

# APPLICATIONS OF FINITE GROUP THEORY TO MULTIPLE-ANTENNA DESIGN

JAMES P. COSSEY

ABSTRACT. In this paper, for Dr. Boston's Math 842 class, we summarize the recent results of Shokrollahi et al in [7] regarding the use of methods in the representation theory of finite groups to produce good (full diversity) constellations for wireless antenna communication.

## 1. INTRODUCTION

Much is known about the efficiency of multiple-antenna wireless links in the situation that the channel is known at the receiver (see [1] and [8]). However, the assumption of a known channel is not always feasible when multiple antennas are used. In this paper, which summarizes the results of [7], we see how a generalization of differential phase-shift keying (DPSK) to multiple antennas produces improved results for both low rates and high rates. In particular, we will examine differential unitary space-time signals, which are unitary matrix valued signals, and the group constellations that these give rise to. This generates problems in the representation theory of finite groups.

We begin with the following situation. We have  $M$  transmitting antennas and  $N$  receiving antennas. We assume that they are operating in a Rayleigh flat-fading environment, with a fading coefficient that is statistically independent, and that the received signal is corrupted by additive noise that is independent among the receiver antennas and the time.

Let  $s_{tm}$  be the signal transmitted at time  $t$  on antenna  $m$ , where  $1 \leq m \leq M$ . Let  $x_{tn}$  be the received signal at time  $t$  on receiver  $n$ , where  $1 \leq n \leq N$ . We are assuming that the fading coefficients are complex valued and statistically independent of  $m$  and  $n$  (though not  $t$ ). We also assume that the fading coefficients are  $\mathcal{CN}(0, 1)$  distributed, as is the additive noise at time  $t$  and receiver  $n$ , denoted by  $w_{tn}$ . We normalize the transmitted signals so that the expected value of

$$(1.1) \quad \sum_{m=1}^M |s_{tm}|^2$$

is 1.

With all of these assumptions, then, the action of the channel is given by

$$(1.2) \quad x_{tn} = \sqrt{\rho} \sum_{m=1}^M h_{tmn} s_{tm} + w_{tn}$$

---

1991 *Mathematics Subject Classification.* No idea.

*Key words and phrases.* Representations, Codes.

and by combining the above two equations, we get that the signal-to-noise ratio is  $\rho$ , which is independent of  $M$ .

We assume that the fading coefficients are constant over some time period of  $T$  signals. Let  $S$  be the  $T \times M$  matrix of sent signals,  $X$  the  $T \times N$  matrix of received signals, and  $W$  the  $T \times N$  additive noise matrix. Since we are assuming the fading coefficients are constant over blocks of  $T$  signals, we can represent the fading coefficients over  $T$  signals with an  $M \times N$  matrix  $H$ . Therefore we can put the above equation in the matrix form

$$(1.3) \quad X = \sqrt{\rho}SH + W.$$

Later we will make assumptions on  $T$  and  $M$ , though this is not yet necessary.

Recall that in differential phase-shift keying, the signals sent were the product of the previously sent signal and the data symbol, which were represented by equally spaced points around the unit circle. The idea here will be similar, only instead of data symbols being complex numbers of unit modulus, we will have data symbols of unitary matrices, and the signal sent will be the (matrix) product of the previous symbol and the data symbol.

Let's look at an example of DPSK. Suppose that we have the  $L$  symbols  $0, 1, \dots, L-1$ , which are positive integers, which we can represent as  $\varphi_\ell = e^{2\pi i \ell / L}$ . To send the integers  $z_1, z_2, \dots$  in  $0, 1, \dots, L-1$ , we first send  $s_1 = \varphi_{z_1}$ , then  $s_2 = s_1 \varphi_{z_2}$ ,  $s_3 = s_2 \varphi_{z_3}$ , etc. Decoding is then accomplished by computing  $\theta_t = \arg(\bar{x}_{t-1} x_t)$ , where  $x_t$  is the received signal. We therefore have  $x_t = \sqrt{\rho} h_t s_t + w_t$ , where  $h_t$  is the fading coefficient. We can think of the signals as being composed of two dimensional vectors (or  $2 \times 1$  matrices) of the form

$$(1.4) \quad \Phi_\ell = \frac{1}{\sqrt{2}} \begin{bmatrix} \varphi_{\ell(1)} \\ \varphi_{\ell(2)} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{2\pi i \ell(1)/L} \\ e^{2\pi i \ell(2)/L} \end{bmatrix}$$

which corresponds to  $\ell \in \{0, 1, \dots, L\}$ . Notice that  $\ell(1) - \ell(2) = \ell$  and the choice of matrix is invariant under scalar multiplication by any element of the form  $e^{2\pi i k / L}$  for  $k \in \{0, 1, \dots, L\}$ . Thus to send  $\ell$ , we can send  $\Phi_\ell$  in any of its equivalent forms. To send a stream  $z_1, z_2, \dots$  of symbols, we choose  $\Phi_{z_1}, \Phi_{z_2}, \Phi_{z_3}, \dots$  of the form

$$(1.5) \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ e^{2\pi i z_1 / L} \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} e^{2\pi i z_1 / L} \\ e^{2\pi i (z_1 + z_2) / L} \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} e^{2\pi i (z_1 + z_2) / L} \\ e^{2\pi i (z_1 + z_2 + z_3) / L} \end{bmatrix}$$

etc. Notice that the second entry in each signal is the first entry in the following signal.

If the signal

$$(1.6) \quad X = \begin{bmatrix} x_{t-1} \\ x_t \end{bmatrix}$$

is received, we can then decode by

$$(1.7) \quad (\hat{z}_t)_{ml} = \arg \max_{\ell=0,1,\dots,L-1} |\Phi_\ell^* X|$$

where  $*$  denotes conjugate transpose. (Compare to the computation of  $\theta_t$  above.)

We are now ready to describe the general situation, in which it is assumed that we have  $M$  transmitting antennas and  $N$  receiving antennas. The signals we send will be  $2M \times M$  matrices, each of which is composed of two  $M \times M$  blocks, and as before, the information will be encoded in the "phase difference" of the two matrices. We now choose  $T = 2M$ , in other words, we are assuming that the fading coefficients are constant over a period of  $2M$  signals. The signals are represented by  $\Phi_0, \Phi_1, \dots, \Phi_{L-1}$ . Let  $\Phi_\ell$  have the  $M \times M$  matrices

$V_{\ell(1)}$  and  $V_{\ell(2)}$  in its first and second block, respectively. Before, we wanted to be able to write the symbol in the form

$$(1.8) \quad \frac{1}{\sqrt{2}} \begin{bmatrix} \varphi_{\ell(1)} \\ \varphi_{\ell(2)} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{2\pi i \ell(1)/L} \\ e^{2\pi i \ell(2)/L} \end{bmatrix},$$

so that we could recover the initial symbol by computing the argument of  $\frac{e^{2\pi i \ell(2)/L}}{e^{2\pi i \ell(1)/L}}$ . Now we want the symbol to be of the form

$$(1.9) \quad \Phi_{\ell} = \frac{1}{\sqrt{2}} \begin{bmatrix} V_{\ell(1)} \\ V_{\ell(2)} \end{bmatrix}, \ell = 0, 1, \dots, L-1,$$

so that we can recover the original symbol by computing  $V_{\ell(2)}V_{\ell(1)}^{-1}$ . To be able to do this overlapping, we need to require that for each  $\ell$  and  $\ell'$  in  $0, 1, \dots, L-1$  there exists a unitary transformation  $\Upsilon_{\ell\ell'}$  such that

$$(1.10) \quad V_{\ell(2)}\Upsilon_{\ell\ell'} = V_{\ell'(2)}$$

Note again that our choice of the form of  $\Phi_{\ell}$  is invariant under multiplication by unitary matrices, similar to our setup in the DPSK case. As in equation 1.1, we require a normalization, which in this case amounts to requiring that  $\Phi_{\ell}^t\Phi_{\ell} = I_M$ , or equivalently,

$$(1.11) \quad V_{\ell(1)}^t V_{\ell(1)} + V_{\ell(2)}^t V_{\ell(2)} = 2I_M$$

where here  $^t$  denotes transpose.

We now discuss the probability of error and the diversity product. Let  $P_e$  be the pairwise probability of error of mistaking a signal  $S_{\ell}$  for  $S_{\ell'}$ . It is shown in [3] that

$$(1.12) \quad P_e \leq \frac{1}{2} \prod_{m=1}^M \left[ 1 + \frac{(\rho T/M)^2 (1 - d_{\ell\ell',m}^2)}{4(1 + \rho T/M)} \right]^{-N}$$

where  $d_{\ell\ell'}$  are the singular values of the  $M \times M$  matrix  $\Phi_{\ell}^* \Phi_{\ell'}$ . Note that by assumption,  $0 \leq d_{\ell\ell',m} \leq 1$  and that as  $d_{\ell\ell',m}$  decreases, then  $P_e$  decreases. We fix a signal-to-noise ratio  $\rho$ , and we thus see that  $P_e$  is dominated by

$$(1.13) \quad \prod_{m=1}^M (1 - d_{\ell\ell',m}^2).$$

One can think of these  $d_{\ell\ell',m}$  as being the cosine of the angle between the one-dimensional subspaces generated by the  $m$ th columns of  $\Phi_{\ell}$  and  $\Phi_{\ell'}$ . We now define

$$(1.14) \quad \zeta_{\ell\ell'} = \left[ \prod_{m=1}^M (1 - d_{\ell\ell',m}^2) \right]^{\frac{1}{2M}},$$

which can be thought of as the geometric mean of the sines of the aforementioned angles. In other words, we want the columns of the different matrices to be as orthogonal as possible. To that end, we let the diversity product  $\zeta$  be given by

$$(1.15) \quad \zeta = \min_{0 \leq \ell < \ell' \leq L-1} \zeta_{\ell\ell'}.$$

We see then that the higher the diversity product is, the lower the probability of error will be. We will say the constellation has full diversity if  $\zeta$  is non-zero. In [2] it is shown that this is equivalent to

$$(1.16) \quad \zeta_{\ell\ell'} = \frac{1}{2} |\det(V_{\ell'} - V_{\ell})|^{\frac{1}{M}}.$$

Thus we want to choose our  $V$  such that the determinant of their difference is nonzero. It is shown in [5] that under the assumptions of equations 1.10 and 1.11, the best diversity product is achieved if the matrices  $V$  are all assumed to be unitary. Since the matrices can be premultiplied by any unitary matrix (because the information is encoded in the “phase shift” between the two blocks of the matrix) we can assume our matrices are of the form

$$(1.17) \quad \Phi_{\ell} = \frac{1}{\sqrt{2}} \begin{bmatrix} I_M \\ V_{\ell} \end{bmatrix}$$

where each  $V_{\ell}$  is unitary.

Recall that each transmitted matrix is the product of the previously transmitted matrix and the signal to be sent. Thus, if the constellation forms a group, one has a number of advantages, not the least of which is that multiplying matrices can be replaced by using a group look-up table. In addition, each transmitted signal is an element of that group. Finally, the computation of  $\zeta$  is easier, because if the constellation forms a group, then

$$(1.18) \quad |\det(V_{\ell'} - V_{\ell})| = |\det(V_{\ell'} V_{\ell'}^{-1} - V_{\ell} V_{\ell}^{-1})| = |\det(I_M - W)|$$

where  $W$  is necessarily in the constellation, and thus one only has to compute  $\zeta_{\ell\ell'}$  for  $L - 1$  pairs, rather than the  $L(L - 1)/2$  pairs if the constellation did not form a group.

Notice that by the above equation, in order to have full diversity (i.e  $\zeta \neq 0$ ), we must have that  $W$  does not have 1 for an eigenvalue for every element of the constellation. Thus, we are looking for finite groups of unitary matrices, none of which (except the identity matrix) have one as an eigenvalue (We say such a group is fixed-point-free). We will discuss that problem in the following sections.

## 2. GROUPS AND REPRESENTATIONS

In this section we review the basic properties of groups, representations, and characters that will be necessary to study the constellations that arise from our assumptions.

Recall that a representation of a finite group  $G$  over a field  $F$  is a homomorphism  $\mathcal{X} : G \rightarrow GL_n(F)$ , i.e.  $\mathcal{X}(gh) = \mathcal{X}(g)\mathcal{X}(h)$  for all  $g, h \in G$ . We will assume throughout that  $F = \mathbb{C}$ , the complex numbers. We say that  $n$  is the degree of  $\mathcal{X}$ . We say that a representation is reducible if there exists a basis for  $\mathbb{C}^n$  such that all of the matrices  $\mathcal{X}(g)$  are of the form

$$(2.1) \quad \mathcal{X}(g) = \begin{pmatrix} \mathcal{Y}(g) & 0 \\ 0 & \mathcal{Z}(g) \end{pmatrix}$$

where  $\mathcal{Y}$  is a  $k$ -dimensional representation of  $G$  and  $\mathcal{Z}$  is an  $m$ -dimensional representation, and  $k + m = n$ . In other words, we say that the representation is reducible if it can be written as a direct sum of two or more smaller representations, and we say that these representations are the constituents of  $\mathcal{X}$ . We say then that a representation is irreducible if it cannot be written in such a form. Also, if  $N \triangleleft G$  is the kernel of  $\mathcal{X}$  then  $\mathcal{X}$  can be

thought of as a representation of the factor group  $G/N$ , and if  $N = 1$ , then  $\mathcal{X}$  is said to be faithful. One basic result we will need is that  $G$  is abelian if and only if every irreducible representation of  $G$  is linear, i.e. has degree 1.

Note that if  $\mathcal{X} : G \rightarrow GL_n(\mathbb{C})$  is a representation, and if  $M \in GL_n(\mathbb{C})$ , then the map  $\mathcal{Y} : G \rightarrow GL_n(\mathbb{C})$  given by  $\mathcal{Y}(g) = M^{-1}\mathcal{X}(g)M$  is also a representation. We say in this situation that  $\mathcal{X}$  and  $\mathcal{Y}$  are equivalent. The first major result in the representation theory of finite groups is that the number of equivalence classes of irreducible representations of a finite group  $G$  is the same as the number of conjugacy classes in  $G$ . Also, if  $\mathcal{X}$  is a representation of  $G$ , we say that  $\mathcal{X}$  affords the character  $\chi \in \text{Char}(G)$  given by  $\chi(g) = \text{trace}(\mathcal{X}(g))$ . If  $\mathcal{X}$  is irreducible, we say that  $\chi$  is irreducible, and let  $\text{Irr}(G)$  denote the set of irreducible representations of  $G$ .

If  $H$  is a subgroup of  $G$  and  $\mathcal{X}$  is a representation of  $G$  with character  $\chi$ , then  $\mathcal{X}_H$  denotes the restriction of  $\mathcal{X}$  to  $H$ , which is then a representation of  $H$ , and  $\chi_H$  is the corresponding character. (We say  $\mathcal{X}$  lies over  $\mathcal{Y}$  if  $\mathcal{Y}$  is one of the constituents of  $\mathcal{X}_H$ .) If  $\mathcal{Y}$  is a representation of  $H$  with character  $\psi$ , then one can define the induced representation  $\mathcal{X} = \mathcal{Y}^G$  of  $G$  with character  $\chi = \psi^G$ . If  $\mathcal{Y}$  has degree  $n$ , then  $\mathcal{Y}^G$  will have degree  $n|G : H|$ .

If  $\sigma$  is an automorphism of  $G$  and  $\mathcal{X}$  is a representation of  $G$ , then the map  $\mathcal{X}^\sigma$  given by  $\mathcal{X}^\sigma(g) = \mathcal{X}(g^\sigma)$  is also a representation of  $G$ . Therefore  $\text{Aut}(G)$  permutes the set of irreducible representations of  $G$ . If  $N$  is a normal subgroup of  $G$ , then  $G$  permutes the representations of  $N$ . Let  $\mathcal{X}$  be a representation of  $G$  and let  $\mathcal{Y}$  be an irreducible constituent of  $\mathcal{X}_N$ . Clifford's Theorem (see Chap 6 [4]) says that the constituents of  $\mathcal{X}_N$  are exactly the  $G$ -conjugates of  $\mathcal{Y}$ , each of which occurs with equal multiplicity, and this multiplicity is the index of the stabilizer of  $\mathcal{Y}$  in  $G$ . Moreover, if we let  $G_{\mathcal{Y}}$  be the stabilizer in  $G$  of  $\mathcal{Y}$ , then the map  $\mathcal{Z} \rightarrow \mathcal{Z}^G$  is a bijection from the set of irreducible representations of  $G_{\mathcal{Y}}$  lying over  $\mathcal{Y}$  to the set of irreducible representations of  $G$  lying over  $\mathcal{Y}$ .

The final basic result (see Chapter 4 of [4]) from the representation theory of finite groups that we need is that if  $\mathcal{X}$  is a representation of the finite group  $G$ , then  $\mathcal{X}$  is equivalent to a representation  $\mathcal{Y}$  of  $G$  such that  $\mathcal{Y}(g)$  is unitary for every  $g \in G$ . Thus the problem stated at the end of Section 1 can be stated as follows: What finite groups have irreducible faithful representations that are fixed point-free? This is the problem we will discuss in the next section.

### 3. FIXED-POINT-FREE GROUPS

We first see that the only type of abelian groups that satisfy our hypothesis are the cyclic groups. This is because every abelian group can be written as a direct product of cyclic groups, and if  $G \cong H_1 \times H_2$ , where  $H_1$  and  $H_2$  are abelian, then the irreducible representations of  $G$  are of the form  $\mathcal{X}(g) = \mathcal{Y}_1(g_1)\mathcal{Y}_2(g_2)$ , where  $\mathcal{Y}_1$  and  $\mathcal{Y}_2$  are (necessarily linear) representations of  $H_1$  and  $H_2$ , and  $g_1$  and  $g_2$  are the factors of  $g$  in  $H_1$  and  $H_2$ , respectively. Thus if  $G$  has a nontrivial factorization, then there are nontrivial elements of  $G$  in the kernel of any irreducible representation of  $G$ , and therefore every nontrivial irreducible representation of  $G$  has an eigenvalue of 1 for some  $\mathcal{X}(g)$ , and thus  $G$  is not fixed-point-free.

We now look at a specific example of a finite group  $G$  that is fixed-point-free, i.e.  $G$  has a faithful, irreducible representation  $\mathcal{X}$  which does not have 1 for an eigenvalue of  $\mathcal{X}(g)$  for any nontrivial element  $g \in G$ . Let  $m = 21$ . Note that the multiplicative order of

$r = 4$  in  $\mathbb{Z}_{21}$  is  $n = 3$ . Let  $t = \frac{m}{\gcd(r-1, m)} = 7$ , and note that  $\gcd(n, t) = 1$ . Let  $G$  be a nonabelian group of order 63 with a cyclic normal subgroup  $N$  of order 21, and suppose  $G$  has generators and relations of the form

$$(3.1) \quad G = \langle \sigma, \tau \mid \sigma^{21} = 1, \tau^3 = \sigma^7, \sigma^\tau = \sigma^4 \rangle.$$

$G$  can be thought of as the semidirect product of a cyclic group  $\langle \tau \rangle$  of order 9 acting on a cyclic group  $\langle \sigma^3 \rangle$  of order 7 in such a way that the kernel of the action is the unique subgroup of  $\langle \tau \rangle$  of order 3.

Let  $\lambda$  be a faithful character (or equivalently, a representation) of  $N$  such that  $\lambda(\sigma) = \eta = e^{\frac{2\pi i}{21}}$ , a 21st root of unity. Using representation theory, we see that  $\tau$  acts on  $N$  and the irreducible characters of  $N$  in the same way, and since  $\sigma$  has a nontrivial orbit under the action of  $G/N$ , then the stabilizer in  $G$  of  $\lambda$  must be  $N$ . Thus by Clifford's Theorem the representation  $\lambda$  induces irreducibly to a representation  $\lambda^G = \mathcal{X}$  of  $G$ . Again, by Clifford's Theorem, we then have that  $\mathcal{X}(\sigma)$  is the direct sum of the elements of the orbit of  $\lambda(\sigma) = \eta$  under the action of  $G$ , so we have that

$$(3.2) \quad \mathcal{X}(\sigma) = A = \begin{pmatrix} \eta & 0 & 0 \\ 0 & \eta^4 & 0 \\ 0 & 0 & \eta^{16} \end{pmatrix}.$$

We see that the kernel of this representation is trivial, and thus our relations dictate that if  $\mathcal{X}(\tau) = B$ , then we must have  $B^3 = A^7$  and  $B^{-1}AB = A^4$ . Also, Clifford's Theorem and the definition of character induction yield that if  $\chi$  is the irreducible character of  $G$  afforded by  $\mathcal{X}$ , then  $\chi(\tau) = 0$ . We are then able to compute that

$$(3.3) \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \eta^7 & 0 & 0 \end{pmatrix}.$$

Or, equivalently we can simply check that the subgroup of  $GL_2(\mathbb{C})$  generated by the above two matrices is isomorphic to  $G$ . Since none of the eigenvalues of either of the above matrices (or any of the matrices that they generate) is 1, then we have constructed a fixed-point-free group of order 63.

The above construction can be generalized in the following way. Suppose  $m$  and  $r$  are integers, and let  $n$  be the order of  $r$  in the multiplicative group  $\mathbb{Z}^*$ . Let  $r_0 = \gcd(r-1, m)$  and  $t = \frac{m}{r_0}$ . Suppose  $\gcd(n, t) = 1$  and that every prime divisor of  $n$  divides  $r_0$ . We say in this case that the pair  $(m, r)$  is admissible. For an admissible pair  $(m, r)$ , define the group  $G_{m,r}$  by

$$(3.4) \quad G_{m,r} = \langle \sigma, \tau \mid \sigma^m = 1, \tau^n = \sigma^t, \sigma^\tau = \sigma^r \rangle.$$

(Note that the group of order 63 above is  $G_{21,4}$  in this notation.) We claim, and provide a sketch of the proof, that these groups are fixed-point free. As before, let  $N = \langle \sigma \rangle$  be a normal subgroup of order  $m$ . Let  $\eta$  be a primitive  $m$ th root of unity, and let  $\mathcal{Y}$  be the one-dimensional representation of  $N$  given by  $\mathcal{Y}(\sigma) = \eta$ . One can see by our assumptions that the stabilizer of  $\mathcal{Y}$  in  $G_{m,r}$  is  $N$ , and thus by Clifford's Theorem,  $\mathcal{Y}$  induces to an irreducible representation  $\mathcal{X}$  of  $G_{m,r}$  of degree  $|G : N| = n$ . As before, since the stabilizer

of  $\mathcal{Y}$  is  $N$ , then

$$(3.5) \quad \mathcal{X}(\sigma) = \begin{pmatrix} \eta & 0 & \cdots & 0 \\ 0 & \eta^r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \eta^{r^{n-1}} \end{pmatrix}.$$

One can then use the ideas of induced representations of groups to compute  $\mathcal{X}(\tau)$ , and we get

$$(3.6) \quad \mathcal{X}(\tau) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \eta^t & 0 & 0 & \cdots & 0 \end{pmatrix}$$

One can easily see that these representations are fixed-point-free, and we have therefore constructed a fixed-point-free group for each admissible pair of positive integers  $(m, r)$ .

We are now ready to state the main result, which is the classification of all nonabelian fixed-point-free groups. This was essentially proven by Zassenhaus in 1936, though there were some holes, which was fixed in [7].

**Theorem 3.1.**  *$G$  is a fixed-point-free group if and only if it belongs to one of the following classes of groups:*

(a)  $G_{m,r}$ , where

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

and  $(m, r)$  is admissible. The order of this group is  $mn$ .

(b)  $D_{m,r,\ell}$ , where

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

and  $r_0$  is as defined above,  $nr_0$  is even,  $(m, r)$  is admissible,  $\ell^2 \equiv 1 \pmod{m}$ ,  $\ell \equiv 1 \pmod{n}$ , and  $\ell \equiv -1 \pmod{s}$ , where  $s$  is the highest power of 2 dividing  $mn$ . This group has order  $2mn$ .

(c)  $E_{m,r}$ , where

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

and  $(m, r)$  is admissible,  $mn$  is odd, and  $nr_0$  is divisible by 3. The order of this group is  $8mn$ .

(d)  $F_{m,r,\ell}$ , where

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

and  $(m, r)$  is admissible,  $mn$  is odd,  $r_0$  is divisible by 3,  $n$  is not divisible by 3,  $\ell^2 \equiv 1 \pmod{m}$ ,  $\ell \equiv 1 \pmod{n}$ , and  $\ell \equiv -1 \pmod{3}$ . the order of this group is  $16mn$ .

(e)  $J_{m,r}$ , where

$$J_{m,r} = SL_2(\mathbb{F}_5) \times G_{m,r}$$

and  $(m, r)$  is admissible, and  $\gcd(mn, 120) = 1$ . The order of this group is  $120mn$ .

(f)  $K_{m,r,\ell}$ , where

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

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  $\mu$  and  $\nu$  are as in  $J_{m,r}$  and  $\ell^2 \equiv 1 \pmod{m}$ , and  $\ell \equiv 1 \pmod{n}$ . The order of this group is  $240mn$ .

We will not prove this theorem here. We note, however, that to prove one direction, we only need to demonstrate a faithful irreducible representation for each of the above groups, and show that it has no non-identity eigenvalues. We will give an explicit calculation for only one of these,  $D_{m,r,\ell}$ , the rest may be found in (Shokrollahi et al).

For  $D_{m,r,\ell}$ , let  $\xi$  be a primitive  $m$ th root of unity. Let  $A_0$  be the  $n \times n$  matrix

$$(3.7) \quad A_0 = \begin{pmatrix} \xi & 0 & 0 & \cdots & 0 \\ 0 & \xi^r & 0 & \cdots & 0 \\ 0 & 0 & \xi^{r^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{r^{n-1}} \end{pmatrix},$$

and let  $B_0$  be the  $n \times n$  matrix

$$(3.8) \quad B_0 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \xi^t & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Then the desired representation  $\mathcal{X}$  of  $D_{m,r,\ell}$  will be given by

$$(3.9) \quad \mathcal{X}(\sigma) = A = \begin{pmatrix} A_0 & 0 \\ 0 & A_0^\ell \end{pmatrix}, \mathcal{X}(\tau) = B = \begin{pmatrix} B_0 & 0 \\ 0 & B_0^\ell \end{pmatrix}, \text{ and } \mathcal{X}(\gamma) = R = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

One can easily check that the subgroup of  $GL_{2n}(\mathbb{C})$  generated by these matrices satisfies the same relations as those defining  $D_{m,r,\ell}$ .

We digress to mention some interesting corollaries. We have already noted that the only class of abelian fixed-point-free groups are the cyclic groups. We see by the above classification that the only type of nonabelian odd fixed-point-free group is  $G_{m,r}$ . Since

one is often interested in the case where there are two transmitter antennas, a natural question is the following: What fixed-point-free groups have a 2-dimensional fixed-point-free representation?

**Corollary 3.2.** *If  $G$  is a fixed-point-free group with a 2-dimensional fixed-point-free representation, then  $G$  is isomorphic to one of the following groups:*

- (a)  $G_{m,r}$  where  $(m,r)$  is admissible and the order of  $r$  in the multiplicative group of  $\mathbb{Z}_m$  is 2.
- (b)  $D_{m,1,\ell}$ .
- (c)  $E_{m,1}$ .
- (d)  $F_{m,1,\ell}$  for  $\ell \equiv 1 \pmod{m/3}$ .
- (e)  $J_{m,1}$ .

Also, each of the above groups has an irreducible 2-dimensional fixed-point-free representation.

We now discuss an outline of the above classification proof. Note that if  $G$  is a fixed-point-free group (with the fixed-point-free representation  $\mathcal{X}$ ), and  $H$  is a subgroup of  $G$ , then  $H$  is a fixed-point-free group with the (not necessarily irreducible) representation  $\mathcal{X}_H$ . In 1905, Burnside showed that if  $G$  is a fixed-point-free  $p$ -group, then  $G$  is cyclic (if  $p$  is odd) or possibly a generalized quaternion group (if  $G$  is even). Thus, if  $G$  is a fixed-point-free group, and if  $G$  is odd, then every Sylow subgroup of  $G$  is cyclic. It is known that if  $G$  is an odd group with this property, then  $G$  is necessarily isomorphic to  $G_{m,r}$ . Moreover, such a group  $G$  is fixed-point-free if and only if the pair  $(m,r)$  is admissible.

The next step is to classify solvable fixed-point-free groups. The following theorem (which properly is a result on Frobenius complements) says that if  $G$  is a solvable fixed-point-free group, then  $G$  has a “large” subgroup  $G_1$  with the property that every Sylow subgroup is a cyclic group.

**Lemma 3.3.** *If  $G$  is a solvable fixed-point-free group, then  $G$  has a normal subgroup  $G_1$  such that  $G/G_1$  is isomorphic to a subgroup of  $Sym(4)$ , the symmetric group on 4 elements, and every Sylow subgroup of  $G_1$  is cyclic.*

A proof of the above result can be found in [6]. One then uses this to show that the only solvable fixed-point-free groups are isomorphic to  $G_{m,r}$ ,  $D_{m,r,\ell}$ ,  $E_{m,r}$ , or  $F_{m,r,\ell}$ .

Finally one must classify the nonsolvable fixed-point-free groups. One can show (see 18.6 of [6]) that if  $G$  is a non-solvable fixed-point-free group, then  $G$  has a normal subgroup  $N$  of index 2 where  $N \cong SL_2\mathbb{F}_5 \times G_{m,r}$ . One then shows that  $G$  must be isomorphic to either  $J_{m,r}$  or  $K_{m,r,\ell}$ .

#### 4. PERFORMANCE AND OTHER QUESTIONS

It has been shown by Shokrollahi et al that in practice many of the above constellation designs perform better (for either known or unknown channels) than previous codes. For example, for two transmitting and one receiving antenna,  $F_{15,1,11}$  outperforms orthogonal, diagonal, and quaternion codes for high signal-to-noise ratio.

The classification of fixed-point-free groups is somewhat limited, however, and one cannot always design good codes for certain values of  $M$ . (For instance, if  $M = 5$  and  $L = 32$ ).

There are three potential ways around this. First, one may use so-called Hamiltonian constellations (which work only if  $M = 2$  but any rate  $R$ ), which involve  $2 \times 2$  unitary matrices, built out of the points on the unit sphere in  $\mathbf{R}^4$ . Secondly, one can create nongroup generalizations of  $G_{m,r}$ . Simply use the same matrices that generate the irreducible fixed-point-free representation of  $G_{m,r}$  to generate a set of  $n \times n$  matrices regardless of whether  $(m, r)$  is admissible or not. This will not be a group, however, much of the same theory goes through in constructing these constellations, and one can get a formula and a good bound for the diversity product. Finally, one can combine two fixed-point-free representations of different finite groups by taking the products of the various matrices in their fixed-point-free representations. This will no longer be a group, but it will have many good properties.

#### REFERENCES

- [1] G. J. Foschini, Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas, *Bell Labs Tech. J.* **1** (1996), 41-59.
- [2] B. Hochwald and W. Sweldens, Differential Unitary Space-Time Modulation, on the web at <http://mars.bell-labs.com>, (2000).
- [3] B. M. Hochwald and T. L. Marzetta, Unitary space-time modulation for multiple-antenna communication in Rayleigh flat-fading, *IEEE Trans. Info. Theory* (2000) 563-564.
- [4] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, New York, 1976.
- [5] P. Oswald, On codes for multiple-antenna differential modulation, on the web at <http://mars.bell-labs.com>
- [6] D. Passman, *Permutation Groups*, W. A. Benjamin, Inc., New York, 1968.
- [7] A. Shokrollahi, B. Hassibi, B. Hochwald, and W. Sweldens, Representation Theory for High-Rate Multiple-Antenna Design, on the web at <http://mars.bell-labs.com>, (2000).
- [8] Capacity of multi-antenna Gaussian channels, *Eur. Trans. Telecom* **10** (1999) 585-595.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WI, 53706  
*E-mail address:* `cossey@math.wisc.edu`