

Space-Time Block Codes from Cyclic Division Algebras: An Introduction

Anders O.F. Hendrickson

December 15, 2004

Coding theory addresses the problem of transmitting information accurately across noisy channels. When a sender transmits a signal s , it will suffer some changes before it reaches the receiver. The receiver then faces the problem of recovering the intended signal, given that he actually received some altered signal r . The challenge of coding theory, then, is to design a system which not only gives the receiver a high probability of determining s given r , but is also fast and inexpensive.

Most solutions to this problem involve choosing, among all the signals that could be transmitted, some subset of “legal” codewords which are not too similar to one another. Then if r is in fact a codeword, the receiver may assume that $r = s$; otherwise, presumably s was a codeword similar to r . Natural languages incorporate such “redundancy” already; if written words are misspelled, the reader can very often reconstruct the original text of the author verbatim. Devising some analogue of this natural process for arbitrary data is the task of coding theory. Historically, the codewords used were vectors, but in recent years codes using matrices have been developed. In early 1998 Tarokh, Seshadri, and Calderbank proposed a system called “space-time coding” [7], and later that year the classical example, the Alamouti scheme, was published [1]. Efforts to generalize Alamouti have recently turned to division algebras to obtain good collections of matrices for codebooks.

This paper will first briefly introduce the basic concepts needed to understand space-time block codes, outlining the criteria a good code must satisfy; it then will summarize the constructions used in two recent papers to produce workable space-time block codes from cyclic division algebras.

1 An Introduction to Space-Time Coding

In certain applications, it is feasible to use multiple channels simultaneously to increase accuracy and/or speed of transmission. For example, multiple antenna could transmit signals to a single cellular phone. The route of the signal from any given transmit antenna to any given receiving antenna will be different from the route taken by any other pair of transmit and receive antennas. That a well-planned scheme using multiple antennas could increase accuracy makes sense on an intuitive level: should one channel become too noisy or even fail altogether, the other channels ought to be able to compensate. Similarly, it makes sense

that with more antennas sending and/or receiving, more information could be transmitted per unit of time.

The key question, of course, is how to translate the data to be sent into the signals for each antenna to transmit, not only in such a way that the receiver will be able to recover the original data, but also so as to maximize both accuracy and speed of transmission. Let us first look at how the information sent reaches the receiver.

1.1 Modelling the Channel

A single transmit antenna during a single time segment sends a signal which can be thought of as a complex number $s \in \mathbb{C}$. As the signal travels to a receiving antenna, it will suffer some distortion, which can be modelled as multiplication by a complex number h which is called the *fade coefficient*. Moreover, the receiving antenna will pick up some noise, which is modelled by adding a complex number η . So the received signal is $r = hs + \eta$.

Now suppose there are N_t transmit antennas transmitting simultaneously to a single receiving antenna. Let $s_j \in \mathbb{C}$ denote the signal sent by the j th antenna ($1 \leq j \leq N_t$). Because they transmit simultaneously, each of these antennas contributes to the signal detected by the receiver. The received signal $r \in \mathbb{C}$ will therefore be some linear combination of those complex numbers, plus some noise:

$$r = h_1 s_1 + h_2 s_2 + \cdots + h_{N_t} s_{N_t} + \eta.$$

Here $h_j \in \mathbb{C}$ is of course the fade coefficient between transmit antenna j and the receiver.

If we now allow for N_r receive antennas, we will have fade coefficients h_{ij} ($1 \leq i \leq N_r$, $1 \leq j \leq N_t$), each corresponding to the path between transmit antenna j and receive antenna i ; we will also have noise at each receiver, which we will call $\eta_1, \dots, \eta_{N_r} \in \mathbb{C}$. For each receive antenna $i \in \{1, \dots, N_r\}$, we then have the equation

$$r_i = h_{i1} s_1 + h_{i2} s_2 + \cdots + h_{iN_t} s_{N_t} + \eta_i.$$

We can consider the channel as a whole by expressing these N_r equations as a single matrix equation:

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{N_r} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1N_t} \\ h_{21} & h_{22} & \cdots & h_{2N_t} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_r 1} & h_{N_r 2} & \cdots & h_{N_r N_t} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{N_t} \end{pmatrix} + \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_{N_r} \end{pmatrix}.$$

which we can write in abbreviated form as

$$\vec{r} = H\vec{s} + \vec{\eta}.$$

Thus far we have potentially increased our accuracy and/or rate of transmission by adding more antennas, providing more paths through space for information to pass from the sender to the receiver; we might call this “spatial diversity.” The other essential part of space-time codes could be called “temporal diversity”: as in an ordinary block code, we let each transmit

antenna (synchronized with the others) send a string of T complex numbers. We shall treat time as discrete, and we transmit one complex number during each interval. Thus for each time t in the block $\{1, \dots, T\}$, the j th transmit antenna j ($1 \leq j \leq N_t$) sends a symbol $s_{jt} \in \mathbb{C}$; similarly, at every time t , the i th receive antenna ($1 \leq i \leq N_r$) will receive a symbol r_{it} .

We shall assume the channel is *quasi-static*; that is, the coefficients h_j remain essentially constant over the duration T it takes to transmit a single code matrix.

Letting \vec{r}_t denote the vector $(r_{1t}, r_{2t}, \dots, r_{N_r t})^T$ of symbols received at time t , and likewise letting $\vec{s}_t = (s_{1t}, s_{2t}, \dots, s_{N_t t})^T$ be the vector of symbols transmitted at time t , we can write

$$\vec{r}_t = H\vec{s}_t + \vec{\eta}_t,$$

where $\vec{\eta}_t$ is the noise vector at time t . We may then assemble these L equations into a single matrix equation:

$$(\vec{r}_1 \ \vec{r}_2 \ \dots \ \vec{r}_T) = H(\vec{s}_1 \ \vec{s}_2 \ \dots \ \vec{s}_T) + (\vec{\eta}_1 \ \vec{\eta}_2 \ \dots \ \vec{\eta}_T);$$

this equation may be abbreviated

$$R = H \cdot S + W. \tag{1}$$

Recall that R is an $N_r \times T$ matrix in which r_{it} represents the symbol received at antenna i at time t ; the channel matrix H has dimensions $N_r \times N_t$ as before; S is an $N_t \times T$ matrix in which s_{jt} is the symbol sent by antenna j at time t ; and the noise matrix W has dimensions $N_r \times T$. (In practice, we often choose $T = N_t$, so that our code matrices will be square.)

Our codewords will thus be the matrices S we send, and will have dimensions $N_t \times T$. To decode, then, the receiver needs to decide which matrix in the codebook \mathcal{C} of “legal” $N_t \times T$ matrices is most likely to have produced the matrix R he actually received. That is, he will decode to that matrix which minimizes W :

$$S \approx \arg \min_{\tilde{S} \in \mathcal{C}} (R - H\tilde{S}).$$

There are a number of algorithms for doing so, include the spherical decoding algorithm of [2]. As any received matrix R has $N_r T$ complex entries, it can be rewritten as a real vector with $2N_r T$ entries by splitting each complex number into its real and imaginary parts. Then $\{HS : S \in \mathcal{C}\}$, the set of images of code matrices under the fading coefficients (but without any noise) form points of a lattice Λ in $\mathbb{R}^{2N_r T}$. The spherical decoding algorithm thinks of the received matrix R as a vector in $\mathbb{R}^{2N_r T}$, and it searches inside a certain sphere with center R for the point of Λ nearest to R . To implement this algorithm, however, requires knowing the channel matrix H , which in practice is not necessarily known. Fortunately, there is a clever way around this problem.

1.2 Differential Modulation for Unknown Channels

We have been assuming that our channel is quasi-static, meaning that the fade coefficients do not change much over the course of our T time segments. If we make the stronger assumption

that the coefficients do not change significantly over a duration of $2T$, then the channel coefficient matrix is approximately the same from one matrix transmission to the next. Let us write H_k for the fade coefficient matrix during the interval $t \in \{kT, kT+1, \dots, kT+T-1\}$ in which we send the k th matrix; we are thus assuming $H_k \approx H_{k+1}$. Then the following procedure, proposed in [4], allows us to decode without needing to know the channel at all.

Suppose that we have a codebook \mathcal{C} of *square* $n \times n$ matrices and that we wish to send the information $V_1, V_2, \dots \in \mathcal{C}$. During time block k , instead of transmitting the matrix V_k , transmit the composite matrix $S_k = I_n V_1 V_2 \cdots V_k$ (where I_n is the $n \times n$ identity matrix). (At block $k = 0$, transmit I_n .) So $S_k = S_{k-1} V_k$.

Then at any time block k , the receiver receives

$$\begin{aligned} R_k &= H_k S_k + W_k \\ &= H_k S_{k-1} V_k + W_k \\ &\approx H_{k-1} S_{k-1} V_k + W_k \\ &= (R_{k-1} - W_{k-1}) V_k + W_k \\ &= R_{k-1} V_k - W_{k-1} V_k + W_k \\ &= R_{k-1} V_k + W'_k. \end{aligned}$$

We have thus evaded the issue of channel coefficients entirely; although the receiver does not know H_k , he *does* know R_{k-1} , the matrix he just received. In effect, he receives a signal at time k as though it were transmitted through a channel with matrix R_{k-1} and noise W'_k ; the price paid is that W'_k is generally noisier than W_k was. If, for example, our codewords are unitary matrices, then W'_k has twice the variance of W_k [4, p. 2046]. The receiver now can assume that V_k is that matrix in the codebook \mathcal{C} which minimizes W'_k ; that is,

$$V_k \approx \arg \min_{S \in \mathcal{C}} (R_k - R_{k-1} S).$$

He may then use the spherical decoding algorithm [2] or another procedure to estimate V_k .

2 Basic Definitions

Having motivated their construction, let us now more carefully define space-time block codes. We begin with a *signal constellation* $S \subset \mathbb{C}$, a finite subset of the complex numbers. Whatever data we wish to transmit will first be converted into sequences of elements of S .

Three of the more common choices of signal constellations are

- An M -PSK constellation, which consists of all M th roots of unity:

$$S_M = \{\omega_M^j : j = 0, 1, \dots, M-1\},$$

where ω_M denotes the principal M th root of unity $e^{2\pi i/M}$.

- An M -QAM constellation (e.g. 4-QAM, 16-QAM, or 64-QAM), which may be thought of as M points in the lattice $\mathbb{Z}[i]$ arranged in a square about the origin:

$$\{a + bi : a, b \text{ are odd and } |a|, |b| < \sqrt{M}\}$$

- A HEX constellation, which is a certain finite subset of the Eistenstein integers $Z[\omega_6]$.

As our previous discussion suggested, a *space-time block code* for N_t transmit antennas and a block length T (that is, an “ $N_t \times T$ STBC”) is a finite “codebook” of complex $N_t \times T$ matrices; that is, any finite $\mathcal{C} \subset M_{N_t \times T}(\mathbb{C})$. In this paper we shall mostly be concerned with square matrices; that is, where $T = N_t$.

We say an STBC \mathcal{C} is *over* a signal constellation S if all the entries of matrices in \mathcal{C} are complex linear combinations of elements of S ; we say \mathcal{C} is *completely over* S if the entries of matrices in \mathcal{C} actually lie in S .

To create good STBCs, we will look for sets of matrices with some algebraic structure. For example, if one’s codebook \mathcal{C} were a group under matrix multiplication, the computations of the matrix products needed for differential modulation could be reduced to simply looking up products in a table [4, p. 2047].

We shall be more interested in situations where \mathcal{C} comes from a *subring* of $\text{GL}_n(\mathbb{C})$. In this case, we shall first find an infinite code $\mathcal{C}_\infty \subseteq \text{GL}_n(\mathbb{C})$ having some of the properties we desire; we then will choose a particular finite subgroup $\mathcal{C} \subseteq \mathcal{C}_\infty$ to be our codebook.

3 Criteria for a Good STBC

There are several criteria for determining how good a particular space-time code is. One of the most important is the diversity advantage, which measures how many of the available channels between transmitter and receiver are being utilized. For a given code and channel, if we vary the signal-to-noise ratio ρ , then the probability of error takes the form $K\rho^{-D}$ for some coding gain constant K and a number D which is called the *diversity advantage*, or simply the *diversity*. Minimizing the probability of error therefore corresponds to maximizing D .

1. In the paper [7] in which they introduced the notion of space-time codes, Tarokh, Seshadri, and Calderbank articulated two basic performance criteria. Suppose we have n transmit and m receive antennas. Under the assumption that the signals transmitted from different antennas undergo independent fades, they derived a bound for the probability of decoding to the codeword W when V was sent. Suppose the elements of the signal constellation S are contracted by a factor of $\sqrt{E_s}$, so that any column of our matrix has an average normalized energy of 1. Then we have

$$\text{prob}(\text{mistaking } V \text{ for } W) \leq (\lambda_1 \lambda_2 \cdots \lambda_r)^{-m} (E_s/4N_0)^{-rm}, \quad (2)$$

In this formula, $N_0/2$ is the noise variance per dimension, and r is the rank and $\lambda_1, \dots, \lambda_r \in \mathbb{R}$ the nonzero eigenvalues of the Hermitian matrix $A = (V - W)(V - W)^*$, where “ $*$ ” denotes the Hermitian conjugate. Note that ρ is proportional to $\frac{E_s}{N_0}$. So the diversity is the power of ρ^{-1} in (2), namely rm . To achieve maximum diversity, we would therefore want A to have full rank for all choices of V and W . Note too that $\text{rank}(A) = \text{rank}(V - W)$.

We thus have the *rank criterion*: for our space-time codebook \mathcal{C} to achieve best results, we must require that

$$\text{rank}(V - W) = n \text{ for any } V, W \in \mathcal{C}. \quad (3)$$

If the rank criterion holds for \mathcal{C} , we say that \mathcal{C} is *full-diversity*.

2. Assume that the rank criterion is fulfilled; then (2) becomes

$$\text{prob}(\text{mistaking } V \text{ for } W) \leq (\lambda_1 \lambda_2 \cdots \lambda_n)^{-m} (E_s/4N_0)^{-nm}.$$

But the product of all n eigenvalues of A is simply its determinant, so we have

$$\text{prob}(\text{mistaking } V \text{ for } W) \leq (\det(A))^{-m} (E_s/4N_0)^{-nm}.$$

To minimize the probability of error, we should therefore maximize the determinant of $A = (V - W)(V - W)^*$, which is the same as maximizing $\det(V - W)$.

Tarokh *et al.* thus derive the *determinant criterion*: we want the minimum determinant

$$\Delta_{\min}(\mathcal{C}) = \min_{\substack{V, W \in \mathcal{C} \\ V \neq W}} |\det(V - W)| \quad (4)$$

to be as large as possible. This is sometimes normalized to $\zeta(\mathcal{C}) = \frac{1}{2} \min_{V \neq W \in \mathcal{C}} |\det(V - W)|^{1/n}$, which is called the *diversity product*, or to $\delta_{\min}(\mathcal{C}) = \min_{V \neq W \in \mathcal{C}} |\det(V - W)|^2$.

3. There are, of course, other measures of how good a code is. The measure known as *rate* measures how quickly information is transmitted by the code; all else being equal, a higher rate is of course better. Roughly speaking, the rate is how many symbols (from our signal constellation S) are transmitted per unit of time. For example, an uncoded transmission from a single antenna of one symbol per time slot would have rate 1. Likewise a rate of k corresponds to sending k symbols from S , which can be done in $|S|^k$ ways.

So let \mathcal{C} be a space-time block code with block length T . Once codeword chosen from $|\mathcal{C}|$ possibilities carries the same amount of information as $\log_{|S|} |\mathcal{C}|$ symbols chosen from S . Since that codeword is transmitted over T time slots, we may define the rate of an STBC as

$$\frac{1}{T} \log_{|S|} |\mathcal{C}|.$$

4 STBCs from Division Algebras

With these criteria in mind, let us now look at some recently developed ways to construct STBCs using division algebras. Recall that a division algebra is a ring with unity in which every element has an inverse, and can be thought of as a “broken field” in which commutativity does not necessarily hold. In this section and section 5 we will follow the work of Sethuraman, Rajan, and Shashidhar in [6]

Let S be our signal constellation and $F = \mathbb{Q}(S)$. Then we want a space-time code $\mathcal{C} \subseteq M_{n \times n}(F)$ which satisfies the rank criterion (3). One way to achieve this would be to find a division algebra $A \subseteq M_{n \times n}(F)$, for if $V, W \in A$, then $V - W \in A$ so $V - W$ is invertible, and hence has full rank.

Fortunately, the algebraic structure of division algebras comes to our aid. Given our matrix ring $M_{n \times n}(F)$, it will suffice to find a division algebra D and a ring homomorphism $\phi : D \rightarrow M_{n \times n}(F)$. Since division algebras have no proper nontrivial ideals, $\ker \phi = 0$, so we in fact have an embedding

$$\phi : D \hookrightarrow M_{n \times n}(F).$$

Thus if we let $\mathcal{C}_\infty = \phi(D)$, then $\mathcal{C}_\infty \cong D$ is a division algebra within $M_{n \times n}(F)$ and hence satisfies the rank criterion. Then any finite subset $\mathcal{C} \subset \mathcal{C}_\infty$ will be a space-time code which also satisfies the rank criterion. For example, we might take $\mathcal{C}_\infty \cap M_{n \times n}(S)$, those matrices whose entries are taken exclusively from our signal constellation S , so that our code \mathcal{C} will be completely over S . How good the diversity product will be remains to be seen.

But we now have our goal: given $F = \mathbb{Q}(S)$, we want to find division algebras D with ring homomorphisms $D \rightarrow M_{n \times n}(F)$. We now turn to methods of constructing appropriate division algebras.

4.1 The Generic Construction

Suppose we have a division algebra D and a field $E \subseteq Z(D)$. (That is, $E \subseteq D$ and $ed = de$ for every $e \in E, d \in D$.) Then D has a natural structure as an E -vector space; let us write D_E when we wish to emphasize that we are treating D as an E -vector space. Then D acts on D_E by left multiplication: for any $d \in D$, we let $\lambda_d : D_E \rightarrow D_E$ be the map given by $x \mapsto dx$. Note that λ_d is an E -linear transformation, since

$$\begin{aligned} \lambda_d(e_1x_1 + e_2x_2) &= d(e_1x_1 + e_2x_2) \\ &= de_1x_1 + de_2x_2 \\ &= e_1dx_1 + e_2dx_2 && \text{(because } E \text{ is central in } D) \\ &= e_1\lambda_d(x_1) + e_2\lambda_d(x_2) \end{aligned}$$

for any $e_1, e_2 \in E, x_1, x_2 \in D_E$. In other words, $\lambda_d \in \text{End}_E(D)$. Moreover, the map $\Lambda : D \rightarrow \text{End}_E(D)$ taking $d \mapsto \lambda_d$ is a ring homomorphism, since if $c, d \in D$,

$$(\lambda_c \cdot \lambda_d)(x) = \lambda_c(\lambda_d(x)) = \lambda_c(dx) = cdx = \lambda_{cd}(x) \text{ and}$$

$$(\lambda_c + \lambda_d)(x) = \lambda_c(x) + \lambda_d(x) = cx + dx = (c + d)x = \lambda_{c+d}(x)$$

for all $x \in D_E$. But of course $\text{End}_E(D) \cong M_{n \times n}(E)$ in a natural way: by picking an E -basis for D , we can write any E -linear transformation as a matrix. So we do have a ring homomorphism

$$\phi : D \xrightarrow{\Lambda} \text{End}_E(D) \xrightarrow{\cong} M_{n \times n}(E),$$

and consequently we can find a full-diversity $n \times n$ space-time code completely over E , where $n = [D : E]$. We let $\mathcal{C}_\infty = \text{Im } \phi$, and we choose any convenient finite subset $\mathcal{C} \subset \mathcal{C}_\infty$ to be our STBC. For example, given n and S , we might like to find a division algebra $D \supseteq F = \mathbb{Q}(S)$ with F central in D , $[D : F] = n$, so as to obtain an STBC completely over F .

4.2 A Commutative Example

In particular, let $F = \mathbb{Q}(S)$ and $n \in \mathbb{N}$ be given. Take any *field* extension K of F with $[K : F] = n$. Then of course $F \subseteq Z(K) = K$. So by the arguments we have just given, we have a natural space-time code over F . Let us construct some nice examples of such codes. Following Sethuraman *et al.*, we will construct successively more amenable field extensions K ending with a concrete example.

4.2.1 The Generic Extension

Let our signal constellation S be given, and set $F = \mathbb{Q}(S)$. Let $n \in \mathbb{N}$, the number of transmit antennas, also be given. Choose any element $\alpha \in \overline{\mathbb{Q}}$ with $\deg(\alpha) = n$. Then its minimal polynomial has the form

$$\min_F(\alpha) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

for some $a_i \in F$. Let $K = F(\alpha)$; then K is an F -vector space of degree n with a natural basis $\mathcal{B} = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. So we can write any element $k \in K$ as $(b_0, b_1, \dots, b_{n-1})$ for $b_i \in F$ such that $k = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$.

Using this basis, the behavior of λ_α on the basis vectors is straightforward:

$$\begin{aligned} \lambda_\alpha(\alpha^i) &= \alpha\alpha^i = \alpha^{i+1} \text{ for } i = 0, \dots, n-2, \text{ but} \\ \lambda_\alpha(\alpha^{n-1}) &= \alpha\alpha^{n-1} = \alpha^n = -a_0 - a_1\alpha^1 - \cdots - a_{n-1}\alpha^{n-1}. \end{aligned}$$

Thus the matrix corresponding to λ_α using the basis \mathcal{B} is

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}, \quad (5)$$

where the matrix multiplication is taken on the *right*; that is, $\lambda_\alpha(b_0, \dots, b_{n-1}) = (b_0, \dots, b_{n-1})M$.

Since λ_α corresponds to the matrix M , we easily see that λ_{α^i} corresponds to the matrix M^i . Thus for any $k = (b_0, \dots, b_{n-1}) \in K$, λ_k corresponds to the matrix $b_0I_n + b_1M + b_2M^2 + \cdots + b_{n-1}M^{n-1}$.

Then if $\phi : K \hookrightarrow \text{End}_F(K) \xrightarrow{\cong} M_{n \times n}(F)$ is our embedding mapping k to the matrix corresponding to λ_k , then

$$\text{Im } \phi = \{b_0I_n + b_1M + b_2M^2 + \cdots + b_{n-1}M^{n-1} : b_i \in F\} \subset M_{n \times n}(F)$$

is a set of matrices satisfying the rank criterion (3). So any finite subset $\mathcal{C} \subset \text{Im } \phi$ will be a space-time code satisfying the rank criterion.

4.2.2 A Well-Chosen Radical Extension

If we choose our field K well, then our formulas become simpler. Let a signal set S and a number of antennas n be given as before. Let $F = \mathbb{Q}(S)$, and let us suppose we can find $\gamma \in F^\times$ such that $X^n - \gamma$ is irreducible in $F[X]$. That is, suppose we have an $\alpha \in \overline{\mathbb{Q}}$ with $\min_F(\alpha) = X^n - \gamma$. Then all our work from section 4.2.1 applies, but the matrix M in (5) now becomes the much simpler

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \gamma \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix},$$

whose powers are easy to compute. Hence if $k = (b_0, \dots, b_{n-1}) \in K$, then λ_k corresponds to

$$M_{(b_0, \dots, b_{n-1})} = \begin{pmatrix} b_0 & \gamma b_{n-1} & \gamma b_{n-2} & \cdots & \gamma b_3 & \gamma b_2 & \gamma b_1 \\ b_1 & b_0 & \gamma b_{n-1} & \cdots & \gamma b_4 & \gamma b_3 & \gamma b_2 \\ b_2 & b_1 & b_0 & \cdots & \gamma b_5 & \gamma b_4 & \gamma b_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ b_{n-2} & b_{n-3} & b_{n-4} & \cdots & b_1 & b_0 & \gamma b_{n-1} \\ b_{n-1} & b_{n-2} & b_{n-3} & \cdots & b_2 & b_1 & b_0 \end{pmatrix}. \quad (6)$$

So we could let $\mathcal{C}_\infty = \{M_{(b_0, \dots, b_{n-1})} : b_i \in F\}$ and choose any finite subset $\mathcal{C} \subset \mathcal{C}_\infty$ to obtain a space-time code with full diversity.

4.2.3 A Well-Chosen Finite Code

In particular, consider the finite subset $\mathcal{C} = \{M_{(b_0, \dots, b_{n-1})} : b_i \in S\}$. Then every matrix $V \in \mathcal{C}$ has all its entries in $S \cup \gamma S$. If, then, we can select our γ so that $\gamma S \subseteq S$, we will be in the very convenient situation that all the entries of matrices in \mathcal{C} come from S itself; that is, \mathcal{C} will be completely over S .

If we are to have $\gamma S \subseteq S$ for a finite $S \subset \mathbb{C}$, then letting $0 \neq s_0 \in S$, we see that the set $\{\gamma s_0, \gamma^2 s_0, \gamma^3 s_0, \dots\} \subseteq S$ must be finite, so we have $\gamma^a s_0 = \gamma^b s_0$ for some $a, b \in \mathbb{N}$, implying that $\gamma^{a-b} = 1$. So γ must be a root of unity, and thus our signal set S must be rotationally symmetric. For example, the M -PSK signal set $S_M = \{\omega_M^j : 0 \leq j < M\}$ is invariant under multiplication by $\gamma = \omega_M = e^{2\pi i/M}$.

In order to have this good situation, we need to find γ a root of unity such that $X^n - \gamma$ is irreducible in $F[X]$; then α will be a primitive n th root of γ , and hence itself a root of unity. Sethuraman *et al.* find such a γ using the following proposition.

Proposition 1 *Let $M \geq 2$, $\omega_M = e^{2\pi i/M}$, and let n be any integer such that*

$$\text{For any prime } p, \text{ if } p \mid n, \text{ then } p \mid M. \quad (7)$$

Then the polynomial $X^n - \omega_M^\ell$ is irreducible in $\mathbb{Q}(\omega_M)$ for any $\ell \in \mathbb{Z}$ such that $\gcd(\ell, M) = 1$.

Then in particular, if we use n transmit antennas and the M -PSK signal constellation, where n and M satisfy condition (7), then for every $\ell \in \{1, \dots, M\}$ relatively prime to M we obtain a $\gamma = \omega_M^\ell$ with $X^n - \gamma$ irreducible in $F[X]$ (where $F = \mathbb{Q}(S) = \mathbb{Q}(\omega_M)$). Our signal constellation S_M is invariant under multiplication by ω_M , and hence invariant under multiplication by γ . We thus obtain a space-time block code

$$\mathcal{C} = \{M_{(b_0, \dots, b_{n-1})} : b_i \in S_M\},$$

where the matrix $M_{(b_0, \dots, b_{n-1})}$ is defined as in (6) with $\gamma = \omega_M^\ell$. Note that the entries of any matrix $V \in \mathcal{C}$ lie in S_M , so \mathcal{C} is completely over S_M . Moreover, $|\mathcal{C}| = |S_M|^n$, so \mathcal{C} has rate 1.

Let us finally look at a concrete STBC obtained by these methods.

Example 1

Let us work with 3 antennas over the 6-PSK signal set $S_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ (where $\omega = \omega_6 = e^{2\pi i/6}$). So $F = \mathbb{Q}(S) = \mathbb{Q}(\omega)$. Note that $n = 3$, $m = 6$ satisfy condition (7), so by Proposition 1, the polynomial $X^3 - \omega$ is irreducible over $\mathbb{Q}(\omega)$. We thus have a full-diversity space-time block code

$$\mathcal{C} = \left\{ \begin{pmatrix} b_0 & \omega b_2 & \omega b_1 \\ b_1 & b_0 & \omega b_2 \\ b_2 & b_1 & b_0 \end{pmatrix} : b_0, b_1, b_2 \in S_6 \right\}.$$

That is, the difference of any two such matrices has full rank. Note that \mathcal{C} is completely over S , and $|\mathcal{C}| = 6^3 = 216$.

5 STBCs using Noncommutative Division Algebras

The previous section discussed STBCs over a signal set S derived from *commutative* division algebras over $\mathbb{Q}(S)$ —that is, field extensions. However, similar procedures will work in a noncommutative situation to produce even better codes.

Let us review a few key facts about division algebras (see for example [3, pp. 91-96]):

- If D is a division algebra, its multiplicative center $Z(D)$ is obviously a field; call it F . Then we will call D a division algebra *over* F .
- D is naturally an F -vector space. We will only consider division algebras for which $[D : F] < \infty$, in which case it is a well-known theorem that $[D : F]$ is a perfect square. Let $n^2 = [D : F]$; then we say n is the *index* of D .
- By a *subfield* of D we mean a field K such that $F \subseteq K \subseteq D$. (Note that we require $F \subseteq K$!) It is known that all *maximal* subfields of D have $[K : F] = n$, the square root of $[D : F]$.

$$F \overset{n}{\subseteq} K \overset{n}{\subseteq} D$$

For example, Hamilton's quaternions \mathbb{H} are a division algebra over \mathbb{R} , with $[\mathbb{H} : \mathbb{R}] = 2^2$. Within \mathbb{H} are many copies of \mathbb{C} , which is a maximal subfield of \mathbb{H} . We thus have

$$\mathbb{R} \overset{2}{\subseteq} \mathbb{C} \overset{2}{\subseteq} \mathbb{H}.$$

5.1 STBCs of dimension n^2 from Division Algebras

We can thus immediately apply the results of section 4.1. Suppose $F = \mathbb{Q}(S)$ and $D \supseteq F$ is a division algebra whose center is F . As we noted above, D is an F -vector space with $[D : F] = n^2$; and by assumption $F = Z(D)$. Then as we showed in section 4.1, there is an $n^2 \times n^2$ full-diversity STBC coming from the action of D on itself by left-multiplication.

Example 2

Consider the division algebra \mathbb{H} , whose center is \mathbb{R} . As an \mathbb{R} -vector space, \mathbb{H} has a natural basis $\mathcal{B} = \{1, \hat{i}, \hat{j}, \hat{k}\}$, where as usual $\hat{i}^2 = \hat{j}^2 = \hat{k}^2 = -1$ and $\hat{i}\hat{j} = -\hat{j}\hat{i} = \hat{k}$. Then for any $x = a + b\hat{i} + c\hat{j} + d\hat{k} \in \mathbb{H}$, λ_x corresponds to the matrix

$$M_x = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & e & -b & a \end{pmatrix} \quad (8)$$

So if we should take a finite signal constellation $S \subset \mathbb{R}$,¹ we could for example have a 4×4 full-diversity STBC completely over S by letting

$$\mathcal{C} = \{M_{a+b\hat{i}+c\hat{j}+d\hat{k}} : a, b, c, d \in S\},$$

where M_x is defined as in (8).

The most obvious limitation of this approach is that the number of transmit antennas N_t is required to be a square. The more fruitful approach comes by looking at D not as an F -vector space, but as a K -vector space where K is a maximal subfield. We cannot simply invoke the results of section 4.1, since K is not central in D . However, by being careful we can still obtain an $n \times n$ STBC completely over K .

5.2 STBCs of dimension n from Division Algebras

The trick is to think of D as a *right* K -vector space; let us write D_K to emphasize this structure. Then D does acts nicely on D_K by *left* multiplication: to every $d \in D$ corresponds $\lambda_d : D_K \rightarrow D_K$ given by $e \mapsto de$. Although K is not central in D , we still have

$$\begin{aligned} \lambda_d(e_1k_1 + e_2k_2) &= \lambda_d(e_1k_1) + \lambda_d(e_2k_2) \\ &= de_1k_1 + de_2k_2 \\ &= \lambda_d(e_1)k_1 + \lambda_d(e_2)k_2, \end{aligned}$$

for every $e_1, e_2 \in D_K$ and $k_1, k_2 \in K$. So λ_d is in fact a K -linear transformation of D_K . Now by the same arguments we saw in section 4.1, we do have an embedding $D \hookrightarrow M_{n \times n}(K)$ taking $d \in D$ to the matrix corresponding to λ_d . Hence we have, in principle, $n \times n$ STBCs completely over K .

To produce concrete STBCs, we will concentrate on a nicely calculable case, when D is a *cyclic* division algebra.

¹Of course, we would never choose $S \subset \mathbb{R}$ in practice!

5.3 Cyclic Division Algebras

Definition 2 A *cyclic division algebra* D over the field F is a division algebra with center F and a maximal subfield K such that K is Galois over F and $\text{Gal}(K/F)$ is cyclic.

Let D be a cyclic division algebra over F of index n , with a maximal subfield K . Let σ be a generator of $\text{Gal}(K/F)$, so that the order of σ is n .

Then it is known that there is a $z \in D$ such that

$$\begin{aligned} z^n &= \delta \text{ for some } \delta \in F^\times, \\ kz &= z\sigma(k) \text{ for all } k \in K, \end{aligned}$$

and most importantly, we can decompose

$$D = K \oplus zK \oplus z^2K \oplus \dots \oplus z^{n-1}K.$$

D is therefore a *right* K -vector space in a very usable way.

Conversely, given any cyclic extension K/F with $[K:F] = n$ and $\text{Gal}(K/F) = \langle \sigma \rangle$, and given any $\delta \in F^\times$, we can construct a right K -vector space with formal basis $\{1, z, z^2, \dots, z^{n-1}\}$ and define a multiplication on it subject to the relations $z^n = \delta$ and $kz = z\sigma(k)$ for all $k \in K$; then this ring is a *cyclic algebra* which we shall write $(K/F, \sigma, \delta)$. It is not guaranteed that the algebra so produced is a division algebra; sufficient conditions to ensure this will be essential to our construction of cyclic division algebras and STBCs.

When we apply the results of section 5.2 to this representation of a cyclic division algebra, the calculations are straightforward. We choose the natural K -basis $\{1, z, z^2, \dots, z^{n-1}\}$ for D . Then for any $d = k_0 + zk_1 + \dots + z^{n-1}k_{n-1} \in D$, we calculate that

$$\begin{aligned} \lambda_d(z^i) &= k_0z^i + zk_1z^i + z^2k_2z^i + \dots + z^{n-1}k_{n-1}z^i \\ &= z^i\sigma^i(k_0) + z^{i+1}\sigma^i(k_1) + z^{i+2}\sigma^i(k_2) + \dots + z^{i+n-1}\sigma^i(k_{n-1}) \\ &= (z^i\sigma^i(k_0) + \dots + z^{n-1}\sigma^i(k_{n-i-1})) + (z^n\sigma^i(k_{n-i}) + z^{n+1}\sigma^i(k_{n-i+1}) + \dots + z^{n+i-1}\sigma^i(k_{n-1})) \\ &= (z^i\sigma^i(k_0) + \dots + z^{n-1}\sigma^i(k_{n-i-1})) + (\delta\sigma^i(k_{n-i}) + z\delta\sigma^i(k_{n-i+1}) + \dots + z^{i-1}\delta\sigma^i(k_{n-1})) \\ &= \delta\sigma^i(k_{n-i}) + z\delta\sigma^i(k_{n-i+1}) + \dots + z^{i-1}\delta\sigma^i(k_{n-1}) + z^i\sigma^i(k_0) + \dots + z^{n-1}\sigma^i(k_{n-i-1}). \end{aligned}$$

Thus in fact the matrix corresponding to λ_d is given by

$$M_d = \begin{pmatrix} k_0 & \delta\sigma(k_{n-1}) & \delta\sigma^2(k_{n-2}) & \dots & \delta\sigma^{n-2}(k_2) & \delta\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \delta\sigma^2(k_{n-1}) & \dots & \delta\sigma^{n-2}(k_3) & \delta\sigma^{n-1}(k_2) \\ k_2 & \sigma(k_1) & \sigma^2(k_0) & \dots & \delta\sigma^{n-2}(k_4) & \delta\sigma^{n-1}(k_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{n-2} & \sigma(k_{n-3}) & \sigma^2(k_{n-4}) & \dots & \sigma^{n-2}(k_0) & \delta\sigma^{n-1}(k_{n-1}) \\ k_{n-1} & \sigma(k_{n-2}) & \sigma^2(k_{n-3}) & \dots & \sigma^{n-2}(k_1) & \sigma^{n-1}(k_0) \end{pmatrix}, \quad (9)$$

which gives rise to an infinite codebook

$$\mathcal{C}_\infty = \{M_{k_0+zk_1+\dots+z^{n-1}k_{n-1}} : k_i \in K\}, \quad (10)$$

where M_d is defined as in (9). Any finite subset of \mathcal{C}_∞ will thus be a full-diversity STBC.

Example 3

The quaternions \mathbb{H} are a division algebra over \mathbb{R} with a maximal subfield $\mathbb{R} \oplus i\mathbb{R}$, which we will identify with \mathbb{C} ; but since \mathbb{C}/\mathbb{R} is a cyclic Galois extension, \mathbb{H} is a cyclic division algebra. In this case, σ is complex conjugation (mapping $a + ib \mapsto a - ib$), and we choose $z = \hat{j}$ and $\delta = z^2 = -1$. We verify that

$$(a + ib)\hat{j} = a\hat{j} + ib\hat{j} = \hat{j}a - \hat{j}ib = \hat{j}(a - ib) = \hat{j}\sigma(a + ib) \text{ for any } a + ib \in \mathbb{C},$$

$$\text{and } \hat{j}^2 = -1 \in \mathbb{R};$$

consequently we have the desired decomposition $\mathbb{H} = \mathbb{C} + \hat{j}\mathbb{C}$.

So we have an infinite codebook of matrices given by 9. They all therefore have the form

$$M_{w_0 + \hat{j}w_1} = \begin{pmatrix} w_0 & -\overline{w_1} \\ w_1 & \overline{w_0} \end{pmatrix},$$

which we recognize as the Alamouti code [1].

5.4 Constructing Cyclic Division Algebras

Suppose we are given n transmit antennas and a signal set $S \subset \mathbb{C}$. We would like to have

$$D \supseteq K \supseteq F \supseteq \mathbb{Q}(S),$$

where D is a cyclic division algebra of index n over F with K a maximal subfield, because in this situation we could construct a full-diversity $n \times n$ STBC over F of the form (10). We shall first construct a cyclic extension K/F and then build the cyclic algebra $D = (K/F, \sigma, \delta)$, carefully choosing σ and δ so that D is a division algebra.

The procedure Sethuraman *et al.* use is the following. Recall from field theory the following:

Proposition 3 *Let F be a field containing a primitive n^{th} root of unity, and let $K \supseteq F$. Then K/F is cyclic of degree n iff K is the splitting field over F of an irreducible polynomial $X^n - a \in F[X]$.*

So first choose any $t \in \mathbb{C}$ transcendental over $\mathbb{Q}(S)$, and let $F_0 = \mathbb{Q}(S, \omega_n, t)$ where as usual $\omega_n = e^{2\pi i/n}$. Then $X^n - t$ is irreducible over $F_0[X]$ (else t would not be transcendental). So if we set $K_0 = F_0(t^{1/n})$, the splitting field of $X^n - t$ over F_0 , we may conclude by Proposition 3 that K_0/F_0 is cyclic of degree n . Let σ_0 be a generator of $\text{Gal}(K_0/F_0)$.

Now choose any $\delta \in \mathbb{C}$ that is transcendental over K_0 . Let $K = K_0(\delta)$ and $F = F_0(\delta)$. Note that δ behaves just as an indeterminate in K and F . Moreover, $K/F = K_0(\delta)/F_0(\delta)$ is still cyclic of degree n , with a Galois group generated by σ which satisfies $\sigma(\delta) = \delta$ and $\sigma|_K = \sigma_0(K)$. We have thus introduced an element δ which will make the following textbook proposition apply:

Proposition 4 *Let K/F be a cyclic degree- n Galois extension with $\text{Gal}(K/F) = \langle \sigma \rangle$ and $\delta \in F^\times$. If δ^t is not the norm of any element in K^\times for $0 < t < n$, then $(K/F, \sigma, \delta)$ is a division algebra.*

We claim this proposition holds in our case. For suppose that $t \in \mathbb{N}$ and $\frac{f(\delta)}{g(\delta)} \in K = K_0(\delta)$ so that $\delta^t = N_{K/F} \left(\frac{f(\delta)}{g(\delta)} \right)$. Then we have a polynomial equation in $K_0[\delta]$

$$\delta^t N_{K/F}(g(\delta)) = N_{K/F}(f(\delta)). \quad (11)$$

But for any polynomial $h(\delta) \in K_0[\delta]$, the δ -degree of its norm is

$$\deg N_{K/F}(f(\delta)) = \sum_{i=0}^{n-1} \deg \sigma^i(f(\delta)) = \sum_{i=0}^{n-1} \deg f(\delta) = n \deg f(\delta) \equiv 0 \pmod{n}!$$

So taking δ -degrees of equation (11) yields $t+0 \equiv 0 \pmod{n}$, and we conclude that t cannot be between 0 and n . So Proposition 4 does imply that $(K/F, \sigma, \delta)$ is a cyclic division algebra; it is apparent that its index is indeed n .

We therefore do have full-diversity STBCs over K , namely finite subsets of

$$\{M_{k_0 + zk_1 + \dots + z^{n-1}k_{n-1}} : k_i \in K\}$$

(with M_d defined as in (9), of course). Sethuraman *et al.* offer the following example:

Example 4

Let $n = 5$ and $S \subset \mathbb{C}$ be our signal set. Then $F_0 = \mathbb{Q}(S, \omega_5, t)$ and $K_0 = F_0(t^{1/5})$, and K_0/F_0 is cyclic with $\sigma : t^{1/5} \mapsto \omega_5 t^{1/5}$ a generator of $\text{Gal}(K_0/F_0)$. Normalizing (10) by $\frac{1}{\sqrt{5}}$, we then have an STBC for 5 antennas:

$$\mathcal{C}_\infty = \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} g_{0,0} & \delta g_{1,4} & \delta g_{2,3} & \delta g_{3,2} & \delta g_{4,1} \\ g_{0,1} & g_{1,0} & \delta g_{2,4} & \delta g_{3,3} & \delta g_{4,2} \\ g_{0,2} & g_{1,1} & g_{2,0} & \delta g_{3,4} & \delta g_{4,3} \\ g_{0,3} & g_{1,2} & g_{2,1} & g_{3,0} & \delta g_{4,4} \\ g_{0,4} & g_{1,3} & g_{2,2} & g_{3,1} & g_{4,0} \end{pmatrix} : \begin{array}{l} g_{i,j} = \sigma^j(k_i), \text{ where} \\ k_i \in K \text{ for } 0 \leq i \leq 4 \end{array} \right\}.$$

Since each $k_i \in K = \mathbb{Q}(S, \omega_5, t, t^{1/5}, \delta)$, we can for simplicity let \mathcal{C} range over those matrices where

$$k_i = s_{i,0} + s_{i,1}t^{1/5} + s_{i,2}t^{2/5} + s_{i,3}t^{3/5} + s_{i,4}t^{4/5}$$

with $s_{i,\ell} \in S$ for $i, \ell \in \{0, 1, 2, 3, 4\}$. Then $|\mathcal{C}| = |S|^{25}$, and so \mathcal{C} has rate $\frac{1}{5} \log_{|S|}(|S|^{25}) = 5$.

6 Perfect Space-Time Block Codes

The methods of construction of Sethuraman *et al.* described in sections 4.2 through 5 concentrate on fulfilling the rank criterion; that is, the difference of any two codeword matrices is required to be of full rank, in which case we say the code has full diversity. And for any full-diversity finite code \mathcal{C} , the minimum determinant $\Delta_{\min}(\mathcal{C}) = \min_{\substack{V, W \in \mathcal{C} \\ V \neq W}} |\det(V - W)|$ is of course nonzero.

But ideally, we would like to maximize $\Delta_{\min}(\mathcal{C})$, and the preceding constructions did not give it any lower bound. Recall that each of our STBCs \mathcal{C} was a finite subset of some \mathcal{C}_∞ , an infinite collection of matrices satisfying the rank criterion. However, if we abuse notation to write

$$\Delta_{\min}(\mathcal{C}_\infty) = \inf_{\substack{V, W \in \mathcal{C} \\ V \neq W}} |\det(V - W)|,$$

then we had no lower bound on $\Delta_{\min}(\mathcal{C}_\infty)$. In fact, in the codes produced in section 5, the determinants $\{\det(V - W) : V, W \in \mathcal{C}_\infty\}$ are a dense subset of \mathbb{C} ! Thus $\Delta_{\min}(\mathcal{C}_\infty) = 0$.

What this means in practice is that for larger signal constellations S , the minimum determinant grows smaller. Since in practice it can be useful to expand the signal set, it would be very good to find infinite codes \mathcal{C}_∞ that not only satisfy the rank criterion, but also themselves have $\Delta_{\min}(\mathcal{C}_\infty) > 0$.

Oggier, Rekaya, Belfiore, and Viterbo have produced a class of codes which they christened “perfect” STBCs to address this problem [5]. Like the codes found above, these come from cyclic division algebras built over $\mathbb{Q}(S)$; this method of construction, however, does not employ transcendental elements, which made the set of determinants dense. Instead, it makes use of the number-theoretic properties of the field extensions. We will summarize their approach, first formally defining a “perfect” space-time block code.

Definition 5 *A **perfect STBC** is an infinite $n \times n$ STBC \mathcal{C}_∞ which satisfies the following:*

1. *The code has full rate and its entries are from QAM or HEX constellations.*
2. *$\Delta_{\min}(\mathcal{C}_\infty) > 0$. (Note that this implies the rank criterion (3).)*
3. *The average energy transmitted per antenna must be constant in every time slot. (This was also satisfied by our earlier codes.)*
4. *A “shaping” criterion: We require that when we rewrite each code matrix as a real vector of length $2n^2$ (by separating real and imaginary components of each entry), the lattice generated by these vectors is either \mathbb{Z}^{2n^2} or $A_2^{n^2}$, where A_2 is the 2-dimensional hexagonal lattice generated by $(1, 0)$ and $(\frac{1}{2}, \frac{\sqrt{3}}{2})$, or perhaps a rotated version of these.*

Condition 4 is to optimize the energy efficiency of the code. It would also seem to make the work of the spherical decoding algorithm easier. For if we let v denote the real vectorization of a complex matrix, then the lattice in $\mathbb{R}^{2N_r n}$ used by the decoder is $\{v(HV) : V \in \mathcal{C}\}$. But this can be rewritten as $\{\tilde{H}v(V) : V \in \mathcal{C}\}$ for an appropriate matrix \tilde{H} , and hence it is \tilde{H} times the lattice $\{v(V) : V \in \mathcal{C}\}$. But condition 4 guarantees that this latter lattice is either \mathbb{Z}^{2n^2} or $A_2^{n^2}$, and hence very amenable to computation.

6.1 Constructing Perfect STBCs

We take the signal constellation to be either QAM, and hence a subset of $Z[i] = \mathcal{O}_{\mathbb{Q}(i)}$, the ring of integers of $\mathbb{Q}(i)$; or HEX, hence a subset of $Z[\omega_6] = \mathcal{O}_{\mathbb{Q}(\omega_6)}$. We therefore set $F = \mathbb{Q}(i)$ (in the former case) or $F = \mathbb{Q}(\omega_6)$ (in the HEX case), so that our signal constellation will always be a subset of \mathcal{O}_F .

Let K be a well-chosen cyclic extension of F with degree n , and let σ be a generator of $\text{Gal}(K/F)$. To obtain a cyclic algebra over K/F , we need only select $\delta \in F^\times$ and construct $D = (K/F, \sigma, \delta)$. In order to satisfy the average transmitted energy constraint, $|\delta|$ must be 1. We further require that $\delta \in \mathcal{O}_F$, which will imply that $\Delta_{\min}(\mathcal{C}_\infty) > 0$.

We will carefully select an ideal $\mathcal{I} \subseteq \mathcal{O}_K$ with desirable properties. Recall that $D = K \oplus zK \oplus z^2K \oplus \cdots \oplus z^{n-1}K$, where $z^n = \delta$ and $kz = z\sigma(k)$ for every $k \in K$; so every element $x \in D$ has the form $x = k_0 + zk_1 + \cdots + z^{n-1}k_{n-1}$. We then define our infinite code as before:

$$\mathcal{C}_\infty = \left\{ M_x = \begin{pmatrix} k_0 & \delta\sigma(k_{n-1}) & \cdots & \delta\sigma^{n-2}(k_2) & \delta\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \cdots & \delta\sigma^{n-2}(k_3) & \delta\sigma^{n-1}(k_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{n-2} & \sigma(k_{n-3}) & \cdots & \sigma^{n-2}(k_0) & \delta\sigma^{n-1}(k_{n-1}) \\ k_{n-1} & \sigma(k_{n-2}) & \cdots & \sigma^{n-2}(k_1) & \sigma^{n-1}(k_0) \end{pmatrix} : k_i \in \mathcal{I} \subseteq \mathcal{O}_K \right\}. \quad (12)$$

There is then a natural way to produce a finite code using a signal constellation $S \subset \mathcal{O}_F$. The ideal $\mathcal{I} \subset \mathcal{O}_K$ has a basis $\{\nu_0, \dots, \nu_{n-1}\}$; so given n^2 elements $s_{i,j} \in S$ (where $i, j \in \{0, \dots, n-1\}$), we let $k_i = s_{i,0}\nu_0 + \cdots + s_{i,n-1}\nu_{n-1} \in \mathcal{O}_K$ and use these k_i to obtain a code matrix. Thus our finite code \mathcal{C} obtained from \mathcal{I} and S will have size $|\mathcal{C}| = |S|^{n^2}$, and thus has rate n .

To summarize, the following choices need to be made:

- K , a cyclic extension of F with $[K : F] = n$.
- $\delta \in \mathcal{O}_F$ with $|\delta| = 1$. (Then $\delta \in \{\pm 1, \pm i\}$ in the QAM case or $\delta \in \{1, \omega_6, \dots, \omega_6^5\}$ in the HEX case.)
- \mathcal{I} an ideal of \mathcal{O}_K .

These choices must be made so as to ensure both (a) that $(K/F, \sigma, \delta)$ is in fact a *division* algebra, and (b) that the shaping criterion is satisfied. Assuming we can do so, however, we do in fact have the nonzero minimal determinant we desired.

Proposition 6 *Let $F = \mathbb{Q}(i)$ or $F = \mathbb{Q}(\omega_6)$. Assuming the notation above, suppose K and δ are indeed chosen so that $(K/F, \sigma, \delta)$ is a division algebra, and let \mathcal{I} be any ideal of \mathcal{O}_K . Let the STBC \mathcal{C}_∞ be defined as in (12). Then $\Delta_{\min}(\mathcal{C}_\infty) > 0$.*

Proof. Since \mathcal{C}_∞ is an additive group, we have

$$\Delta_{\min}(\mathcal{C}_\infty) = \inf_{\substack{V, W \in \mathcal{C}_\infty \\ V \neq W}} |\det(V - W)| = \inf_{0 \neq V \in \mathcal{C}_\infty} |\det(V)|.$$

But every nonzero matrix $V \in \mathcal{C}_\infty$ comes from an element $x = k_0 + zk_1 + \cdots + z^{n-1}k_{n-1} \in D$ with each $k_i \in \mathcal{O}_K$, and its determinant has the form

$$\det(V) = \det \begin{pmatrix} k_0 & \delta\sigma(k_{n-1}) & \cdots & \delta\sigma^{n-2}(k_2) & \delta\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \cdots & \delta\sigma^{n-2}(k_3) & \delta\sigma^{n-1}(k_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{n-2} & \sigma(k_{n-3}) & \cdots & \sigma^{n-2}(k_0) & \delta\sigma^{n-1}(k_{n-1}) \\ k_{n-1} & \sigma(k_{n-2}) & \cdots & \sigma^{n-2}(k_1) & \sigma^{n-1}(k_0) \end{pmatrix} \quad (13)$$

This is a polynomial with integral coefficients in $\sigma^i(k_j)$ and δ . But $k_j \in \mathcal{O}_K$ implies $\sigma^i(k_j) \in \mathcal{O}_K$ for all $\sigma^i \in \text{Gal}(K/F)$, and we have also explicitly chosen $\delta \in \mathcal{O}_F \subseteq \mathcal{O}_K$. Hence $\det(V) \in \mathcal{O}_K$.

On the other hand, the determinant (13) is precisely the reduced norm of $x = k_0 + zk_1 + \dots + z^{n-1}k_{n-1} \in D$, which is guaranteed to be in F . Thus $\det(V) \in \mathcal{O}_K \cap F = \mathcal{O}_F$. And therefore

$$\Delta_{\min}(\mathcal{C}_\infty) = \inf_{0 \neq V \in \mathcal{C}_\infty} |\det(V)| \geq \inf_{0 \neq y \in \mathcal{O}_F} |y| = 1$$

(since \mathcal{O}_F is either $\mathbb{Z}[i]$ or $\mathbb{Z}[\omega_6]$). \square

Note that this proof nowhere used the fact that each x_i is actually in \mathcal{I} ; if $\mathcal{I} < \mathcal{O}_K$, this restriction will affect our minimum determinant. Oggier *et al.* prove that $\Delta_{\min}(\mathcal{C}_\infty)^2 \geq N(\mathcal{I})$, the norm of \mathcal{I} , and equality holds if \mathcal{I} is a principal ideal.

The method used to produce suitable choices of K , δ , and \mathcal{I} is unfortunately not general: for $n = 2, 3, 4$, and 6 , Oggier *et al.* proceed case by case to choose QAM or HEX signals, name a concrete cyclic extension K with $[K : F] = n$, pick a good unit $\delta \in \mathcal{O}_K^*$, and then laboriously check that these choices both produce a division algebra (using Proposition 4) and satisfy the shaping conditions.

Example 5

A 3×3 perfect STBC is given as follows: let $F = \mathbb{Q}(\omega_6)$ (so we are using HEX symbols). Let $\theta = \omega_7 + \omega_7^{-1} = 2 \cos\left(\frac{2\pi}{7}\right)$, and set $K = F(\theta)$. Then it turns out that $[K : F] = 3$, and K/F is cyclic with generator $\sigma : \omega_7 + \omega_7^{-1} \mapsto \omega_7^2 + \omega_7^{-2}$. If we choose $\delta = \omega_3$, it can be proven using class field theory that neither δ nor δ^2 is a norm in K/F , and hence by Proposition 4, $(K/F, \sigma, \delta)$ is a division algebra.

We then factor $(7)\mathcal{O}_K = \mathcal{P}^3\mathcal{Q}^3$, and without loss of generality choose the prime ideal \mathcal{P} of norm 7 to be our \mathcal{I} .

We thus obtain a 3×3 perfect STBC using a HEX signal constellation. It turns out that its minimum determinant is $\frac{1}{7}$.

Although the constructions are so laborious, Oggier *et al.* also prove a useful nonexistence result: perfect codes can only exist for $n = 2, 3, 4$, and 6 , precisely the cases for which they have constructed examples.

7 Conclusion

Hopefully this report has provided a good introduction to the basic concepts of space-time coding, as well as summarizing methods used in two recent papers to construct cyclic division algebras and space-time block codes based on them. A few natural questions arise after this short survey. Is there any more unified way to construct perfect STBCs, without lengthy *ad hoc* number theoretic computations for each n ? Moreover, although perfect STBCs can only exist for 2, 3, 4, or 6 antennas, but they are required to satisfy several strict requirements. Are there STBCs in other dimensions which satisfy $\Delta_{\min}(\mathcal{C}_\infty) > 0$, perhaps at the price of poor shaping? Are there codes that are “close to perfect” in some measurable sense?

References

- [1] Siavash M. Alamouti, *A simple transmit diversity technique for wireless communications*, IEEE Journal on Select Areas in Communications **16** (1998), no. 8, 1451–1458.
- [2] Oussama Damen, Ammar Chkeif, and Jean-Claude Belfiore, *Lattice code decoder for space-time codes*, IEEE Communications Letters **4** (2000), no. 5, 161–163.
- [3] I.N. Herstein, *Noncommutative rings*, Carus Mathematical Monographs, Mathematical Association of America, Washington, D.C., 1968.
- [4] Bertrand M. Hochwald and Wim Sweldens, *Differential unitary space-time modulation*, IEEE Transactions on Communications **48** (2000), no. 12, 2041–2052.
- [5] Frédérique Oggier, Ghaya Rekaya, Jean-Claude Belfiore, and Emanuele Viterbo, *Perfect space time block codes*, not yet published; available at “<http://www.comelec.enst.fr/~belfiore/perfect2346.pdf>”.
- [6] B.A. Sethuraman, B. Sundar Rajan, and V. Shashidhar, *Full-diversity, high-rate space-time block codes from division algebras*, IEEE Transactions on Information Theory **49** (2003), no. 10, 2596–2616.
- [7] V. Tarokh, N. Seshadri, and A.R. Calderbank, *Space-time codes for high data rate wireless communication: Performance criterion and code construction*, IEEE Transactions on Information Theory **44** (1998), no. 2, 744–764.