Multi-Antenna Differential Modulation: From Fixed-Point-Free Groups to Cauchy Random Matrices

Babak Hassibi

Outline

- **Introduction**
  - multiple antenna communication
  - differential modulation
- **Problem Formulation**
  - constellation design for multi-antenna differential modulation
- **Constellations from Groups**
  - fixed-point-free (fpf) groups
  - finite groups, Lie groups
- **Constellations from Cayley Transform**
  - Cauchy random matrices
  - sphere decoding
- **Conclusion**

Multi-Antenna Communications

Multiple antennas have generated great interest for *high data rate* wireless communications, since in a *rich-scattering environment* they can

- significantly boost channel capacity
  - at high SNR, capacity grows linearly in the (minimum of the) number of transmit and receive antennas (Foschini, Telatar, '95)
- lower the probability of error

of a wireless communications link. (Key: *spatial diversity*)

Applications abound and include:

- wireless LAN, mobile wireless, wireless Internet, etc.

Challenge: to devise practical space-time transmission schemes that are *simple, yet effective.*

Fading Channels

- In wireless communications one is often confronted with a fading channel
  - fading is usually continuous
  - the main source of fading is mobility
  - another source is local oscillator instability
- One method to deal with fading:
  - periodically transmit training (pilot) symbols
  - perform channel tracking, e.g., automatic gain control (AGC), in between
- In the multi-antenna case this is both complicated and resource-consuming (both time and power)
  - channel has MN coefficients (M number of transmit and N number of receive antennas)

Differential Modulation

- In single antenna systems a simple method to combat fading is to employ differential modulation
- The transmitted signals have constant-modulus—one typically uses m-PSK modulation
- Information is encoded differentially on the *phase* of the transmitted signals
- No need to know the channel or to track it (as long as the phase of the channel remains (relatively) constant during two subsequent channel uses)

We are interested in the generalization to multiple antennas

The Model

Consider a (M, N) multi-antenna system (*rich-scattering* and *narrow-band*), where the channel is constant for (at least) M channel uses. Then we can write

$$X = \sqrt{\rho} S H + W,$$

where $E \mathrm{tr} S S^* = M$, ρ is the SNR, and

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

The channel $H \in \mathcal{C}^{M \times N}$ and additive noise $W \in \mathcal{C}^{M \times N}$ are unknown with independent $\mathcal{CN}(0, 1)$ entries.

Multi-Antenna Differential Modulation

(Hughes '99, Hochwald and Sweldens '99, Tarokh and Jafarkhani '99)

Assume that for each *block-time* i (consisting of M channel uses):

$$S_i = V_i S_{i-1} = V_i V_{i-1} \dots V_0.$$

Then assuming that the channel is constant for $2M$ channel uses:

$$\begin{aligned} X_i = \sqrt{\rho} S_i H + W_i &= \sqrt{\rho} V_i S_{i-1} H + W_i \\ &= V_i (X_{i-1} - W_{i-1}) + W_i, \end{aligned}$$

so that

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

Thus, we have eliminated the need to know the channel H!

The Transmitted Signals

- Clearly, the matrices V_ℓ must be unitary, otherwise the product $S_i = V_i V_{i-1} \ldots V_0$ goes to zero, infinity, or both.
- When V_i is unitary the additive noise term:

$$W_i^{'} = W_i - V_i W_{i-1},$$

becomes independent of V_i, and so the ML decoder takes the form:

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

- We therefore must construct a constellation $\mathcal{V} = \{V_0, \ldots, V_{L-1}\}$ of $M \times M$ unitary matrices.

But how to do this?...

The Optimal Input Distribution

Given that we must transmit unitary matrices, a natural question is what is the optimal distribution on these unitary matrices?

Theorem 1 (Hassibi and Hochwald, 2000) *Consider the following differential set-up*

$$\begin{bmatrix} X_{i-1} \\ X_i \end{bmatrix} = \sqrt{\frac{\rho}{M}} \begin{bmatrix} S_{i-1} \\ V_i S_{i-1} \end{bmatrix} H + \begin{bmatrix} W_{i-1} \\ W_i \end{bmatrix},$$

where $S_{i-1} = V_{i-1}V_{i-2}\ldots$ and $H, W_{i-1}, W_i \in \mathcal{C}^{M\times N}$ are unknown with independent $\mathcal{CN}(0,1)$ entries. Then the mutual-information-maximizing *V_ℓ's are isotropically-random-unitary-distributed and independent.*

Side: An isotropically-random (i.r.) unitary matrix V is one for which

$$p(V) = p(\Theta V) = p(V\Theta),$$

for all unitary Θ.

The Multi-Antenna Constellation

- The previous result may not *appear* very useful for the design of an actual constellation $\mathcal{V} = \{V_0, \ldots, V_{L-1}\}$ of $M \times M$ unitary matrices.

A more useful criterion is the probability of mistaking one symbol of $\mathcal{V}$ for another.

- At high SNR, this pairwise probability of error is dominantly dependant on the determinant of $V_\ell - V_{\ell'}$.
- We therefore measure the quality of the constellation by

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

- This leads us to the following design problem:
  - *given M and R, 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.*

“Fully Diverse” Constellations

- We shall call any constellation $\mathcal{V}$ with the property that the determinants of the pairwise differences are all nonzero, *fully diverse.*
- The reason is the following: 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
- In its full generality, the design problem is extremely difficult
  - the search space (of all $M \times M$ unitary matrices) is highly nonlinear, the cost is non-convex, and the problem size is huge (we seek $L = 2^{MR}$ matrices)
- Therefore one must restrict the search to specific structures

Orthogonal Designs (Alamouti, 1997)

- Let x and y be complex numbers such that $|x|^2 + |y|^2 = 1$. Then an *orthogonal design* is the unitary matrix:

$$V = \begin{bmatrix} x & -y^* \\ y & x^* \end{bmatrix}$$

- Orthogonal designs have various interesting properties, in particular,

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

  Thus, the design problem reduces to the design of spherical codes on the 3-dimensional real sphere (in 4-space).

- The drawback is that orthogonal designs exist only in 2×2 case.

Constellations from Groups

- Various authors have looked at other structures (such as diagonal constellations), but with limited success

To break the logjam, and for various other reasons, let us investigate the case where $\mathcal{V}$ forms a group under matrix multiplication.

- The design problem also simplifies, since

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

Fixed-Point-Free Groups

- Although our aim is to maximize

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

  it is at this point not even clear whether, or when, this quantity is zero for a given group G.

- Clearly, $\zeta_{\mathcal{V}}$ will be nonzero if and only if all the matrices $V \neq I$ have no eigenvalues at unity.

- Groups that have representations with this property are referred to as *fixed-point-free groups* — an eigenvalue at unity implies $Vx = x$, for some vector x, i.e., that V has a fixed-point.

- Therefore we need to search for fixed-point-free groups.

Zassenhaus' Characterization

Zassenhaus in 1936 gave an *almost* complete characterization of finite fixed-point-free groups. Here is his result for groups of odd order:

Theorem 2 (Zassenhauss) *Let G be a fixed point free group of odd order L. Then there exist integers m and r such that G is isomorphic to the group*

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

where

(i) $L = mM$.

(ii) *M is the smallest integer such that $r^M \equiv 1 \bmod (m)$.*

(iii) $\gcd(M, t) = 1$, *where* $t = \frac{m}{\gcd(r-1,m)}$.

All Odd-Order Fixed-Point-Free Groups

Using Zassenhaus' partial characterization, we have been able to show the following result.

Theorem 3 (Hassibi etal, 2000) *A finite group G of odd order, L, is fixed point free if and only if it is isomorphic to a group*

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

for some integers m and r such that:

(i) $L = mM$.

(ii) *M is the smallest integer such that* $r^M \equiv 1 \mathrm{mod}(m)$.

(iii) $\gcd(M, t) = 1$, *where* $t = \frac{m}{\gcd(r-1,m)}$.

(iv) *All prime divisors of M divide* $\gcd(r-1, m)$.

The Group Representation

The representation of the group takes the form:

$$\mathcal{V} = \left\{ \Delta(\sigma)^{\ell} \Delta(\tau)^{k} \,|0 \leq \ell \leq m-1, 0 \leq k \leq M-1 \right\},$$

where

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

and $\eta = e^{j2\pi/m}$.

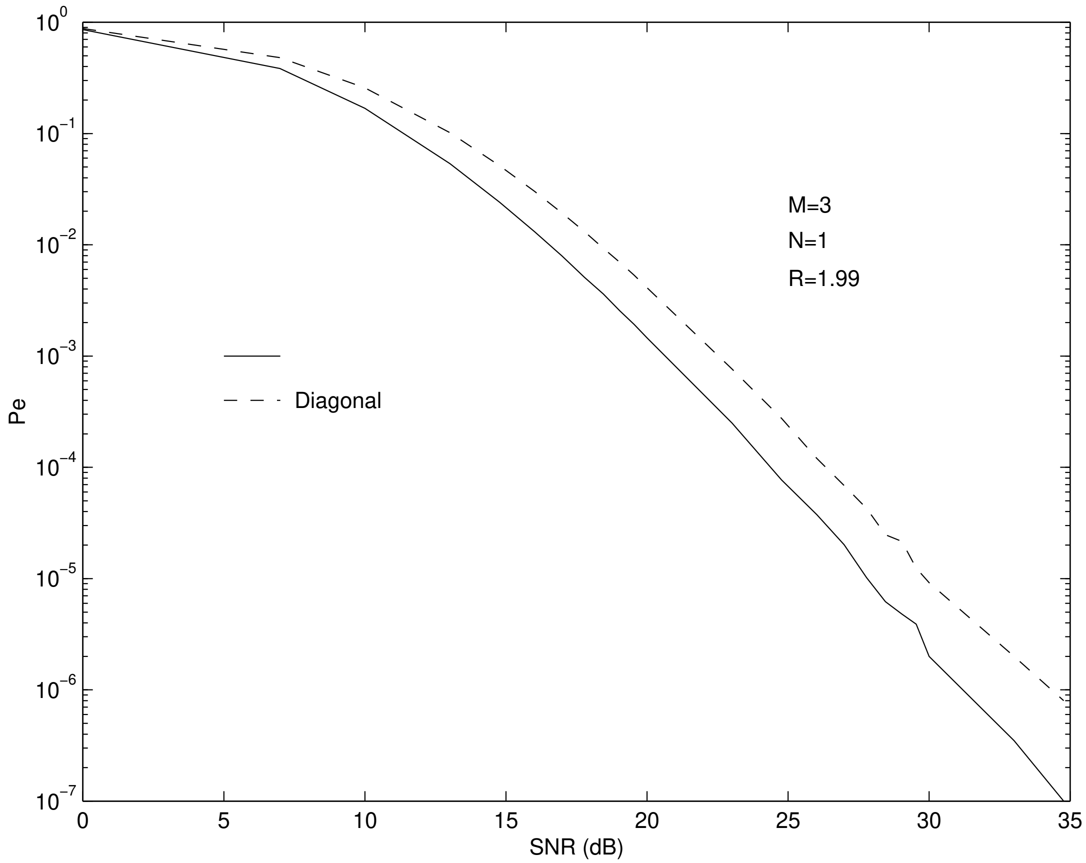
Example, $M = 3$

Let $M = 3$ and take $r = 4$ and $m = 21$. Then we have $t = 7$, and it can be verified that conditions (i)-(iv) of the theorem are all satisfied. Thus, define $\eta = e^{j2\pi/21}$, and set

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

The 63 matrices $A^\ell B^k$, where $0 \le \ell \le 20$ and $0 \le k \le 2$ form a group under matrix multiplication and the corresponding ζ-value can be computed to be $\zeta = 0.3851$. This 3-antenna, 63-element, constellation is by one element shy of producing a constellation of rate 2.

$G_{21,4}$ vs. Diagonal Constellation



Even-Order Fixed-Point-Free Groups

- The classification of even-order fixed-point-free groups is slightly more involved.
- In addition to $G_{m,r}$, there are five other group types.
- One interesting even-order fixed-point-free group is $SL_2(\mathcal{F}_5)$, the group of 2×2 matrices over $\mathcal{F}_5$ with determinant unity. This group has 120 elements and can be expressed as

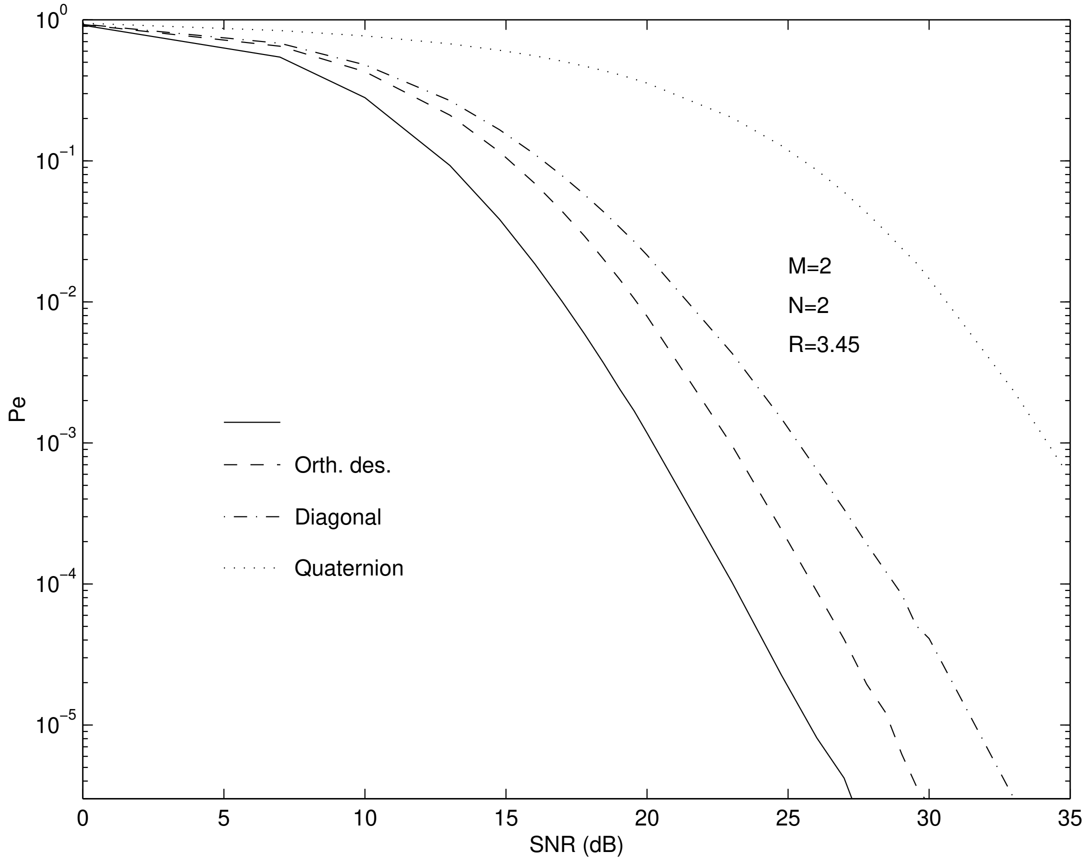
$$SL_2(\mathcal{F}_5) = \langle \mu, \gamma \mid \mu^2 = \gamma^3 = (\mu\gamma)^5, \mu^4 = 1 \rangle.$$

The representation of its generators is given by

$$\Delta(\mu) = \frac{1}{\sqrt{5}} \begin{bmatrix} \eta^2 - \eta^3 & \eta - \eta^4 \\ \eta - \eta^4 & \eta^3 - \eta^2 \end{bmatrix}, \quad \Delta(\gamma) = \frac{1}{\sqrt{5}} \begin{bmatrix} \eta - \eta^2 & \eta^2 - 1 \\ 1 - \eta^3 & \eta^4 - \eta^3 \end{bmatrix}$$

where $\eta = e^{2\pi i/5}$.

$M = 2$, $N = 2$ and $R = 3.45$



Remarks

- We have thus classified all *finite* fpf groups
  - there are some star performers among these ($SL_2(\mathcal{F}_5)$)
  - they are generally few and far between
  - the best constellations are not obtained for very high rates or for a large number of antennas
- This brings up the question of whether there are any *infinite* fpf groups?

In turns out that there are (and they are widely-used in communications), though they were never thought of as fpf groups.

Phase Modulation: Consider the group of unit-modulus complex scalars:

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

which is clearly fpf

- widely used: PM, FM, single-antenna differential modulation
- constellation design: choose (equi-distant) points on the unit-circle—PSK signals, QPSK modulation, etc.

Alamouti's Scheme:

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

It is easy to see that orthgonal designs

- form a group (the group of unit-determinant unitary matrices)
- are fpf: the eigenvalues of V are $\{e^{j\theta}, e^{-j\theta}\}$, $\theta = \cos^{-1}(\frac{x+x^*}{2})$.

Other Infinite Fixed-Point-Free Groups?

- **Countable groups**
  - not interesting, not clear how to sample,...
- **Continuous groups**
  - most interesting case is that of a Lie group (the above two examples are Lie groups)
  - with a Lie group the problem of constellation design becomes one of sampling the group's underlying manifold (the unit-circle, in the first case, the 3-dimensional sphere, in the second)
  - in fact, our star performer, $SL_2(\mathcal{F}_5)$ is an orthogonal design with an optimal sampling of 120 points on the 3-dimensional sphere

We therefore focus on Lie groups. But what are they?...

Lie Groups

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 θ on the manifold there is an element $g(\theta)$ of the group. Moreover, the mappings from (θ_1, θ_2) to θ_3 defined via $g(\theta_1)g(\theta_2) = g(\theta_3)$, as well as the mapping from θ to ϕ defined via $g^{-1}(\theta) = g(\phi)$, are analytic.

Examples:

- $GL(n)$: nonsingular $n \times n$ matrices
- $U(n)$: $n \times n$ unitary matrices (phase modulation is $U(1)$)
- $SU(n)$: unit-determinant $n \times n$ unitary matrices (OD is $SU(2)$)
- Heisenberg group: upper-triangular unit-diagonal matrices

All Fixed-Point-Free Lie Groups

Theorem 4 (Hassibi and Khorrami, 2000) *The only fpf Lie groups are $U(1)$ and $SU(2)$. Their only irreducible representations are 1- and 2-dimensional, respectively.*

Thus, phase modulation and Alamouti's scheme are all there are.

Remarks

- We have thus exhausted the group possibilities. These yield excellent constellations for $M \leq 2$, and for $M > 2$ and low to moderate rates—but not for high rates.
- The reason is that at high rates, i.e., when the size of the constellation is very large, we expect a "good" constellation to have the "appearance" of an isotropically-random unitary constellation. The structure of the fpf groups, however, (except for at $M = 1, 2$) does not permit this.

But is this a problem with groups, or a problem with the fully-diverse constraint?

- We suspect that it is a problem with the latter: at high rates the "worst-case performance" of the constellation is not as crucial as its "general structure".

High Rate Constellations

But what to do for high rates?

- construct a random constellation?
  - too unstructured, decoding intractable

Challenge: Construct *simple* yet *effective* differential schemes:

- simple, so that decoding can be done in real-time
- effective, so that the high rates predicted by theory can be achieved

To do this we need to further understand unitary matrices.

Parametrization of Unitary Matrices

The space of $M \times M$ unitary matrices is called the *Stiefel manifold* and can be described by M^2 real parameters. Some parametrizations include:

- product of $M(M-1)/2$ Givens (planar) rotations, a unitary diagonal, and another $M(M-1)/2$ Givens rotations
  - too nonlinear
- product of M Householder reflections and a unitary diagonal
  - too nonlinear
- $\Phi = e^{jA}$, with A Hermitian
  - suggested by Lie algebra, not one-to-one

The Cayley Transform

Cayley transform:

$$\Phi = (I + jA)^{-1}(I - jA)$$

with A Hermitian ($R \stackrel{\Delta}{=} jA$ skew-Hermitian).

- not too nonlinear
- is one-to-one: A can be found from the inverse Cayley transform $jA = (I + \Phi)^{-1}(I - \Phi)$

Let's first make sure it works (since $(I - jA)$ and $(I + jA)$ commute):

$$\begin{aligned} \Phi\Phi^* &= (I + jA)^{-1}(I - jA)\left[(I + jA)^{-1}(I - jA)\right]^* \\ &= (I + jA)^{-1}(I - jA)(I + jA)(I - jA)^{-1} = I \end{aligned}$$

and

$$\begin{aligned} R^* &= (I - \Phi^*)(I + \Phi^*)^{-1} = (\Phi - I)\Phi^*\Phi(\Phi + I)^{-1} \\ &= -(I + \Phi)^{-1}(I - \Phi) = -R \end{aligned}$$

Some Properties

- The Cayley transform therefore maps unitary matrices to skew-Hermitian ones and vice-versa. This transforms the nonlinear Stiefel manifold to the linear space of skew-Hermitian matrices.
- Is the matrix generalization of $z = \frac{1-jw}{1+jw}$ that maps the real line to the unit circle.
- In general, maps matrices with eigenvalues inside the unit circle to matrices with eigenvalues in the right-half-plane (RHP).

Some applications of Cayley transforms:

- *Control theory:* maps continuous-time systems to discrete-time systems (since stability is preserved), maps bounded real functions to positive real functions, contractive systems to passive ones, etc.
- *Lie groups:* solutions of differential equations over Lie groups

The Cauchy Distribution

- When Φ is isotropically-distributed, the distribution of A is

$$p(A) = \frac{C}{\det(I + A^2)^M},$$

which is the matrix generalization of the *Cauchy distribution*:

$$p(a) = \frac{1}{\pi(1 + a^2)}.$$

ϕ uniform implies $a = j\frac{1-e^{j\phi}}{1+e^{j\phi}} = \tan(\phi/2)$ is Cauchy.

- A scalar Cauchy random variable is often regarded as the ratio of two independent Gaussian random variables. It is (in)famous for the following two reasons:
  - it has infinite variance
  - the mean of n independent Cauchy random variables is Cauchy distributed—does not satisfy the law of large numbers!

Some Further Properties

- A matrix and its Cayley transform commute: hence are simultaneously diagonalizable
- Note that

$$
\begin{aligned}
\Phi_1 - \Phi_2 &= (I+R_1)^{-1}(I-R_1) - (I-R_2)(I+R_2)^{-1} \\
&= (I+R_1)^{-1}\left[(I-R_1)(I+R_2) - (I+R_1)(I-R_2)\right](I+R_2)^{-1} \\
&= 2(I+R_1)^{-1}\left[R_2 - R_1\right](I+R_2)^{-1}
\end{aligned}
$$

Therefore a set of unitary matrices is fully-diverse iff the set of Cayley transformed skew-Hermitian matrices is fully-diverse.

Decoding

Recall that the equation for differential modulation was

$$
\begin{aligned}
X_i &= V_i X_{i-1} + W_i - V_i W_{i-1} \\
&= (I + jA)^{-1}(I - jA)X_{i-1} + W_i - (I + jA)^{-1}(I - jA)W_{i-1}
\end{aligned}
$$

so that

$$
(I + jA)X_i = (I - jA)X_{i-1} + (I + jA)W_i - (I - jA)W_{i-1},
$$

or

$$
X_i - X_{i-1} = A\frac{1}{j}(X_i + X_{i-1}) + (I + jA)W_i - (I - jA)W_{i-1},
$$

which linearizes the problem in A!

The Constellation

To facilitate decoding, we therefore propose the following *linear* constellation:

$$A = \sum_{q=1}^{Q} \alpha_q A_q$$

where

- the α_q are real scalars
- the A_q are fixed $M \times M$ Hermitian matrices
- the code is determined by $\{A_q\}$
- the codeword is determined by the scalars $\{\alpha_q\}$

Decoding

The ML decoder is given by

$$\arg\min_{\{\alpha_q\}} \left\| \left(I + j \sum_{q=1}^{Q} \alpha_q A_q \right)^{-1} \left(X_i - X_{i-1} - \frac{1}{j} \sum_{q=1}^{Q} \alpha_q A_q (X_i + X_{i+1}) \right) \right\|^2$$

which is a non-quadratic problem.

However, ignoring the variance of the noise leads to the "linearized" ML decoder

$$\arg\min_{\{\alpha_q\}} \left\| X_i - X_{i-1} - \frac{1}{j} \sum_{q=1}^{Q} \alpha_q A_q (X_i + X_{i+1}) \right\|^2$$

- Since it is quadratic in the $\{\alpha_q\}$, this latter cost function can be readily minimized using nulling and cancelling (a la BLAST), or sphere decoding.

- Sphere decoding can be regarded as a generalization of nulling and cancelling where at each step, rather than making a hard decision on the corresponding α_q, we consider *all* those α_q that lie within a sphere of a certain radius.
- In fact, at high SNR, one can compute the optimal solution using sphere decoding with complexity close to that of nulling and cancelling.
- The degradation in performance, due to the linearized cost, compared to ML is not too severe. Moreover, the solution can used as an initial condition for Newton-Raphson-type methods applied to the true ML cost.

Constellation Design

How to design Q, $\{\alpha_q\}$ and $\{A_q\}$?

- Choosing Q:
  - to make the constellation as rich as possible we should make Q (the degrees of freedom) as large as possible
  - to allow for linear decoding, Q should not be larger than the number of *independent* equations
  - Q cannot be larger than the degrees of freedom in a unitary (or skew-Hermitian) matrix: $Q \leq M^2$
  - these lead to: $Q = \min(N, M) \max(2M - N, M)$

- Choosing $\{\alpha_q\}$: via discretization of a scalar Cauchy distribution
  - $L = 2$: $\alpha_q \in \{\tan(3\pi/4), \tan(\pi/4)\} = \{-1, 1\}$
  - $L = 4$: $\alpha_q \in \{\tan(7\pi/8), \tan(5\pi/8), \tan(\pi/8), \tan(3\pi/8)\} = \{-2.41, -0.41, 0.41, 2.41\}$
  - $L = 8$: $\alpha_q \in \{-5.03, -1.50, -0.67, -0.20, 0.20, 0.67, 1.50, 5.03\}$
- Choosing $\{A_q\}$:
  - We know that the optimal distribution on the unitary matrices is isotropically-random. Therefore we need to choose the $\{A_q\}$ so that the constellation is as "isotropically-random looking" as possible.
  - But how to do this? The next result suggests a solution.

An Optimality Result

Theorem 5 (Hassibi and Hochwald, 2000) *Let* Φ_1 *and* Φ_2 *be* $M \times M$ *independent random unitary matrices chosen according to some distribution* $p_\Phi(\cdot)$. *Then the cost function*

$$\frac{1}{M} E \log det \left(\Phi_1 - \Phi_2\right) \left(\Phi_1 - \Phi_2\right)^*$$

is maximized when $p_\Phi(\cdot)$ *is the i.r. distribution. Moreover, the maximum value of the cost is zero.*

We therefore propose to choose the $\{A_q\}$ to maximize the cost

$$\max_{\{A_q\}} \frac{1}{M} E \log\det\left(\Phi_1 - \Phi_2\right)\left(\Phi_1 - \Phi_2\right)^*$$

where $\Phi_k = (I + R_k)^{-1}(I - R_k)$, $k = 1, 2$ and

$$R_1 = j\sum_{q=1}^{Q} \alpha_q A_q \quad , \quad R_2 = j\sum_{q=1}^{Q} \beta_q A_q$$

and the expectation is taken over the independent Cauchy random variables $\{\alpha_q, \beta_q\}$.

The above cost function further simplifies to:

$$\max_{\{A_q\}} \left[\log 8 + \frac{1}{M} E \log\det A^2 - \frac{2}{M} E \log\det(I + A^2)\right],$$

where $A = \sum_{q=1}^{Q} \alpha_q A_q$ and the expectation is taken over the independent Cauchy random variables $\{\alpha_q\}$.

Maximization of the cost can be readily performed using gradient search.

$M = N = 2,\ R = 6$

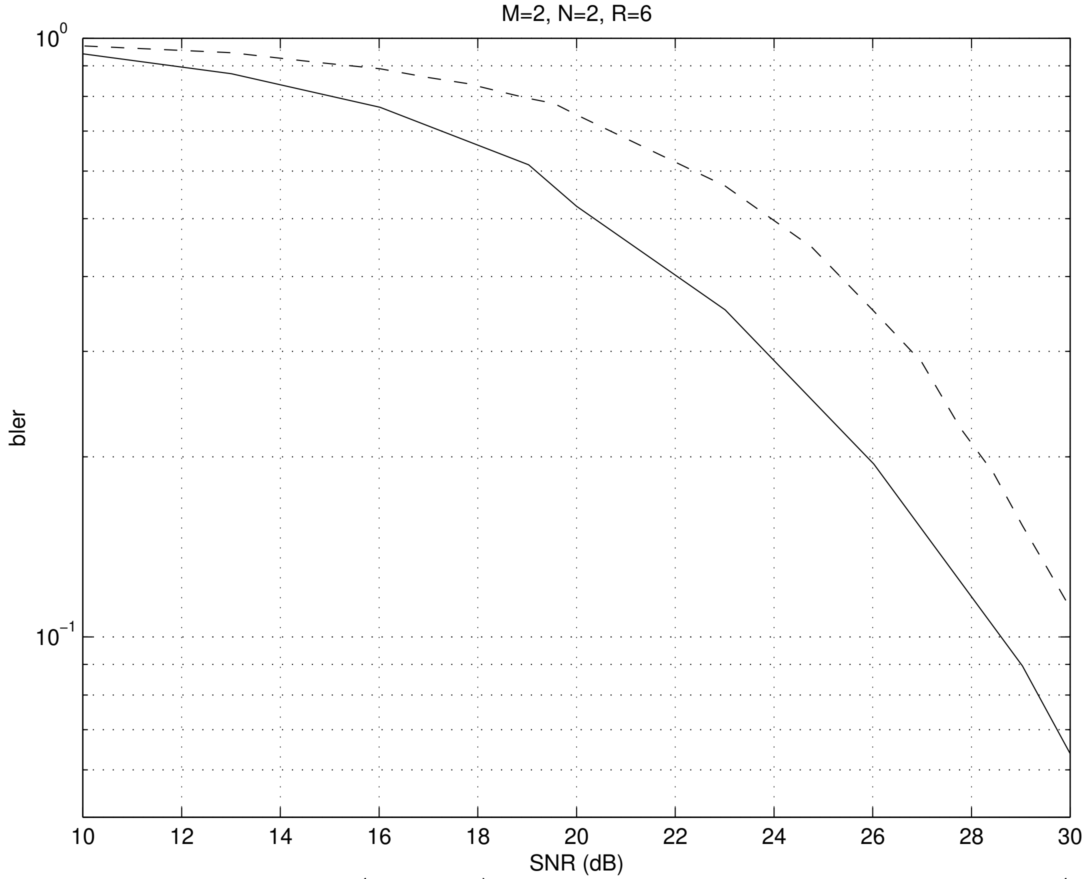


Figure 1: Cayley code (solid) vs. orthogonal design (dashed)

$M = 4,\ N = 2,\ R = 4$: ML vs. "Linearized" ML

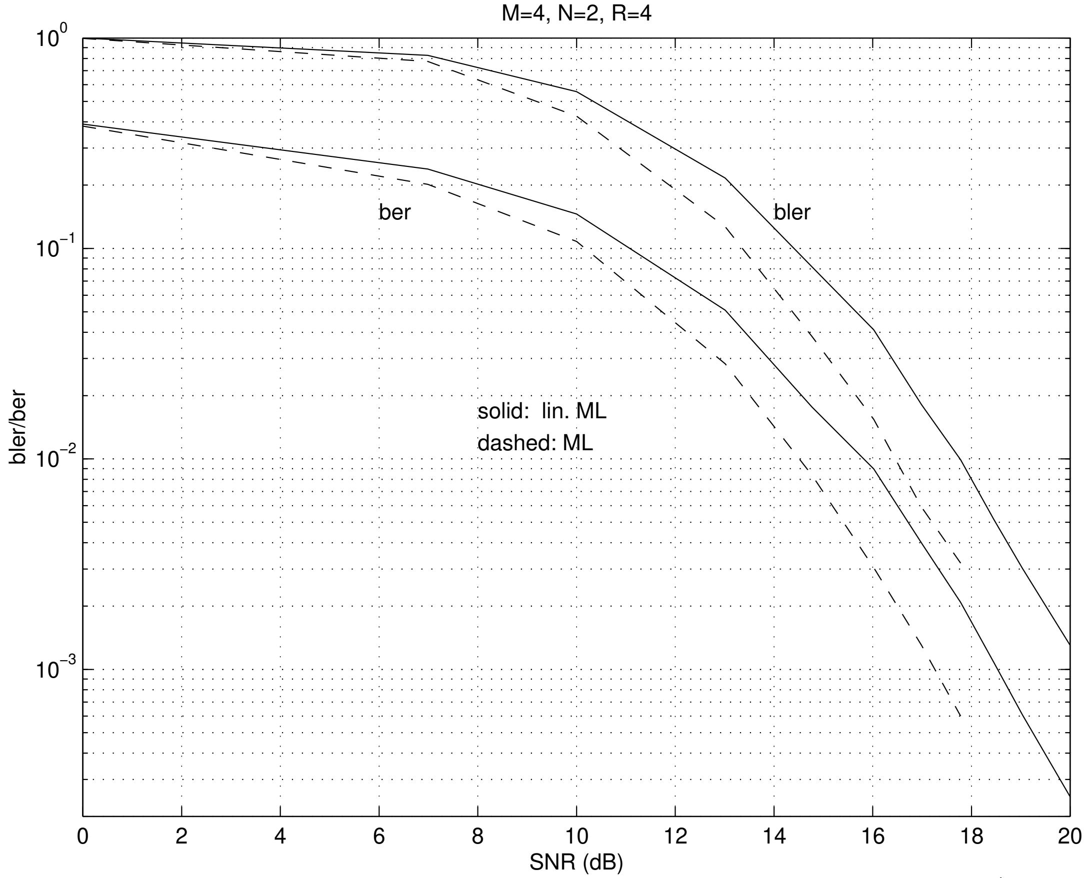


Figure 2: Cayley code decoded by "linearized" ML (solid) vs. true ML (dashed)

$M = N = 4$, $R = 8$: Sphere vs. BLAST decoding

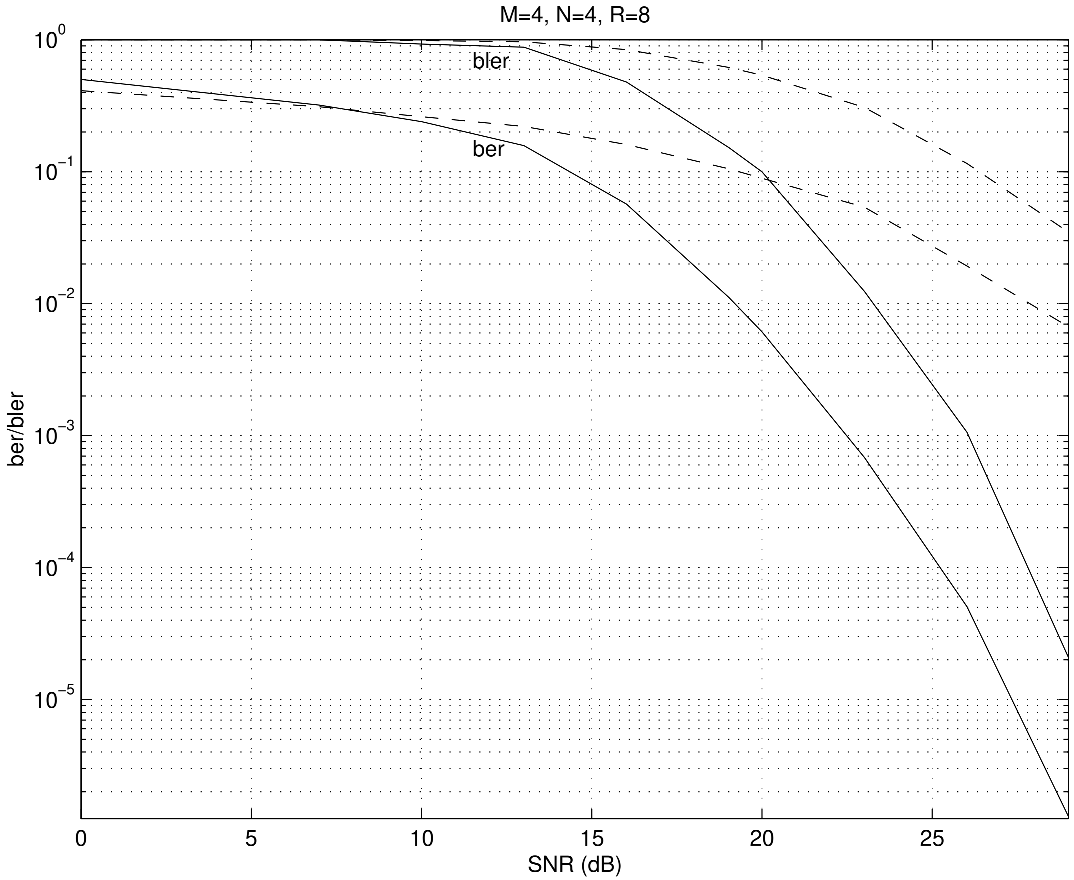


Figure 3: Cayley code decoded by sphere decoding (solid) vs. BLAST decoding (dashed)

Conclusion

Summary: Studied the problem of signal constellation design for multi-antenna differential modulation

- Used group-theoretic methods to construct *fully-diverse* constellations:
  - characterized all finite and Lie fpf groups
  - resulting constellations are multi-antenna analogs of PSK signals
  - have excellent performance at low to moderate rates
- Introduced a class of signal constellations based on the Cayley transform which
  - is applicable for high rates
  - can be used for any number of transmit and receive antennas
  - has very simple encoding and efficient $O(N^3)$ decoding
  - satisfies a probabilistic criterion: tries to match the mutual-information-maximizing distribution