}} \leqslant 1$. The exponent $\frac{1}{M}$ essentially gives the geometric mean of the M singular values since the modulus of the determinant is the product of the singular values. Clearly, a constellation with larger $\zeta_{\mathcal{V}}$ is superior. Any constellation with $\zeta_{\mathcal{V}} > 0$ is said to have full diversity. When $\zeta_{\mathcal{V}} > 0$ and the SNR is high, we note that no two distinct transmitted signals can give the same received signal X, for any H. In this paper we consider only full-diversity constellations and, in particular, we try to find constellations with diversity product $\zeta_{\mathcal{V}}$ as large as possible.

3 Summary of prior work and this paper

3.1 Prior work

We briefly review some of the unitary space-time constellations that have been considered in prior work.

Cyclic group codes In [1] cyclic groups are introduced for differential modulation. In this case, V_ℓ are diagonal Lth roots of unity. In particular,

$$V_\ell = V_1^\ell, \quad \text{where} \quad V_1 = \text{diag}\,[e^{i2\pi u_1/L} \ \cdots \ e^{i2\pi u_M/L}],$$

and $u_1, \ldots, u_M$ are taken from the set $\{0, \ldots, L-1\}$. Without loss of generality, we can let $u_1 = 1$. The constellation is thus specified by the integers $u_2, \ldots, u_M$. The u_m are generally chosen to maximize ζ as defined in (9) and given by

$$\zeta_{\mathcal{V}} = \min_{\ell=1,\ldots,L-1} \left| \prod_{m=1}^{M} \sin \frac{\pi u_i \ell}{L} \right|^{\frac{1}{M}}. \tag{10}$$

In this constellation, the transmitter antennas are activated one at a time and always in the same order.

Orthogonal designs In [10] a two-antenna differential scheme is introduced that uses orthogonal designs. A two-dimensional orthogonal design is a matrix parameterization given by [5]

$$\mathrm{OD}(x,y) = \frac{1}{\sqrt{2}} \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}, \tag{11}$$

where $|x|^2 = |y|^2 = 1$; observe that $\mathrm{OD}(x,y)$ is unitary. Constellations of size $L = Q^2$ are obtained by letting x and y range over the Qth roots of unity $1,\, e^{2\pi i/Q}, \ldots, e^{2\pi i(Q-1)/Q}$, yielding

$$\mathcal{V} = \left\{ \mathrm{OD}(x,y) \mid x,\, y \in \{1,\, e^{2\pi i/Q}, \ldots, e^{2\pi i(Q-1)/Q}\} \right\}.$$

The diversity product of this constellation is

$$\zeta_{\mathcal{V}} = \frac{\sin(\pi/Q)}{\sqrt{2}}. \tag{12}$$

These constellations do not generally form a group; thus, when used differentially, orthogonal designs transmit potentially arbitrary symbols.

Generalized quaternion (also called dicyclic) codes In [9] constellations for $M = 2$ antennas are built from cyclic groups, and also so-called "dicyclic" groups of the form

$$Q_p = \langle \sigma, \eta \mid \sigma^{2^p} = 1, \eta^2 = \sigma^{2^{p-1}}, \eta\sigma\eta^{-1} = \sigma^{-1} \rangle, \qquad p \geqslant 1,$$

where the notation $\langle \cdot \rangle$ refers to the group generated by the elements enclosed within the brackets. These are commonly called generalized quaternion groups, and have order $L = 2^{p+1}$ or rate $R = (p+1)/2$. They are equivalently generated by the two unitary matrices

$$\left\langle \begin{bmatrix} e^{2\pi i/2^p} & 0 \\ 0 & e^{-2\pi i/2^p} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle .$$

For comparison, Table 1 lists some cyclic groups, generalized quaternion groups, and orthogonal designs. The cyclic groups are chosen to have the highest ζ found by searching over $u_2, \ldots, u_M \in \{0, \ldots, L-1\}$. (For large L and M this search was done randomly.) Only for $R = 1.5$ is the quaternion group better than the best cyclic group. Some of the fractional-rate groups in this table are included for later comparison.

3.2 Summary of this paper

This paper classifies *all* possible finite groups of matrices with $\zeta_{\mathcal{V}} > 0$ for all numbers of antennas M and all possible rates R. The groups considered in [1] and [9] appear as special cases of our classification theorems. Our classification includes many new groups that are neither cyclic nor quaternionic, with large $\zeta_{\mathcal{V}}$ and excellent performance.

The classification is based on the theory of fixed-point-free groups. A group is defined to be fixed-point-free if it has a representation in $M \times M$ matrices, for some M, that has positive $\zeta_{\mathcal{V}}$. (Section 4 has a much more detailed description of these group-theoretic concepts and terms.) An early partial classification of these groups appears in a 1905 paper of Burnside [11] where he shows that all groups that are fixed-point-free with order a power of a prime number must either be cyclic or Q_p for some integer p, with an $M = 2$ matrix representation.

A 1936 paper by Zassenhaus [12] gives a more complete classification of the fixed-point-free groups. After reviewing cyclic groups in some detail in Section 4.2, we examine a group described by Zassenhaus in his classification and compute its representations in detail in Section 4.3. This new group turns out to allow one to find all possible constellations for odd M.

Zassenhaus' classification, however, is not complete and contains errors and omissions. We therefore complete the classification in Section 5. Theorem 1 is the main classification theorem. Its proof is long and incorporates many of Zassenhaus' techniques and appears in Appendix A. Having the groups does not mean that we also automatically have the matrix representations with full diversity. Deriving these representations is often tedious, but the result is the content of Theorem 2 and its proof is in Appendix B.

Armed with a complete classification, we explore in Section 6 some of the implications of the classification theorems. Because of the practical interest in $M = 2$ transmitter antennas, Theorem 3 explicitly lists all of

M	L	R	ζ	comments
2	4	1	0.7071	orthogonal design with ± 1
2	4	1	0.7071	cyclic group $u = (1, 1)$
2	4	1	0.7071	quaternion group Q_1
2	8	1.5	0.5946	cyclic group $u = (1, 3)$
2	8	1.5	0.7071	quaternion group Q_2
2	16	2	0.5000	orthogonal design with 4th-roots of unity
2	16	2	0.3827	cyclic group $u = (1, 7)$
2	16	2	0.3827	quaternion group Q_3
2	32	2.5	0.2494	cyclic group $u = (1, 7)$
2	32	2.5	0.1951	quaternion group Q_4
2	64	3	0.2706	orthogonal design with 8th-roots of unity
2	64	3	0.1985	cyclic group $u = (1, 19)$
2	64	3	0.0980	quaternion group Q_5
2	121	3.46	0.1992	orthogonal design with 11th-roots of unity
2	120	3.45	0.1353	cyclic group $u = (1, 43)$
2	128	3.5	0.0491	quaternion group Q_6
2	128	3.5	0.1498	cyclic group $u = (1, 47)$
2	240	3.95	0.1045	cyclic group $u = (1, 151)$
2	256	4	0.1379	orthogonal design with 16th-roots of unity
2	256	4	0.0988	cyclic group $u = (1, 75)$
2	256	4	0.0245	quaternion group Q_7
3	8	1	0.5134	cyclic group $u = (1, 1, 3)$
3	63	1.99	0.3301	cyclic group $u = (1, 17, 26)$
3	64	2	0.2765	cyclic group $u = (1, 11, 27)$
4	16	1	0.5453	cyclic group $u = (1, 3, 5, 7)$
4	240	1.98	0.2145	cyclic group $u = (1, 31, 133, 197)$
4	256	2	0.2208	cyclic group $u = (1, 25, 97, 107)$
5	32	1	0.4095	cyclic group $u = (1, 5, 7, 9, 11)$
5	1024	2	0.1787	cyclic group $u = (1, 31, 355, 425, 581)$
6	64	1	0.3792	cyclic group $u = (1, 7, 15, 23, 25, 31)$
6	4096	2	0.1428	cyclic group $u = (1, 599, 623, 1445, 1527, 1715)$
7	128	1	0.3487	cyclic group $u = (1, 13, 17, 27, 29, 45, 49)$
7	16384	2	0.1213	cyclic group $u = (1, 1875, 5207, 5551, 7687, 7827, 9013)$

Table 1: Summary of some cyclic group and $M = 2$ quaternion and orthogonal design constellations

the groups with full diversity for $M = 2$. For odd M, the possible types of groups are very limited and are contained in Theorem 4. For some concrete examples, Section 7 lists the simplest (smallest) group of each type classified. In this section, one non-obvious example of a fixed-point-free group that stands out is $\mathrm{SL}_2(\mathbb{F}_5)$, the group of 2×2 matrices over the field $\mathbb{F}_5$ with determinant 1. This group has 120 elements and an $M = 2$ matrix representation; its rate is $R = \log(120)/2 = 3.45$. (In this paper, all logarithms are base-two.) For this group $\zeta_{\mathrm{SL}_2(\mathbb{F}_5)} = 0.3090$, which far exceeds $\zeta_{\mathcal{V}}$ for any other constellation we have been able to generate with $M = 2$ and comparable rate R.

Because the list of possible group structures that yield full diversity is limited, especially when M is large and odd, we explore the design of some nongroup constellations in Section 8. Although not groups, these constellations have structures that are inspired by the groups and therefore share some of their properties. Unlike group constellations, however, we make no attempt to exhaustively explore all nongroup alternatives.

In Section 9, the reader can find a list of some of the new constellations in Tables 3 and 4, along with their performance on a wireless fading channel. For example, Figures 1 and 3 demonstrate the excellent performance of $\mathrm{SL}_2(\mathbb{F}_5)$ for $M = 2$ transmitter antennas, and Figure 7 gives the performance a binary extension of this group for $M = 4$ antennas. We also include the results of an experiment with three antennas in the hallways of Bell Laboratories (Figure 6). There are also many other groups and nongroups whose performances are evaluated. Comparisons are made with cyclic and quaternion groups, and orthogonal designs, when they exist.

Maximum likelihood decoding of the group constellations requires a search over the constellation set and can be cumbersome if the number of signals in the constellation $L = 2^{RM}$ is large. For example, with $M = R = 4$, there are $L = 65,536$ signals in the constellation set. To simplify decoding for large L, we therefore discuss fast approximate maximum likelihood algorithms in Section 10. These algorithms exploit the constellation structures and are polynomial, rather than exponential, in the rate R.

Finally, Appendices A-C develop most of the group-theoretic machinery this paper requires. We have also included Appendix D, which uses an information-theoretic argument to further motivate the design of effective constellations of unitary matrices.

We now proceed with the paper.

4 Group construction

4.1 Group representations

We wish to find a set $\mathcal{V}$ of L unitary matrices for which the diversity product $\zeta_{\mathcal{V}}$ in (9) is as large as possible. In this section we constrain $\mathcal{V}$ to form a group under matrix multiplication. Recall that a set G together with a binary multiplication operation is a group if it is closed under this operation, satisfies the associative law, has an identity element 1_G, and contains a multiplicative inverse for each element. With the group requirement, since $|\det(V_\ell - V_{\ell'})| = |\det(I - V_\ell V_{\ell'}^*)| = |\det(I - V)|$, where $V = V_\ell V_{\ell'}^*$ is another element in $\mathcal{V}$, the design problem becomes that of finding a group of L unitary $M \times M$-matrices such that

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{I \neq V \in \mathcal{V}} |\det(I_M - V)|^{\frac{1}{M}}$$

is as large as possible. (The matrix I_d denotes the $d \times d$-identity matrix. We later omit the dimension d if it is clear from the context.)

Our construction uses the representation theory of finite groups. For readers who are not familiar with this theory, we briefly review the main concepts. Two good references for more details are [14, 15]. A *group homomorphism* is a mapping between two groups that respects group multiplication. An M*-dimensional representation* of a group G is a group homomorphism $\Delta(\cdot)$ from G to the group $\mathrm{GL}_M(\mathbf{C})$ of invertible $M \times M$ complex matrices. For instance, the trivial map taking all group elements to the $M \times M$ identity matrix I_M is a representation of a group.

Two representations Δ and Δ' of G are called *equivalent* if there is an invertible matrix $T \in \mathrm{GL}_M(\mathbf{C})$ such that $\Delta(g) = T\Delta'(g)T^{-1}$ for all $g \in G$. The *direct sum* $\Delta \oplus \Delta'$ of two representations Δ and Δ' of dimensions d and d', respectively, is the $(d + d')$-dimensional representation whose value at g is the matrix

$$(\Delta \oplus \Delta')(g) = \begin{bmatrix} \Delta(g) & 0_{d \times d'} \\ 0_{d' \times d} & \Delta'(g) \end{bmatrix},$$

where $0_{k \times \ell}$ denotes a $k \times \ell$ matrix of zeros. A representation is called *reducible* if it is equivalent to a direct sum of two (or more) representations. Otherwise, it is called *irreducible*. Any representation Δ of a finite group can be represented as a direct sum of irreducible representations [14, Theorem 8.7], called the *irreducible constituents* of Δ.

In this paper we are particularly interested in representations using unitary matrices. The following standard argument shows that any representation is equivalent to a representation using only unitary matrices. Choose a square matrix T that satisfies

$$T^*T = \sum_{g \in G} \Delta^*(g)\Delta(g).$$

The matrix T is invertible since each $\Delta(g)$ is invertible so that the sum T^*T is positive definite. Because G is a group, it follows that $\Delta^*(g)T^*T\Delta(g) = T^*T$, for any g. Thus, we see that $T\Delta(g)T^{-1}$ is a unitary matrix, and the representation $T\Delta T^{-1}$ is a unitary representation.

We call a one-dimensional representation of a group a *character* of that group. Hence, a character is a multiplicative mapping which maps elements of the group to complex roots of unity. A character that is injective is called *primitive*; it maps only 1_G into 1.

Our strategy is to take certain groups G and use unitary representations to build group constellations $\mathcal{V}$. We denote this by $\mathcal{V} = \Delta(G)$. The diversity product is then given by

$$\zeta_{\Delta(G)} = \frac{1}{2} \min_{1_G \neq g} |\det\left(I_M - \Delta(g)\right)|^{\frac{1}{M}}. \tag{13}$$

Equivalent representations have the same diversity products.

Although our aim is to maximize $\zeta_{\Delta(G)}$, it is at this point not clear whether this quantity is ever nonzero for a given group G. From (13) it follows that $\zeta_{\Delta(G)}$ is nonzero if and only if for any $g \in G$ such that $g \neq 1_G$, the matrix $\Delta(g)$ does not have an eigenvalue at unity. Such representations have been studied before and are called *fixed-point-free representations*. We call a group *fixed-point-free* if it has a fixed-point-free representation. Such groups arise in the investigation of near-fields [12], in geometry [16], and in the investigation of finite subgroups of skew fields [17]. The present application of these groups, however, appears to be new.

4.2 Cyclic groups are fixed-point-free

We start out with a class of groups that are always fixed-point-free: the class of cyclic groups. We denote a cyclic group G, generated by an element σ, as $G = \langle \sigma \rangle$. If G has order L, then $G = \{\sigma^\ell \mid \ell = 0, \ldots, L-1\}$. In the following, we compute all fixed-point-free representations of this group. It suffices to determine all the irreducible fixed-point-free representations, since the irreducible constituents of a fixed-point-free representation have to be fixed-point-free themselves. But fixed-point-free irreducible representations of cyclic groups are trivial: irreducible representations of Abelian groups are one-dimensional [14, Theorem 9.8], i.e., they are characters of the group. A character is fixed-point-free if and only if it is primitive (if it is not primitive, it maps a non-identity element to one and thereofe has a unit eigenvalue at a non-identity element). Hence, irreducible fixed-point-free representations of cyclic groups are exactly the primitive characters of the group, and these are characters that map a generator of the group to a primitive Lth root of unity.

The Abelian group G has L characters given by $\chi_u(\sigma^\ell) = e^{2\pi i u\ell/L}$ for $u = 0, \ldots, L-1$, but not all are primitive. The character χ_u is primitive if and only if u and L are relatively prime, implying that there are $\varphi(L)$ primitive characters, where $\varphi(L)$ is the *Euler totient function* of L (which denotes the number of positive integers less than L that are relatively prime to L). An M-dimensional representation Δ of G is built as a direct sum of M characters

$$\begin{aligned}\Delta(\sigma) &= \begin{pmatrix} \chi_{u_1}(\sigma) & 0 & \cdots & 0 \\ 0 & \chi_{u_2}(\sigma) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \chi_{u_M}(\sigma) \end{pmatrix} \\ &= \begin{pmatrix} \eta^{u_1} & 0 & \cdots & 0 \\ 0 & \eta^{u_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \eta^{u_M} \end{pmatrix}, \qquad \eta = \mathrm{e}^{2\pi i/L}.\end{aligned}$$

For the representation of σ^ℓ, we use the fact that Δ is a multiplicative map. Hence, for all $g \in G$ $\Delta(g^\ell) = \Delta(g)^\ell$. This implies that

$$\Delta(\sigma^\ell) = \begin{pmatrix} \eta^{\ell u_1} & 0 & \cdots & 0 \\ 0 & \eta^{\ell u_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \eta^{\ell u_M} \end{pmatrix}. \tag{14}$$

These reducible representations are identical to the diagonal code constructions given in [1], and they are fixed-point-free if and only if $u_1, \ldots, u_M$ are relatively prime to L. As shown in [1], either an exhaustive or random search can find the u_m with the highest diversity product $\zeta_{\Delta(G)}$; see also Table 1.

We see that an Abelian group is fixed-point-free if and only if it has a primitive character. Recall that a primitive character defines an injective map from the Abelian group into the group of nonzero complex numbers. Hence, the image of this map is a subgroup of the nonzero complex numbers, isomorphic to the original Abelian group. But subgroups of the nonzero complex numbers are necessarily cyclic. (This is a well-known fact: all elements of a finite subgroup of order n of $\mathbf{C}$ are solutions to $x^n - 1$, hence are nth roots of unity.) We conclude that *an Abelian group has a nonzero diversity product if and only if it is cyclic*.

As shown in [1], the performance of cyclic groups when used for multiple-antenna constellations is good at low rates, when $R < 2$, but degrades for $R \geqslant 2$. This is probably because the antennas are activated only one at a time and always in the same order. Since we seek groups with superior performance, we necessarily must consider non-Abelian groups.

4.3 A non-Abelian class of fixed-point-free groups

An early reference to fixed-point-free representations is a paper of Burnside [11]. An almost complete classification of fixed-point-free groups appears in a paper of Zassenhaus [12]. We use the qualifier "almost" because Zassenhaus' description does not cover some classes of groups that are fixed-point-free. In this paper, we fix the oversight and make the classification complete. The complete classification appears in Section 5.

In Section 5 we give the matrix representations of all the fixed-point-free groups. As it is often difficult and tedious to compute these representations, we generally omit the details. In this section, we therefore indicate how these computations are done by computing the fixed-point-free representations of a particular class of fixed-point-free groups in detail. As shown in Section 5, this class is the only class of groups with odd order, and the only class with irreducible representations in an odd dimension M.

Let

$$G_{m,r} = \langle \sigma, \tau \mid \sigma^m = 1, \tau^n = \sigma^t, \sigma^\tau = \sigma^r \rangle,$$

where n is the order of r modulo m (i.e., n is the smallest positive integer such that $r^n \equiv 1 \bmod m$), $t = m/\gcd(r-1, m)$, and we have $\gcd(n, t) = 1$. (We use the notation σ^τ for $\sigma, \tau \in G$ to mean the element $\tau\sigma\tau^{-1}$.) The group $G_{m,r}$ has order mn because it contains the subgroup $\langle\sigma\rangle$ of order m and index n (the term "index" refers to the number of cosets). Note that the class of groups $G_{m,r}$ contains the class of cyclic groups since $G_{m,1}$ is cyclic of order m.[2] Appendices A and B show that $G_{m,r}$ is fixed-point-free if and only if all prime divisors of n divide $\gcd(r-1, m)$. When $G_{m,r}$ is cyclic, we have that $n = 1$ and therefore all cyclic groups are fixed-point-free; this just confirms what we already know from the previous section. We now compute all the irreducible fixed-point-free representations of $G_{m,r}$.

The cyclic group $H = \langle\sigma\rangle$ is a normal subgroup of $G_{m,r}$. (A subgroup H is normal in G if $ghg^{-1} \in H$

[2] $r = 1$ implies $n = 1$ and $t = 1$. Thus, $\tau = \sigma$ and so $G_{m,1} = \langle\sigma\rangle$.

for all $g \in G$ and $h \in H$.) We need to study how the representations of $G_{m,r}$ interact with H. Denote the restriction of a representation Δ to H by $\Delta \downarrow H$. If Δ is fixed-point-free, so is $\Delta \downarrow H$. Because H is cyclic $\Delta \downarrow H$ has to be equivalent to a direct sum of primitive characters of H (see Section 4.2).

Alternatively, representations on subgroups induce representations on the group itself. Such *induced representations* (see, e.g. [15, Section 5.9]) can be computed from the restricted representation. Let F be an irreducible representation of the cyclic group $H = \langle \sigma \rangle$. The induction of F to G is denoted $F \uparrow G$ and, in our case, is irreducible. For a representation F of H and $\mu \in G$ we consider the the representation F^{μ} with $F^{\mu}(h) = F(\mu h \mu^{-1})$. (Note that because H is a normal subgroup of G, then F^{μ} is a valid representation of H.) The *inertia group* of F is the group of all $\mu \in G$ such that F^{μ} is equivalent to F. It is easy to see that the inertia group of the one-dimensional representation F of H is equal to H if F is primitive. Hence, by [15, Theorem 5.20, Cor. 3] $F \uparrow G$ is irreducible if F is primitive, i.e., fixed-point-free. To get the representations of G, we may thus compute the inductions to G of fixed-point-free representations of H. We choose this route because, as shown in Section 4.2, the fixed-point-free representations of H are simple to compute when H is cyclic.

These inductions can be computed as follows; see, for example, [15, Section 5.9]. Note that $\{1 \cdot H, \tau \cdot H, \ldots, \tau^{n-1} \cdot H\}$ is a set of representatives of the cosets G/H. For the element $\sigma \in G$, we ask if $\tau^i \sigma \tau^{-j} \in H$, for $i, j = 0, \ldots, n-1$? If yes, then the (i,j)th block of $(F \uparrow G)(\sigma)$ is set equal to $F(\tau^i \sigma \tau^{-j})$. If no, then this block is set to zero. But $\tau^i \sigma \tau^{-j} \in H$ if and only if $i = j$. Therefore,

$$(F \uparrow G)(\sigma) = \begin{pmatrix} F(\sigma) & 0 & \cdots & 0 \\ 0 & F(\sigma)^r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & F(\sigma)^{r^{n-1}} \end{pmatrix}. \tag{15}$$

For the element $\tau \in G$, we ask in a similar fashion whether $\tau^i \tau \tau^{-j} \in H$, for $i, j = 0, \ldots, n-1$? If yes, then the (i,j)th block of $(F \uparrow G)(\tau)$ is set equal to $F(\tau^i \tau \tau^{-j}) = F(\tau^{i+1-j})$. If no, then this block is set to zero. But $\tau^{i+1-j} \in H$ if and only if $j - i \equiv 1 \mod n$. For $i = 0, \ldots, n-2$, this holds if $j = i+1$, and in this case $F(\tau^{i+1-j}) = F(\tau^0) = F(1)$. But for $i = n-1$, this holds if $j = 0$, and in this case

$F(\tau^{i+1-j}) = F(\tau^n) = F(\sigma^t)$. Therefore

$$(F \uparrow G)(\tau) = \begin{pmatrix} 0 & F(1) & 0 & \cdots & 0 \\ 0 & 0 & F(1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & F(1) \\ F(\sigma)^t & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{16}$$

Since F is an irreducible representation of the cyclic subgroup H, it is in fact one-dimensional, i.e., it is a character. Because F is a primitive character, $F(\sigma) = \eta$ where η is a primitive mth root of unity. Substituting for $F(\sigma)$ into (15) and (16) gives the explicit representation Δ given by

$$\Delta(G_{m,r}) = \Big\{ (F \uparrow G)(\sigma^\ell)(F \uparrow G)(\tau^k) \ \mid \ell = 0, \ldots, m-1, \ k = 0, \ldots, n-1 \Big\}, \tag{17}$$

where $\gcd(r-1, m) = r_0$, $r_0 t = m$, $\gcd(n, t) = 1$, n is the order of r modulo m, and where

$$\Delta(\sigma) = \begin{pmatrix} \eta & 0 & \cdots & 0 \\ 0 & \eta^r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \eta^{r^{n-1}} \end{pmatrix}, \quad \Delta(\tau) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \eta^t & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{18}$$

These matrices are suitable for transmission with $M = n$ antennas because they are unitary and have dimension n.

In computing the fixed-point-free irreducible representation of $G = G_{m,r}$, we have not explicitly chosen the primitive mth root of unity η. But it is easy to see that the choice of η does not change the group generated by $\Delta(\sigma)$ and $\Delta(\tau)$. Any such choice makes the representation Δ irreducible and fixed-point-free and does not affect the diversity product $\zeta_{\Delta(G)}$.

Even though the constellation (taken in its entirety) does not depend on the choice of η, the representations obtained from different η are not necessarily equivalent. There are, in fact, $\varphi(m)/n$ pairwise inequivalent fixed-point-free irreducible representations of $G_{m,r}$ and they are obtained by choosing η as $e^{2\pi i z/m}$ where z runs over a set of representatives of $(\mathbb{Z}/m\mathbb{Z})^\times$ modulo the subgroup of order n generated by $r \bmod m$. To see this, let F be the irreducible representation of $H = \langle \sigma \rangle$ mapping σ to η, and let F^s be another representation mapping σ to η^s. Then $F \uparrow G$ and $F^s \uparrow G$ are equivalent if and only if there exists an invertible $n \times n$-matrix T such that

$$T(F \uparrow G)(\sigma) = (F^s \uparrow G)(\sigma)T, \quad T(F \uparrow G)(\tau) = (F^s \uparrow G)(\tau)T. \tag{19}$$

Let $T = \{t_{ij}\}$. The equality on the left involving σ implies that $t_{ij}\eta^{r^{j-1}} = t_{ij}\eta^{sr^{i-1}}$ for all i, j. Hence, if s is not in the group generated by $r \bmod m$, then $t_{ij} = 0$ for all i, j, and the representations F and F^s are inequivalent. On the other hand, if $s \equiv r^a \bmod m$ for some a, then setting $t_{ij} = 0$ for $i \not\equiv j + a \bmod m$, and $t_{ij} = 1$ otherwise, satisfies both the above relations and shows that F and F^s are equivalent. A similar argument applies to the equality on the right side of (19) involving τ. Thus, there are $\varphi(m)/n$ pairwise inequivalent fixed-point-free irreducible representations of $G_{m,r}$.

The value of $\zeta_{\Delta(G)}$ for the representations characterized in this section can be computed via the following lemma.

Lemma 1. *For any fixed-point-free representation $\Delta = F \uparrow G$ of $G = G_{m,r}$, we have*

$$\zeta_{\Delta(G)} = \frac{1}{2} \min_{\substack{\ell \in \{0,\ldots,m-1\} \\ k \in \{0,\ldots,n-1\} \\ (\ell,k) \neq (0,0)}} \left| \prod_{j=1}^{q} \left(1 - \eta^{\frac{k}{q}t + \ell r^{j-1}\frac{r^n-1}{r^q-1}}\right) \right|^{\frac{1}{n}}, \tag{20}$$

where $q = \gcd(n, k)$ and $\eta = \mathrm{e}^{2\pi i/m}$.

Proof. We need to compute the determinant of $I_n - (F \uparrow G)(g)$ for all $g \in G_{m,r}$ or, equivalently, the determinant of $I_n - ((F \uparrow G)(\sigma))^\ell((F \uparrow G)(\tau))^k$ for all $\ell = 0, \ldots, m-1$, $k = 0, \ldots, n-1$, such that $(\ell, k) \neq (0, 0)$. This is done using the matrix representations (18) and Lemma 6 in Appendix C. □

We now present a few examples of the fixed-point-free groups $G_{m,r}$.

Example 1 (3 antennas). *Let $n = 3$ and take $r = 4$ and $m = 21$. Then we have $r_0 = 3$, $t = 7$, $\gcd(n, t) = \gcd(3, 7) = 1$, and all prime divisors of n (i.e., the prime 3) divide r_0. Hence, $G_{21,4}$ is a fixed-point-free group. Thus, if we set $\eta = \mathrm{e}^{2\pi i/21}$, and*

$$A = \begin{pmatrix} \eta & 0 & 0 \\ 0 & \eta^4 & 0 \\ 0 & 0 & \eta^{16} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \eta^7 & 0 & 0 \end{pmatrix}.$$

then the 63 matrices $A^\ell B^k$, $\ell = 0, \ldots, 20$, $k = 0, 1, 2$, form a group under matrix multiplication. We have

$\zeta_{\Delta(G_{21,4})} \sim 0.3851$. *This* 3*-antenna,* 63*-element constellation is one element shy of having rate* $R = 2$*.*

Example 2 (9 antennas). *Let* $n = 9$ *and take* $r = 4$ *and* $m = 57$*. Then we have* $r_0 = 3$ *and* $t = 19$*,* $\gcd(n, t) = 1$*, and all prime divisors of* n *divide* r_0*. Hence* $G_{57,4}$ *is fixed-point-free. Thus, if we set* $\eta = \mathrm{e}^{2\pi i/57}$*, and*

$$A = \mathrm{diag}\,(\eta, \eta^4, \eta^{16}, \eta^7, \eta^{28}\eta^{55}, \eta^{49}, \eta^{25}, \eta^{43}), \quad B = \begin{pmatrix} 0 & I_8 \\ \eta^{19} & 0 \end{pmatrix},$$

where $\mathrm{diag}\,(a_1, \ldots, a_n)$ *denotes the diagonal matrix with diagonal entries* $a_1, \ldots, a_n$*, then the* 513 *matrices* $A^\ell B^k$*, where* $\ell = 0, \ldots, 56$*, and* $k = 0, \ldots, 8$ *form a group under matrix multiplication. We have* $\zeta_{\Delta(G_{57,4})} \sim 0.361$*. This* 9*-antenna,* 513*-element constellation exceeds rate* 1 *by one element.*

5 A classification of fixed-point-free groups

In this section we classify all fixed-point-free groups and compute all the irreducible fixed-point-free representations of these groups.

5.1 The group types

One type of fixed-point-free group is presented in Section 4.3, but there are five more types. Since the groups $G_{m,r}$ are an important part of the classification theorem, the following convention is introduced. Given a pair of integers (m, r), we implicitly define n to be the order of r modulo m; we define $r_0 = \gcd(r - 1, m)$; and $t = m/r_0$. We call the pair (m, r) *admissible*, if $\gcd(n, t) = 1$, and all prime divisors of n divide r_0. The six group types are:

1. $\boldsymbol{G_{m,r}}$ (These appear in Section 4.3.):

$$G_{m,r} = \langle \sigma, \tau \mid \sigma^m = 1, \tau^n = \sigma^t, \sigma^\tau = \sigma^r \rangle,$$

where (m, r) is admissible. The order of $G_{m,r}$ is $L = mn$.

2. $\boldsymbol{D_{m,r,\ell}}$:

$$D_{m,r,\ell} = \langle \sigma, \tau, \gamma \mid \sigma^m = 1, \tau^n = \sigma^t, \sigma^\tau = \sigma^r, \sigma^\gamma = \sigma^\ell, \tau^\gamma = \tau^\ell, \gamma^2 = \tau^{nr_0/2} \rangle,$$

where nr_0 is even, (m,r) is admissible, $\ell^2 \equiv 1 \bmod m$, $\ell \equiv 1 \bmod n$, and $\ell \equiv -1 \bmod s$, where s is the highest power of 2 dividing mn. The order of $D_{m,r,\ell}$ is $L = 2mn$.

3. $\boldsymbol{E_{m,r}}$:

$$\begin{aligned} E_{m,r} &= \langle \sigma, \tau, \mu, \gamma \mid \sigma^m = 1, \tau^n = \sigma^t, \sigma^\tau = \sigma^r, \mu^{\sigma^{m/t}} = \mu, \gamma^{\sigma^{m/t}} = \gamma, \\ &\quad \mu^4 = 1, \mu^2 = \gamma^2, \mu^\gamma = \mu^{-1}, \mu^\tau = \gamma, \gamma^\tau = \mu\gamma \rangle, \end{aligned}$$

where (m,r) is admissible, mn is odd, and nr_0 is divisible by 3. The order of $E_{m,r}$ is $8mn$.

4. $\boldsymbol{F_{m,r,\ell}}$:

$$\begin{aligned} F_{m,r,\ell} &= \langle \sigma, \tau, \mu, \gamma, \nu \mid \sigma^m = 1, \tau^n = \sigma^t, \sigma^\tau = \sigma^r, \mu^{\sigma^{m/t}} = \mu, \gamma^{\sigma^{m/t}} = \gamma, \mu^\tau = \gamma, \gamma^\tau = \mu\gamma, \\ &\quad \mu^4 = 1, \mu^2 = \gamma^2, \mu^\gamma = \mu^{-1}, \nu^2 = \mu^2, \sigma^\nu = \sigma^\ell, \tau^\nu = \tau^\ell, \mu^\nu = \gamma^{-1}, \gamma^\nu = \mu^{-1} \rangle, \end{aligned}$$

where (m,r) is admissible, mn is odd, r_0 is divisible by 3, n is not divisible by 3, $\ell^2 \equiv 1 \bmod m$, $\ell \equiv 1 \bmod n$, and $\ell \equiv -1 \bmod 3$. The order of $F_{m,r,\ell}$ is $16mn$.

5. $\boldsymbol{J_{m,r}}$:

$$J_{m,r} = \mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r},$$

where (m,r) is admissible, $\gcd(mn, 120) = 1$, and $\mathrm{SL}_2(\mathbb{F}_5)$ is the group of 2×2-matrices over $\mathbb{F}_5$ with determinant 1. $\mathrm{SL}_2(\mathbb{F}_5)$ has the generators and relations

$$\mathrm{SL}_2(\mathbb{F}_5) = \langle \mu, \gamma \mid \mu^2 = \gamma^3 = (\mu\gamma)^5, \mu^4 = 1 \rangle.$$

The order of $J_{m,r}$ is $120mn$.

6. $\boldsymbol{K_{m,r,\ell}}$:

$$K_{m,r,\ell} = \langle J_{m,r}, \nu \rangle$$

with the relations

$$\nu^2 = \mu^2, \mu^\nu = (\mu\gamma)^7(\gamma\mu)^2\gamma(\gamma\mu)^2, \gamma^\nu = \gamma, \sigma^\nu = \sigma^\ell, \tau^\nu = \tau^\ell,$$

where μ and γ are as in $\boldsymbol{J_{m,r}}$, and where $\ell^2 \equiv 1 \bmod m$, $\ell \equiv 1 \bmod n$. The order of $K_{m,r,\ell}$ is $240mn$.

We can now state our first main result.

Theorem 1. *A finite group is fixed-point-free if and only if it is isomorphic to either $G_{m,r}$, $D_{m,r,\ell}$, $E_{m,r}$, $F_{m,r,\ell}$, $J_{m,r}$, or $K_{m,r,\ell}$.*

The proof that a fixed-point-free group must be one of these types appears in Appendix A. Next, we concentrate on showing that the above groups are fixed-point-free and computing their fixed-point-free representations. In all cases, all the inequivalent irreducible representations of the same group yield the exact same set of matrices (in different order). Hence, the signal constellations produced by inequivalent representations of the same group are identical. We therefore present only one of the inequivalent representations.

Theorem 2. (1) *$G_{m,r}$ for admissible (m,r) has an irreducible n-dimensional fixed-point-free representation given by*

$$\sigma \mapsto A = \begin{pmatrix} \xi & 0 & 0 & \cdots & 0 \\ 0 & \xi^r & 0 & \cdots & 0 \\ 0 & 0 & \xi^{r^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{r^{n-1}} \end{pmatrix}, \quad \tau \mapsto B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \xi^t & 0 & 0 & \cdots & 0 \end{pmatrix},$$

and $\xi = e^{2\pi i/m}$. The corresponding constellation is given by the matrices $A^s B^k$, $s = 0, \ldots, m-1$, $k = 0, \ldots, n-1$. We note here (and omit in the remaining descriptions) that, implicitly, in this representation the matrix A becomes a scalar and B becomes undefined when $r = 1$ because $G_{m,1}$ is cyclic.

(2) *$D_{m,r,\ell}$ with admissible (m,r) has an irreducible $2n$-dimensional fixed-point-free representation given by*

$$\sigma \mapsto A \quad = \quad \begin{pmatrix} A_0 & 0 \\ 0 & A_0^\ell \end{pmatrix}, \quad A_0 = \begin{pmatrix} \xi & 0 & 0 & \cdots & 0 \\ 0 & \xi^r & 0 & \cdots & 0 \\ 0 & 0 & \xi^{r^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{r^{n-1}} \end{pmatrix},$$

$$\begin{aligned}
\tau \mapsto B &= \begin{pmatrix} B_0 & 0 \\ 0 & B_0^{\ell} \end{pmatrix}, \quad B_0 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \xi^t & 0 & 0 & \cdots & 0 \end{pmatrix}, \\
\eta \mapsto R &= \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix},
\end{aligned}$$

where $\xi = \mathrm{e}^{2\pi i/m}$. *The corresponding constellation is given by* $A^s B^k R^j$, $s = 0, \ldots, m-1$, $k = 0, \ldots, n-1$, $j = 0, 1$.

(3) $E_{m,r}$ *for admissible* (m,r) *has an irreducible* $2n$*-dimensional fixed-point-free representation given by*

$$\begin{aligned}
\sigma \mapsto A_z &= \begin{pmatrix} A_{0,z} & 0 & 0 & \cdots & 0 \\ 0 & A_{0,z}^{r} & 0 & \cdots & 0 \\ 0 & 0 & A_{0,z}^{r^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A_{0,z}^{r^{n-1}} \end{pmatrix}, \quad A_{0,z} = \frac{\mathrm{e}^{10\pi i/8}\mathrm{e}^{2\pi i z/m}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \\
\tau \mapsto B_z &= \begin{pmatrix} 0 & I_2 & 0 & \cdots & 0 \\ 0 & 0 & I_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & I_2 \\ A_{0,z}^{t} & 0 & 0 & \cdots & 0 \end{pmatrix}, \\
\mu \mapsto P &= \begin{pmatrix} F_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & F_1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & F_2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & F_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & F_{(n-1 \bmod 3)} \end{pmatrix},
\end{aligned}$$

$$\gamma \mapsto Q = \begin{pmatrix} F_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & F_2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & F_0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & F_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & F_{(n \bmod 3)} \end{pmatrix},$$

$$F_0 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad F_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

where $z = 1$ if 9 divides m, and $z = 3$ otherwise. The corresponding constellation is given by $A_z^s B_z^k P^j Q^p$, $s = 0, \ldots, m-1$, $k = 0, \ldots, n-1$, $j = 0, \ldots, 3$, $p = 0, 1$.

(4) *If $n > 1$ or $\ell \not\equiv 1 \bmod (m/3)$, then $F_{m,r,\ell}$ with admissible (m,r) has an irreducible $4n$-dimensional representation given by*

$$\sigma \mapsto A = \begin{pmatrix} A_z & 0 \\ 0 & A_z^\ell \end{pmatrix}, \qquad \tau \mapsto B = \begin{pmatrix} B_z & 0 \\ 0 & B_z^\ell \end{pmatrix}$$
$$\mu \mapsto P = \begin{pmatrix} P & 0 \\ 0 & Q^{-1} \end{pmatrix}, \qquad \gamma \mapsto Q = \begin{pmatrix} Q & 0 \\ 0 & P^{-1} \end{pmatrix},$$
$$\nu \mapsto R = \begin{pmatrix} 0 & I_{2n} \\ -I_{2n} & 0 \end{pmatrix},$$

where A_z, B_z, P, Q are the matrices defined for the group $E_{m,r}$, and $z = 1$ if 9 divides m, and $z = 3$ otherwise. If $r = 1$ and $\ell \equiv 1 \bmod (m/3)$, then $F_{m,1,\ell}$ has an irreducible 2-dimensional fixed-point-free representation given by

$$\sigma \mapsto A = A_{0,3}, B = I_2, \quad \mu \mapsto P = F_0, \quad \gamma \mapsto Q = F_1, \quad \nu \mapsto R = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \\ -1 & i \end{pmatrix},$$

where $A_{0,3}$, F_0, and F_1 are the matrices defined for $E_{m,r}$. The corresponding constellation is given by $A^s B^k P^j Q^p R^q$, where $s = 0, \ldots, m-1$, $k = 0, \ldots, n-1$, $j = 0, \ldots, 3$, $p = 0, 1$, $q = 0, 1$.

(5) *$J_{m,r}$ has an irreducible $2n$-dimensional fixed-point-free representation given by*

$$
\begin{aligned}
\sigma \mapsto A &= I_2 \otimes \begin{pmatrix} \xi & 0 & 0 & \cdots & 0 \\ 0 & \xi^r & 0 & \cdots & 0 \\ 0 & 0 & \xi^{r^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{r^{n-1}} \end{pmatrix}, \\
\tau \mapsto B &= I_2 \otimes \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \xi^t & 0 & 0 & \cdots & 0 \end{pmatrix}, \\
\mu \mapsto P &= P_0 \otimes I_n, \quad P_0 = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^2 - \eta^3 & \eta - \eta^4 \\ \eta - \eta^4 & \eta^3 - \eta^2 \end{pmatrix}, \\
\gamma \mapsto Q &= Q_0 \otimes I_n, \quad Q_0 = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta - \eta^2 & \eta^2 - 1 \\ 1 - \eta^3 & \eta^4 - \eta^3 \end{pmatrix},
\end{aligned}
$$

where $\eta = e^{2\pi i/5}$, $\xi = \mathrm{e}^{2\pi i/m}$, and $\otimes$ denotes Kronecker-product. The corresponding constellation consists of the matrices $A^sB^k(PQ)^jX$, $s = 0,\ldots,m-1$, $k = 0,\ldots,n-1$, $j = 0,\ldots,9$, and X runs over the set $\{I_{2n}$, P, Q, QP, QPQ, $QPQP$, QPQ^2, $QPQPQ$, $QPQPQ^2$, $QPQPQ^2P$, $QPQPQ^2PQ$, $QPQPQ^2PQP\}$.

(6) *$K_{m,r,\ell}$ has an irreducible $4n$-dimensional fixed-point-free representation given by*

$$
\sigma \mapsto A = \begin{pmatrix} A_0 & 0 \\ 0 & A_0^\ell \end{pmatrix}, \quad A_0 = I_2 \otimes \begin{pmatrix} \xi & 0 & 0 & \cdots & 0 \\ 0 & \xi^r & 0 & \cdots & 0 \\ 0 & 0 & \xi^{r^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{r^{n-1}} \end{pmatrix},
$$

$$\begin{aligned}
\tau \mapsto B &= \begin{pmatrix} B_0 & 0 \\ 0 & B_0^{\ell} \end{pmatrix}, \quad B_0 = I_2 \otimes \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \xi^t & 0 & 0 & \cdots & 0 \end{pmatrix}, \\
\mu \mapsto P &= \begin{pmatrix} P_0 & 0 \\ 0 & \tilde{P}_0 \end{pmatrix} \otimes I_n, \quad P_0 = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^2 - \eta^3 & \eta - \eta^4 \\ \eta - \eta^4 & \eta^3 - \eta^2 \end{pmatrix}, \quad \tilde{P}_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\
\gamma \mapsto Q &= \begin{pmatrix} Q_0 & 0 \\ 0 & Q_0 \end{pmatrix} \otimes I_n, \quad Q_0 = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta - \eta^2 & \eta^2 - 1 \\ 1 - \eta^3 & \eta^4 - \eta^3 \end{pmatrix}, \\
\nu \mapsto R &= \begin{pmatrix} 0 & I_{2n} \\ -I_{2n} & 0 \end{pmatrix},
\end{aligned}$$

where $\eta = e^{2\pi i/5}$, $\xi = \mathrm{e}^{2\pi i/m}$, and $\otimes$ denotes Kronecker-product. The corresponding constellation is given by $A^s B^k (PQ)^j X R^p$, $s = 0, \ldots, m-1$, $k = 0, \ldots, n-1$, $j = 0, \ldots, 9$, $p = 0, 1$, and X runs over the set $\{I_{4n}$, P, Q, QP, QPQ, $QPQP$, QPQ^2, $QPQPQ$, $QPQPQ^2$, $QPQPQ^2P$, $QPQPQ^2PQ$, $QPQPQ^2PQP\}$.

A proof of this theorem can be found in Appendix B. Table 2 summarizes the results of this section. The first column indicates the type of the group, the second its order, and the third the dimension of its representation.

Remark 1. *Theorems 8 and 16 in Zassenhaus' paper [12] classify the fixed-point-free groups. Although the proof techniques in the paper are novel and essentially correct, the final assertions contain errors and shortcomings which make them unsuitable for the present application. For instance, Zassenhaus' classification does not cover the groups $D_{m,r,\ell}$ for odd n, nor does it cover some subtypes of the groups $E_{m,r}$ and $F_{m,r,\ell}$. The explicit description of the groups in Part (E) of Theorem 7 on page 203 of [12] appears to be incorrect, since $R^2 = P$ (in his terminology) and $RAR^{-1} = A^{\ell}$ are incompatible requirements. Furthermore, only necessary conditions are proven for a group to be fixed-point-free, although it is hinted that these necessary conditions are also sufficient.*

Despite these shortcomings, we emphasize that our classification closely follows Zassenhaus' elegant techniques and would not have been possible without his work.

	Group type	L	M	Comments
1.	$G_{m,r}$	mn	n	
2.	$D_{m,r,\ell}$	$2mn$	$2n$	
3.	$E_{m,r}$	$8mn$	$2n$	
4.	$F_{m,r,\ell}$	$16mn$	$4n$	if $n > 1$ or $\ell \not\equiv 1 \bmod m/3$
	$F_{m,1,\ell}$	$16mn$	2	if $\ell \equiv 1 \bmod m/3$
5.	$J_{m,r}$	$120mn$	$2n$	
6.	$K_{m,r,\ell}$	$240mn$	$4n$	

Table 2: There are 6 types of fixed-point-free groups: For each group G, L is the order of G (the size of the constellation) and M is the dimension of the representation of G (number of transmitter antennas).

6 Consequences of the classification for $M = 2$ and M odd

We present some immediate consequences of the main classification theorem.

The most elementary consequence (that we already know from Section 4.2) is that cyclic groups are fixed-point-free, because in our classification a cyclic group of order m corresponds to $G_{m,1}$: in this case $n = 1$ because the order of $1 \bmod m$ is 1.

A class of fixed-point-free groups that appears in [9] as a constellation for differential multiple antenna modulation is the generalized quaternion groups, reviewed in Section 3 and defined as

$$Q_p = \langle \sigma, \eta \mid \sigma^{2^p} = 1, \eta^2 = \sigma^{2^{p-1}}, \sigma^\eta = \sigma^{-1} \rangle.$$

In our classification, we have $Q_p = D_{2^p,1,-1}$. In [9] it is proved that if G is a fixed-point-free group that has 2^{p+1} elements for some integer p, and has a fixed-point-free representation of dimension 2, then G is either cyclic or a generalized quaternion group (also called a “dicyclic group” in that paper). This theorem is actually quite old, going back to Burnside [11] in a more general form (see Theorem 7 in Appendix A). It is also consistent with our classification, and we may make a stronger conclusion: assume only that G is a fixed-point-free group of order 2^{p+1} (do not impose any restriction on the dimension of its representation); then G is either a $G_{m,r}$ or a $D_{m,r,\ell}$. (It cannot be of the $E_{m,r}$ or $F_{m,r,\ell}$ types since they require that mn be odd, which contradicts the assumption that the number of elements, $8mn$ and $16mn$ be powers of two. It also cannot be $J_{m,r}$ or $K_{m,r,\ell}$ since the number of elements, $120mn$ and $240mn$ can never be powers of 2.) If $G = G_{m,r}$, then mn has to be a power of 2. Suppose both m and n are even. Then, since $\gcd(t, n) = 1$, t must be odd. But since $t = \gcd(r - 1, m)$, this can only happen if $r - 1$ is odd. This, on the other hand, contradicts $r^n \equiv 1 \bmod (m)$ since both r and m are even. Thus, m and n cannot be simultaneously even, and so either $m = 1$, or $n = 1$. Since $m = 1$ contradicts the admissibility of (m, r) (all prime divisors of n have to divide r_0 and hence m), this implies that $n = 1$. This means that G is cyclic.

If $G = D_{m,r,\ell}$, then $n = 1$ and $m = 2^p$, hence $\ell \equiv -1 \bmod m$, which shows that G is a generalized quaternion group and therefore has a 2-dimensional irreducible representation. Note that we did not need to assume anything about the dimension of the representation for G; the dimension came as a conclusion.

Our classification shows that all non-Abelian fixed-point-free groups of order 2^p have their irreducible fixed-point-free representations in two dimensions. Because it is often practical to use two transmitter antennas, one may ask more generally for a classification of all fixed-point-free groups whose irreducible fixed-point-free representations are 2-dimensional. The following result answers this question.

Theorem 3. *Any fixed-point-free group that has an irreducible 2-dimensional fixed-point-free representation is isomorphic to one of the following:*

1) $G_{m,r}$ *such that (m, r) is admissible and the order of r modulo m is 2.*

2) $D_{m,1,\ell}$.

3) $E_{m,1}$.

4) $F_{m,1,\ell}$ *for* $\ell \equiv 1 \bmod m/3$.

5) $J_{m,1}$.

Conversely, any of these groups has an irreducible 2-dimensional fixed-point-free representation.

Proof. The proof follows by noting that n, the order of r modulo m, is 1 if and only if $r = 1$, and comparing with Table 2. □

Using the classification in this paper, we can also produce constellations for an odd number of antennas M.

Theorem 4. *Any group with a fixed-point-free representation of odd dimension M is isomorphic to $G_{m,r}$ for some admissible (m, r).*

Proof. If G has a fixed-point-free representation Δ of odd dimension, then it has an irreducible fixed-point-free representation. Since all irreducible fixed-point-free representations of G have the same dimension d (see Table 2), the dimension of Δ is a multiple of d. Hence, if the dimension of Δ is odd, then d must be odd. It therefore suffices to consider only groups G that have an irreducible fixed-point-free representation of odd dimension. A look at Table 2 reveals that G has to be isomorphic to $G_{m,r}$. □

7 Some explicit simple constellations

In this section we produce simple examples of some of the classes of fixed-point-free groups. For reasons of simplicity, we will identify the groups with images of their fixed-point-free representations computed in the pervious sections, and list the group elements as matrices.

Using Theorem 3, we start with groups that have an irreducible fixed-point-free representation for $M = 2$ transmitter antennas.

1. The smallest example of a $G_{m,r}$ having a 2-dimensional irreducible fixed-point-free representation is $G_{6,-1}$. The corresponding constellation consists of the 12 matrices $A^s B^k$, $s = 0, \dots, 5$, $k = 0, 1$, where
$$A = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$
and $\xi = \mathrm{e}^{2\pi i/6}$. Its rate is $R = \log(12)/2 = 1.79$, and its diversity product is $\zeta_{G_{6,-1}} = 0.5$. This value for ζ is not particularly impressive because, as we see from Table 1, the orthogonal designs (although they are not a group) have the same ζ, but with $R = 2$.

2. The smallest example of the group $D_{m,1,\ell}$ is the quaternion group $Q_2 = D_{4,1,-1}$ of order 8 given as the set of matrices $P^j Q^p$, $j = 0, \dots, 3$, $p = 0, 1$, where
$$P = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$
We have $\zeta_{Q_2} = \sqrt{2}/2 \approx 0.7071$. This group appears in Table 1.

3. The smallest example of a group $E_{m,1}$ is the group $E_{3,1}$ of order 24. This group is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$ [12], the group of two-dimensional matrices over $\mathbb{F}_3$ with determinant 1. The constellation is

given by the 24 matrices $A^s P^j Q^p$, where $s = 0, 1, 2$, $j = 0, \dots, 3$, $p = 0, 1$, and

$$A = \frac{\mathrm{e}^{10\pi i/8}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -1 \end{pmatrix}, \quad P = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Its rate is $R = 2.29$, and $\zeta_{E_{3,1}} = 0.5$, which outperforms all constellations with $R \geqslant 2$ in Table 1.

4. The smallest example of a group $F_{m,1,\ell}$ is the group $F_{3,1,-1}$ which has 48 elements. It consists of the matrices $A^s P^j Q^p R^q$, where $s = 0, 1, 2$, $j = 0, \dots, 3$, $p = 0, 1$, $q = 0, 1$, and A, P, Q are as above while

$$R = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \\ -1 & i \end{pmatrix}.$$

Because $n = 1$, the matrix B does not appear. The constellation has rate $R = 2.79$, and $\zeta_{F_{3,1,-1}} = \sqrt{2 - \sqrt{2}}/2 \approx 0.3868$.

5. The smallest example of $J_{m,r}$ is $J_{1,1}$ which is isomorphic to $\mathrm{SL}_2(\mathbb{F}_5)$. This constellation has 120 elements given by the matrices $(PQ)^j X$, where $j = 0, \dots, 9$, X runs over the set $\{I_2, P, Q, QP, QPQ, QPQP, QPQ^2, QPQPQ, QPQPQ^2, QPQPQ^2P, QPQPQ^2PQ, QPQPQ^2PQP\}$, and

$$P = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^2 - \eta^3 & \eta - \eta^4 \\ \eta - \eta^4 & \eta^3 - \eta^2 \end{pmatrix}, \quad Q = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta - \eta^2 & \eta^2 - 1 \\ 1 - \eta^3 & \eta^4 - \eta^3 \end{pmatrix},$$

where $\eta = \mathrm{e}^{2\pi i/5}$. It has rate $R = 3.45$, and $\zeta_{\mathrm{SL}_2(\mathbb{F}_5)} = \frac{1}{2}\sqrt{(3 - \sqrt{5})/2} \approx 0.3090$. This group performs remarkably, as described in Section 9.

6. The simplest example of a fixed-point-free group with irreducible fixed-point-free representations for $M = 3$ is the group $G_{21,3}$ described in Section 4.3.

7. The smallest example of a fixed-point-free group with an irreducible 4-dimensional fixed-point-free representation is $D_{6,-1,-1}$. It has 24 elements, with rate $R = \log(24)/4 = 1.15$, and $\zeta_{D_{6,-1,-1}} = 0.5$. This performance is not very impressive since the group $K_{1,1,-1}$ with $L = 240$ elements (rate $R = 1.98$) has $\zeta_{K_{1,1,-1}} = 0.5$. The elements of this constellation are given by $(PQ)^j X R^p$, where

$j = 0, \ldots, 9$, $p = 0, 1$, X runs over the same set as in 5), but with

$$P = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^2 - \eta^3 & \eta - \eta^4 & 0 & 0 \\ \eta - \eta^4 & \eta^3 - \eta^2 & 0 & 0 \\ 0 & 0 & 0 & -\sqrt{5} \\ 0 & 0 & \sqrt{5} & 0 \end{pmatrix},$$

$$Q = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta - \eta^2 & \eta^2 - 1 & 0 & 0 \\ 1 - \eta^3 & \eta^4 - \eta^3 & 0 & 0 \\ 0 & 0 & \eta - \eta^2 & \eta^2 - 1 \\ 0 & 0 & 1 - \eta^3 & \eta^4 - \eta^3 \end{pmatrix},$$

$$R = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

We defer a detailed description of the performance of these multiple-antenna constellations until Section 9.

8 Group-inspired constellations

Theorems 1 and 2 are key because they allow us to compute all fixed-point-free groups of finite order. For many combinations of M and R these groups result in constellations with excellent ζ and performance, as shown in Section 9. For other combinations of M and R, groups with irreducible fixed-point-free representations do not exist, especially when M is large and odd. We can consider reducible representations, but then the groups can have large cyclic components and sparse matrix representations, which do not necessarily perform well. For example, Theorem 1 shows that it is not possible to construct irreducible constellations with $R \approx 1$ for matrix dimensions $M = 5$ and $M = 7$, since there exist no irreducible fixed-point-free group representations for $M = 5$ with $L \approx 32$, or $M = 7$ with $L \approx 128$.

To construct constellations for arbitrary M and R, it appears that we need to consider also nongroups. We are therefore once again considering the problem of constructing an L-element set of $M \times M$ unitary matrices with large ζ—but we do not start from scratch. We show how the group constellations can suggest simple nongroup constellations that perform well.

We consider three specific structures. The first, called Hamiltonian constellations, works only for $M = 2$ and has some similarities with the orthogonal designs described in Section 2. These exist for any rate R. The second is a nongroup generalization of the group $G_{m,r}$. These yield constellations, for arbitrary M and R that effectively boost the size of any diagonal constellation by the factor M without decreasing ζ. The rate of the diagonal constellation is increased by $\frac{\log M}{M}$. The third is a constellation based on the matrix product of two different representations of any finite fixed-point-free group. This doubles the rate of the constellation and appears to yield excellent high rate constellations. These three constructions just scratch the surface of the problem of designing nongroup constellations from groups.

8.1 Hamiltonian constellation

A Hamiltonian constellation is defined to be a set of 2×2 unitary matrices that can be built from points on the unit sphere in $\mathbf{R}^4$. We start with the parameterization of a 2×2 unitary matrix

$$\mathcal{H}(x, y) = \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}.$$

where $x, y \in \mathbf{C}$ and $|x|^2 + |y|^2 = 1$. Unlike with orthogonal designs, the constraint $|x| = |y|$ is not imposed. These matrices form the (infinite) group of Hamiltonian quaternions of norm 1. The pairwise diversity product between two such matrices is given by

$$\zeta(\mathcal{H}(x, y), \mathcal{H}(x', y')) = \frac{1}{2}\sqrt{|x - x'|^2 + |y - y'|^2}. \tag{21}$$

Consider the natural embedding of $\mathbf{C}^2$ in $\mathbf{R}^4$. Then (x, y) and (x', y') are points on the unit sphere in $\mathbf{R}^4$ and the pairwise diversity product between $\mathcal{H}(x, y)$ and $\mathcal{H}(x', y')$ is simply one half their Euclidean distance. The Hamiltonian constellation is formed by building the unitary matrices from a set of points on the sphere in $\mathbf{R}^4$. It immediately follows that the behavior of the diversity product for the Hamiltonian constellation is given by

$$\zeta(\mathcal{V}_{\mathcal{H}}) = O(L^{-1/3})$$

for large L. If we impose the constraint $|x| = |y|$, we are effectively restricted to a two-dimensional torus, and the asymptotic behavior of the orthogonal design (OD) is given in (12):

$$\zeta(\mathcal{V}_{\mathrm{OD}}) = \frac{\sin(\pi/\sqrt{L})}{\sqrt{2}} = O(L^{-1/2}) < \zeta(\mathcal{V}_{\mathcal{H}}).$$

Hence, for large rates orthogonal designs underperform Hamiltonian constellations.

Some references for large-minimum-distance packings of points on a sphere in $\mathbf{R}^4$ include [18, 19]. Any of the packings immediately builds a Hamiltonian constellation. Thus Hamiltonian constellations essentially exist for any rate. The Hamiltonian constellations, like the orthogonal designs, in general do not form a group. The only exceptions are the ones mentioned in Theorem 3.

Decoding Hamiltonian constellations is simple because we need to choose a point from our constellation with least Euclidean distance in $\mathbf{R}^4$ from our measurement. Given that the points are well separated, a standard technique such as bucketing [20] does this in constant time as a function of the rate R.

8.2 Nongroup generalization of $G_{m,r}$

As shown in Theorem 2, the group $G_{m,r}$ has a fixed-point-free representation of dimension n, where n is the order of r modulo m. We now let n be arbitrary, and let η and β be primitive mth and sth roots of unity, and let $u_1, \ldots, u_n$ be integers. Consider the $n \times n$ matrices

$$A = \begin{pmatrix} \eta^{u_1} & 0 & \cdots & 0 \\ 0 & \eta^{u_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \eta^{u_n} \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \beta & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{22}$$

and the set $\mathcal{S}_{m,s}$ consisting of the matrices $A^\ell B^k$ where $\ell = 0, \ldots, m-1$ and $k = 0, \ldots, p-1$, where $p = \min(s, n)$. Note that if we take $u_i = r^{i-1}$, for $i = 0, \ldots, n-1$, and $s = \gcd(r-1, m) \geqslant n$, where (m, r) is any admissible pair, then we obtain the group $G_{m,r}$. In general, the set $\mathcal{S}_{m,s}$ is not a group. Nonetheless, the structure of $\mathcal{S}_{m,s}$ allows ζ to be computed in closed-form. We can therefore determine whether the resulting constellation is fully diverse or not.

Since the matrices A and B are unitary, it follows that

$$\left|\det\left(A^{\ell_1}B^{k_1}-A^{\ell_2}B^{k_2}\right)\right| = \left|\det\left(A^{\ell_1-\ell_2}-B^{k_2-k_1}\right)\right| = \left|\det\left(I-A^{\ell_2-\ell_1}B^{k_2-k_1}\right)\right|.$$

Furthermore, since the matrices $I_n, A, \ldots, A^{m-1}$ form a group, $\zeta_{\mathcal{S}}$ is given by

$$\zeta_{\mathcal{S}} = \frac{1}{2} \min_{\substack{\ell=0,\ldots,m-1\\ k=-p+1,\ldots,p-1\\ (\ell,k)\neq(0,0)}} \left|\det\left(I_n - A^{\ell}B^{k}\right)\right|^{\frac{1}{n}}.$$

For $0 \leqslant k < p$, we have

$$B^k = \begin{pmatrix} 0_{(n-k)\times k} & I_{(n-k)\times(n-k)} \\ \beta I_{k\times k} & 0_{k\times(n-k)} \end{pmatrix},$$

and for $-p < -k \leqslant 0$,

$$B^{-k} = \beta^{-1}B^{n-k}$$

since $B^kB^{n-k} = \beta I_n$. Thus, for $0 \leqslant k < p$, we may write

$$\begin{aligned} \det\left(I_n - A^{\ell}B^{k}\right) &= \det\left(I_n - \begin{pmatrix} 0_{(n-k)\times k} & \operatorname{diag}\left(\eta^{lu_1},\ldots,\eta^{lu_{n-k}}\right) \\ \operatorname{diag}\left(\beta\eta^{lu_{n-k+1}},\ldots,\beta\eta^{lu_n}\right) & 0_{k\times(n-k)} \end{pmatrix}\right) \\ &= \prod_{j=1}^{q}\left(1-\beta^{\frac{k}{q}}\eta^{l\sum_{i=0}^{\frac{n}{q}-1}u_{iq+j}}\right), \quad q = \gcd(n, n-k) = \gcd(n,k) \end{aligned}$$

and, for $-p < -k \leqslant 0$,

$$\begin{aligned} \det\left(I_n - A^{\ell}B^{k}\right) &= \det\left(I_n - \begin{pmatrix} 0_{k\times(n-k)} & \operatorname{diag}\left(\beta^{-1}\eta^{lu_1},\ldots,\beta^{-1}\eta^{lu_k}\right) \\ \operatorname{diag}\left(\eta^{u_{k+1}},\ldots,\eta^{u_n}\right) & 0_{(n-k)\times k} \end{pmatrix}\right) \\ &= \prod_{j=1}^{q}\left(1-\beta^{-\frac{k}{q}}\eta^{l\sum_{i=0}^{\frac{n}{q}-1}u_{iq+j}}\right), \end{aligned}$$

where in the second step of both equalities we have used Lemma 6 in Appendix C.

We thus have the following result.

Lemma 2 (ζ for $\mathcal{S}_{m,s}$). *Let η and β be primitive m-th and s-th roots of unity, respectively, and let $u_1, \ldots, u_n$ be integers. Denote by $\mathcal{S}_{m,s}$ the set of matrices $A^{\ell}B^{k}$ where $\ell = 0, \ldots, m-1$, $k = 0, \ldots, p-1$ and*

$p = \min(s, n)$*, with* A *and* B *given by (22). Then*

$$\zeta_{\mathcal{S}} = \frac{1}{2} \min_{\substack{\ell=0,\ldots,m-1 \\ k=-p+1,\ldots,p-1 \\ (\ell,k)\neq(0,0)}} \left| \prod_{j=1}^{q} \left(1 - \beta^{\frac{k}{q}} \eta^{l} \textstyle\sum_{i=0}^{\frac{n}{q}-1} u_{iq+j} \right) \right|^{\frac{1}{n}}, \tag{23}$$

where $q = \gcd(n, |k|)$.

Remarks

1. The nongroup constellation $\mathcal{S}_{m,s}$ has $L = mp$ elements. From (9), we observe that for a general nongroup constellation, ζ is the minimum of $L(L-1)/2$ pairwise distances between the elements of the constellation. However, (23) shows that $\mathcal{S}_{m,s}$ has at most $m(2p-1) = 2L - m$ distinct pairwise differences. Hence, even though $\mathcal{S}_{m,s}$ is not necessarily a group, it exhibits a considerable amount of symmetry. Compare the maximum of $2L - m$ pairwise distances with the maximum of $L - 1$ distances found in a group.

2. Lemma 2 allows us to construct constellations for any number of antennas M and any target rate $R = \frac{1}{M} \log L$. We need only to set $M = n$ and decompose L as $L = mp$, with $p \leqslant n$, and then use equation (23) to maximize the value of $\zeta_{\mathcal{S}}$ by performing a search over the integers $u_1, \ldots, u_n$ (all of which lie between 0 and $n-1$) and $s \leqslant p$. In practice, one can always take $p = n$.

3. Note that we may write (23) more explicitly as

$$\zeta_{\mathcal{S}} = \frac{1}{2} \min_{\substack{\ell=0,\ldots,m-1 \\ k=-p+1,\ldots,p-1 \\ (\ell,k)\neq(0,0)}} \begin{cases} \left| \prod_{j=1}^{n} \left(1 - \eta^{\ell u_j}\right) \right|^{\frac{1}{n}} & k = 0 \\ \left| \prod_{j=1}^{q} \left(1 - \beta^{\frac{k}{q}} \eta^{\ell} \textstyle\sum_{i=0}^{\frac{n}{q}-1} u_{iq+j} \right) \right|^{\frac{1}{n}} & 0 < |k| < p \end{cases}. \tag{24}$$

   The expression for $k = 0$ is the ζ for a diagonal constellation with $u_1, \ldots, u_n$ (see Sec. 4.2). Thus, if

$$\min_{\ell=0,\ldots,m-1} \left| \prod_{j=1}^{n} \left(1 - \eta^{\ell u_j}\right) \right|^{\frac{1}{n}} \leqslant \min_{\substack{\ell=0,\ldots,m-1 \\ k=-p+1,\ldots,p-1 \\ (\ell,k)\neq(0,0)}} \left| \prod_{j=1}^{q} \left(1 - \beta^{\frac{k}{q}} \eta^{\ell} \textstyle\sum_{i=0}^{\frac{n}{q}-1} u_{iq+j} \right) \right|^{\frac{1}{n}},$$

   then $\zeta_{\mathcal{S}}$ is determined by the ζ of the diagonal constellation. Since this can often be arranged by choosing β appropriately, we conclude that with our construction it is possible to boost the size of the diagonal constellation $\{A^{\ell}\}$ by the factor n while keeping ζ unchanged. This is effectively done by post-multiplying the constellation by B^k.

4. When n is prime, the expressions simplify considerably since $q = n$ when $k = 0$, and $q = 1$ otherwise. In this case, (24) reduces to

$$\zeta_{\mathcal{S}} = \frac{1}{2} \min_{\substack{\ell=0,\ldots,m-1 \\ k=-p+1,\ldots,p-1 \\ (\ell,k)\neq(0,0)}} \left\{ \begin{array}{ll} \left|\prod_{j=1}^{n} \left(1 - \eta^{\ell u_j}\right)\right|^{\frac{1}{n}} & k = 0 \\ \left|1 - \beta^k \eta^{\ell \sum_{i=0}^{n-1} u_{i+1}}\right|^{\frac{1}{n}} & 0 < |k| < p \end{array} \right. . \qquad (25)$$

This expression simplifies further if we assume

$$\sum_{i=0}^{n-1} u_{i+1} \equiv 0 \mod m, \qquad (26)$$

in which case

$$\zeta_{\mathcal{S}} = \frac{1}{2} \left[\min \left(\min_{0<|k|<p} \left|1 - \beta^k\right|, \min_{0<\ell<m} \left| \prod_{j=1}^{n} \left(1 - \eta^{\ell u_j}\right) \right| \right) \right]^{\frac{1}{n}} . \qquad (27)$$

The first of the above expressions depends only on β, while the second depends only on η. Thus, it is always possible to choose β so that the minimum is provided by the second term and the constellation inherits the same ζ as a diagonal constellation with m elements.

We have observed that the constraint (26), does not affect the performance of the diagonal constellation adversely. Therefore, in searching for good constellations we have found this constraint useful, even for nonprime n.

5. The increase in the constellation size by the factor $n = M$ over the diagonal constellation increases the rate by $\frac{1}{M} \log M$.

8.3 Products of group representations

The constellations described above have the advantage that they can be constructed for any M and $R = \frac{1}{M} \log L$, and that they are M times larger than an equivalent diagonal constellation. However, the matrices in the constellations are sparse (only one transmit antenna is active at any given time). We seek constellations that achieve better performance at high rates by employing more "full" matrices.

As has been noted earlier, one reason why the group constellations have excellent performance is that, because of their symmetry, they reduce the $L(L-1)/2$ pairwise distances between the elements of the constellation to at most $L-1$ distinct distances. Since our performance measure ζ is the minimum of these pairwise distances, the group is likely to have a larger minimum distance, all other properties being equal.

Therefore, although we shall relax the group requirement, we will still insist that the constellation exhibit symmetries with respect to the ζ cost. Thus, consider two fixed-point-free groups, $\mathcal{G}_A$ and $\mathcal{G}_B$, and let $\mathcal{V}_A = \{A_1, \ldots, A_{L_A}\}$ and $\mathcal{V}_B = \{B_1, \ldots, B_{L_B}\}$ be $M \times M$ unitary representations of these groups. Assume that $A_0 = B_0 = I$.

Consider the set of pairwise products

$$\mathcal{S}_{A,B} = \{A_j B_k,\, j = 1, \ldots, L_A,\, k = 1, \ldots, L_B\}\,. \tag{28}$$

Clearly, $\mathcal{S}_{A,B}$ has at most $L = L_A L_B$ distinct elements. This results in a constellation of rate at most $R = R_A + R_B$, where $R_A = (1/M)\log L_A$ and $R_B = (1/M)\log L_B$. The diversity product for this set is

$$\begin{aligned}
\zeta_{\mathcal{S}} &= \frac{1}{2}\min_{(j,k)\neq(j',k')}\left|\det\left(A_j B_k - A_{j'} B_{k'}\right)\right|^{\frac{1}{M}} \\
&= \frac{1}{2}\min_{(j,k)\neq(j',k')}\left|\det\left(A_{j'}^{-1} A_j - B_{k'} B_k^{-1}\right)\right|^{\frac{1}{M}} \qquad (A_{j'} \text{ and } B_k \text{ are unitary}) \\
&= \frac{1}{2}\min_{(\ell,\ell')\neq(0,0)}\left|\det\left(A_\ell - B_{\ell'}\right)\right|^{\frac{1}{M}} \qquad (\mathcal{G}_A \text{ and } \mathcal{G}_B \text{ are groups})
\end{aligned}$$

One concludes that even though $\mathcal{S}_{A,B}$ is not necessarily a group, it has the desirable property of having at most $L-1$, rather than $L(L-1)/2$, distinct pairwise distances. In particular, $\zeta_{\mathcal{S}}$ depends only on the "co-distance" between the elements of the constellations $\mathcal{V}_A$ and $\mathcal{V}_B$.

It remains to choose the constellations $\mathcal{V}_A$ and $\mathcal{V}_B$. Assume $\mathcal{G}_A = \mathcal{G}_B$; we are therefore doubling the rate of the original group constellation. The case where $\mathcal{G}_A \neq \mathcal{G}_B$ can be treated in a similar fashion and is omitted for brevity. We also assume that $\mathcal{V}_A$ and $\mathcal{V}_B$ are equivalent representations, i.e., there exists a unitary matrix T such that

$$B_j = T A_j T^*, \quad j = 1, \ldots L_A. \tag{29}$$

In particular,

$$\zeta_{\mathcal{S}} = \frac{1}{2}\min_{(j,k)\neq(0,0)}\left|\det\left(A_j - T A_k T^*\right)\right|^{\frac{1}{M}}\,. \tag{30}$$

By letting $A_0 = I_n$ we see that for $\zeta_{\mathcal{S}}$ to be nonzero the group $\mathcal{G}_A$ must be fixed-point-free. Thus, we may use any of the groups of Theorem 1 as a candidate for $\mathcal{G}_A$. However, the next result shows that the only representations of $\mathcal{G}_A$ that can lead to a nonzero $\zeta_{\mathcal{S}}$ are *reducible* representations.

Theorem 5 (Products of Group Representations). *Let $\mathcal{V}_A = \{A_j\}$ be an M-dimensional representation of the fixed-point-free finite group $\mathcal{G}_A$. Assume that there exists some unitary T such that*

$$\zeta_{\mathcal{S}} = \frac{1}{2} \min_{(j,k)\neq(0,0)} |\det(A_j - TA_kT^*)|^{\frac{1}{M}} > 0.$$

Then the representation $\mathcal{V}_A$ must be reducible, and $|\mathcal{G}_A|$ must be odd.

Proof: Note that if the representation $\{A_j\}$ has an element that is a scalar, i.e., $A_j = e^{i\alpha}I$ for some j and $\alpha \neq 0$, then $\zeta_{\mathcal{S}}$ must be zero since

$$A_j - TA_jT^* = e^{i\alpha}I - e^{i\alpha}TT^* = 0,$$

for any unitary T. We show that the fixed-point-free representations of Theorem 2, all of which are irreducible representations, have scalar elements. In addition, we show that if the group has even order, then *all* irreducible fixed-point-free representations of the group contain the negative of the identity matrix. Thus, any representation that leads to a nonzero $\zeta_{\mathcal{S}}$ must be reducible, and the size of the group must be odd. In the following, I will denote an identity matrix of appropriate dimension.

1. $G_{m,r}$: We show that A^t is scalar. Note that $G_{m,1}$ is cyclic, since the smallest integer n such that $r^n = 1^n \equiv 1 \bmod m$ is $n = 1$, and all one-dimensional fixed-point-free groups are cyclic. Moreover, all elements of its representation are scalar and so $\zeta_{\mathcal{S}}$ is zero. Thus, let $r > 1$ and $n > 1$. Since all prime divisors of n must divide $r_0 = \text{gcd}(m, r-1)$, we conclude that $r_0 > 1$ and $t = m/r_0 < m$. Now

$$A^t = \text{diag}(\eta^t, \eta^{rt}, \ldots, \eta^{r^{n-1}t}) = \text{diag}(\eta^t, \eta^{(r-1)t+t}, \ldots, \eta^{(r^{n-1}-1)t+t}).$$

   But for all $k = 1, \ldots n-1$, the quantity $(r^k - 1)t$ is a multiple of m because

$$(r^k - 1)t = (r^{k-1} + \ldots + 1)(r-1)t = (r^{k-2} + \ldots + 1)\frac{r-1}{r_0}r_0t = (r^{k-1} + \ldots + 1)\frac{r-1}{r_0}m,$$

   and hence $\eta^{(r^k-1)t} = 1$. Therefore $A^t = \eta^t I$. Furthermore, if mn is even, then m is even since (m, r) is admissible. In that case $A^{m/2} = \eta^{m/2}I = -I$ for any choice of η as a primitive mth root of unity.

2. $D_{m,r,\ell}$: We show that $A^{m/2} = -I$. We first assert that $r_0 = \gcd(r-1, m)$ is even. Since nr_0 must be even, this is true when n is odd. It is also true when n is even since all prime divisors of n must divide r_0. Thus, $m = r_0t$ must also be even. On the other hand, ℓ must be odd, since $\ell^2 \equiv 1 \bmod m$. Consider

now $A^{m/2} = \text{diag}(A_0^{m/2}, A_0^{\ell m/2})$. Since m is the smallest integer, such that $\xi^m = 1$, it is also the smallest integer such that $A_0^m = I = e^{2\pi i} I$. Therefore $A^{m/2} = \text{diag}(e^{\frac{2\pi i}{2}} I, e^{\frac{2\pi i \ell}{2}} I) = \text{diag}(-I_n, -I_n)$ because ℓ is odd.

3. $E_{m,r}$: $P^2 = -I$.

4. $F_{m,r,\ell}$: $P^2 = -I$.

5. $J_{m,r}$: $(PQ)^5 = -I$.

6. $K_{m,r,l}$: $R^2 = -I$.

□

Thus, we are left only with the possibility of using reducible representations of fixed-point-free groups. These are essentially obtained by forming a direct sum of two (or more) inequivalent representations of any of the irreducible representations of Theorem 2. In what follows, we shall, for simplicity, focus on reducible representations of cyclic groups.

As noted in Section 4.2, M-dimensional reducible representations of cyclic groups take the form

$$A_k = A^k = \text{diag}\,(\eta^{u_1 k}, \eta^{u_2 k}, \ldots, \eta^{u_M k}), \quad k = 0, \ldots, L_A - 1$$

where η is a primitive L_A-th root of unity and $u_1, \ldots u_M$ are integers between 1 and $L_A - 1$. The next result gives us the family of cyclic groups that yield nonzero $\zeta_{\mathcal{S}}$.

Theorem 6 (Products of Cyclic Group Representations). *Let $A_0, \ldots, A_{L_A - 1}$ be an M-dimensional reducible representation of a cyclic group:*

$$A_k = A^k = \text{diag}\,(\eta^{u_1 k}, \eta^{u_2 k}, \ldots, \eta^{u_M k}), \quad k = 0, \ldots, L_A - 1.$$

Then there exists a unitary matrix T such that

$$\zeta_{\mathcal{S}} = \frac{1}{2} \min_{(j,k) \neq (0,0)} \left| \det\left(A^j - T A^k T^*\right) \right|^{\frac{1}{M}} > 0 \tag{31}$$

if and only if, for all $K > M/2$, there exists no K-tuple $(u_{j_1}, \ldots u_{j_K})$ such that

$$\gcd\left(|u_{j_1} - u_{j_K}|, \ldots, |u_{j_{K-1}} - u_{j_K}|, L_A\right) > 1. \tag{32}$$

Moreover, if (32) holds, then (31) holds generically for all unitary T.

Proof: Let us partition the identity matrix I and the unitary matrix T into its columns:

$$I = \begin{pmatrix} e_1 & \ldots & e_M \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} t_1 & \ldots & t_M \end{pmatrix}.$$

Then we may write

$$\begin{aligned} A_k - TA_\ell T^* &= \sum_{i=1}^{M} \eta^{u_i k} e_i e_i^* - \sum_{i=1}^{M} \eta^{u_i \ell} t_i t_i^* \\ &= \sum_{i=1}^{M} \eta^{u_i k} e_i e_i^* - \sum_{i=1}^{M-1} \eta^{u_i \ell} t_i t_i^* - \eta^{u_M \ell} \left(\sum_{i=1}^{M} e_i e_i^* - \sum_{i=1}^{M-1} t_i t_i^* \right) \\ &= \sum_{i=1}^{M} (\eta^{u_i k} - \eta^{u_M \ell}) e_i e_i^* - \sum_{i=1}^{M-1} (\eta^{u_i \ell} - \eta^{u_M \ell}) t_i t_i^*, \end{aligned}$$

where in the second step we use $TT^* = I$.

Since the $2M-1$ rank-one matrices $\{e_1 e_1^*, \ldots, e_M e_M^*, t_1 t_1^*, \ldots, t_{M-1} t_{M-1}^*\}$ are (generically) linearly independent, $A_k - TA_l T^*$ is singular if and only if at least $K_1 \geqslant M$ of the $2M-1$ coefficients $\{\eta^{u_1 k} - \eta^{u_M l}, \ldots, \eta^{u_M k} - \eta^{u_M l}, \eta^{u_1 l} - \eta^{u_M l}, \ldots, \eta^{u_{M-1} l} - \eta^{u_M l}\}$ are zero. This can happen if, and only if, at least $K > M/2$ of the M scalars $(\eta^{u_1 k}, \ldots, \eta^{u_M k})$ or $K > M/2$ of the M scalars $(\eta^{u_1 \ell}, \ldots, \eta^{u_M \ell})$ are identical. Assuming, without loss of generality, that this is true of the first set of M scalars means that there must exist some K-tuple $(u_{i_1}, \ldots u_{i_K})$ such that

$$\eta^{u_{i_1} k} = \eta^{u_{i_2} k} = \ldots = \eta^{u_{i_K} k},$$

or, equivalently, $u_{i_1} k \equiv u_{i_2} k \equiv \ldots \equiv u_{i_K} k \bmod L$. This last condition can be written as

$$(u_{i_1} - u_{i_K})k \equiv (u_{i_2} k - u_{i_K}) \equiv \ldots \equiv (u_{i_{K-1}} - u_{i_K})k \equiv 0 \bmod L_A,$$

which is equivalent to

$$\gcd(|u_{i_1} - u_{i_K}|, \ldots, |u_{i_{K-1}} - u_{i_K}|, L_A) > 1.$$

This establishes the first claim of the theorem. The second claim follows from the fact that all our claims about rank and nonsingularity are generic in terms of the unitary matrix T.

□

Remarks

- The condition (32) essentially states that $\zeta_{\mathcal{S}}$ is nonzero if and only if no element of the cyclic group has $K > M/2$ equal diagonal entries.

- A simple sufficient condition that guarantees nonzero $\zeta_{\mathcal{S}}$ is that L be prime.

- Once we have found a cyclic group for which $\zeta_{\mathcal{S}}$ is nonzero we can optimize the value of $\zeta_{\mathcal{S}}$ by performing a search over the set of $M \times M$ unitary matrices T and using (30). Intuitively, the matrix T should be a "full" matrix with the property that the constellations $\{A_j\}$ and $\{B_j = TA_jT^*\}$ be "spread apart" from one another, since $\zeta_{\mathcal{S}}$ depends on the co-distance between these two constellations. Since the search space is small (it is a single $M \times M$ unitary matrix), methods such as random search can be used to find a good T.

- When $\mathcal{G}_A$ is not cyclic, one can use reducible $M \times M$ representations:

$$A_i = \begin{pmatrix} \Delta_1(g_i) & & \\ & \ddots & \\ & & \Delta_k(g_i) \end{pmatrix},$$

  where Δ_1 to Δ_k are irreducible fixed-point-free representations of $\mathcal{G}_A$ whose dimensions add up to M.

- It is also possible to use representations of two different groups $\mathcal{G}_A$ and $\mathcal{G}_B$.

9 Constellations and their performance

In this section, we display the performance of some of the group and nongroup constellations derived in the previous sections. To evaluate the performance, we use the differential transmission framework described in Section 2.3, with a receiver that does not know the channel and decodes using the metric (7).

Most of the constellations were computer-simulated with fading coefficients that were chosen randomly but held constant for two consecutive matrix-valued signals, as described in Section 2.3. In one exceptional case described below, the constellation was transmitted over a functional three-transmitter-antenna wireless channel. The resulting figures plot the block probability of decoding a matrix incorrectly, denoted P_e.

9.1 Group constellations

Figure 1 displays the simulated performance of the group $\mathrm{SL}_2(\mathbb{F}_5)$ which has 120 elements, and therefore has rate $R = \log(120)/2 \approx 3.45$. We also compare the best Abelian group we could find (which is necessarily cyclic), and the orthogonal design with 121 elements obtained by filling the matrix (11) with 11th-roots of unity. The excellent performance of $\mathrm{SL}_2(\mathbb{F}_5)$ is evidenced by the approximately 2.5 dB improvement over the orthogonal design (which is not a group), the 6.5 dB improvement over the Abelian group, and the 13 dB improvement over the quaternion group. Table 3 in Section 9 and Table 1 in Section 2 list more details about these constellations.

Figure 2 is the same as Figure 1 except that the receiver is assumed to know the channel and demodulate coherently. The constellation performances all gain approximately 3 dB over the unknown channel, as explained in Section 2.3.

Figure 3 is also the same as Figure 1 except that we now assume $N = 2$ receive antennas. The difference in performance of the various constellations becomes more pronounced, and there is a clear advantage of having two receivers over one receiver.

Figure 4 compares the performances of various constellations with $R \approx 4$. The group constellation is $F_{15,1,11}$ with $L = 240$ elements ($R = 3.95$). The other constellations are the best orthogonal design, diagonal constellation and quaternion groups of comparable rate.

Figure 5 shows the performance advantage of the $M = 3$ antenna 63-element ($R = 1.99$) group $G_{21,4}$ compared with the best three-antenna 63-element diagonal constellation. We were also able to transmit this constellation over a wireless apparatus located within a hallway at Bell Laboratories, Murray Hill. The three transmit antennas were separated from the one receive antenna by approximately 10 meters around a bend in the hallway lined with metal walls and equipment, thus creating a quasi-static scattering environment. Figure 6 shows the performance.

Figure 7 shows the performance of $K_{1,1,-1}$, the binary extension of $\mathrm{SL}_2(\mathbb{F}_5)$ for $M = 4$ transmitter antennas, and compares it with the best Abelian group we found. Again, the performance gain of this group over the Abelian group is evident.

Table 3 collects together some of the group constellations that we have found with high ζ for different numbers of antennas M and rates R. The list includes many of the constellations that are also described in other sections of this paper, but it is not exhaustive. There are many other groups within our classification that we have not explored and are therefore not on the list.

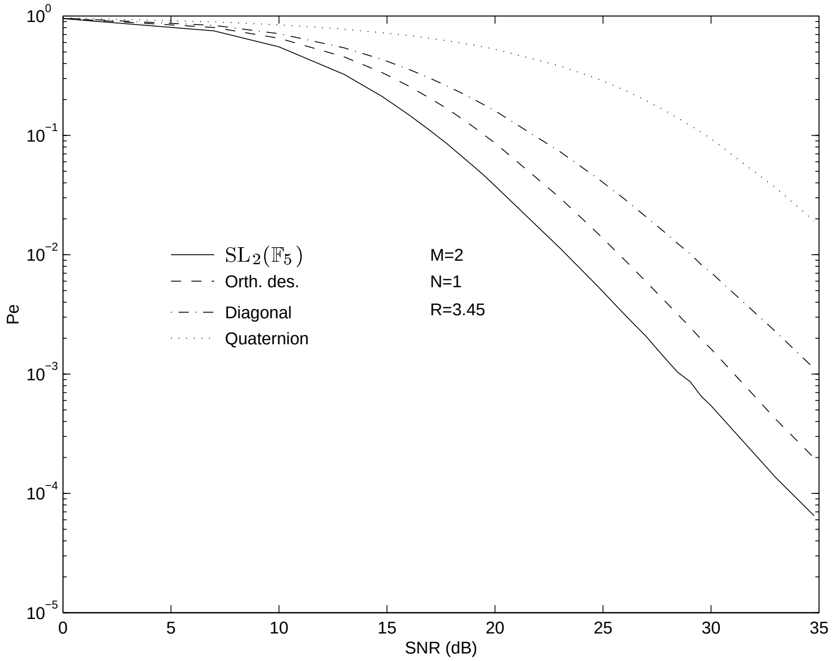

Figure 1: Block-error rate performance of the group $\mathrm{SL}_2(\mathbb{F}_5)$ compared with constellations from previous constructions for $M = 2$ transmitter antennas and $N = 1$ receiver antenna. The solid line is $\mathrm{SL}_2(\mathbb{F}_5)$, which has $L = 120$ unitary matrices ($R \approx 3.45$). The dashed line is an orthogonal design with 11th roots of unity ($R \approx 3.46$). The dashed-dotted line is the best diagonal (Abelian group) construction ($R \approx 3.45$). The dotted line is the quaternion group with $L = 128$ matrices ($R = 3.5$). (The latter three constellations are listed in Table 1).

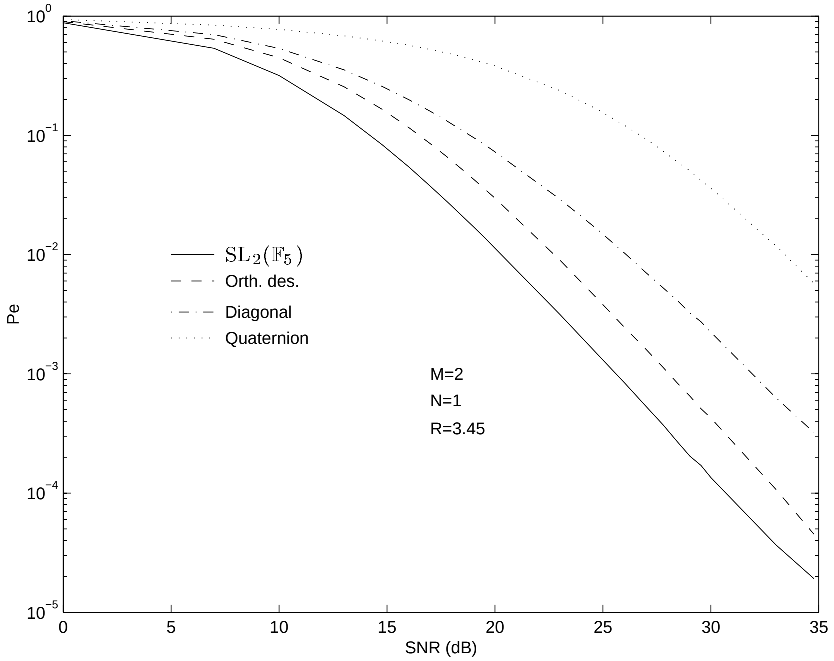

Figure 2: Same as in Figure 1, except the receiver is assumed to know the channel perfectly and demodulate coherently. The performance gain is approximately 3 dB over the unknown channel.

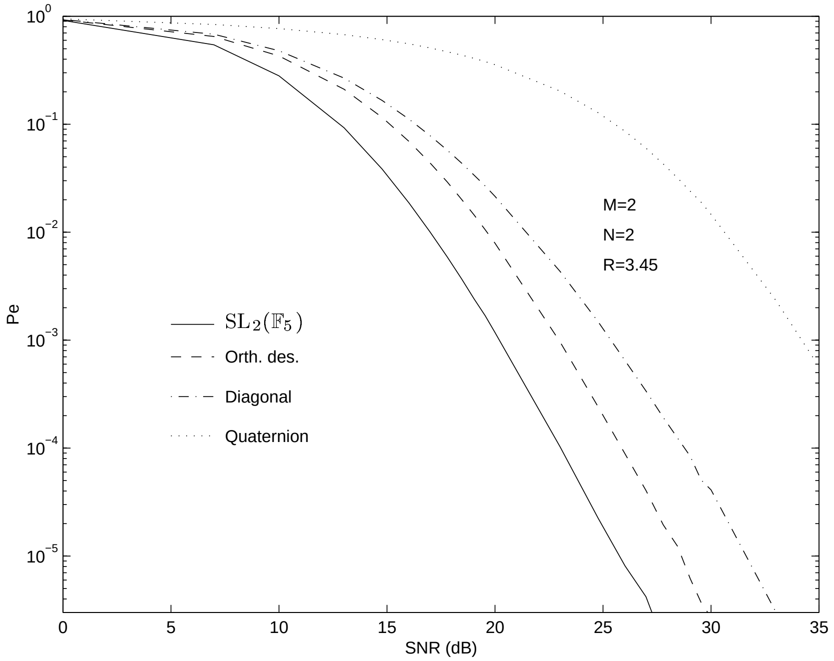

Figure 3: Same as in Figure 1, except with $N = 2$ receiver antennas. The coding advantage of the group $\mathrm{SL}_2(\mathbb{F}_5)$ becomes more pronounced as the number of receiver antennas increases.

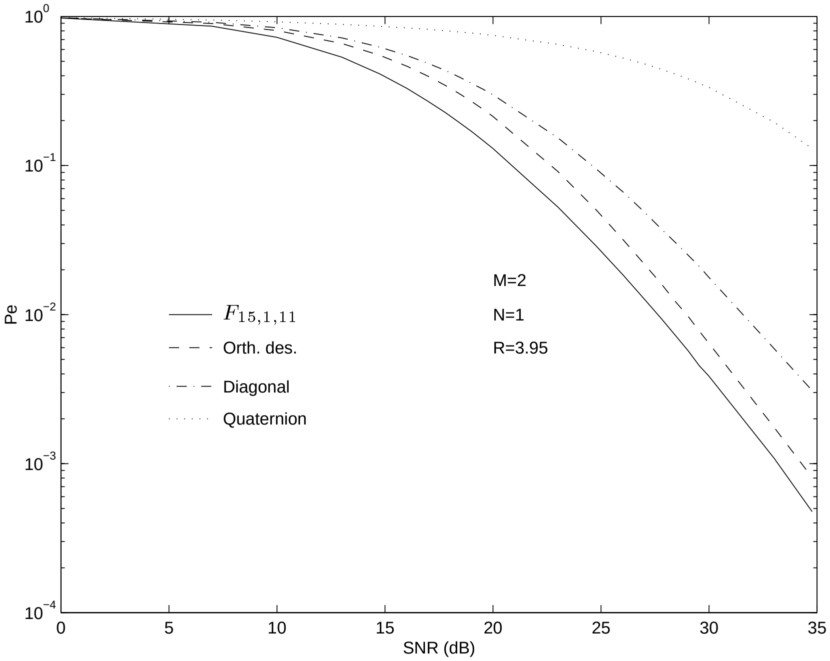

Figure 4: Block-error rate performance of the group $F_{15,1,11}$ for $M = 2$ transmitter antennas and $N = 1$ receiver antenna. The solid line is $F_{15,1,11}$, which has $L = 240$ unitary matrices ($R \approx 3.95$). The dashed line is an orthogonal design with 16th roots of unity ($R = 4$). The dashed-dotted line is the best diagonal (Abelian group) construction ($R \approx 3.95$). The dotted line is the quaternion group with $L = 256$ matrices ($R = 4$). (The latter three constellations are listed in Table 1).

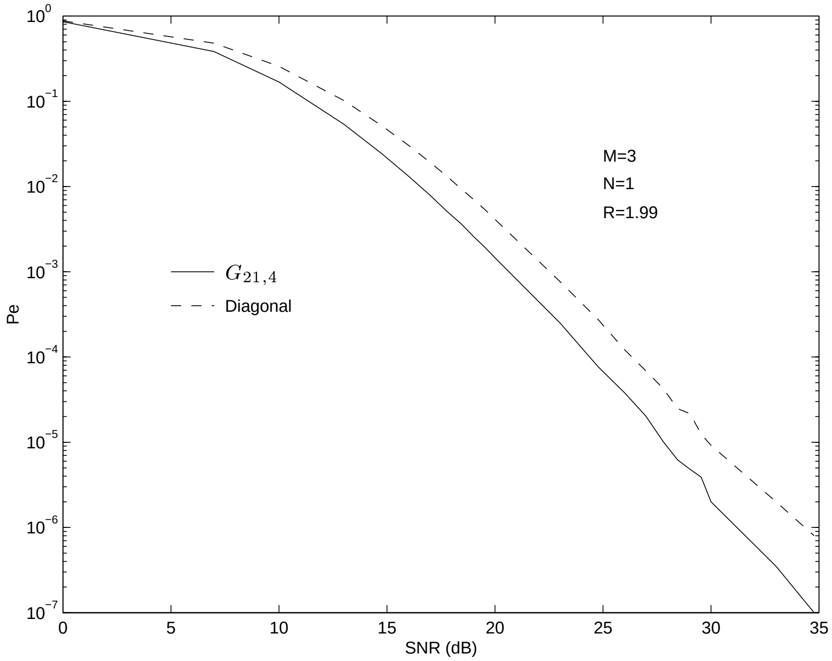

Figure 5: Block-error rate performance of the group $G_{21,4}$, which has an irreducible representation of $L = 63$ matrices for $M = 3$ antennas ($R \approx 1.99$), and best diagonal (Abelian group) constellation with the same rate, described in Table 1, for $N = 1$ receiver antenna.

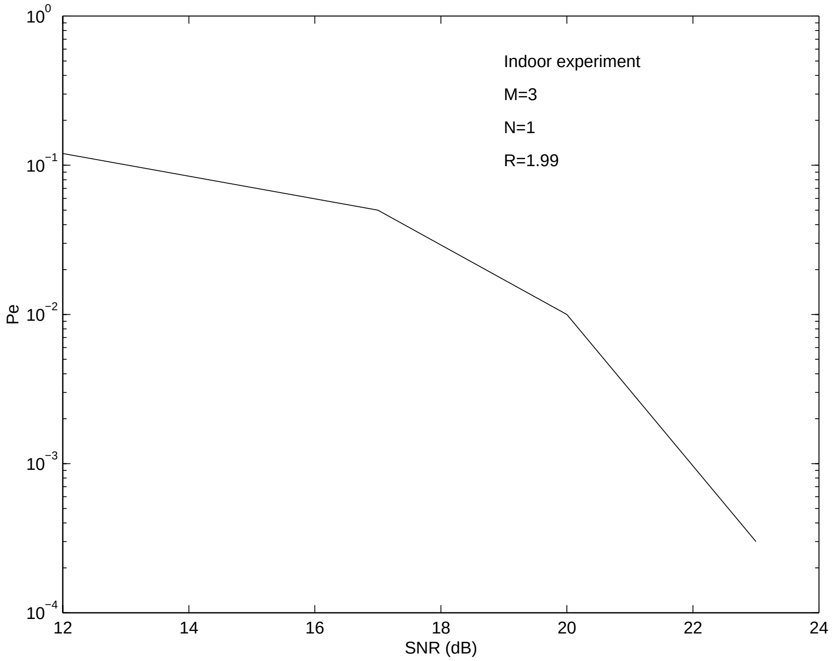

Figure 6: Block-error rate performance of the group $G_{21,4}$ (as in Figure 5) transmitted over wireless apparatus in a Bell Laboratories hallway.

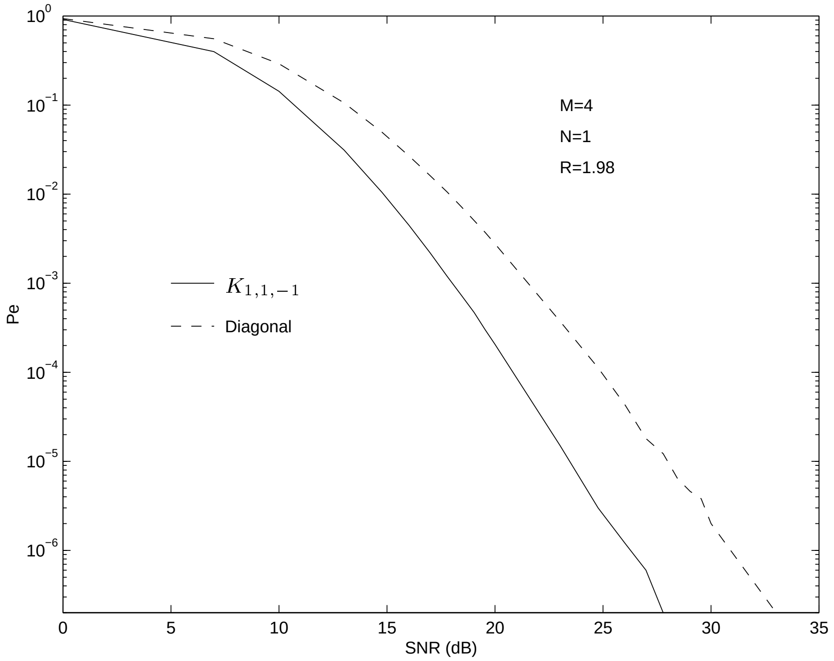

Figure 7: Block-error rate performance of the group $K_{1,1,-1}$ compared with the best diagonal code for $M = 4$ transmitter antennas and $N = 1$ receiver antenna. The solid line is $K_{1,1,-1}$ the binary extension of the group $\mathrm{SL}_2(\mathbb{F}_5)$ having $L = 240$ unitary matrices ($R \approx 1.98$). The dashed line is the diagonal construction with the same rate, described in Table 1.

M	L	R	ζ	Comments	Reference
-	2	-	1	$\{I, -I\}$ for any M	
2	24	2.29	0.5000	$E_{3,1} = \mathrm{SL}_2(\mathbb{F}_3)$	pg. 28
2	48	2.79	0.3868	$F_{3,1,-1} = \mathrm{SL}_2(\mathbb{F}_3)$	pg. 29
2	120	3.45	0.3090	$J_{1,1} = \mathrm{SL}_2(\mathbb{F}_5)$	pg. 29 & Figs. 1 & 3
2	240	3.95	0.2257	$F_{15,1,11}$	Fig. 4
3	9	1.06	0.6004	cyclic group $G_{9,1}$ with $u = (1, 2, 5)$	
3	63	1.99	0.3851	$G_{21,4}$	pg. 18 & Fig. 5
3	513	3.00	0.1353	$G_{171,64}$ ($t = 19$)	
3	4095	4.00	0.0361	$G_{1365,16}$ ($t = 91$)	
3	32445	5.00	0.0131	$G_{10815,46}$ ($t = 721$)	
4	240	1.98	0.5000	$K_{1,1,-1}$	Fig. 7
5	1025	2.00	0.1679	$G_{205,16}$ ($t = 41$)	
5	33825	3.01	0.0503	$G_{6765,16}$ ($t = 451$)	
5	1021025	3.99	0.0037	$G_{204205,21}$ ($t = 40841$)	
7	16513	2.00	0.0955	$G_{2359,8}$ ($t = 337$)	
9	513	1.00	0.3610	$G_{57,4}$	pg. 19

Table 3: Summary of some group constellations and their diversity products.

9.2 Nongroup constellations

For comparison, Table 4 collects some of the nongroup constellations with high ζ.

Figure 8 shows the performance of the nongroup $M = 5$, $R = 1$ constellation $\mathcal{S}_{11,3}$ compared with the best group constellation. The only group constellation with $M = 5$ and $R = 1$ is a reducible (diagonal) representation of an Abelian (cyclic) group, since the closest nondiagonal group is $G_{25,6}$ which has 125 elements and corresponds to $R \approx 1.39$. We can see the performance advantage of the non-diagonal nongroup constellation over the diagonal constellation.

Figure 9 shows the performance of $R = 4$ nongroup constellations of Table 4 for $M = 2, 3, 4$ transmitter antennas and $N = 1$ receiver antenna. We see the diversity gain of increasing the number of transmit antennas.

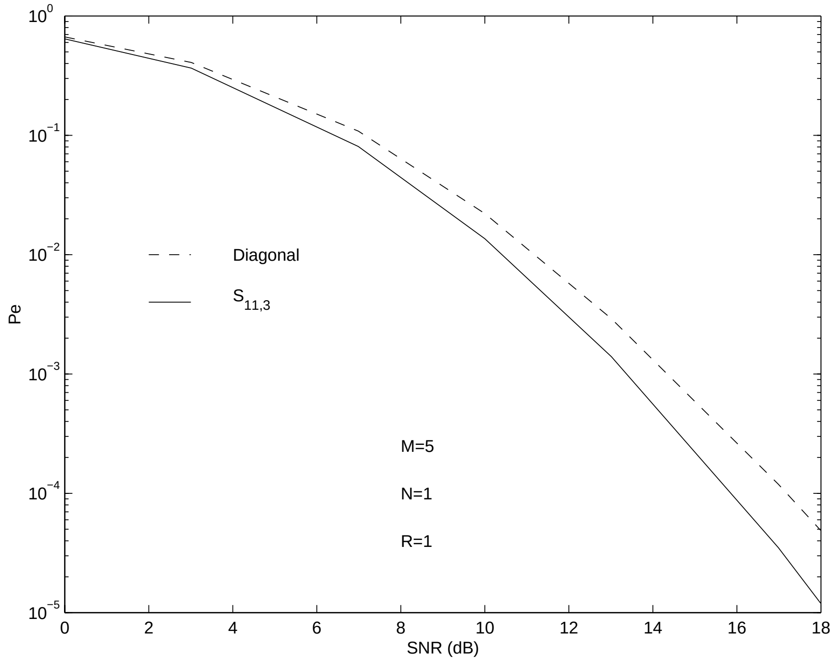

Figure 8: Block-error rate performance for $M = 5$ transmitter antennas, $N = 1$ receiver antenna, and rate $R = 1$. The solid line is the nongroup $\mathcal{S}_{11,3}$ having 33 elements ($R \approx 1.01$). The dashed line is the best $R = 1$ group construction: in this case the best 32-element diagonal constellation.

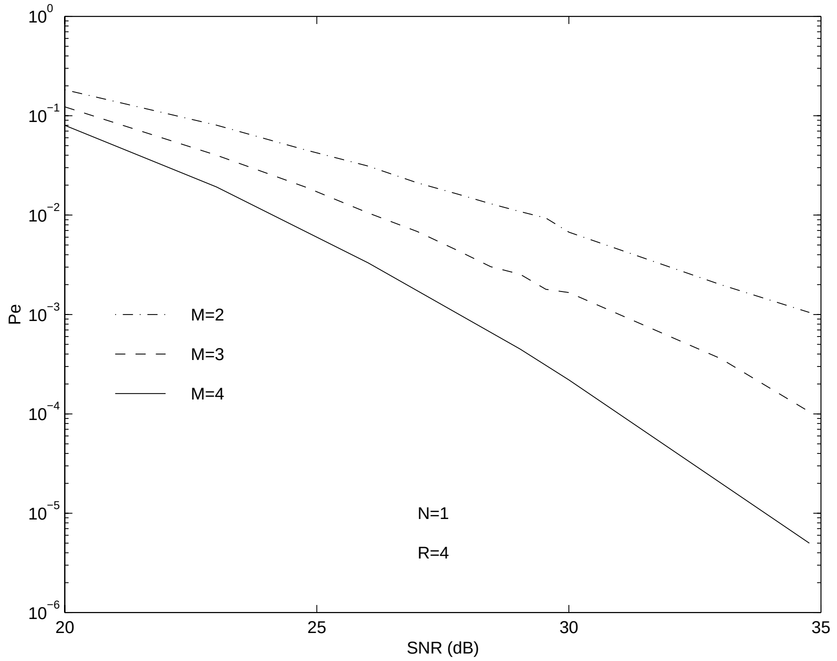

Figure 9: Block-error rate performance for $M = 2, 3, 4$ transmitter antennas and rate $R = 4$. The constellations are described in Table 4.

M	L	R	ζ	Comments	Ref.
2	81	3.17	0.2417	product of groups, $L_A = 9$, $u = (1, 2)$	
2	289	4.09	0.1625	product of groups, $L_A = 17$, $u = (1, 12)$	Fig. 9
2	1089	5.04	0.0794	product of groups, $L_A = 33$, $u = (1, 26)$	
2	4225	6.02	0.0436	product of groups, $L_A = 65$, $u = (1, 19)$	
2	16641	7.01	0.0212	product of groups, $L_A = 129$, $u = (1, 80)$	
2	66049	8.01	0.0106	product of groups, $L_A = 257$, $u = (1, 186)$	
3	57	1.94	0.4845	$\mathcal{S}_{57,3}$, $u = (1, 7, 11)$	
3	529	3.02	0.1863	product of groups, $L_A = 23$, $u = (1, 13, 19)$	
3	4225	4.01	0.0933	product of groups, $L_A = 65$, $u = (1, 17, 23)$	Fig. 9
3	34969	5.03	0.0458	product of groups, $L_A = 187$, $u = (1, 30, 114)$	
4	289	2.04	0.3105	product of groups, $L_A = 17$, $u = (1, 3, 4, 11)$	
4	4225	3.01	0.1539	product of groups, $L_A = 65$, $u = (1, 14, 21, 34)$	
4	66049	4.00	0.0678	product of groups, $L_A = 257$, $u = (1, 148, 160, 229)$	Fig. 9
5	33	1.01	0.5580	$\mathcal{S}_{11,3}$, $u = (1, 3, 4, 5, 9)$	Fig. 8
5	1369	2.08	0.2307	product of groups, $L_A = 37$, $u = (1, 6, 8, 14, 27)$	
5	34969	3.02	0.1065	product of groups, $L_A = 187$, $u = (1, 23, 37, 91, 135)$	
5	1054729	4.00	0.0557	product of groups, $L_A = 1027$, $u = (1, 239, 350, 439, 986)$	
6	72	1.03	0.5000	$\mathcal{S}_{12,6}$, $u = (1, 1, 7, 7, 7, 1)$	
6	3969	1.99	0.2723	doubling the $M = 3$, $L = 63$ constellation $G_{21,4}$	
6	4225	2.01	0.2084	product of groups, $L_A = 65$, $u = (1, 9, 21, 51, 53, 57)$	
7	133	1.01	0.4900	$\mathcal{S}_{19,7}$, $u = (1, 3, 6, 7, 15, 17, 8)$	
7	16513	2.00	0.1802	product of groups, $L_A = 131$, $u = (1, 8, 9, 42, 48, 68, 101)$	

Table 4: Summary of nongroup constellations with best diversity product.

10 Fast decoding

As shown in Section 2.3, a constellation $\mathcal{V}$ consist of $L = 2^{RM}$ symbols V_ℓ and the maximum likelihood (ML) decoder is given by

$$\hat{z}_\tau^{\mathrm{ML}} = \arg \min_{\ell=0,\ldots,L-1} \|X_\tau - V_\ell X_{\tau-1}\| \, .$$

The ML decoder can be computed by simply trying all $V_0, \ldots, V_{L-1}$ and retaining the one that minimizes the above expression, but the search time of this naive algorithm is exponential both in the rate R and the number of antenna M. Therefore, for large M or R it is important in practical applications to look for a faster, i.e. polynomial time, algorithm, even if the algorithm is only approximate. We touch briefly upon such algorithms.

10.1 Cyclic groups

In [21] a fast approximate ML algorithm for decoding cyclic groups is proposed, which we briefly review and then adapt for our noncyclic constellations. For simplicity, we focus on $N = 1$ receive antenna.

The received signals form a length M vector X_τ whose elements we denote as $x_{\tau;m}$. The maximum likelihood decoder for diagonal codes can be written as

$$\hat{z}_\tau^{\mathrm{ML}} = \arg\,\min_\ell \|X_\tau - V_\ell\, X_{\tau-1}\|^2 = \arg\,\min_\ell \sum_{m=1}^{M} \left| x_{\tau;m} - e^{i2\pi u_m \ell/L} x_{\tau-1;m} \right|^2 .$$

The summands are equal to

$$|x_{\tau;m}|^2 + |x_{\tau-1;m}|^2 - 2\, |x_{\tau;m}\, x_{\tau-1;m}|\, \cos(\arg x_{\tau;m} - \arg x_{\tau-1;m} - 2\pi u_m \ell/L).$$

Given that only the cosine depends on ℓ the maximum likelihood decoder is equivalent to

$$\hat{z}_\tau^{\mathrm{ML}} = \arg\,\max_\ell \sum_{m=1}^{M} A_m^2 \cos((u_m \ell - \varphi_m)\, 2\pi/L), \tag{33}$$

where $A_m = |x_{\tau;m}\, x_{\tau-1;m}|^{1/2}$ and $\varphi_m = \arg\,(x_{\tau;m}/x_{\tau-1;m})\, L/2\pi$.

From this we see that M-dimensional representations of cyclic groups can be thought of as M-dimensional lattices. The cosine function in (33) is 2π periodic and the arguments thus can be reduced to the interval $[0, 2\pi)$; the argument of the mth term can be written as

$$[(u_m \ell - \varphi_m) \mod L]\, 2\pi/L.$$

If we define the M-vector $\mathbf{u} = [u_1 \;\cdots\; u_M]^t$, then the vectors $\ell\mathbf{u} \bmod L$ for $\ell = 0, \ldots, L-1$ form the part of a lattice which lies in $[0, L)^M$. The cosine can be approximated as $\cos\alpha \approx 1 - \alpha^2/2$. Hence we can approximate the maximization of (33) by a minimizing of the sum of the squares of the arguments of the cosines. Then the expression becomes the square of a Euclidean distance:

$$\min_\ell \sum_m A_m \left((u_m \ell - \varphi_m) \mod L\right)^2 .$$

The vectors with components $A_m u_m \ell \bmod A_m L$ form a lattice where each dimension m has been scaled by A_m. Approximating the maximum likelihood decoding with a problem involving the closest point in a lattice does not immediately lead to fast decoding because finding the closest point in a lattice is NP-hard in M. However, there is a well-known approximation algorithm introduced by Lenstra, Lenstra, and Lovász in [22] and commonly referred to as "the LLL algorithm." Its complexity is polynomial in M and hence polylog in L ($\log^\beta L$ for some $\beta > 0$). The LLL algorithm relies on the observation that when a lattice has an orthogonal basis, the closest point can be found trivially by rounding each component to the closest lattice component. Thus for a given lattice the LLL algorithm attempts to find the "most orthogonal" basis, or more precisely the basis with the shortest vectors, and then use component wise rounding to approximate the closest lattice point. Finding the basis with the shortest vectors itself is a NP-hard problem; LLL tries to find a basis with reasonably short vectors. In [21] it is shown that for constellations with over 16 elements, lattice decoding is much faster than a complete ML search and has comparable performance. Lattice decoding can be easily implemented on digital signal processors (DSP's).

10.2 Non Abelian groups

Most of the non Abelian groups discussed in this paper have large cyclic subgroups and we can apply fast lattice decoding within these subgroups and use a naive method across subgroups. We illustrate this using the $G_{m,r}$ groups introduced in Section 4.3. From (17), we see that the constellation is given by

$$\mathcal{V} = \{A^\ell B^k \mid \ell = 0, \ldots, m-1, k = 0, \ldots, n-1, A = (F \uparrow G)(\sigma), B = (F \uparrow G)(\tau)\}.$$

Here A is a diagonal matrix with mth roots of unity on the diagonal. ML decoding is

$$\min_{\substack{\ell=0,\ldots,m-1 \\ k=0,\ldots,n-1}} \left\| X_\tau - A^\ell B^k X_{\tau-1} \right\| .$$

If we define $X'_{k,\tau-1}$ to be $B^k X_{\tau-1}$, then the problem can be written as

$$\min_{k=0,\ldots,n-1} \min_{\ell=0,\ldots,m-1} \left\| X_\tau - A^\ell X'_{k,\tau-1} \right\| .$$

For each k the inner minimization can approximated using the fast lattice decoding for cyclic groups described above, while the outer minimization can be solved naively. Because the dimension of the representation (n) is equal to the number of transmitter antennas ($M = n$), the resulting algorithm is still polynomial in M.

A similar algorithm works for the non group generalizations of $G_{m,r}$ described in Section 8.2. We omit the details.

10.3 Hamiltonian constellations

As mentioned in Section 8.1, decoding the $M = 2$ Hamiltonian constellations has constant complexity in the rate R.

10.4 Products of groups

We next consider decoding the products of groups introduced in Section 8.3. The constellation is given by

$$\mathcal{V} = A^j T A^k T^* \mid j, k = 0, \ldots, L_A - 1,$$

where A is a diagonal matrix with L_Ath roots of unity on the diagonal and T is an artfully chosen unitary matrix. ML decoding is

$$\min_{(j,k)} \left\| X_\tau - A^j T A^k T^* X_{\tau-1} \right\| . \tag{34}$$

Using the fast lattice decoding for cyclic codes, the problem (34) can be solved approximately for a fixed j with complexity polylog in L_A. By checking every j an approximate answer can be found in $O(L_A \log^\beta L_A) = O(\sqrt{L} \log^\beta L)$ since $L = L_A^2$.

11 Conclusion and future work

Future wireless communication systems will probably incorporate multiple antennas to boost system capacity and lower error probability, but the use of multiple transmit antennas requires effective full-diversity space-time signals. Prior studies have indicated that groups of unitary matrices could serve as effective space-time signals. In this paper, we have completely characterized all groups of full-diversity unitary space-time signals. In the process, we have found many nontrivial groups with excellent performance at high rates, especially for four or fewer transmitter antennas. We hope that these groups will have practical significance, especially since many of them can be decoded quickly using algorithms that can be easily implemented on DSP's.

We have also found that groups with full-diversity irreducible representations do not exist for all combinations of M and R. This led to the design of some nongroup constellations with good high-rate performance. These nongroups have some of the symmetry properties inspired by the group constellations, but they do not generally have the size or dimension constraints. Nevertheless, our proposed designs of nongroup constellations for all numbers of antennas and rates sometimes require trial and error. It is therefore still an open problem to find a systematic design of nongroup constellations for all rates and for which decoding is not a burden when $M >> 2$.

There are many other aspects to the unitary signal design problem that we have only touched upon. For example, while we have characterized all the groups, we have not tested them all for performance, and, specifically, we have not examined all possible *reducible* representations that have these groups as constituents. The diagonal constellations represent the simplest form of a reducible representation, but there may be others that may perform much better.

In this paper, our classification considered only finite fixed-point-free groups. The unitary group (in any dimension) is infinite but clearly does not have full diversity. We may ask, is it possible to classify the infinite subgroups of the unitary group that have full diversity? This is another possible area for future work.

Acknowledgment

We are especially grateful to Joe Buhler and Zinovy Reichstein for pointing out reference [17]. We also thank Mike Andrews at Bell Laboratories, Murray Hill, for allowing us to use his three-antenna testbed.

References

[1] B. Hochwald and W. Sweldens, "Differential unitary space time modulation," tech. rep., Bell Laboratories, Lucent Technologies, Mar. 1999. Submitted to *IEEE Trans. Comm.*. Download available at `http://mars.bell-labs.com`.

[2] I. E. Telatar, "Capacity of multi-antenna gaussian channels," tech. rep., Bell Laboratories, Lucent Technologies, 1995. Download available at `http://mars.bell-labs.com`.

[3] 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.

[4] 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, 1998.

[5] V. Tarokh, H. Jafarkani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Info. Theory.*, vol. 45, pp. 1456–1467, July 1999.

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

[7] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat-fading," *IEEE Trans. Info. Theory*, Mar. 2000 (to appear). Download available at `http://mars.bell-labs.com`.

[8] B. Hassibi, B. Hochwald, and T. Marzetta, "Space-time autocoding," *submitted to IEEE Trans. Info. Theory*, 1999.

[9] B. Hughes, "Differential space-time modulation," *submitted to IEEE Trans. Info. Theory*, 1999.

[10] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *to appear in J. Sel. Area Comm.*, 2000.

[11] W. Burnside, "On a general property of finite irreducible groups of linear substitutions," *Messenger of Mathematics*, vol. 35, pp. 51–55, 1905.

[12] H. Zassenhaus, "Über endliche Fastkörper," *Abh. Math. Sem. Hamburg*, vol. 11, pp. 187–220, 1936.

[13] D. Warrier and U. Madhow, “Noncoherent communication in space and time,” *submitted to IEEE Trans. Info. Theory*, 1999.

[14] G. James and M. Liebeck, *Representations and Characters of Groups*. Cambridge, England: University Press, 1993.

[15] N. Jacobson, *Basic Algebra II*. New York: W. H. Freeman and Co., 1989.

[16] G. Vincent, “Les groupes linéaires finis sans points fixés,” *Comment. Math. Helv.*, vol. 20, pp. 117–171, 1947.

[17] S. A. Amitsur, “Finite subgroups of division rings,” *Trans. Amer. Math. Soc.*, vol. 80, pp. 361–386, 1955.

[18] J. Hamkins and K. Zeger, “Asymptotically dense spherical codes,” *IEEE Trans. Info. Theory*, vol. 43, pp. 1774–1798, 1997.

[19] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York: Springer-Verlag, 1988.

[20] L. Devroye, *Lecture Notes on Bucket Algorithms*. Boston, MA: Birkhäuser, 1986.

[21] K. L. Clarkson, W. Sweldens, and A. Zheng, “Fast multiple antenna differential decoding,” tech. rep., Bell Laboratories, Lucent Technologies, October 1999. Submitted to *IEEE Trans. Comm.*. Download available at `http://mars.bell-labs.com`.

[22] A. K. Lenstra, H. W. Lenstra, and L. Lovász, “Factoring polynomials with rational coefficients,” *Math. Ann.*, pp. 515–534, 1982.

[23] D. Passman, *Permutation Groups*. New York: W. A. Benjamin, Inc, 1968.

[24] B. Huppert, *Endliche Gruppen*, vol. I. Springer Verlag, Berlin, second ed., 1983.

[25] M. Schönert et al., *GAP–Groups, Algorithms, and Programming*. Lehrstuhl D für Mathematik, Rheinisch Westfälische Hochschule, Aachen, Germany, 4th ed., 1994.

[26] S. Lang, *Algebra*. Menlo Park, CA: Addison-Wesley, 3rd ed., 1993.

[27] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*. No. 21 in London Mathematical Society Student Texts, Cambridge University Press, 1991.

A A classification of fixed-point-free groups

Our aim in this section is to give a proof of “half of” Theorem 1: We show that if G is fixed-point-free, then it is isomorphic to one of the groups classified in Section 5.1. The converse statement is proven, along with Theorem 2, in Appendix B.

We start our classification of fixed-point-free groups by recalling several useful theorems. Since subgroups of fixed-point-free groups are fixed-point-free themselves, it makes sense to classify the Sylow subgroups of fixed-point-free groups. The following theorem is due to Burnside [11] (see also [23, Th. 18.1]).

Theorem 7. *Let G be a fixed-point-free p-group. If p is odd, then G is cyclic. If p is even, then G is either cyclic, or a generalized quaternion group.*

A group in which all Sylow subgroups are cyclic is called a *Z-group*. Note that the previous theorem implies that all fixed-point-free groups of *odd* order are Z-groups. By [12, Satz 5] any Z-group is isomorphic to a $G_{m,r}$ for some m and some r. Not all Z-groups are fixed-point-free, however. A classification of all fixed-point-free Z-groups is given in the following [23, Th. 18.2]

Theorem 8. *Any Z-group is isomorphic to $G_{m,r}$. Moreover, it is fixed-point-free if and only if (m, r) is admissible.*

Later, we compute all the fixed-point-free representations of $G_{m,r}$.

The next step is to classify all *solvable* fixed-point-free groups. For this, we need the following theorem of Zassenhaus [12, Satz 6].

Theorem 9. *Let G be a solvable fixed-point-free group. Then G has a normal subgroup G_1 which is a Z-group such that G/G_1 is isomorphic to either the trivial group, or a cyclic group of order 2, or the alternating group A_4 on four elements, or the symmetric group S_4 on four elements.*

For a proof of a weaker version of this theorem we refer the reader to [23, Th. 18.2]. We now use the above theorem to derive descriptions of solvable fixed-point-free groups in terms of generators and relations. This has already been essentially done in Zassenhaus' paper [12, Satz 7,8], and we use most of his proof techniques.

Given (m, r), we freely refer to n as the order of r modulo m, to r_0 as $\gcd(r - 1, m)$, and to t as m/r_0. The following remark is quite useful. For a proof see [17, pp. 362].

Remark 2. *Let (m, r) be an admissible pair. Then $\gcd(r_0, t) = 1$.*

Theorem 10. *Any solvable fixed-point-free group is isomorphic to $G_{m,r}$, $D_{m,r,\ell}$, $E_{m,r}$, or $F_{m,r,\ell}$.*

Proof. We use Theorem 9. Let G be a fixed-point-free group and G_1 be the normal subgroup of G with the properties stated in that theorem.

(1) If G/G_1 is the trivial group, then $G = G_1 = G_{m,r}$ is a Z-group and we are done.

(2) Suppose that G/G_1 is isomorphic to a cyclic group of order 2. We may assume that G is not a Z-group itself, since we are done otherwise. If G_1 has odd order, then all the Sylow subgroups of G are cyclic, and G is a Z-group. We may therefore suppose that G_1 has even order. From Theorem 8 G_1 is isomorphic to $G_{m,r}$ for some admissible (m, r). We want to show that t is odd. Suppose on the contrary, that t is even. Then r is odd (otherwise $r^n - 1$ is odd, hence is not congruent to 1 modulo t), and $1 = \gcd(r-1, t)$ is even, a contradiction. Hence, t is odd, and since the order of G_1 which is equal to nm is even, we have that nr_0 is even.

Since G_1 is a Z-group, its 2-Sylow subgroup is cyclic, and generated by an element α of order 2^p, say. Since G is not a Z-group, its 2-Sylow subgroup is a generalized quaternion group by Theorem 7. Therefore, G contains an element γ of order 4 that is not in G_1. Since G/G_1 is of order 2, γ^2 is an element in G_1, hence it equals $\tau^{nr_0/2}$ which is in the center of G_1. So, conjugation with γ defines an automorphism of order 2 of G_1. It is easily seen that the only cyclic subgroup of G_1 of order m is the group generated by the element σ. Hence, $\sigma^\gamma = \sigma^q$ for some integer q such that $q^2 \equiv 1 \bmod m$. The only subgroups of order nr_0 of G_1 are generated by conjugates of τ. These are $\langle\tau\rangle, \langle\tau^\sigma\rangle, \ldots, \langle\tau^{\sigma^{t-1}}\rangle$. Since their number is t, which is odd, and since conjugation with γ is an automorphism of order 2 on G_1, at least one of these groups of order nr_0 is fixed under conjugation with γ. Hence, there is some element τ' conjugate to τ in G_1, such that $(\tau')^\gamma = (\tau')^{q'}$ for some q'. Without loss of generality, let $\tau' = \tau$. Note that

$$\gamma\tau\sigma\tau^{-1}\sigma^{-1} = \gamma\sigma^r\gamma^{-1} = \sigma^{qr}.$$

Further,

$$\gamma\tau\sigma\tau^{-1}\sigma^{-1} = \gamma\tau\gamma^{-1}\gamma\sigma\gamma^{-1}\gamma\tau^{-1}\sigma^{-1} = \tau^{q'}\sigma^q\tau^{-q'} = \sigma^{qr^{q'}}.$$

This shows that $r^{q'-1} \equiv 1 \bmod m$, hence $q' \equiv 1 \bmod n$. Observe that

$$(\sigma^t)^\gamma = (\tau^n)^\gamma = \tau^{nq'}$$

and

$$(\sigma^t)^\gamma = \sigma^{tq} = \tau^{nq}.$$

This shows that $q \equiv q' \bmod r_0$. Chinese remaindering shows that we can find ℓ such that $\ell \equiv q \bmod m$ and $\ell \equiv q' \bmod n$. It follows that $\ell \equiv 1 \bmod n$ and $\ell^2 \equiv 1 \bmod m$, and $\sigma^\gamma = \sigma^\ell$, $\tau^\gamma = \tau^\ell$.

To prove that G is isomorphic to $D_{m,r,\ell}$, we are left with showing that $\ell \equiv -1 \bmod s$, where s is the highest power of 2 dividing mn. To this end, consider the 2-Sylow subgroup of G_1 contained in the cyclic group $\langle\tau\rangle$, and assume that it is generated by $x = \tau^a$, say. x together with an element γ' of order 4 of G generate a 2-Sylow subgroup of G, which is a generalized quaternion group. We may without loss of generality assume that γ is γ'. Then $x^\gamma = x^{-1}$, and $x^\gamma = (\tau^a)^\gamma = (\tau^a)^\ell = x^\ell$. Hence, $\ell \equiv -1 \bmod s$.

(3) Suppose now that G/G_1 is isomorphic to A_4. In [12, pp. 203] it is proved that G contains a normal subgroup G_2 of odd order which commutes with a 2-Sylow subgroup Σ_2 of G, such that $N = \Sigma_2 \times G_2$ is a normal subgroup of index 3 of G, and such that there exists an element $x \in G \setminus N$ of odd order with $x^3 \in G_2$. We may assume that Σ_2 is a generalized quaternion group since otherwise G would be isomorphic to a Z-group and we would be done. We will first show that Σ_2 is in fact a quaternion group of order 8. Conjugation with x defines an automorphism of order 3 on Σ_2 because $x^3 \in G_2$ and Σ_2 and G_2 commute. By [24, Aufgabe 56, p. 94] we know that the automorphism group of a generalized quaternion group of order larger than 8 is a 2-group, whereas the automorphism group of the quaternion group of order 8 has 24 elements. This shows that Σ_2 is a quaternion group of order 8, and there are μ and γ such that $\Sigma_2 = \langle \mu, \gamma \mid \mu^4 = 1, \mu^2 = \gamma^2, \mu^\gamma = \mu^{-1}\rangle$. One automorphism of order 3 of Σ_2 is given by $\mu \mapsto \gamma$, $\gamma \mapsto \mu\gamma$, as is easily checked. It can be shown that *any* automorphism of order 3 of Σ_2 is conjugate (in the automorphism group of Σ_2) to either this automorphism, or to its square. Thus, by replacing x with x^2 if necessary, and by replacing μ and γ with two other appropriate generators of Σ_2, we may assume that $\mu^x = \gamma$ and $\gamma^x = \mu\gamma$.

Since G_2 is a normal subgroup of G, conjugation with x leaves G_2 invariant, so $\langle G_2, x\rangle$ is a subgroup of G of odd order $3|G_2|$. Hence, G_2 and x generate a group isomorphic to $G_{m,r}$ for some admissible (m, r): $\langle G_2, x\rangle = \langle \sigma, \tau \mid \sigma^m = 1, \tau^n = \sigma^t, \sigma^\tau = \sigma^r\rangle$.

We want to show that $\tau \notin G_2$ and $\sigma^{m/t} \in G_2$. If $\tau \in xG_2$, this would show that $\mu^\tau = \gamma, \gamma^\tau = \mu\gamma, \mu^{\sigma^{m/t}} = \mu, \gamma^{\sigma^{m/t}} = \gamma$, since G_2 and Σ_2 commute. If $\tau \in x^2G_2$, this would show that $\mu^\tau = \mu\gamma$, and $\gamma^\tau = \mu$, so interchanging μ and γ would take us back to the previous case, and hence to the description of $E_{m,r}$.

Suppose first that $\sigma^{m/t} \notin G_2$. Then 3 does not divide m/t, so 3 divides t, since 3 divides mn, the order of $G_{m,r}$. By Remark 2, we see that 3 does not divide nr_0. This shows that $\tau \in G_2$. So, $\mu^{\sigma^\tau} = \mu^\sigma$, since Σ_2 and G_2 commute. On the other hand, $\mu^{\sigma^\tau} = \mu^{\sigma^r}$, which shows that $r \equiv 1 \bmod 3$. This contradicts the assumption $\gcd(r-1,t) = 1$, and proves that $\sigma^{m/t}$ is in G_2.

Suppose now that $\tau \in G_2$. This shows that $\sigma \notin G_2$, since otherwise $G_{m,r} = G_2$. Therefore, 3 divides m/t, since $\sigma^{m/t} \in G_2$. But $\tau^n = \sigma^t \notin G_2$, which contradicts the assumption. Therefore, $\tau \notin G_2$, and we are done.

(4) Suppose that G/G_1 is isomorphic to the symmetric group S_4. Obviously, G contains a normal subgroup G_2 of index 2 such that G_2/G_1 is isomorphic to A_4. Hence, G_2 is either of type $G_{m,r}$ or of type $E_{m,r}$. If G_2 is of type $G_{m,r}$, then we are back in case (2), since G/G_2 is cyclic of order 2. So, we may suppose that G_2 is of type $E_{m,r}$. We denote the generators of this group by $\sigma, \tau, \mu, \gamma$. In [12, pp. 204] it is proved that there is an element ν of order 4 in $G \setminus G_2$ such that conjugation with ν leaves $H = \langle \sigma, \tau \rangle$ fixed. Since fixed-point-free groups have at most one element of order 2, we see that $\nu^2 = \mu^2$. Hence, ν^2 commutes with all the elements of H, and conjugation with ν is an automorphism of order 2 on H. In the same way as in (2), it can now be shown that $\sigma^\nu = \sigma^\ell$ and $\tau^\nu = \tau^\ell$, where $\ell^2 \equiv 1 \bmod m$ and $\ell \equiv 1 \bmod n$. Conjugation with ν is an automorphism of order 2 of Σ_2, the 2-Sylow subgroup of G (this is because Σ_2 is a characteristic subgroup). As in part (3), we may w.l.o.g. that $\mu^\nu = \gamma^{-1}$ and $\gamma^\nu = \mu^{-1}$. To see that $\ell \equiv -1 \bmod 3$, we compute the quantity $\mu^{\tau^\ell} = \mu^{\tau^\nu} = \mu^{\nu\tau\nu^{-1}} = ((\mu^{\nu^{-1}})^\tau)^\nu = ((\gamma^{-1})^\tau)^\nu = (\gamma^{-1}\mu^{-1})^\nu = \mu\gamma$. Note that $\mu^\tau = \gamma$, $\mu^{\tau^2} = \mu\gamma$, and $\mu^{\tau^3} = \mu$, so $\mu^{\tau^\ell} = \mu\gamma$ if and only $\ell \equiv -1 \bmod 3$. Since $\ell \equiv 1 \bmod n$, we also conclude that 3 does not divide n. On the other hand, 3 divides nr_0 since G contains the group G_2 of type $E_{m,r}$. As a result, 3 divides r_0.

□

The next step of the classification theorem consists of identifying the non-solvable fixed-point-free groups. As it turns out, the prototype of non-solvable fixed-point-free groups is given by the group $\mathrm{SL}_2(\mathbb{F}_5)$ of 2×2-matrices of determinant 1 over the field $\mathrm{GF}(5)$. This group has the following generators and relations [12, pp. 210]:

$$\mathrm{SL}_2(\mathbb{F}_5) = \langle \mu, \gamma \mid \mu^2 = \gamma^3 = (\mu\gamma)^5, \mu^4 = 1 \rangle. \tag{A.1}$$

We gather some basic useful facts about this group.

Lemma 3. (1) *The right cosets of* $\mathrm{SL}_2(\mathbb{F}_5)$ *modulo the cyclic subgroup* H *of order* 10 *generated by* $\mu\gamma$ *are given by* $1, \mu, \gamma, \gamma\mu, \gamma\mu\gamma, (\gamma\mu)^2, \gamma\mu\gamma^2, (\gamma\mu)^2\gamma, (\gamma\mu)^2\gamma^2, (\gamma\mu)^2\gamma^2\mu, (\gamma\mu)^2\gamma^2\mu\gamma, (\gamma\mu)^2\gamma(\gamma\mu)^2$.

(2) *The group generated by μ and $\lambda = (\mu\gamma)^7(\gamma\mu)^2\gamma(\gamma\mu)^2$ is a 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{F}_5)$ and it is isomorphic to a quaternion group.*

Proof. (1) This assertion can be proved using any of the usual coset counting algorithms like the Todd-Coxeter algorithm. We have used the computer algebra package GAP [25] to compute the cosets.

(2) The 2-Sylow subgroups of $\mathrm{SL}_2(\mathbb{F}_5)$ are of order 8. Further, it is easily checked that $\mu^\gamma = (\mu\gamma)^5\gamma\mu\gamma^2$. This shows that $\mu^\lambda = \mu^{-1}$. Further, $\lambda^2 = \mu^2$, as can be checked directly. Hence, $\langle \mu, \lambda \rangle$ is a generalized quaterion group and the assertion is proved. □

The following theorem classifies all non-solvable fixed-point-free groups. It has been essentially proved in [12, Satz 16] and [23, Th. 18.6]. Our contribution is the derivation of the group description in terms of generators and relations.

Theorem 11. *Let G be a non-solvable fixed-point-free group. Then G is isomorphic to one of the following groups.*

(1) *The group*

$$J_{m,r} = \mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r},$$

with admissible (m, r) such that $\gcd(mn, 120) = 1$.

(2) *The group*

$$K_{m,r,\ell} = \langle J_{m,r}, \nu \rangle$$

with the relations

$$\nu^2 = \mu^2, \mu^\nu = (\mu\gamma)^7(\gamma\mu)^2\gamma(\gamma\mu)^2, \gamma^\nu = \gamma, \sigma^\nu = \sigma^\ell, \tau^\nu = \tau^\ell,$$

where $\ell^2 \equiv 1 \bmod m$, $\ell \equiv 1 \bmod n$ and $\ell \equiv -1 \bmod s$.

Proof. By [23, Th. 18.6] G contains a normal subgroup N of index 1 or 2 where $N = \mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r}$ with (m, r) admissible and $\gcd(mn, 120) = 1$. If $G = N$, then we are in case (1) and are done. Otherwise, let S denote a 2-Sylow subgroup of G. Since any 2-Sylow subgroup of N is a 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{F}_5)$, S is a quaternion group of order 8 by Lemma 3(2). By the same lemma, we may take $S = \langle \mu, \lambda \rangle$, where μ is the generator of $\mathrm{SL}_2(\mathbb{F}_5)$ as given in (A.1), and λ is, as before, the element $\lambda = (\mu\gamma)^7(\gamma\mu)^2\gamma(\gamma\mu)^2$.

Hence, the 2-Sylow subgroups of G are generalized quaternion groups of order 16. Let S' be a 2-Sylow subgroup of G such that $S' \cap N = S$. Then S' has two generators α, β such that $\alpha^8 = 1$, $\alpha^4 = \beta^2$, $\alpha^\beta = \alpha^{-1}$, and $\mu = \beta$, and $\lambda = \alpha^2\beta$. The element $\nu = \alpha\beta \in S'$ satisfies $\mu^\nu = \lambda$, $\lambda^\nu = \mu$, and $\nu^2 = \mu^2$. To compute γ^ν we proceed as follows. Let $x = \gamma^\nu$. Then we have $x^3 = (\gamma^3)^\nu = (\mu^2)^\nu = \mu^2 = \gamma^3$. Further, using the definition of λ, we see that

$$\mu = \lambda^\nu = (\lambda x)^7 (x\lambda)^2 x (x\lambda)^2.$$

We search over all 120 elements of $\mathrm{SL}_2(\mathbb{F}_5)$ to find an element x satisfying the above equality together with $x^3 = \gamma^3$. This reveals that there are only two possibilities for x: $x = \gamma$ or $x = \gamma^{-1}$. Both these choices lead to isomorphic groups; namely, if $x = \gamma^{-1}$, then replace γ by $(\mu\gamma)^6\mu$. This preserves the relations among μ and γ, and additionally implies $\gamma^\nu = \gamma$. (All these steps require calculations in the group $\mathrm{SL}_2(\mathbb{F}_5)$ which we did using GAP [25].)

This explains the action of ν on the characteristic subgroup $\mathrm{SL}_2(\mathbb{F}_5)$ of N. Since $G_{m,r}$ is also a characteristic subgroup of N, ν together with $G_{m,r}$ generate a group of type $D_{m,r,\ell}$, and we obtain the relations $\ell^2 \equiv 1 \bmod m$ and $\ell \equiv 1 \bmod n$. □

B Irreducible representations of the fixed-point-free groups

In this section we prove Theorem 2 which will also provide the proof of the second half of Theorem 1.

The fixed-point-free representations of the groups $G_{m,r}$ are computed in Section 4.3. We briefly summarize the method. The cyclic group N generated by σ is a normal subgroup of $G = S_{m,r}$. If Δ is an irreducible fixed-point-free representation of G, then $\Delta \downarrow N$ is a direct sum of primitive characters of N. On the other hand, if χ is a primitive character, then its inertia group is N, which means that the induction of χ to N is irreducible. Hence, all irreducible fixed-point-free representations of G are obtained as inductions of primitive characters of N. Two such inductions only differ by a Galois conjugation (since any two primitive characters of N differ only by a Galois conjugation), hence either they are all fixed-point-free, or none of them is fixed-point-free. Invoking [12, Satz 9] or Lemma C.1, we see that indeed all these representations are fixed-point-free.

Our strategy for computing the fixed-point-free representations of the classified groups is similar to the above. For solvable groups, we study restrictions of fixed-point-free representations to normal subgroups, compute their inertia groups, and then extend and/or induce those representations. For non-solvable groups, the strategy is more ad hoc and is explained below.

The first part of this appendix considers solvable groups.

Proof of Theorem 2—Solvable groups: in this part we prove items (1)–(4) of Theorem 2.

(1) Let Δ be a fixed-point-free representation of $G = G_{m,r}$. The restriction of Δ to $N = \langle \sigma \rangle$ is a direct sum of primitive characters of N. On the other hand, it is easily shown that the inertia group of any primitive character of N coincides with N. Hence, by Frobenius reciprocity [26, XVIII, Th. 6.1], all irreducible fixed-point-free representations of G are obtained as inductions of primitive characters of N. These inductions are given in the statement of the theorem and are derived in Section 4.3. We only need to show that all of them are indeed fixed-point-free. Note that Theorem 10 implies that the condition of (m, r) being admissible is necessary for G to be fixed-point-free. Hence, we are left with proving the sufficiency of this condition. To do this, we need to show that for any $x = 0, \dots, m-1$ and $k = 0, \dots, n-1$, $(x, k) \neq (0, 0)$ the matrix $I_n - A^x B^k$ is invertible, where A and B are defined in the statement of Theorem 2. The assertion is obviously clear for $k = 0$. Hence, we may suppose that $k > 0$. Now we invoke the determinant formula (C.1) to obtain

$$\det\left(I_n - A^x B^k\right) = \prod_{i=0}^{q-1} \left(1 - \xi^{tk/q} \prod_{j=0}^{n/q-1} \xi^{xr^{jq+i}}\right), \tag{B.2}$$

where $q = \gcd(n-k, n) = \gcd(n, k)$. It is required to show that this determinant is nonzero. This is the case if

$$\xi^{xr^i \frac{r^n-1}{r^q-1} + tk/q} \neq 1,$$

or, equivalently, if

$$t\frac{k}{q} + \frac{r^n-1}{r^q-1} xr^i \not\equiv 0 \bmod m$$

for all $i = 0, \dots, q-1$, $k = 1, \dots, n-1$ and $x = 0, \dots, m-1$. But by Lemma 5 (which is proven later) this is true since (m, r) is admissible.

(2) Let $N = \langle \sigma, \tau \rangle = G_{m,r}$. We first prove that the induction of a fixed-point-free representation of N to $G = D_{m,r,\ell}$ is irreducible. By [15, Theorem 5.20, Cor. 3] it is sufficient to show that there is no invertible matrix T such that $TF(\sigma^\gamma)T^{-1} = F(\sigma)$ and $TF(\tau^\gamma)T^{-1} = F(\tau)$. This is left to the reader. This shows that the inertia group of F is N, hence the induction of F to G is irreducible. On the other hand, the restriction of any fixed-point-free representation of G to N is a direct sum of fixed-point-free representations of N. Invoking the Frobenius reciprocity [26, XVIII, Th. 6.1], we see that all irreducible fixed-point-free representations of G are obtained from inductions of irreducible fixed-point-free representations of N. The representations given in the statement of the theorem are precisely these inductions. We only need to prove

now that the representations computed are in fact fixed-point-free. For this, we need to show that for any $x = 0, \ldots, m-1$, $y = 0, \ldots, n-1$, $z = 0, 1$, $(x, y, z) \neq (0, 0, 0)$, the matrix $I_{2n} - A^x B^y R^z$ is invertible, where A, B, R are as in the statement of the theorem. If $z = 0$, then this follows from the previous part by noting that (m, r) is admissible. Hence, we may suppose that $z = 1$. In this case we immediately obtain

$$\det{(I_{2n} - A^x B^y R)} = \det{(I_n + A_0^{\ell x} B_0^{\ell y} A_0^x B_0^y)}.$$

Since $B_0^{nr_0/2} = -I_n$ it suffices to show that

$$\det{(I_n - B_0^{nr_0/2} A_0^{\ell x} B_0^{\ell y} A_0^x B_0^y)} \neq 0.$$

In view of the previous part, this is equivalent to showing that

$$\tau^{nr_0/2} \sigma^{\ell x} \tau^{\ell y} \sigma^x \tau^y \neq 1.$$

Equivalently, we need to show that

$$\sigma^{\ell x} \tau^{\ell y} \sigma^x \tau^y \neq \tau^{nr_0/2}.$$

Let $\alpha = \sigma^x \tau^y$. Then, the latter condition is equivalent to $\alpha^\gamma \alpha \neq \gamma^2$, or $(\gamma\alpha)^2 \neq 1$. Suppose that $(\gamma\alpha)^2 = 1$. Since all elements of $D_{m,r\ell}$ commute with $\tau^{nr_0/2}$, this condition shows that $(\gamma\alpha)$ and $\tau^{nr_0/2}$ generate an abelian group of order 4 which is not cyclic. But this is a contradiction, since the 2-Sylow subgroups of $D_{m,r,\ell}$ are generalized quaternion groups and they do not contain a non-cylic subgroup of order 4.

(3) We compute the irreducible fixed-point-free representations of $G = E_{m,r,\ell}$ by considering the tower of normal subgroups

$$N = \langle \mu, \gamma \rangle \subset H = \langle \sigma, \mu, \gamma \rangle \subset G.$$

First, observe that $N = D_{4,1,-1}$. Hence, using the previous step, we see that N has exactly one irreducible fixed-point-free representation F given by

$$F(\mu) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad F(\gamma) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

F can be extended to an irreducible representation of H (which we denote by F as well). Indeed, it can be shown that any matrix C for which $CF^{\sigma}C^{-1} = F$ is a multiple of

$$T = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}.$$

We may thus set $F(\sigma) = cT$ for some constant c which can be determined using the identity $F(\sigma^m) = I_2$. Because 3 divides m, we have $(cT)^m = c^m 2^{m/2} \xi^{m/3} I_2$, where $\xi = \mathrm{e}^{2\pi i/8}$. This shows that $c = \mathrm{e}^{2\pi iz/m}\xi^5/\sqrt{2}$, where z and $m/3$ are coprime (otherwise there is a power of cT other than m which is the identity matrix). It is easy to check that the inertia group of F is equal to H, so that the induction of F to G is irreducible. This induction has been given in the statement of the theorem. Conversely, any fixed-point-free representation of G restricted to H is a direct sum of irreducible fixed-point-free representations of H, and by Frobenius reciprocity we see that all irreducible fixed-point-free representations are inductions of irreducible fixed-point-free representations of N.

To show that the representations computed are in fact fixed-point-free, we proceed as follows. We first show that the restriction of the representation to $N = \langle \sigma, \mu, \gamma \rangle$ is fixed-point-free. We recall that $z = 1$ if 9 divides m and is 3 otherwise. First, we show the assertion in the case $(m, r) = (3, 1)$. Here we have to check the eigenvalues of the 24 matrices generated by

$$A_{0,3} = \frac{\xi^5}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \quad F_0 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad , F_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We leave this simple calculation to the reader.

Next, note that, for any k, we have the following:

$$A_{0,z}^{3k} = \alpha^{3k} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_{0,z}^{3k+1} = \alpha^{3k+1} \frac{\xi^5}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \quad A_{0,z}^{3k+2} = \alpha^{3k+2} \left(\frac{\xi^5}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \right)^2,$$

where $\alpha = \mathrm{e}^{2\pi iz/m}$. We will now have to show that $A_{0,z}^x F_0^y F_1^u$ does not have eigenvalue 1 if it is not the identity matrix. Let $x = 3k$. Then $A_{0,z}^x F_0^y F_1^u = \alpha^{3k} U$, where $U = F_0^y F_1^u$. Note that the eigenvalues of U are roots of unity of even order if U is not the identity matrix, since the group $\langle F_0, F_1 \rangle$ has order 8. On the other hand, α^{3k} is a root of unity of odd order (since α is a root of unity of odd order). Hence $\alpha^{3k} U$ has eigenvalue 1 if and only if $\alpha^{3k} = 1$ and U is the identity matrix, i.e., if and only if $A_{0,z}^x F_0^y F_1^u$ is the identity matrix. Next suppose that $x = 3k + 1$. Then $A_{0,z}^x F_0^y F_1^u = \alpha^{3k+1} M$, where M is a matrix in $E_{3,1}$. Since $E_{3,1}$ has order 24, all matrices in this group have eigenvalues which are 24th roots of unity. So, if $\alpha^{3k+1}M$ has eigenvalue one, then α^{3k+1} is a 24th root of unity, i.e., $24z(3k+1) \equiv 0 \bmod m$. If 9 divides m, then $z=1$, and this implies that $3k+1 \equiv 0 \bmod m/3$, which is a contradiction. If 9 does not divide m, then $z=3$, and the condition is $3k+1 \equiv 0 \bmod (m/3)$, which implies $\alpha^{3k+1}=1$. In that case, M has to be the identity matrix, since we know that $E_{3,1}$ is fixed-point-free and $\alpha^{3k+1}M$ has eigenvalue 1 by assumption. Altogether, this shows that $A_{0,z}^x F_0^y F_1^u$ has eigenvalue 1 only if it is the identity matrix. The case $x=3k+2$ is handled analogously. This completes the proof of the fact that the restriction of the representation given in the statement of the theorem to N is fixed-point-free.

Next, we study $I_{2n} - A_z^x P^y Q^v B_z^u$ for $x=0,\dots,m-1$, $y=0,\dots,3$, $v=0,1$, and $u=0,\dots,n-1$. We may suppose that $u>0$, since we have already shown that the restriction of the representation to N is fixed-point-free. A slight generalization of Lemma C.1 shows that

$$\det\left(I_{2n} - A_z^x P^y Q^v B_z^u\right) = \prod_{i=0}^{q-1} \det\left(I_2 - \prod_{j=0}^{n/q-1} \left(A_{0,z}^{r^{qj+i}x} F^y_{(jq+i) \bmod 3} F^u_{(jq+i+1) \bmod 3}\right) A_{0,z}^{tu/q}\right),$$

where $q=\gcd(n,u)$. Let $M=A^x$. Note that $M^k U M^{-k} \in \langle P,Q\rangle$ for $U \in \langle P,Q\rangle$ and any k, since $\langle P,Q\rangle$ is a normal subgroup of the constellation. Collecting terms, we see that

$$I_2 - \prod_{j=0}^{n/q-1} \left(A_{0,z}^{r^{qj+i}x} F^y_{(jq+i) \bmod 3} F^u_{(jq+i+1) \bmod 3}\right) A_{0,z}^{tu/q} = I_2 - U A_{0,z}^{tu/q+(r^n-1)/(r^q-1)xr^i},$$

for some $U \in \langle P,Q\rangle$. Since we have shown that the restriction of the representation to N is fixed-point-free, we know that the matrix above is invertible if it is nonzero. But since the order of $A_{0,z}$ is odd and that of U is a power of 2, the matrix is nonzero if and only if $tu/q + (r^n-1)/(r^q-1)xr^i \not\equiv 0 \bmod m$ for any $i=0,\dots,q-1$, $u=1,\dots,n-1$, and $x=0,\dots,m-1$. Lemma 5 proves that the latter condition is satisfied if (m,r) is admissible, and we are done.

(4) $G=F_{m,r,\ell}$ has the normal subgroup $E=\langle\sigma,\tau,\mu,\gamma\rangle$ of type $E_{m,r}$ of index 2. Let Δ be one of the irreducible fixed-point-free representations of E as computed in the previous part of the proof. It is easily checked that Δ^ν is not equivalent to Δ if $n>1$, by considering $\Delta(\tau^\nu)=\Delta(\tau^\ell)$. In this case, the induction of Δ to G is irreducible, and it has been computed in the assertion of the theorem. If $n=1$, then Δ may or may not be extendable to G. To see when it is and when it is not, we first look at $\Delta^\nu(\mu)$ and $\Delta^\nu(\gamma)$. From this, we easily check that any matrix T for which $T\Delta^\nu T^{-1}=\Delta$ has to be a multiple of R. By checking the condition $T\Delta^\nu(\sigma)T^{-1}=\Delta(\sigma)$, we arrive at $R_0 A_{0,z}^\ell = A_{0,z} R_0$. This shows that $z(\ell-1) \equiv 0 \bmod m$,

and since z and $m/3$ are coprime, we see that $\ell \equiv 1 \bmod m/3$, which also shows that $m/3 \not\equiv 0 \bmod 3$, since $\ell \equiv -1 \bmod 3$. Hence, $z \equiv 0 \bmod 3$. Altogether, this shows that in case $\ell \equiv 1 \bmod m/3$ and $n = 1$, representations Δ mapping σ to A_z with z divisible by 3 are extendable to G; and if 3 does not divide z, then the induction of this representation is irreducible.

If Δ can be extended, then $\Delta(\nu) = cR$ for some constant c which is determined by the requirements $\Delta(\nu^4) = I_{2n}$, $\Delta(\nu^2) \neq I_{2n}$. Since $R^2 = -I_{2n}$, this leaves the choices $c = 1$ and $c = -1$ of which we choose $c = 1$.

The proof that the computed representations are indeed fixed-point-free is similar to part (3). □

Next we concentrate on computing the irreducible fixed-point-free representations of the non-solvable groups of the previous section. We need the following isolated result.

Lemma 4. *The only fixed-point-free representations of* $\mathrm{SL}_2(\mathbb{F}_5)$ *are the two* 2*-dimensional representations given by*

$$\begin{aligned} \gamma \mapsto P &= \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^2 - \eta^3 & \eta - \eta^4 \\ \eta - \eta^4 & \eta^3 - \eta^2 \end{pmatrix}, \\ \nu \mapsto Q &= \frac{1}{\sqrt{5}} \begin{pmatrix} \eta - \eta^2 & \eta^2 - 1 \\ 1 - \eta^3 & \eta^4 - \eta^3 \end{pmatrix}, \end{aligned}$$

where $\eta \in \{e^{2\pi i/5}, -e^{4\pi i/5}\}$.

Proof. It can be easily verified that the given maps are indeed fixed-point-free representations of the group $G = \mathrm{SL}_2(\mathbb{F}_5)$. One needs to check that $P^2 = Q^3 = (PQ)^5$ and $P^4 = 1$. Further, it is easily checked that the two representations given are inequivalent.

Showing that these representations are the only fixed-point-free representations of G is slightly involved. Basically, we need to compute all the irreducible representations of G, and test whether they are fixed-point-free. We sketch an alternative to this method by using the character table of G rather than all the representations. The *character* of a representation at a given group element is the trace of the representation evaluated at that element. Characters are obviously constant on conjugacy classes of G. The character table of G is an $h \times h$-matrix where h is the number of conjugacy classes of G, whose rows are indexed by the irreducible representations of G and whose columns are indexed by the conjugacy classes. Position (i, j) of this matrix contains the value of the character of the ith irreducible representation of G at an arbitrary element of the jth conjugacy class.

Let χ denote the character of a representation Δ and suppose that Δ is d-dimensional. Then, for any element σ in G the eigenvalues of $\Delta(\sigma)$ can be recovered from $\chi(\sigma), \chi(\sigma^2), \ldots, \chi(\sigma^d)$ (up to permutation). To see this, note that $\chi(\sigma^k)$ equals $\omega_1^k + \cdots + \omega_d^k$, where $\omega_1, \ldots, \omega_d$ are the eigenvalues of $\Delta(\sigma)$. Hence, if we know the character table of G, and, for each element σ, the conjugacy class of $\sigma, \sigma^2, \ldots, \sigma^d$, then we can compute for each irreducible representation the eigenvalues of that representation on the group elements and test whether we encounter the eigenvalue 1.

The character table of G can be found in [27, p. 155]. Applying the procedure outlined above, we see that the only fixed-point-free representations of G are the ones given above. □

Proof of Theorem 2—Non-solvable groups: here, we concentrate on proving items (5) and (6) of Theorem 2. The assertions on the explicit form of the constellations follows from Lemma 3(1).

(5) The irreducible representations of $\mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r}$ are of the form $\Delta \otimes F$, where Δ and F run over a set of pairwise inequivalent irreducible representations of S and $G_{m,r}$, respectively. Clearly, for $\Delta \otimes F$ to be fixed-point-free, both Δ and F have to be fixed-point-free. This necessary condition is also sufficient if $\gcd(|S|, |G_{m,r}|) = 1$. (To see this, note that the eigenvalues of $A \otimes B$ are products of the eigenvalues of A and B. If A and B have eigenvalues that are roots of unity of coprime orders, the products of these eigenvalues cannot be one.) So, the irreducible fixed-point-free representations of $\mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r}$ are given by $\sigma \mapsto I_2 \otimes A_0$, $\tau \mapsto I_2 \otimes B_0$, $\gamma \mapsto P_0 \otimes I_n$, $\nu \mapsto Q_0 \otimes I_n$, with the matrices A_0, B_0, P_0, Q_0 given above.

(6) $\mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r}$ is a normal subgroup of $K_{m,r,\ell}$ of index 2. It is easily seen that the inertia groups of the representations computed in the previous part coincide with $\mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r}$; hence their induction is irreducible, and all irreducible fixed-point-free representations are obtained this way. The representation given in the statement of the theorem is an induction of a fixed-point-free representation of $N = \mathrm{SL}_2(\mathbb{F}_5) \times G_{m,r}$ along the cosets $N, \nu N$. It is easy to show that the representations given are in fact fixed-point-free. The proof can be accomplished along the lines of the other proofs of this type outlined in the paper, and is left to ther reader. □

We close this section by stating and proving a lemma that has been used extensively above.

Lemma 5. *Let (m, r) be an admissible pair of integers, n be the order of r modulo m, $r_0 = \gcd(m, r-1)$, $t = m/r_0$, $k \in \{1, \ldots, n-1\}$, and $x \in \{0, \ldots, m-1\}$. Furthermore, let $q = \gcd(k, n)$ and $i \in \{0, \ldots, q-1\}$. Then we have*

$$t\frac{k}{q} + \frac{r^n - 1}{r^q - 1} x r^i \not\equiv 0 \bmod m.$$

Proof. We first transform the statement of the theorem into a simpler form. Since $x \in \{0, \dots, m-1\}$, we can replace xr^i with x, so that we may assume w.l.o.g. that $i = 0$. Further, it is well-known and easy to prove that an equation $a + by \equiv 0 \bmod m$ has a solution for y if and only if $\gcd(b, m)$ divides a. Hence, denoting by d the value $\gcd(m, (r^n - 1)/(r^q - 1))$, we see that the statement of the theorem is equivalent to $tk/q \not\equiv 0 \bmod d$. We now prove that any prime p dividing n/q also divides d. This proves the desired result, since the prime p cannot divide t (since $\gcd(n, t) = 1$), it also cannot divide k/q (since $q = \gcd(n, k)$), and so d cannot divide tk/q (otherwise any prime factor of d would have to divide either t or k/q). Let p be a prime dividing n/q. Since (m, r) is admissible, any prime divisor of n divides $\gcd(m, r-1)$, which implies that $r \equiv 1 \bmod p$. Now

$$\frac{r^n - 1}{r^q - 1} = 1 + r^q + \cdots + r^{(n/q-1)q} \equiv \frac{n}{q} \equiv 0 \bmod p,$$

which proves the desired assertion. $\square$

C The determinant of doubly-banded matrices

Lemma 6. *Let $a_1, \dots, a_M$, $b_1, \dots, b_M$ be arbitrary, and let $1 \leqslant K \leqslant M$. Define the $M \times M$ doubly-banded matrix*

$$D(M,K) = \begin{pmatrix}
a_1 & 0 & \cdots & 0 & -b_1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
0 & a_2 & \cdots & 0 & 0 & -b_2 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_{s-1} & 0 & 0 & \cdots & -b_{s-1} & 0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & a_s & 0 & \cdots & 0 & -b_s & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & a_{s+1} & \cdots & 0 & 0 & -b_{s+1} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & a_{K-1} & 0 & 0 & \cdots & -b_{K-1} \\
-b_K & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a_K & 0 & \cdots & 0 \\
0 & -b_{K+1} & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & a_{K+1} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & -b_M & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & a_M
\end{pmatrix}.$$

Then

$$\det D(M,K) = \prod_{i=1}^{q} \left(\prod_{j=0}^{\frac{M}{q}-1} a_{jq+i} - \prod_{j=0}^{\frac{M}{q}-1} b_{jq+i} \right), \tag{C.1}$$

where $q = \gcd(M, K-1)$*. In particular, when* $q = 1$*, we have*

$$\det D(M,K) = a_1 \cdots a_M - b_1 \cdots b_M. \tag{C.2}$$

Proof. We first prove the result for $q = 1$, using induction on M. For $M = 2$, we have

$$\det \begin{pmatrix} a_1 & -b_1 \\ -b_2 & a_2 \end{pmatrix} = a_1 a_2 - b_1 b_2,$$

as desired. Assume now that for all matrix dimensions less than M, whenever $q = 1$, equation (C.2) holds. We shall show that (C.2) holds for matrices of dimension M. Let K be chosen such that $\gcd(M, K-1) = 1$ and assume, without loss of generality, that $K - 1 < M - K + 1$ (we can always arrange this by considering the transpose of $D(M,K)$). Partition $D(M,K)$ as

$$D(M,K) = \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix},$$

where

$$D_{11} = \text{diag}\,(a_1, \ldots, a_{K-1}), \quad D_{12} = \begin{pmatrix} 0_{(K-1)\times(M-2K+2)} & \text{diag}\,(-b_1, \ldots, -b_{K-1}) \end{pmatrix}$$

and

$$D_{21} = \begin{pmatrix} \text{diag}\,(-b_K, \ldots, -b_{2K-2}) \\ 0_{(M-2K+2)\times(K-1)} \end{pmatrix}, \quad D_{22} = \begin{pmatrix} a_K & & & \\ & \ddots & & \\ -b_{2K-1} & & \ddots & \\ & \ddots & & \ddots & \\ & & -b_M & & a_M \end{pmatrix}.$$

We have

$$\begin{aligned}
\det D(M,K) &= \det D_{11} \det \left(D_{22} - D_{21} D_{11}^{-1} D_{12}\right) \\
&= \det (D_{11}) \det \underbrace{\begin{pmatrix} \text{diag}\,(a_K, \ldots, a_{2K-2}) & \text{diag}\,(-\frac{b_1 b_K}{a_1}, \ldots, -\frac{b_{K-1} b_{2K-2}}{a_{K-1}}) \\ \text{diag}\,(-b_{2K-1}, \ldots, -b_M) & \text{diag}\,(a_{2K-1}, \ldots, a_M) \end{pmatrix}}_{\bar{D}} .
\end{aligned}$$

Note that $\bar{D}$ is a $(M-K+1) \times (M-K+1)$ doubly-banded matrix and that $\gcd(M-K+1, K-1) = 1$. Thus,

$$\det \bar{D} = a_K \ldots a_M - \frac{b_1 \ldots b_M}{a_1 \ldots a_{K-1}},$$

so that

$$\det D(M,K) = a_1 \cdots a_M - b_1 \cdots b_M,$$

which is the desired result.

When $\gcd(M, K-1) = q$, $D(M,K)$ can be partitioned into $q \times q$ diagonal blocks, as follows:

$$D(M,K) = \begin{pmatrix}
A_1 & & & -B_1 & & \\
& \ddots & & & \ddots & \\
& & A_{\frac{K-1}{q}} & & & -B_{\frac{K-1}{q}} \\
-B_{\frac{K-1}{q}+1} & & & A_{\frac{K-1}{q}+1} & & \\
& \ddots & & & \ddots & \\
& & -B_{\frac{M}{q}} & & & A_{\frac{M}{q}}
\end{pmatrix},$$

where

$$A_i = \text{diag}\ \left(a_{(i-1)q+1}, \ldots, a_{(i-1)q+q}\right), \quad B_i = \text{diag}\ \left(b_{(i-1)q+1}, \ldots, b_{(i-1)q+q}\right).$$

Repeating the arguments for $q = 1$, to the above block diagonal matrix (since $\gcd(\frac{M}{q}, \frac{K-1}{q}) = 1$ and diagonal matrices commute), we have:

$$\det D(M,K) = \det\ \left(A_1 \ldots A_{\frac{M}{q}} - B_1 \ldots B_{\frac{M}{q}}\right),$$

which yields the desired result (C.1). □

D Information-theoretic aspects of differential modulation

We briefly justify the design of good constellations of unitary-space time signals by computing the information rates theoretically achievable with differential modulation. We show that, for large M, differential modulation as presented in Section 2.3 can theoretically achieve rates of approximately $N \log(1 + \rho/2)$, only slightly less than the space-time autocapacity of the channel $N \log(1 + \rho)$ [8] (achievable as $M \to \infty$). Thus, differential modulation can attain a significant fraction of the channel capacity without further channel coding. To save space, our reasoning is intuitive and physical and avoids extensive rigor.

D.1 Mutual information for differential unitary space-time modulation

We refer to the model (1) and employ differential modulation (5), where the channel is constant over $2M$ time samples. Thus,

$$\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \sqrt{\rho} \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} H + \begin{pmatrix} W_1 \\ W_2 \end{pmatrix}, \tag{D.1}$$

where H, W_1, and W_2 are $M \times N$ matrices of independent $\mathcal{CN}(0, 1)$-distributed random variables. We assume that our constellation of differential signals is well approximated by a constellation of randomly chosen isotropically distributed unitary matrices. An isotropically distributed random matrix has a probability distribution that does not change when the matrix is pre- or post-multiplied by a deterministic unitary matrix (see, e.g., [6, 8]). Therefore, the matrices S_1 and S_2 are $M \times M$ and unitary and are independent and isotropically distributed.

In [8] it is proven that there is a space-time *autocapacity* given by $C_a = N \log(1 + \rho)$ associated with transmitting information in a single $M \times 2M$ block of symbols, as $M \to \infty$. We therefore consider the mutual information within a differential modulation block and compare it to the autocapacity. The mutual information between the transmitted signals $\{S_1, S_2\}$ and the received signals $\{X_1, X_2\}$ is

$$I(X_1, X_2; S_1, S_2) = \frac{1}{2M} \left[h(X_1, X_2) - h(X_1, X_2 | S_1, S_2) \right], \tag{D.2}$$

where $h(\cdot)$ denotes entropy. (We normalize the mutual information by the factor $1/2M$ for convenience, since $2M$ is the number of time samples) Note that $\{X_1, X_2\}$, conditioned on $\{S_1, S_2\}$, are zero-mean Gaussian distributed random matrices. Computing the covariance matrix of $\{X_1, X_2\}$ shows that

$$\begin{aligned} h(X_1,X_2|S_1,S_2) &= 2NM\log\pi e + N\log\det\left[I_{2M} + \rho\begin{pmatrix} S_1 \\ S_2\end{pmatrix}\begin{pmatrix} S_1^* & S_2^*\end{pmatrix}\right] \\ &= 2NM\log\pi e + N\log\det\left[I_M + \rho\begin{pmatrix} S_1^* & S_2^*\end{pmatrix}\begin{pmatrix} S_1 \\ S_2\end{pmatrix}\right] \\ &= 2NM\log\pi e + N\log\det\left[I_M + 2\rho I_M\right] \\ &= 2NM\log\pi e + NM\log(1+2\rho). \end{aligned} \tag{D.3}$$

Since H is $M \times N$ complex Gaussian, if we perform the QR decomposition $H = QR$, then Q is $M \times N$ isotropically distributed and independent of R, which is $N \times N$ upper triangular. We may write

$$\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \sqrt{\rho M}\begin{pmatrix} S_1Q \\ S_2Q\end{pmatrix}\frac{1}{\sqrt{M}}R + \begin{pmatrix} W_1 \\ W_2\end{pmatrix} = \sqrt{\rho M}\begin{pmatrix} S_1' \\ S_2'\end{pmatrix}\frac{1}{\sqrt{M}}R + \begin{pmatrix} W_1 \\ W_2\end{pmatrix}, \tag{D.4}$$

where $S_1' = S_1Q$ and $S_2' = S_2Q$ are $M \times N$ independent isotropically unitary random matrices. Furthermore,

$$\begin{aligned} \frac{1}{2M}h(X_1,X_2) &= \frac{1}{2M}h\left(X_1,X_2|\frac{1}{\sqrt{M}}R\right) + \frac{1}{2M}I\left(\frac{1}{\sqrt{M}}R;X_1,X_2\right) \\ &= \frac{1}{M}h\left(X_1|\frac{1}{\sqrt{M}}R\right) + \frac{1}{2M}I\left(\frac{1}{\sqrt{M}}R;X_1,X_2\right), \end{aligned}$$

where the second step uses the conditional independence and identical distributions of X_1 and X_2.

We focus on this expression when M grows but N remains fixed, for then $\frac{1}{\sqrt{M}}R$ converges (with probability one) to an $N \times N$ identity matrix. We therefore have $\frac{1}{2M}I\left(\frac{1}{\sqrt{M}}R|X_1,X_2\right) \to 0$. On the other hand, in this regime $\sqrt{M}S_1'$ behaves as a $M \times N$ matrix of independent $\mathcal{CN}(0,1)$ random variables. Thus, X_1 has the same entropy as a zero-mean complex Gaussian $M \times N$ random matrix with variance $1+\rho$, implying that

$$\lim_{M\to\infty}\frac{1}{M}h\left(X_1|\frac{1}{\sqrt{M}}R\right) = N\log\pi e + N\log(1+\rho).$$

Combining this result with (D.3) yields

$$\lim_{M\to\infty} I(X_1,X_2;S_1,S_2) = N\left[\log(1+\rho) - \frac{1}{2}\log(1+2\rho)\right]. \tag{D.5}$$

Because two consecutive $2M \times M$ signals are overlapped in differential space-time modulation, the maximum achievable rate is twice (D.5), or

$$\lim_{M\to\infty} I_{\text{diff}} = N\left[2\log(1+\rho) - \log(1+2\rho)\right] = N\log\left(1 + \frac{\rho^2}{1+2\rho}\right).$$

At high SNR this mutual information is $N\log(1+\rho/2)$, which is approximately 3 dB less in SNR than $N\log(1+\rho)$, the space-time autocapacity of this channel. (It suffices to say that the autocapacity is the rate theoretically achievable in one channel use as $M \to \infty$ [8].) Thus, for constellations that are composed of approximately independent isotropically distributed random matrices, differential modulation can achieve a significant fraction of the channel capacity.