# Fully-Diverse Multiple-Antenna Signal Constellations and Fixed-Point-Free Lie Groups

Babak Hassibi* Mohammad Khorrami†

*Bell Laboratories, Lucent Technologies
600 Mountain Avenue, Murray Hill, NJ 07974
hassibi@bell-labs.com

†Institute for Advanced Studies in Basic Sciences
P. O. Box 159, Zanjan, 45195, IRAN
and
Institute for Studies in Theoretical Physics and Mathematics
P. O. Box 5531, Tehran, 19395, IRAN

October 30, 2000

A group of unitary matrices is called fixed-point-free (fpf) if all non-identity elements of the group have no eigenvalues at unity. Such groups are useful in multiple-antenna communications, especially in multiple-antenna differential modulation, since they constitute a fully-diverse constellation. In [1] all finite fpf groups have been classified. In this note we consider infinite groups and, in particular, their most interesting case, Lie groups. Two such fpf Lie groups are currently widely used in communications: the group of unit modulus scalars, from which various phase modulation schemes, such as QPSK, are derived, and the $2 \times 2$ orthogonal designs of Alamouti, on which many two-transmit-antenna schemes are based. In Lie-group-theoretic jargon these are referred to as $U(1)$ and $SU(2)$. A natural question is whether there exist other fpf Lie groups. We answer this question in the negative: $U(1)$ and $SU(2)$ are all there are.

## 1 Introduction and Model

Consider a narrow-band flat-fading multiple-antenna communication system with $M$ transmit and $N$ receive antennas (see, e.g., [2]). Assuming that the $M \times N$ channel matrix is constant for (at least) $M$ channel uses, we may write

$$X = \sqrt{\frac{\rho}{M}} SH + W, \quad E\mathrm{tr} SS^* = M^2 \tag{1}$$

where $E$ denotes expectation and

$$X = \begin{bmatrix} x_{11} & \dots & x_{1N} \\ x_{21} & \dots & x_{2N} \\ \vdots & & \vdots \\ x_{M1} & \dots & x_{MN} \end{bmatrix}, \quad S = \begin{bmatrix} s_{11} & \dots & s_{1M} \\ s_{21} & \dots & s_{2M} \\ \vdots & & \vdots \\ s_{M1} & \dots & s_{MM} \end{bmatrix}$$

are the received and transmitted matrices, respectively. In the above matrices, time runs vertically and space runs horizontally: thus $x_{tn}$ ($s_{tm}$) is the received (transmitted) signal at channel use time $t$ and receive (transmit) antenna $n$ ($m$). The channel matrix $H \in \mathcal{C}^{\mathcal{M}\times N}$ and additive noise $W \in \mathcal{C}^{M\times N}$ are both assumed to be comprised of independent $\mathcal{CN}(0,1)$ (zero-mean unit-variance complex-Gaussian) entries. They are also assumed to be unknown to the both the receiver and transmitter. The normalization factor $\sqrt{\frac{\rho}{M}}$ in (1), along with the transmit power constraint $E\mathrm{tr}SS^* = M^2$, guarantee that $\rho$ is the SNR at the receiver.

### 1.1 Multiple-Antenna Differential Modulation

In what follows, we shall study the channel (1) as used in block-channel-uses of length $M$ each. Assume now at each *block-time* $i$, the $M \times M$ transmit matrix takes the form

$$S_i = V_i S_{i-1} = V_i V_{i-1} \dots V_0, \tag{2}$$

where the the $V_i$ are $M \times M$. If we further assume that the channel is constant for $2M$ channel uses:

$$X_i = \sqrt{\frac{\rho}{M}} S_i H + W_i = \sqrt{\frac{\rho}{M}} V_i S_{i-1} H + W_i = V_i(X_{i-1} - W_{i-1}) + W_i,$$

where we have used the fact that $X_{i-1} = \sqrt{\frac{\rho}{M}} S_{i-1} H + W_{i-1}$. Therefore

$$X_i = V_i X_{i-1} + \underbrace{W_i - V_i W_{i-1}}_{W_i'},$$

and we can decode the $i$-th signal $V_i$ from $X_i$ and $X_{i-1}$, without needing to know the channel. In fact the maximum-likelihood decoder can be shown to be [3, 4]

$$\hat{V}_i = \arg\min_{V_\ell} \|X_i - V_\ell X_{i-1}\|_F \,, \tag{3}$$

where $\|\cdot\|_F$ denotes the Frobenius norm.

## 2 The Constellation Design

We thus need to look for a constellation $\mathcal{V} = \{V_0, \ldots, V_{L-1}\}$ of $M \times M$ matrices. We first note that the $V_\ell$ must be unitary, otherwise as $i \to \infty$ the product $S_i = V_i V_{i-1} \ldots V_0$ will go to zero, infinity, or both (in different spatial and temporal directions), thereby violating the transmit power constraint. Furthermore, the quality of a constellation $\mathcal{V}$ is determined by the probability of error of mistaking one symbol of $\mathcal{V}$ for another. At high SNR it can be shown [3, 4] that this probability is dominantly dependant on the determinant of $V_\ell - V_{\ell'}$. We therefore measure the quality of the constellation by [1]

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{0 \leq \ell < \ell' < \mathcal{L}} |\det(V_\ell - V_{\ell'})|^{1/M} \,. \tag{4}$$

Our design problem is thus reduced to the following: "given $M$ (the number of transmit antennas) and $R$ (the transmission rate), find a set $\mathcal{V}$ of $L = 2^{MR}$, $M \times M$ unitary matrices, such that the minimum of the absolute value of the determinant of their pairwise differences is as large as possible".

We therefore call any constellation $\mathcal{V}$ with the property that the determinants of the pairwise differences are all nonzero, *fully diverse*. Fully-diverse constellations have the following further interpretation: for any channel matrix $H$,

$$V_\ell H \neq V_{\ell'} H \quad \text{whenever} \quad \ell \neq \ell'.$$

In other words, there exists no channel $H$ for which any two elements of $\mathcal{V}$ respond identically.

### 2.1 Constellations from Groups

The design problem just introduced is especially confounded for two reasons. First, both the cost (the absolute value of a determinant) as well as constraint set (the space of $M \times M$ unitary matrices, the so-called Stiefel manifold) are highly non-convex. Second, the size of the problem can be huge (we seek $L = 2^{MR}$ matrices). Therefore exact solutions appear to be intractable and we need to impose some structure on the constellation to have hope of obtaining a solution.

To break the logjam, [1] investigates the case where $\mathcal{V}$ forms a group under matrix multiplication. This simplifies the cost, since

$$\begin{aligned}
\zeta_{\mathcal{V}} &= \frac{1}{2} \min_{0 \le \ell < \ell' < \mathcal{L}} |\det(V_\ell - V_{\ell'})|^{1/M} \\
&= \frac{1}{2} \min_{0 \le \ell < \ell' < \mathcal{L}} \left|\det(V_\ell) \det\left(I - V_\ell^{-1} V_{\ell'}\right)\right|^{1/M} \\
&= \frac{1}{2} \min_{I \neq V \in \mathcal{V}} |\det(I - V)|^{\frac{1}{M}}.
\end{aligned}$$

Since all finite groups can be faithfully represented as a set of unitary matrices, any finite group is a potential candidate for a signal constellation.[1] However, if we insist on a fully-diverse constellation then we must have $\zeta_{\mathcal{V}} \neq 0$, which from the above equation implies that all non-identity elements in the constellation must have no eigenvalues at one. This leads us to the following definition.

**Definition 1 (Fixed-Point-Free Group).** *A group $\mathcal{G}$ is called fixed-point-free (fpf) if, and only if, it has a representation as unitary matrices with the property that the representation of each non-unit element of the group has no eigenvalue at unity.*

Note that the above definition does not imply that *every* representation of an fpf group is fixed-point-free. In fact, any non-faithful representation cannot be fixed-point-free. For a non-faithful representation of an fpf group $\mathcal{G}$, there exist distinct elements $G_1, G_2 \in \mathcal{G}$, such that the representations of $G_1$ and $G_2$ are identical. This implies that the representation of the non-unit element $G_1 G_2^{-1}$ is the identity matrix, and so has eigenvalues at one, thereby implying that the representation is not fpf. The reason why we have defined fpf groups as those for which the representation of each non-unit element in the group, rather than each non-identity matrix in the representation, have no eigenvalue at unity is that had we not done so, all groups would have been fpf if represented as the identity matrix.

In [1] all *finite* fpf groups have been classified. Although there are an infinite number of finite fpf groups, it turns out that they are few and far between. In fact, there are only six different group types. There are some groups among these with excellent performance. One example is the two-dimensional unitary representation of $SL(2, \mathcal{F}_5)$, the 120-element group of $2 \times 2$ unit-determinant matrices with entries in the Galois field $\mathcal{F}_5$. However, the best constellations are not obtained for very high rates or for a large number of antennas.

[1]Briefly, a representation of an abstract group $\mathcal{G}$ is a mapping from $\mathcal{G}$ to the group of $M \times M$ invertible complex matrices, $GL(M, \mathcal{C})$, that respects group multiplication.

This brings up the question of whether there exist any *infinite* fpf groups? It turns out that there are (and they are widely-used in communications), though they were never thought of, nor recognized, as fpf groups.

### 2.1.1 Phase Modulation

Consider the group of unit-modulus complex scalars:

$$e^{j\omega}, \quad \omega \in [0, 2\pi[$$

This is trivially an fpf group. It is also widely used in communications: PM, FM, single-antenna differential modulation, etc. To design a constellation from this group we need to choose points on the unit circle. Clearly, the optimal choice is to choose equidistant points, which results in the wellknown QPSK constellations.

### 2.1.2 Orthogonal Designs

Orthogonal designs were originally introduced in communications in [5] and used for multi-antenna differential modulation in [6]. An *orthogonal design* is the unitary matrix:

$$V = \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}, \quad |x|^2 + |y|^2 = 1. \tag{5}$$

It is easy to see that orthogonal designs form a group under matrix multiplication (the group of unit-determinant unitary matrices). Furthermore, since their eigenvalues are given by $\{e^{j\theta}, e^{-j\theta}\}$, where $\theta = \cos^{-1}(\frac{x+x^*}{2})$, it follows that they are fpf. (Indeed, if $e^{j\theta} = 1$ then $e^{-j\theta} = 1$, which means that the matrix must be the identity matrix.)

In particular, our cost of interest takes the form

$$\det(V_1 - V_2) = \det \begin{bmatrix} x_1 - x_2 & -(y_1 - y_2)^* \\ y_1 - y_2 & (x_1 - x_2)^* \end{bmatrix} = |x_1 - x_2|^2 + |y_1 - y_2|^2 \,, \tag{6}$$

which is the Euclidean distance between the 2-dimensional complex (or 4-dimensional real) vectors $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$ and $\begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$. Thus, for orthogonal designs, our design problem reduces to the design of spherical codes on the real 3-dimensional sphere in 4-space, i.e., on $|x|^2 + |y|^2 = 1$.

## 2.2 Other Infinite Fixed-Point-Free Groups?

In the remainder of this note we are interested in the question of whether there exist other infinite fpf groups. One possibility is *countable* groups. However, we shall not focus on these since for our current application they are not very interesting[2] and, more importantly, because it is not clear how one should sample them to obtain a finite-size constellation.[3]

The other possibility is to consider *continuous* groups. Among these, the most interesting and most well-studied are *Lie groups*. Indeed the above two examples (phase modulation and orthogonal designs) are Lie groups.

Since our ultimate goal is to construct a finite-size constellation of unitary matrices, we must appropriately sample the continuous group. This will not necessarily lead to a finite group itself (if it did then we would obtain one of the fpf groups classified in [1]). When we have a Lie group then the problem of constellation design becomes one of appropriately sampling the group's underlying manifold. For example, for phase modulation the underlying manifold is the unit circle, whereas

[2]Countable fpf groups often have a finite number of generators and relie on the fact that the eigenvalues of these generators are relatively irrational, a condition that cannot be met in finite precision.

[3]As we shall presently see, continuous groups have an underlying manifold which allows sampling of the group via sampling of the manifold.

for orthogonal designs the underlying manifold is the three dimensional unit sphere. In fact, the star performer in [1], the 2-dimensional unitary representation of $SL(2, \mathcal{F}_5)$, is an orthogonal design with an optimal sampling of 120 points on the three dimensional unit sphere. (Here by optimal we mean that the 120 points have the largest possible minimum Euclidean distance.)

# 3 Lie Groups

In this section we briefly review some concepts from Lie groups and Lie algebras, focusing only on those we require to prove our main result. For much more details, and many more results, the interested reader may consult [7, 8, 9] and the references therein.

A *Lie group* is a set endowed with the structures of both a group and a $\mathcal{C}^\infty$ manifold. In other words, we have some manifold, such that for every point $\theta$ on the manifold there corresponds an element $g(\theta) \in \mathcal{G}$ of the group. Moreover, the mappings from $(\theta_1, \theta_2)$ to $\theta_3$ defined via

$$g(\theta_1)g(\theta_2) = g(\theta_3),$$

as well as the mapping from $\theta$ to $\phi$ defined via

$$g^{-1}(\theta) = g(\phi),$$

are analytic.

Examples of Lie groups abound. The real line with addition as the group operation is a Lie group, as is $\mathcal{R}^{M\times N}$ with matrix addition. Another important class of groups is that of linear groups, i.e., continuous groups of linear transformations. For example, the Lie group $\mathcal{R}^{M\times N}$ with matrix addition is isomorphic to the linear group

$$\begin{bmatrix} I_M & A \\ 0 & I_N \end{bmatrix}.$$

The group of upper triangular matrices with unit diagonal (the so-called Heisenberg group) is another example of a linear group, as is the group of planar rotations

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}.$$

## 3.1 The Classical Lie Groups

The last examples we give are all subgroups of $GL(n, \mathcal{C})$, the Lie group of $n \times n$ invertible matrices with complex entries. The first four are referred to as the *classical groups:*

- $GL(n, \mathcal{C})$: nonsingular $n \times n$ complex matrices.
- $SL(n, \mathcal{C})$: unit-determinant nonsingular $n \times n$ complex matrices.
- $O(n, \mathcal{C})$: $n \times n$ complex orthogonal matrices, $\Theta^t \Theta = I_n$.
- $Sp(2n, \mathcal{C})$: $2n \times 2n$ complex matrices that leave $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$ invariant, i.e., $\Theta^t J \Theta = J$.

And the remaining some other useful Lie groups:

- $U(n)$: $n \times n$ complex unitary matrices.
- $SU(n)$: unit-determinant $n \times n$ unitary matrices.
- $SU(p, q)$: unit-determinant $n \times n$ matrices. that leave $J = \begin{bmatrix} I_p & 0 \\ 0 & -I_q \end{bmatrix}$ invariant $(n = p + q)$.

### 3.2 Lie Algebras

Since underlying any Lie group there is an analytic manifold, we can look at the tangent space to the manifold. In particular, we can look at the tangent space at the identity element.

For example, take the unitary group $U(n)$, and let $\Phi(t)$ be any curve passing through the identity:

$$0 = \left.\frac{d\Phi\Phi^*}{dt}\right|_{t=0} = \dot{\Phi}(0)\Phi^*(0) + \Phi(0)\dot{\Phi}^*(0) = \dot{\Phi}(0) + \dot{\Phi}^*(0), \tag{7}$$

so that the tangent space is the space of skew-Hermitian matrices.

As another example, take $SL(n, \mathcal{C})$ and let $A(t)$ be any curve passing through the identity:

$$0 = \left.\frac{d\det A}{dt}\right|_{t=0} = \mathrm{tr}\left(A^{-1}(0)\dot{A}(0)\right)\det A(0) = \mathrm{tr}\dot{A}(0), \tag{8}$$

so that the tangent space is the space of traceless matrices.

Once the tangent space is determined, at least locally, each element $G$ in the group can be written as

$$G = e^g,$$

where $g$ is an element in the tangent space. (The $g$ are sometimes called the *infinitesmal* generators of the group.)

The tangent space is clearly a linear vector space $\mathbf{g}$. But what can we say about the $g \in \mathbf{g}$, knowing that the $G = e^g \in \mathcal{G}$ form a group? It turns out that when $\mathcal{G}$ is a linear group, $\mathbf{g}$ forms what is called a *Lie algebra*:

$$g_1, g_1 \in \mathbf{g} \ \text{ implies } \ [g_1, g_2] = g_1g_2 - g_2g_1 \in \mathbf{g}. \tag{9}$$

(The case of a more general, not necessarily linear, Lie group can also be studied. This leads to a different definition for the commutator operator $[\cdot,\cdot]$, but we shall not be concerned with this here.) In fact, for "close enough" $g_1$ and $g_2$ we have the Campbell-Hausdorff formula: if $e^{g_1}e^{g_2} = e^{g_3}$, then

$$g_3 = g_1 + g_2 + \frac{1}{2}[g_1, g_2] + \frac{1}{12}\left([g_1,[g_1,g_2]] - [g_2,[g_2,g_1]]\right) + \dots \tag{10}$$

The relationship between Lie groups and Lie algebras can be given by the following two theorems.

**Theorem 1.** *Let $\mathcal{G}$ be a Lie group of matrices. Then* $\mathbf{g}$*, the set of tangent vectors to all curves in $\mathcal{G}$ at the identity, is a Lie algebra.*

**Theorem 2.** *Let* $\mathbf{g}$ *be a linear algebra generated by the basis $g_1, \dots g_n$. Then $g(\theta) = e^{\theta_1 g_1 + \dots \theta_n g_n}$ is a local Lie group for small enough $\theta$.*

The general situation is a bit more involved and will not concern us here. (The correspondence between a Lie algebra and a *simply-connected* Lie group is, for example, one-to-one.) The important conclusion is that to obtain many, if not most, of its properties, one can study the Lie algebra, rather than the Lie group.

Returning back to the fpf Lie groups of Secs. 2.1.1 and 2.1.2, we note that the group of unit-modulus scalars is simply $U(1)$. The corresponding Lie algebra, $u(1)$, is the one of imaginary numbers. The orthogonal designs are simply $SU(2)$. The corresponding Lie algebra, $su(2)$, is the one of $2 \times 2$ traceless skew-Hermitian matrices:

$$\begin{bmatrix} j\alpha_1 & \alpha_2 + j\alpha_3 \\ -\alpha_2 + j\alpha_3 & -j\alpha_1 \end{bmatrix},$$

where the $\alpha_k$ are real scalars. One possible basis for it is

$$g_1 = \begin{bmatrix} j & 0 \\ 0 & -j \end{bmatrix} \ , \ g_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \ , \ , g_3 = \begin{bmatrix} 0 & j \\ j & 0 \end{bmatrix},$$

which is clearly a Lie algebra since

$$[g_1, g_2] = 2g_3 \quad , \quad [g_2, g_3] = 2g_1 \quad , \quad [g3, g1] = 2g_2.$$

Note that both the Lie algebras $u(1)$ and $su(2)$ are *real.* In other words, $e^{\sum_k \alpha_k g_k}$ is an element of the corresponding group if, and only if, the scalars $\alpha_k$ are real (rather than complex).

### 3.3 Levi's Decomposition

An algebra $\mathbf{g}$ is the *semi-direct sum* of two algebras $\mathbf{a}$ and $\mathbf{b}$ if $\mathbf{g} = \mathbf{a} + \mathbf{b}$ as a vector space, but $[\mathbf{a}, \mathbf{b}] \subset \mathbf{a}$. In this case, we write $\mathbf{g} = \mathbf{a} \oplus_s \mathbf{b}$. A subalgebra $\mathbf{s}$ is an *ideal* of $\mathbf{g}$ if $[\mathbf{s}, \mathbf{g}] \subset \mathbf{s}$. For example, $\mathbf{a}$ is an ideal of $\mathbf{a} \oplus_s \mathbf{b}$.

The set of commutators $\mathbf{g}^{(1)} \triangleq [\mathbf{g}, \mathbf{g}]$ is an ideal of $\mathbf{g}$. This is also true for $\mathbf{g}^{(n+1)} = [\mathbf{g}^{(n)}, \mathbf{g}^{(n)}]$, $n = 1, 2, \ldots$. If this sequence of subalgebras terminates to zero after a finite number of steps, then we say $\mathbf{g}$ is *solvable.*

A Lie algebra is called *semi-simple* if it contains no Abelian ideals (other than $\{0\}$).

**Theorem 3 (Levi's Decomposition).** *Every Lie algebra is the semi-direct sum of a solvable Lie algebra and a semi-simple Lie algebra.*

Thus, the problem of classifying all Lie algebras (and hence all Lie groups) reduces to the following three problems:

1. Classifying all semi-simple Lie algebras.

2. Classifying all solvable Lie algebras.

3. Figuring out how to paste these two together in a semi-direct sum.

Problem 1 was solved by Cartan in 1914. Problems 2 and 3 are open (see, e.g., [7] Chapter 9). For future reference, we mention that Cartan's classification of all semi-simple Lie algebras is in terms of the algebra's *rank*, defined as the maximal number of basis matrices in the algebra that can be chosen such that they commute.

## 4 The Classification of Fixed-Point-Free Lie Groups

We are now in a position to derive the main result of this note, the classification of all fpf Lie groups. To obtain this classification we shall use Levi's decomposition. Even though the question of classifying all solvable Lie algebras is open, there is some hope here since we are not looking for arbitrary solvable Lie groups, but for ones that have unitary representations and are fixed-point-free. We begin with some simple preliminary results.

**Lemma 1.** *A Lie group has a representation as unitary matrices if its algebra has a representation as skew-Hermitian matrices.*

**Proof:** Simply take the derivative of any curve of unitary matrices passing through the identity. (See (7) above.)

■

**Lemma 2.** *A unitary matrix $G = e^g$, with $g$ skew-Hermitian, has no eigenvalue at unity if, and only if, $g$ has no eigenvalue that is an integer multiple of $j2\pi$. Moreover, the number of unit eigenvalues of $e^g$ is equal to the number of eigenvalues of $g$ that are integer multiples $j2\pi$.*

**Proof:** Since $g$ is skew-Hermitian we may write $g = \Phi j \Lambda \Phi^*$, where $\Phi$ is unitary and $\Lambda$ is diagonal with real entries. The lemma now follows from $G = \Phi e^{j\Lambda} \Phi^*$.

■

The above lemmas imply that we must look for Lie algebras that have matrix representations that are skew-Hermitian and have no eigenvalues that are integer multiples of $j2\pi$. In particular, the Lie algebra should have a representation with *nonsingular* skew-Hermitian matrices.

One further result will be useful.

**Lemma 3.** *Let $\mathcal{G}$ be an fpf Lie group of unitary matrices. Then all the eigenvalues of every element in $\mathcal{G}$ are of the form $e^{j\theta}$ and $e^{-j\theta}$, with possibly different mutiplicities, for some $0 \leq \theta < 2\pi$.*

**Proof:** Note that for every element $G = e^g \in \mathcal{G}$, we have $e^{\alpha g} \in \mathcal{G}$ for all real-valued scalars $\alpha$. Therefore if $e^g$ has two eigenvalues $e^{j\theta_1}$ and $e^{j\theta_2}$ (the eigenvalues are unit-modulus since $e^g$ is unitary), then $e^{\alpha g}$ has two eigenvalues $e^{j\alpha\theta_1}$ and $e^{j\alpha\theta_2}$. Since for fpf groups if one eigenvalue is unity then all eigenvalues must be unity, we require that $j\alpha\theta_1$ be an integer multiple of $j2\pi$ if, and only if, $j\alpha\theta_2$ is an integer multiple of $j2\pi$. This can happen if, and only if, $\theta_1 = \theta_2$, or $\theta_1 = -\theta_2$, which yields the desired result.

■

We can now proceed with the main result. Let us first focus on solvable Lie algebras and then on semi-simple ones.

## 4.1 The Solvable Case

Suppose $\mathbf{g}$ is a solvable Lie algebra and consider any of its faithful[4] matrix representations as skew-Hermitian matrices. Furthermore, let $\mathbf{g}^{(n)}$ be the last nonzero commutator, i.e., $\mathbf{g}^{(n)} \neq \{0\}$ and

[4]Recall that if the representation is not faithful it will not be fpf.

$[\mathbf{g}^{(n)}, \mathbf{g}^{(n)}] = \{0\}$. Clearly, $\mathbf{g}^{(n)}$ is Abelian. Now $\mathbf{g}^{(n)}$ is an algebra of skew-Hermitian matrices so that each of its elements can be diagonalized. Since it is also Abelian, this implies that all its elements can be simultaneously diagonalized by a single similarity transformation.

Now $\mathbf{g}^{(n)}$ is itself a Lie algebra. (in fact, all $\mathbf{g}^{(s)}$, $s \leq n$ are Lie algebras.) Let us now study the cardinality of a minimal basis of $\mathbf{g}^{(n)}$. If $\mathbf{g}^{(n)}$ has two (or more) independent basis matrices, say $g_1$ and $g_2$, then since both $g_1$ and $g_2$ are diagonal with imaginary diagonal entries, there always exists real-valued scalars[5] $\alpha_1$ and $\alpha_2$ such that $\alpha_1 g_1 + \alpha_2 g_2$ is singular. Therefore there is a nonzero matrix in the representation of $\mathbf{g}$ that is singular and so by Lemma 2, $\mathcal{G}$ cannot be fixed-point-free.

We therefore must suppose that $\mathbf{g}^{(n)}$ has a single basis matrix $d$ that is diagonal. Without loss of generality, we may permute the diagonal entries of $d$ so that

$$d = \begin{bmatrix} d_1 I_{m_1} & 0 & \dots & 0 \\ 0 & d_2 I_{m_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_k I_{m_k} \end{bmatrix},$$

where $d_1, d_2, \dots, d_k$ are *distinct* non-zero imaginary scalars.[6]

Recall that $\mathbf{g}^{(n)} = [\mathbf{g}^{(n-1)}, \mathbf{g}^{(n-1)}]$ and let $g \in \mathbf{g}^{(n-1)}$. Then we must have $[g, d] = \alpha d$, for some $\alpha \in \mathcal{R}$. Writing out this commutator equation and using the above expression for $d$ shows that

[5]Recall that any algebra of skew-Hermitian matrices is real.

[6]In fact, from Lemma 3 we know that $k$ can be no larger than 2. But we need not insist on this here.

$\alpha = 0$ and that $g$ must have the form

$$g = \begin{bmatrix} g_1 & 0 & \dots & 0 \\ 0 & g_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g_k \end{bmatrix},$$

where each $g_i$ is a $m_i \times m_i$ matrix. Let $h \in \mathbf{g}^{(n-1)}$. By the same argument, $h$ must have the same block-diagonal structure as $g$. Now we must have $[g, h] = \beta d$, for some $\beta \in \mathcal{R}$. But,

$$[g,h] = \begin{bmatrix} [g_1,h_1] & 0 & \dots & 0 \\ 0 & [g_2,h_2] & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & [g_k,h_k] \end{bmatrix} = \begin{bmatrix} \beta d_1 I_{m_1} & 0 & \dots & 0 \\ 0 & \beta d_2 I_{m_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta d_k I_{m_k} \end{bmatrix},$$

implies that $\beta$ must be zero and that the $g_i$ and $h_i$ must commute. [Note that $[g_i, h_i]$ has zero trace, so that for the above equality to hold we must have $\beta = 0$.] But this further implies that $[\mathbf{g}^{(n-1)}, \mathbf{g}^{(n-1)}] = \{0\}$. But since our representation was faithful this contradicts the fact that $\mathbf{g}^{(n)}$ is the first commutator that terminates to zero. We therefore conclude that for $\mathbf{g}$ to be fpf we must have $\mathbf{g} = \mathbf{g}^{(n)} = \{\alpha d | \alpha \in \mathcal{R}\}$, which really means that $n = 0$. More importantly, we conclude that $e^{\alpha D}$, where $D$ is a nonsingular diagonal matrix with imaginary entries, is the only candidate for a solvable fpf Lie group. Since this is a representation for $U(1)$ we conclude that $U(1)$ *is the only solvable fixed-point-free group.* The irreducible representation of $U(1)$ is fpf and 1-dimensional. The reducible fpf representations have elements whose eigenvalues are of the form $e^{j\theta}$ and $e^{-j\theta}$.

### 4.2 The Semi-Simple Case

As mentioned earlier, the semi-simple Lie algebras are classified in terms of their rank, the maximal number of independent basis matrices that can be chosen such that they commute. Using an argument similar to the one presented above, any semi-simple Lie algebra with rank greater than one cannot be fpf since we can always find a real linear combination of two diagonal (with imaginary entries) basis matrices that is singular.

Therefore we must focus on semi-simple Lie algebras of rank one. By Cartan's classification, it is wellknown that there is only one semisimple complex lie algebra with rank 1, the algebra $sl(2)$. This is the algebra of traceless $2 \times 2$ matrices, and corresponds to the Lie group of unimodular (unit-determinant) $2 \times 2$ matrices. This algebra has two real forms, $su(2)$ and $sl(2, \mathcal{R})$. $sl(2, \mathcal{R})$ is the same as $sl(2)$, with the restriction that the elemenets of the $2 \times 2$ matrices are real. It is known that it has no finite-dimensional unitary representation. The other real form is the same as $sl(2)$, with the restriction that the $2 \times 2$ matrices are skew-Hermitian. The group corresponding to $su(2)$ is $SU(2)$, the group of $2 \times 2$ unimodular unitary matrices.

The unitary representations of $su(2)$ are all finite-dimensional. $su(2)$ has three generators $L_1$, $L_2$, and $L_3$, with the commutation relation

$$[L_1, L_2] = L_3, \qquad [L_2, L_3] = L_1, \qquad [L_3, L_1] = L_2.$$

It is known that in a $2k+1$-dimensional irreducible representation, where $2k$ is a non-negative integer, the eigenvalues of each generator are $\{jk, j(k-1), \ldots, -j(k-1), -jk\}$. This means that the eigenvalues of the corresponding elements of the group are $\{e^{jk}, e^{j(k-1)}, \ldots, e^{-j(k-1)}, e^{-jk}\}$. But Lemma 3 now implies that the only fpf representation corresponds to $k = \frac{1}{2}$, i.e., it is the

2-dimensional one.

To summarize, the only fpf semi-simple group is $SU(2)$. Its only irreducible fpf representation is the 2-dimensional one.

### 4.3 Main Result

**Theorem 4 (All Fixed-Point-Free Lie Groups).** *The only fpf Lie groups are $U(1)$ and $SU(2)$. Their only fpf irreducible representations are 1- and 2-dimensional, respectively.*

**Proof:** By Levi's decomposition $\mathbf{g}$ is the semi-direct sum of a solvable algebra $\mathbf{r}$ and a semi-simple algebra $\mathbf{s}$. We know that to be fpf $\mathbf{r}$ must have a representation with a single diagonal basis matrix. Since $\mathbf{r}$ is an ideal of $\mathbf{g} = \mathbf{r} \oplus_s \mathbf{s}$, we can use an argument similar to the one given for solvable Lie algebras to show that the representation of all the elements of $\mathbf{s}$ are block-diagonal (with the same blocks as the representation of $\mathbf{r}$). But this means that the representaion of the whole algebra is reducible (if the representation of $\mathbf{r}$ had two or more blocks). So the only remaining case is that the representation of $\mathbf{r}$ be just a multiple of the identity matrix, which clearly commutes with everything. That is, in this representation, $\mathbf{g}$ is in fact the direct sum of $\mathbf{r}$ and $\mathbf{s}$.

As this representation of $\mathbf{r}$ commutes with $\mathbf{s}$, the representation of $\mathbf{s}$ should be irreducible to make the representation of the whole $\mathbf{g}$ irreducible. This shows that $\mathbf{s}$ should be $su(2)$, and the representation should be 2-dimensional. Adding the representation of $\mathbf{r}$ to this, we arrive at the 2-dimensional representation of $u(2)$, which is clearly not fpf. So Levi's decomposition should be so that either $\mathbf{r}$ or $\mathbf{s}$ be zero. If $\mathbf{s}$ is zero, we have the 1-dimensional representation of $u(1)$. If $\mathbf{r}$ is zero, we have the 2-dimensional representation of $su(2)$.

■

## 5 Discussion and Conclusion

We have essentially obtained a negative result. The only fpf Lie groups are the ones currently employed in practice $U(1)$, the group of unit modulus scalars, and $SU(2)$, the $2 \times 2$ orthogonal designs of Alamouti. Therefore our investigation has not led to any new group or new constellation.

However, our studies suggest two possible venues for further work and possible multi-antenna constellation design. One is to search for non-group constellations of unitary matrices of the form $e^{\sum_k \alpha_k S_k}$ where the $\{S_k\}$ are skew-Hermitian basis matrices and the $\{\alpha_k\}$ are real-valued scalars. This would require an appropriate design of the $\{S_k\}$ (to ensure a fully-diverse constellation, say) as well as a suitable choice of the $\{\alpha_k\}$.

The other is to relax the fpf condition and to classify all Lie groups whose non-unit elements have no more than $k > 0$ unit eigenvalues. ($k = 0$ corresponds to fpf groups.) Since in designing a constellation of finite size we need to sample the Lie group's underlying manifold, the reasoning is that if $k$ is small there is a good chance that, if the sampling is performed appropriately, the resulting constellation will be fully diverse.

To end this note we give a result which is a first step in obtaining the aforementioned classification. Because of this result and Cartan's classification of semi-simple algebras in terms of their rank, there is hope in being able to obtain the classification.

**Theorem 5 (Lie Groups with Unitary Representations).** *A Lie group has a representation as unitary matrices if, and only if, it is a compact semi-simple algebra or the direct sum of $U(1)$ and a compact semi-simple algebra.*

**Proof:** We first consider a solvable Lie algebra, $\mathbf{g}$, and modify slightly the argument of Sec. 4.1. Thus, let $\mathbf{g}^{(n)}$ be the last nonzero algebra in the chain of $\mathbf{g}^{(k)}$'s. $\mathbf{g}^{(n)}$ is Abelian and, by virtue of being an algebra of skew-Hermitian matrices, all its elements are simultaneously diagonalizable.

Consider a basis, $\{d^{(1)}, d^{(2)}, \ldots, d^{(p)}\}$, for the diagonal representation of $\mathbf{g}^{(n)}$. Without loss of generality, we can permute the diagonal entries of $d^{(1)}$ to write

$$d^{(1)} = \begin{bmatrix} d_1^{(1)} I_{m_1} & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & d_k^{(1)} I_{m_k} \end{bmatrix},$$

where $d_1^{(1)}, \ldots, d_k^{(1)}$ are distinct imaginary scalars. The diagonal entries of the remaining basis matrices $\{d^{(2)}, \ldots, d^{(p)}\}$ will not necessarily be constant within the block entries of $d^{(1)}$. Nonetheless, within each block entry of $d^{(1)}$, we can permute the diagonal entries of $d^{(2)}$ such that they fall into blocks with distinct diagonals. We can then continue this process: within each block in which the entries of *both* $d^{(1)}$ and $d^{(2)}$ are constant, we can permute the diagonal entries of $d^{(3)}$ such that they fall into blocks with distinct diagonals, and so on. The upshot of this permutation process is that the representation space $V$ is broken up into the direct sum of subspaces $V_i$, such that the representation of each basis matrix in $V_i$ is simply a multiple of the identity matrix.

Consider now $\mathbf{g}^{(n-1)}$ and an arbitrary element $g \in \mathbf{g}^{(n-1)}$. Following the argument of Sec. 4.1 writing out the commutator equation $[g, d^{(1)}] = \sum_{k=1}^{p} \alpha_k d^{(k)}$ implies that $g$ must be block-diagonal with blocks corresponding to those of $d^{(1)}$. Further writing out the commutator equation of $g$ with $d^{(2)}$ implies that $g$ must be block-diagonal with blocks corresponding to where $d^{(1)}$ and $d^{(2)}$ are *both* multiples of the identity matrix. Continuing with this argument until $d^{(p)}$, we conclude that $g$ is block-diagonal with blocks corresponding to the subspaces $V_i$.

Since $g$ was arbitrary, any $h \in \mathbf{g}^{(n-1)}$ must have the same block-diagonal structure. Writing out the commutator equation $[g, h] = \sum_{k=1}^{p} \beta_k d^{(k)}$ one notes that the commutator of each block diagonal of $g$ and $h$ must be a multiple of the identity matrix. By the same trace argument as Sec. 4.1, we conclude that the block-diagonals of $g$ and $h$, and hence $g$ and $h$ themselves, must commute. But this implies that $[\mathbf{g}^{(n-1)}, \mathbf{g}^{(n-1)}] = \{0\}$, which, assuming that the representation is faithful, is a contradiction and further implies $\mathbf{g} = \mathbf{g}^{(n)}$, i.e., $n = 0$. To summarize, any solvable algebra with skew-Hermitian representation (so that the group has unitary representation) is Abelian, consisting of diagonal elements.

Now consider the Levi decomposition $\mathbf{g} = \mathbf{r} \oplus_s \mathbf{s}$, where $\mathbf{r}$ is solvable $\mathbf{s}$ is semi-simple. As the sum is a semidirect sum, $\mathbf{r}$ is an ideal and $[\mathbf{r}, \mathbf{s}] \subseteq \mathbf{r}$. But one can repeat the above arguement to show that the representation of $\mathbf{s}$ is block-diagonal in the same blocks of the representation of $\mathbf{r}$, and commutes with the corresponding representation of $\mathbf{r}$. Thus, we conclude that the representation of the whole algebra is reducible, unless the representation of $\mathbf{r}$ consists of just one block. In the latter case, the representation of $\mathbf{r}$ is just the representation of $u(1)$. We have thus proved the desired result: any unitary irreducible representation of a Lie algebra is isomorphic to either a unitary representation of a semi-simple Lie algebra, or a unitary representation of the direct sum of a semi-simple Lie algebra and the algebra $u(1)$. By the Peter-Weyl theorem (see, e.g., [8]), for the representation of the semi-simple Lie algebra to be unitary, the semi-simple algebra should be compact, that is it should correspond to a compact Lie group.

$\blacksquare$

# References


[1] B. Hassibi, A. Shokrollahi, B. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *submitted to IEEE Trans. Info. Theory*, 2000. Download available at `http://mars.bell-labs.com`.

[2] 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.

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

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

[5] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Sel. Area Comm.*, pp. 1451–1458, Oct. 1998.

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

[7] D. Sattinger and O. Weaver, *Lie Groups and Algebras with Applications to Physics, Geometry and Mechanics.* Springer-Verlag, New York, 1986.

[8] W. Fulton and J. Harris, *Representation Theory: A First Course.* Springer-Verlag, New York, 1991.

[9] R. Gilmore, *Lie Groups, Lie Algebras, and Some of Their Applications.* John-Wiley, New York, 1974.