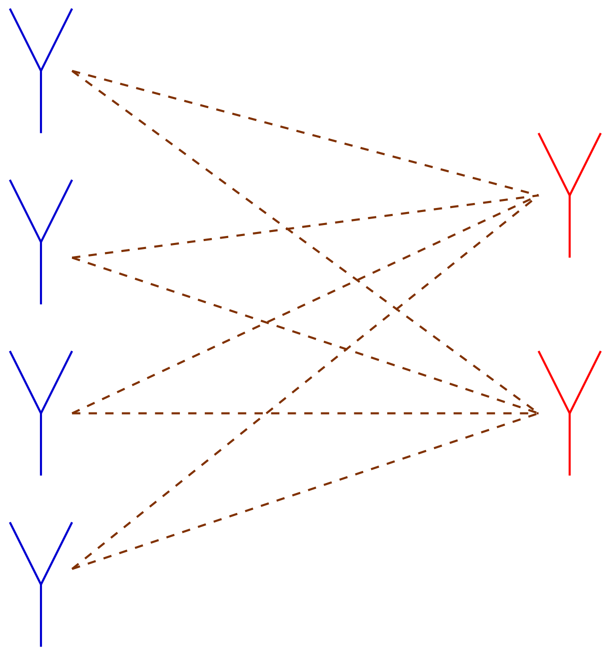
Packing Unitary Matrices

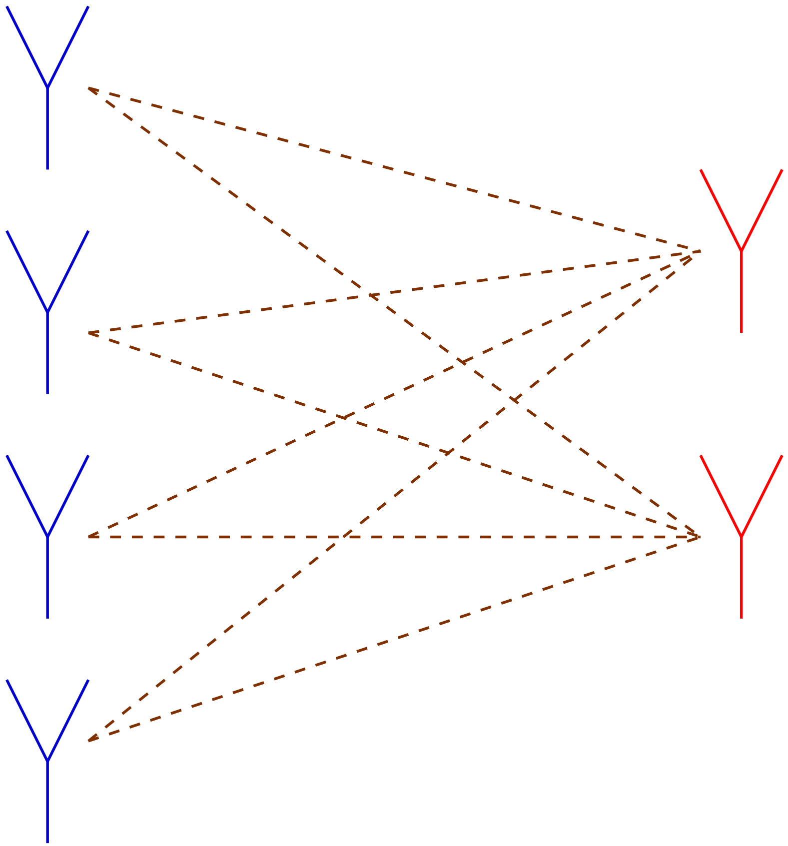


Amin Shokrollahi

digitalfountain

Outline

Want to introduce a new packing problem related to the design of multiple antenna wireless networks.



Transmission: Rayleigh Flat Fading

M transmit antennas, N receiving antennas, coherence interval T.

$$\begin{pmatrix} s_{T,1} & s_{T-1,1} & \cdots & s_{1,1} \\ s_{T,2} & s_{T-1,2} & \cdots & s_{1,2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{T,M} & s_{T-1,M} & \cdots & s_{1,M} \end{pmatrix} =: S.$$

Received signal:

$$X := \underbrace{\sqrt{\rho}}_{\text{SNR}} \cdot \underbrace{H}_{\text{Fading}} \cdot \underbrace{S}_{\text{Signal}} + \underbrace{W}_{\text{Noise}},$$

where H is $N \times T$ and W is $N \times W$ and entries are independent $CN(0,1)$ random variables.

Decoding: Compute S from X.

Codebook Modulation

$\mathcal{S} = \{S_1, S_2, \ldots, S_L\}$.

String $(e_0, \ldots, e_{\ell-1})$ corresponds to

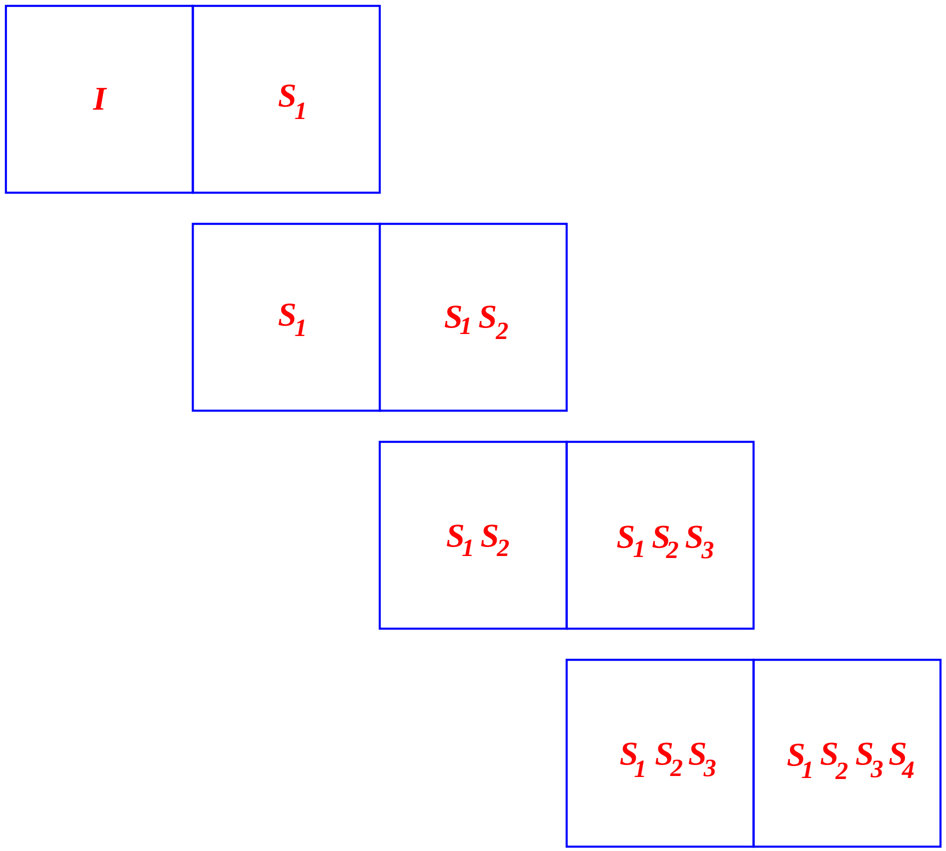
$$S_i, \qquad i = e_0 + 2e_1 + \cdots + 2^{\ell-1} e_{\ell-1}.$$

Simple encoding possible if presentation of $\mathcal{S}$ is appropriate.

Mobile Communication: H is unknown

Use differential encoding.

$T = 2M$.



Differential Encoding

Codebook consists of L unitary $M \times M$-matrices $\{S_1, S_2, \dots, S_L\}$ and is called a unitary space-time code.

Signals transmitted:

$$S_{i_1}, S_{i_1}S_{i_2}, S_{i_1}S_{i_2}S_{i_3}, \dots .$$

H is eliminated:

$$X = HS + W, \qquad Y = HSR + W, \qquad XS + \tilde{W} = Y.$$

Unknown Channel: Decoding and Probability of Error

Maximum likelihood decoding: given $X, Y \in \mathbb{C}^{N \times M}$, find $S \in \mathcal{S}$ that minimizes

$$||XS - Y||$$

for some matrix norm $|| \cdot ||$.

Probability $P(S, R)$ of mistaking S for R (Hochwald-Sweldens)

$$P(S, R) \leq \frac{1}{2} \left(\frac{8}{\rho} \right)^{MN} |\det(S - R)|^{-2N},$$

(for high SNR ρ).

Unknown Channel: Probability of Error

Probability of mistaking S and R is lower the larger the diversity distance

$$d(S,R) := \frac{1}{2}|\det(S-R)|^{1/M}$$

is.

Diversity product of S:

$$\zeta(\mathcal{S}) := \min_{S,R\in\mathcal{S},S\neq R} \frac{1}{2}|\det(S-R)|^{1/M}.$$

Design problem:

Find a large set $\mathcal{S}$ of unitary $M\times M$-matrices for which $\zeta(\mathcal{S})$ is as large as possible.

Diversity "Distance" and Packing Problems

Diversity distance is **NOT** a metric!

$$d\left(\begin{matrix}-1 & 0\\ 0 & -1\end{matrix}, \begin{matrix}1 & 0\\ 0 & -1\end{matrix}\right) + d\left(\begin{matrix}1 & 0\\ 0 & -1\end{matrix}, \begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right) = 0$$

$$\not\geq d\left(\begin{matrix}-1 & 0\\ 0 & -1\end{matrix}, \begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right) = 1.$$

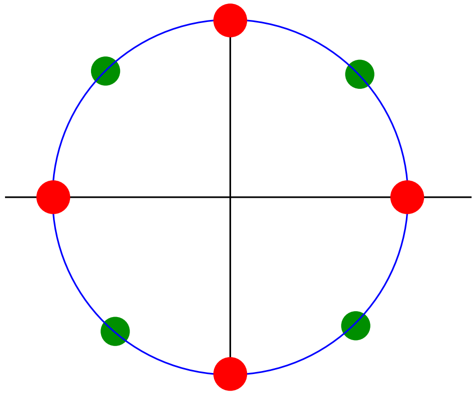
So, design problem is HARD.

Main function:

$$A(M, L) := \sup\{\epsilon \mid \exists \mathcal{S} \subset U(M), \#\mathcal{S} = L, \zeta(\mathcal{S}) \geq \epsilon\}.$$

Special Cases

- $A(M,2) = 1$: $\{I_M, -I_M\}$.
- $A(M,3) = \sqrt{3}/2$? ((S)-Sturmfels-Woodward for $SU(M)$).
- $A(1,L) = 2\sin(\pi/L)$.



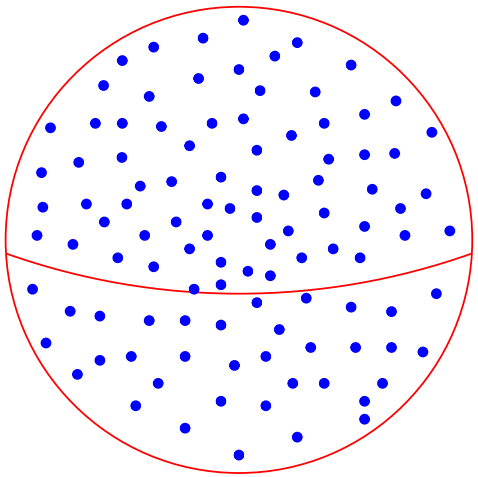
- $A(2,L) = ?$

$$A(2, L)$$

$$SU(2) = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \middle| \operatorname{Re}(a)^2 + \operatorname{Im}(a)^2 + \operatorname{Re}(b)^2 + \operatorname{Im}(b)^2 = 1 \right\} \simeq \mathbb{H}^\times,$$

so nonzero differences in $SU(2)$ are invertible!

$(SU(2), d(\cdot, \cdot))$ is isometric to $\mathbb{S}^3$ with euclidean distance, so good spherical codes in $\mathbb{R}^4$ yield good differential codes for two transmit antennas



Open question: Can we improve performance by going to $U(2)$?

$A(2, L)$: **Historical Note**

- Use of matrices $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ with a, b roots of unity proposed by

  Alamouti in 1998 for known channel.

- Use of same matrices proposed by Tarokh-Jafarkhani in 1999 for unknown channel (mobile).

- Connection to packings in $\mathbf{S}^3$ (re-)discovered by Oswald-Sweldens-S in 1999, works both for known and the unknown channel.

Group Codes

Want to construct finite sets $\mathcal{S}$ of unitary $M \times M$-matrices that form a group under matrix multiplication, and for which

$$\zeta(\mathcal{S}) = \frac{1}{2} \min_{S,R \in \mathcal{S}, S \neq R} |\det(S - R)|^{1/M} \neq 0.$$

Why a group?

- Multiplication of matrices can be done symbolically.
- We have
$$\zeta(\mathcal{S}) = \frac{1}{2} \min_{\mathcal{S} \ni S \neq I} |\det(I - S)|^{1/M}.$$
- Mathematically interesting.

Group Representations

A homomorphism

$$\Delta: \quad G \to \mathrm{U}(M)$$

is called an M-dimensional representation of the group G.

For instance,

$$\langle \sigma \mid \sigma^L = 1 \rangle \quad \to \quad \mathrm{U}(1)$$

$$\sigma \quad \mapsto \quad \mathrm{e}^{2\pi i/L}$$

is a 1-dimensional representation of the cyclic group of order L.

Diagonal Codes

Homomorphism

$$\Delta\colon \quad \langle \sigma \mid \sigma^L = 1 \rangle \quad \to \quad \mathrm{U}(M)$$

$$\sigma \quad \mapsto \quad \begin{pmatrix} \eta^{u_1} & 0 & \cdots & 0 \\ 0 & \eta^{u_2} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \eta^{u_M} \end{pmatrix},$$

where $\eta = \mathrm{e}^{2\pi i/L}$ is a reducible representation of the cyclic group with L elements.

Other abelian constellations? NO!

Group Constellations

Want groups that have a representation Δ such that $\Delta(g)$ does not have eigenvalue 1 for any $g \in G$ except for the identity.

fixed-point-free groups, fixed-point-free representations.

Example: Quaternion group of order 8:

$$Q := \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = \sigma^2, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle.$$

The elements of this group are

$$1, \sigma, \sigma^2, \sigma^3$$

$$\tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3$$

The Quaternion Group

Fixed-point-free representation: $\Delta\colon Q \to U(2)$

$$\Delta(\sigma) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \Delta(\tau) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Same for generalized Quaternion groups

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

The General Case

All fixed-point-free groups have been classified by Zassenhaus in 1936 (with some minor shortcomings)!

After correcting the shortcomings we constructed all fixed-point-free representations of these groups.

This gives us a list of all group constellations (up to equivalence and reducibility).

Glimpse of ideas

Observation.

- Subgroups of fixed-point-free groups are fixed-point-free.
- Cyclic groups are fixed-point-free.
- Abelian fixed-point-free groups are cyclic.

Proof. G fixed-point-free and cyclic via character χ. Then χ has trivial kernel. So, G is cyclic.

p-Groups for odd p

Theorem (Burnside–1905). G p-group and fixed-point-free, p odd. Then is G cyclic.

Proof. $\#G = p^n$. Induction for n. Trivial for $n = 0$.

– G has normal subgroup of index p which is cyclic (by induction hypothesis), generated by σ, say.

– $G = \langle \sigma, \tau \mid \sigma^{p^{n-1}} = 1, \tau^p = \sigma^k, \tau^{-1}\sigma\tau = \sigma^\ell \rangle$, $k \equiv 0 \bmod p$ (assuming G not cyclic), $\ell^p \equiv 1 \bmod p^{n-1}$, and $\ell \not\equiv 1 \bmod p^{n-1}$ (since G not abelian).

p-Groups continued

- G has an irreducible representation Δ of degree p which satisfies

$$\Delta(\sigma) = \begin{pmatrix} \eta & 0 & 0 & \cdots & 0 \\ 0 & \eta^{\ell} & 0 & \cdots & 0 \\ 0 & 0 & \eta^{\ell^2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \eta^{\ell^{p-1}} \end{pmatrix}, \qquad \Delta(\tau) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \eta^{k} & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

- We have $\det(I - \Delta(\sigma^s \tau^u)) = 1 - \eta^{s\frac{\ell^p - 1}{\ell - 1} + ku}$, $\eta = \mathrm{e}^{2\pi i/p^{n-1}}$.
- For any $u \not\equiv 0 \bmod p$ there exists $s \not\equiv 0 \bmod p^{n-1}$ such that $s\frac{\ell^p - 1}{\ell - 1} + ku \equiv 0 \bmod p^{n-1}$.
- G is not fixed-point-free.

Groups of Odd Order

All fixed-point-free groups of odd order are of the type

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

where n is the order of r mod m, $t = m/\gcd(m, r-1)$, and all prime divisors of n divide $\gcd(r-1, m)$.

- Are connected to the classification of near-fields.
- $G_{m,1}$ is the cyclic group of order m.
- $G_{21,4}$ gives constellation with 63 signals and $\zeta = 0.3851$.

$$\Delta(\sigma) = \begin{pmatrix} \eta & 0 & 0 \\ 0 & \eta^4 & 0 \\ 0 & 0 & \eta^{16} \end{pmatrix}, \quad \Delta(\tau) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \eta^7 & 0 & 0 \end{pmatrix}, \qquad \eta = e^{2\pi i/21}.$$

2-Groups

Theorem (Burnside–1905). G 2-group and fixed-point-free.
Then is G either cyclic or a generalized Quaternion group.

Proof. Similar to p-groups for odd p.

Group Codes for Two Transmit Antennas

– Cyclic groups,

– $G_{m,r}$ for appropriate (m, r),

– Quaternion groups,

– The group E_m of order $24m$ generated by

$$\frac{a}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

for appropriate a.

– The group of order 120 generated by the two matrices

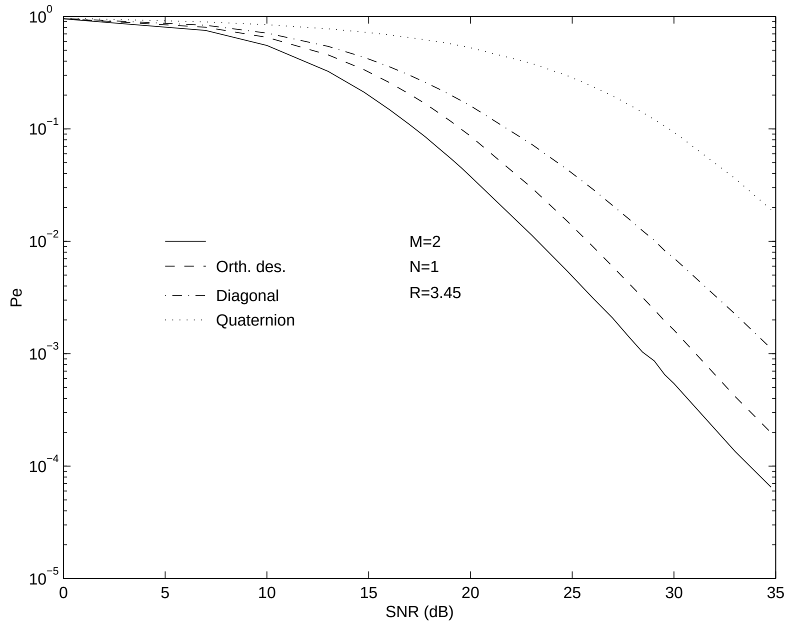
$$\frac{1}{\sqrt{5}}\begin{pmatrix} \mu^2 - \mu^3 & \mu - \mu^4 \\ \mu - \mu^4 & \mu^3 - \mu^2 \end{pmatrix}, \quad \frac{1}{\sqrt{5}}\begin{pmatrix} \mu - \mu^2 & \mu^2 - 1 \\ 1 - \mu^3 & \mu^4 - \mu^3 \end{pmatrix},$$

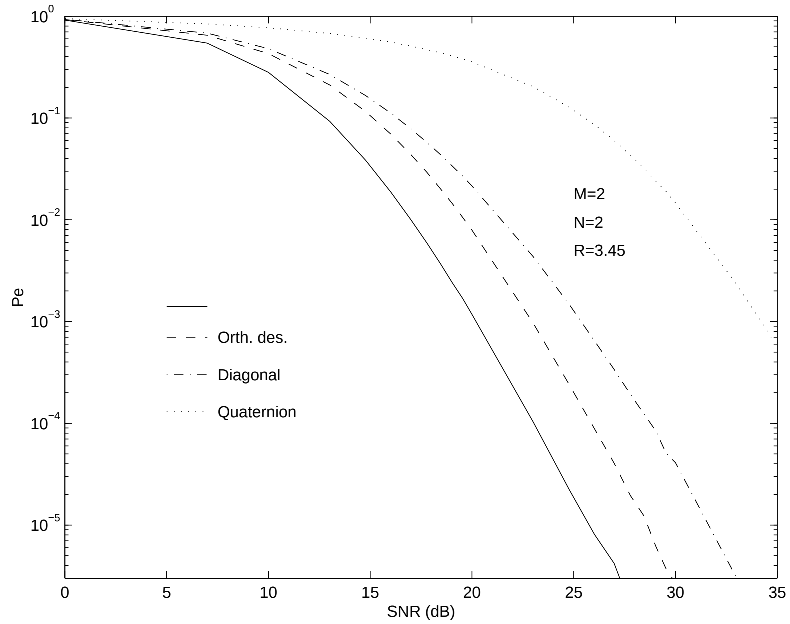
where $\mu = e^{2\pi i/5}$, which is ismorphic to $SL_2(\mathbb{F}_5)$.

– A direct product of any of these groups if the orders are co-prime.

The Group $SL_2(\mathbb{F}_5)$

We have $\zeta(\mathrm{SL}_2(\mathbb{F}_5)) = 0.309$. Excellent performance in simulations.



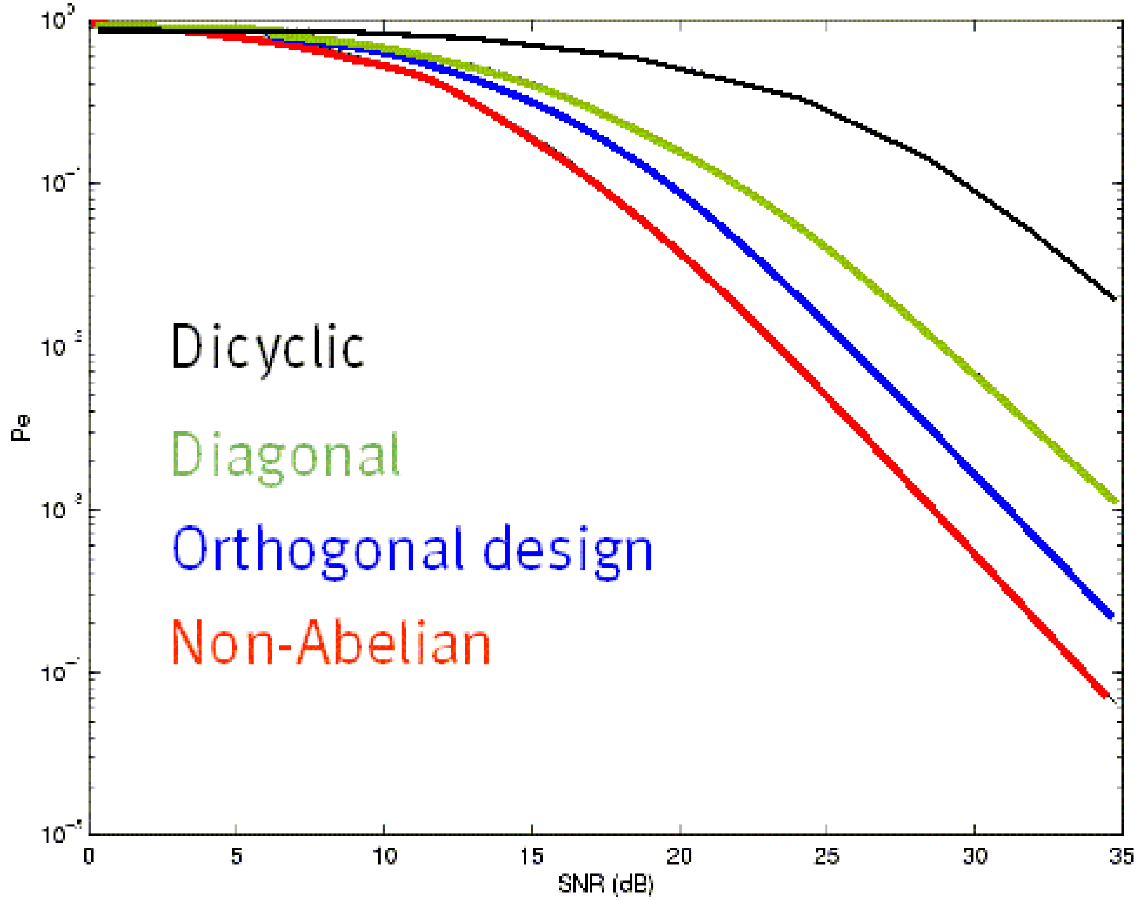


All Groups

Hassibi-Hochwald-S-Sweldens:

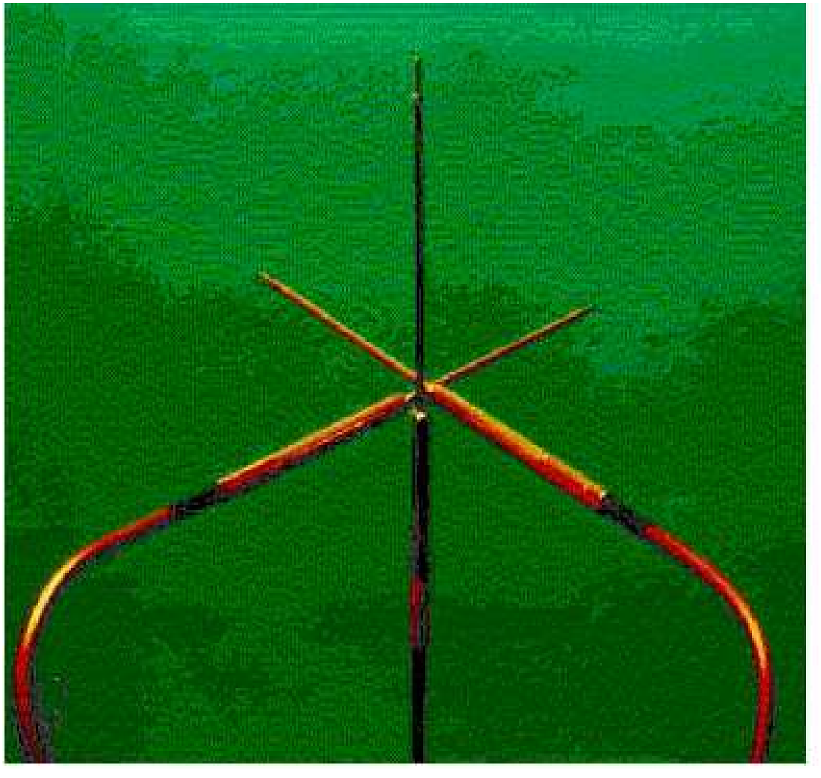
Group type	order	dim of rep
$G_{m,r}$	mn	n
$D_{m,r,\ell}$	$2mn$	$2n$
E_m	$24m$	2
$F_{m,r}$	$2mn$	$2n$
$H_{m,\ell}$	$48m$	4
$\mathrm{SL}_2(\mathbb{F}_5)$	120	2
$K_{m,r,\ell}$	$240mn$	$4n$
$U \times H$	$\|U\|\|H\|$	$\dim(U)\dim(H)$

Performance



Practical!

The group $G_{21,4}$ with 63 elements is being used on a prototypical 3-antenna constellation in the Bell Labs hallways. (Mike Andrews, Wim Sweldens)



Further Work

- Group-inspired constructions (Hassibi-Hochwald-S-Sweldens)
- Fast decoding using closest vector approximation in lattices (Clarkson-Sweldens-Zheng, HHSS)
- Representations of certain compact Lie groups (S)
- Representations of non fixed-point free groups (S, Feit-S)
- Reducible representations (S)

Representations of Compact Lie Groups

Observation of Hassibi-Khorrami: the only fixed-point-free Lie groups are $U(1)$ and $SU(2)$.

Only hope: restrict representations of Lie groups to appropriate subsets.

Need copmact Lie groups to guarantee that irreducible representations are unitary and finite dimensional.

Representations of $SU(2)$

Use 4-dimensional representation R of $SU(2)$ given by action on homogenous bivariate polynomials of degree 3:

$$R\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = \begin{pmatrix} a^3 & \sqrt{3}a^2b & \sqrt{3}ab^2 & b^3 \\ -\sqrt{3}a^2\overline{b} & a(|a|^2-2|b|^2) & b(2|a|^2-|b|^2) & \sqrt{3}\overline{a}b^2 \\ \sqrt{3}a\overline{b}^2 & \overline{b}(|b|^2-2|a|^2) & \overline{a}(2|b|^2-|a|^2) & \sqrt{3}b\overline{a}^2 \\ -\overline{b}^3 & \sqrt{3}\;\overline{b}^2a & -\sqrt{3}\;\overline{b}\overline{a}^2 & \overline{a}^3 \end{pmatrix}.$$

Eigenvalues: $\eta, \overline{\eta}, \eta^3, \overline{\eta}^3$, if eigenvalues of original matrix are $\eta, \overline{\eta}$.

4-dimensional Representation of $SU(2)$

Want subset $\mathcal{S}$ of $SU(2)$ such that for any $A, B \in \mathcal{S}$ the matrices $AB*$ and $(AB^*)^3$ are "away" from the identity matrix.

Restricted spherical codes: no two points too close and no two points have angle close to $2\pi/3$.

Can be constructed from normal spherical codes.

Representations of other groups could lead to interesting results.

Open Question

Upper and (better) lower bounds for $A(M, L)$.