Fast Decodability of Space-Time Block Codes, Skew-Hermitian Matrices, and Azumaya Algebras

B.A. Sethuraman
(joint with Gregory Berhuy and Nadya Markin)

Department of Mathematics
California State University Northridge

June 5, 2014

Table of contents

Context

- Transmission and reception simultaneously on several antennas.
- Higher data capacity and lower error probability for not much increase in power usage.
- First studied in mid-90's, but already 2-transmit antenna systems are common.

Bare-Bones Definition

A space-time code is a set of $\mathbb{R}$-linearly independent invertible matrices A_1, $\ldots$, A_{2l} in $M_n(\mathbb{C})$, for some $l \leq n^2$.

The integer l is called the rate of the code.

Usage

- Let $S = \{-2K-1, -2K+1, \ldots, -1, 1, \ldots, 2K-1, 2K+1\}$ for some $K \geq 0$.
- The data to be transmitted is first coded as $2l$-tuples from S.
- As $\mathbf{s} = (s_1, \ldots, s_{2l})$ varies in S^{2l}, form the matrix

$$X(\mathbf{s}) = \sum_{i=1}^{2l} s_i A_i$$

- Each column of $X(\mathbf{s})$ is transmitted simultaneously from n transmit antennas, and after n columns are transmitted, receive antennas process received data and try to recover $\mathbf{s}$.
- Data received at the n receive antennas during the n transmissions is modeled by

$$Y = HX + N,$$

where Y, H and N are $n \times n$ matrices. Y contains the received data, H contains multiplicative noise and N contains additive noise.

Definition of Mutual Orthogonality

Two matrices A and B in $M_n(\mathbb{C})$ are said to be mutually orthogonal if $AB^* + BA^* = 0$.

The following are easy to see:

- If A and B are mutually orthogonal, so are MA and MB for any $M \in M_n(\mathbb{C})$.
- If $A_1, \ldots, A_k$ are mutually orthogonal, then $A_1^{-1}A_2, \ldots, A_1^{-1}A_k$ are skew-Hermitian and pairwise skew commute ($XY + YX = 0$).

Fast Decodability

The space-time code $\{A_1, \ldots, A_{2l}\}$ in $M_n(\mathbb{C})$ is said to be fast decodable if

- For $g \geq 2$,
- there exist a partition of $\{1, \ldots, 2l\}$:
- $\Gamma_1, \ldots, \Gamma_g, \Gamma_{g+1}$, with Γ_{g+1} possibly empty,
- of cardinalities $n_1, \ldots, n_g, n_{g+1}$ respectively,
- such that for all $u \in \Gamma_i$ and $v \in \Gamma_j$ $(1 \leq i < j \leq g)$, the generating matrices A_u, A_v are mutually orthogonal.

Motivation for Fast Decodability Definition

The definition is chosen because, a key matrix in the decoding process that depends on the A_i and the multiplicative noise matrix H has the following block form for all choices of noise matrix H:

$$\begin{pmatrix} B_1 & & & & N_1 \\ & B_2 & & & N_2 \\ & & \ddots & & \vdots \\ & & & B_g & N_g \\ & & & & N_{g+1} \\ & & & & \end{pmatrix} \tag{1}$$

for some matrices $B_1, \ldots, B_g$, and $N_1, \ldots, N_{g+1}$. Here, all empty spaces are filled by zeros, the B_i are of size $n_i \times n_i$ and N_{g+1} is of size $n_{g+1} \times n_{g+1}$.

Consequences of Fast Decodability

When key matrix has form in Equation 1, can fix guesses for data symbols in the $(g+1)$-th block, and independently decode the first g blocks in (parallel).

Decoding complexity reduces from $|S|^{2l}$ to $|S|^{n_{g+1}+\max n_i}$ $(i = 1, \ldots, g)$.

When Γ_{g+1} is empty, i.e, matrices $N_1, \ldots, N_{g+1}$ are not present in Equation 1 and matrix is block diagonal, code is said to be g-group decodable. Decoding in this case proceeds in parallel in each of the g group without having to condition another set of data symbols.

Some Questions

- For full rate codes ($l = n^2$), what is the lowest decoding complexity possible?
- For full rate codes, what is the highest number g such that code is g group decodable?
- Possibly sacrificing full rate property, what is the maximum number of groups g possible?

Full Rate Codes

Recall that a full rate code is one where $l = n^2$. Using very elementary arguments, we show the following:

Theorem

The decoding complexity for a full rate code cannot be made better than $|S|^{n^2+1}$.

Theorem

A full rate code does not admit g-group decodability for any g.

Typical argument: There can be at most $n^2 - 1$ $\mathbb{R}$-linearly independent matrices in $M_n(\mathbb{C})$ that are both skew-Hermitian and pairwise mutually orthogonal.

Maximum Number of Groups

For arbitrary rate $l \leq n^2$, we study how many groups possible in a space-time code, i.e, how many disjoint subsets $\Gamma_1, \ldots, \Gamma_g$ of $\{A_1, \ldots, A_{2l}\}$ such that $A_u A_v^* + A_v A_u^* = 0$ for all A_u and A_v in distinct Γ_i.

Pick one matrix A_i from each Γ_i, and then consider the matrices $A_1^{-1} A_i$, for $i = 2, \ldots, g$. These matrices are skew-Hermitian and skew-commute. So, we have $g - 1$ skew commuting $n \times n$ complex matrices, and we ask for maximum $g - 1$.

Maximum Number of Skew-Commuting Elements in Central Simple Algebras

For performance reasons, space-time codes are typically chosen from some division algebra D of index n with center $\mathbb{Q}[\imath]$, embedded into $M_n(\mathbb{C})$. This therefore leads us to the following more general question:

Question: Given a central simple algebra $\mathcal{A}$ with center a number field k, how many elements $u_1, \ldots, u_r$ can we find in $\mathcal{A}^*$ that pairwise skew-commute?

Algebra Generated by u_i

Given $u_1, \ldots, u_r$ in $\mathcal{A}^*$ that pairwise skew-commute, consider the subring

$$R = k[u_1^2, u_1^{-2}, \ldots, u_r^2, u_r^{-2}].$$

The relation $u_i u_j + u_j u_i = 0$ shows that u_i and u_j^2 commute, and hence R is a commutative ring.

Quaternion Algebra over R: If R is *any* commutative ring of characteristic not 2, and if a and b are in R^*, we can define the quaternion algebra $(a, b)_R$ as follows: $\mathbf{i}^2 = a$, $\mathbf{j}^2 = b$, $\mathbf{ij} = -\mathbf{ji}$. This is an Azumaya algebra over R.

Azumaya Algebras

Given a commutative ring R, an Azumaya algebra over R is an R-algebra $\mathcal{A}$ that is a finitely generate R-module and is such that $\mathcal{A}/m\mathcal{A}$ is a central simple algebra over R/m for all maximal ideals m of R.

- Azumaya algebras “globalize” central simple algebras over fields.
- Tensor products of Azumaya algebras over R are also Azumaya algebras.
- R-algebra maps $f : \mathcal{A} \mapsto B$, where B is any R algebra, are necessarily injective.

Azumaya Algebras

Theorem

Let $u_1, \dots, u_r$ be skew commuting elements of $\mathcal{A}^*$, where $\mathcal{A}$ is a central simple algebra over a number field k. Let $R = k[u_1^2, u_1^{-2}, \dots, u_r^2, u_r^{-2}]$ as above. Write $r = 2s$ or $r = 2s + 1$ as appropriate. Then, the k-subalgebra of $\mathcal{A}$ generated by the u_i is an Azumaya algebra over R isomorphic to

$$(a_1, b_1)_R \otimes_R \cdots \otimes_R (a_s, b_s)_R$$

for suitable a_i, b_i, $i = 1, \dots, s$.

Hauptsatz

Theorem

Let $u_1, \ldots, u_r$ be skew commuting elements of $\mathcal{A}^*$, where $\mathcal{A}$ is a central simple algebra over a number field k. For any integer t, we write $\nu_2(t)$ for the 2-adic value of t, i.e., the highest power of 2 that divides t. Then we have

$$r \leq 2\nu_2\left(\frac{\deg(\mathcal{A})}{\mathrm{ind}(\mathcal{A})}\right) + 2 \text{ if } r \text{ is even}$$

and

$$r \leq 2\nu_2\left(\frac{\deg(\mathcal{A})}{\mathrm{ind}(\mathcal{A})}\right) + 3 \text{ if } r \text{ is odd.}$$

Corollaries

Corollary

When our space-time codes come from a division algebra, then $g \leq 4$. The best decoding complexity of any space-time code from a division algebra cannot be better than $|S|^{\lceil l/2 \rceil}$.

Corollary

When the r skew-commuting invertible matrices are not restricted to be in any sub algebra of $M_n(\mathbb{C})$, then $r \leq 2\nu_2(n) + 3$.

Hurwitz-Radon-Eckmann Bound

The Hurwitz-Radon-Eckmann result concerns the maximum number of (invertible) matrices A_i in $M_n(\mathbb{C})$ that satisfy the following:

1. $A_iA_j + A_jA_i = 0$ for all $i \neq j$,
2. $A_i^2 = -I_n$, and
3. $A_iA_i^* = I_n$

The HRE bound is that the maximum number is $2\nu_2(n) + 1$.

For comparison, our bound is $2\nu_2(n) + 3$. Note however that we do not require conditions 2 and 3 in our space-time code considerations. Also, we consider the more general case where our matrices arise from a k-central simple algebra embedded in $M_n(\mathbb{C})$.