Perfect Space-Time Block Codes

Christopher Holden

December 14, 2004

Overview of MIMO and STBC

Wireless systems of communication have recently turned to a strategy known as Multiple Input Multiple Output (MIMO) to improve the quality (bit-error rate) and data rate (bits/sec). This advantage can increase the quality of service and revenues of the operator. This is done by using multiple transmit and receive antennas, as well as appropriate coding techniques. They take advantage of spatial and temporal diversity to combat the random fading induced by multi-path propagation of the signal and maximize efficient use of bandwidth. There is also a fundamental gain in transmitting data over a matrix rather than vector channel. Transmission of data over MIMO channels has traditionally focused on data rate maximization or diversity maximization, and space-time codes were developed as a means to the latter. Two types of STCs have been developed, Trellis Codes and Block Codes. "The decoding complexity of space-time trellis decoding (measured by number of trellis states at the decoder) increases exponentially as a function of the diversity level and transmission rate" p. 288 in [5]. The Space-Time Block Codes we'll discuss here are often preferred because, under the assumption of flat fading Rayleigh channels (whose coefficients are constant and scalar), they can be decoded using simple linear processing at the receiver (the Maximal Likelihood Sphere Decoder) [5].

Space-Time Coding Model

Suppose we have a MIMO system with n transmit antennas and m receive antennas. At the transmitter, information symbols belonging to a constellation set, such as QAM or HEX, are parsed into blocks: $\mathbf{s}(n) = [s(nK), \ldots, s(nK + K - 1)]^T$ of size $K \times 1$. The block $\mathbf{s}(n)$ is encoded by the ST encoder which maps $\mathbf{s}(n)$ to column vectors in the following n$\times$ m ST code matrix

$$\mathbf{c} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1P} \\ c_{21} & c_{22} & \cdots & c_{2P} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nP} \end{bmatrix} \tag{1}$$

where the coded symbol c_{ij} belong to the constellation set and P is the frame(block) length. At each time slot t, signals c_{it}, $i = 1, 2, \ldots, n$ are transmitted simultaneously from the n transmit antennas [6]. Ultimately, each transmit antenna sees a differently encoded version of the same signal. Upon being received, these signals are resolved by the receiver into a single signal. This has the effect of combatting multi-path fading that has occurred in the separate channels. There have been many approaches to STBCs , the scheme of Alamouti being the first [1]. Very recently [2] and [7] have developed what they call *P*erfect STCs. These codes are so called because they satisfy a number of design criteria and only occur in a few cases. Simulation results suggest that these PSTBCs often outperform other STBCs p. 26 in [7].

Creation of Perfect Space-Time Block Codes

The basic tool for constructing *P*erfect codes is the cyclic division algebra. The first step to full diversity (of which we'll say more shortly) is in making the code a group with respect to multiplication (and addition). That is $m = n$ and we take additional steps to ensure that each block of code has an inverse. One way to do this is to use diagonal matrices, whose multiplicative group is that of a field, but a more general method is to include our code in a noncommutative division ring. Given a field $\mathbb{F}$, let $\mathbb{K}$ be a cyclic extension of $\mathbb{F}$ of degree n, that is $Gal(\mathbb{K}/\mathbb{F}) =< \sigma >\simeq \mathbb{Z}/n$. Then we define an algebra from $\mathbb{K}$

$$\mathbf{D} \triangleq \mathbb{K} \cdot 1 \oplus \mathbb{K} \cdot e \oplus \ldots \mathbb{K} \cdot e^{n-1} \tag{2}$$

so that for some $\gamma \in \mathbb{F}^*$, $e^n = \gamma$ and $\forall x \in \mathbb{K}$, $e^{-1}xe = \sigma(x)$.

•**D** is a division algebra $\iff$ $\gamma^k \neq N_{\mathbb{K}/\mathbb{F}}(y)$ for any $y \in \mathbb{K}$ and $1 \leq k \leq n-1$.

• This e may seem somewhat nebulous. The reason for this is that e is the source of noncommutativity of **D** and as such can't be fully described in terms of the (commutative) fields $\mathbb{F}$ or $\mathbb{K}$. However, matrix groups are naturally noncommutative objects; e finds its natural expression there. The reason for developing **D** as we are, rather than as a matrix ring, is that it is easier on the eye and it is simpler to see γ as a parameter of **D** which must be chosen carefully.

Next, we obtain the *left regular representation* of **D** as follows. For $x \in \mathbf{D}$, ($x = x_0 + x_1 e + \ldots + x_n e^{n-1}$ with $x_i \in \mathbb{K}$) let λ_x be the linear map that sends **D** to itself via multiplication by x. If we then write out the matrix that represents λ_x, we get a matrix for each $x \in \mathbf{D}$.

$$\mathbf{x} = \begin{pmatrix} x_0 & x_1 & x_2 & \ldots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \sigma(x_1) & \ldots & \sigma(x_{n-2}) \\ \vdots & & & \ddots & \vdots \\ \gamma\sigma(x_2) & \gamma\sigma(x_3) & \gamma\sigma(x_4) & \ldots & \sigma^{n-2}(x_1) \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \gamma\sigma^{n-1}(x_3) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \tag{3}$$

We have thus embedded **D** in $GL_n(\mathbb{K})$ via $x \longmapsto \mathbf{x}$ and call the image $\mathcal{C}_\infty$ or the infinite code. By only using x_i which belong to an ideal $\mathcal{I}$ of the ring of integers $\mathcal{O}_\mathbb{K}$ of $\mathbb{K}$, we obtain

the Space-Time Block Code $\mathcal{C}_\mathcal{I}$ as a restriction of the codewords in $\mathcal{C}_\infty$. More about $\mathcal{I}$ later.

Of course, when constructing such a code, the devil's in the details. We have $\mathbb{F}$, $\mathbb{K}$, γ and $\mathcal{I}$ to determine in order to optimize this code. Presently, we'll look at design criteria that come from the engineering side of things and how they define a *P*erfect code. We'll also explain how these criteria determine the above parameters and define *P*erfect codes so that they only occur for 2,3,4 and 6 antennas.

Engineering Requirements

Rank Criterion and Diversity

In order for a code to be easily decoded and fully diverse, the **strict rank criterion** must be fulfilled. That is

$$\zeta(\mathcal{C}_\mathcal{I}) = \min_{\mathbf{x},\mathbf{y}\in C_\mathcal{I},\mathbf{x}\neq\mathbf{y}} |\det(\mathbf{x}-\mathbf{y})|^2 > 0. \tag{4}$$

Decoding is becomes easier if our codewords are invertible matrices, and the rank criterion is effectively determinable if the sum of any two codewords is again a codeword. This gives us reason to place the code inside a division algebra. In this situation, the rank criterion becomes

$$\zeta(\mathcal{C}_\mathcal{I}) = \min_{\mathbf{x}\in C_\mathcal{I},\mathbf{x}\neq 0} |\det(\mathbf{x})|^2 > 0. \tag{5}$$

Since the determinant of any invertible matrix is nonzero, we can satisfy the rank criterion for the infinite code (and hence for $\mathcal{C}_\mathcal{I}$) by slightly restricting our choice of γ and satisfying a necessary criteria for $\mathbb{F}$.

Theorem 1: Suppose $\gamma \in \mathcal{O}_\mathbb{F}$. Then $\forall \mathbf{x} \in \mathcal{C}_\infty$, $det(\mathbf{x}) \in \mathcal{O}_\mathbb{F}$.

proof: That $\det(\mathbf{x}) \in \mathbb{F}$ can by seen by noticing that the determinant of (3) is invariant under σ, and $\det(\mathbf{x})$ is clearly in $\mathcal{O}_\mathbb{K}$ if $\gamma \in \mathcal{O}_\mathbb{F}$. Then $\det(\mathbf{x}) \in \mathbb{F} \cap \mathcal{O}_\mathbb{K} = \mathcal{O}_\mathbb{F}$.

Theorem 2: $\mathcal{O}_\mathbb{F}$ is discrete in $\mathbb{C} \iff \mathbb{F}$ is an imaginary quadratic extension of $\mathbb{Q}$ (i.e. $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$ for d a positive square-free integer).

proof: See [4]

If we choose $\gamma \in \mathcal{O}_{\mathbb{F}}$, Theorems 1 and 2 give us that

$$\zeta(\mathcal{C}_{\mathcal{I}}) \geq \zeta(\mathcal{C}_{\infty}) \geq \min_{z \in \mathcal{O}_{\mathbb{F}}, z \neq 0}(z) > 0 \tag{6}$$

where the strict inequality holds $\iff \mathbb{F} = \mathbb{Q}(\sqrt{-d})$.

In addition, to be fully diverse the code must have uniform average transmitted energy per antenna in all time slots. This means that all the coded symbols in the code matrix should have the same average energy.

Because of this, $|\gamma| = 1$ and so γ must be a unit in $\mathcal{O}_{\mathbb{F}}$. But the only units in $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$ are ± 1 unless $\mathbb{F} = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$ where j is a nonreal third root of unity. For such $\mathbb{F}$, the rank criterion is satisfied since $\det(\mathbf{x}) \in \mathcal{O}_{\mathbb{F}}$ implies $|\det(\mathbf{x})| \geq 1$ where equality holds if we let $x_0 = 1$ and all other $x_i = 0$. Thus,

$$\zeta(\mathcal{C}_{\infty}) = 1 \tag{7}$$

It turns out that at this point, we have enough information to restrict the number of antennas for which a PSTBC exists.

γ, $\mathbb{F}$ and the Existence of PSTBCs

By the arguments above, we have that γ can only be -1, $\pm i$, $\pm j$, $\pm j^2$. Then $\gamma^k = 1$ for $k \leq 6$, and hence γ is a norm for such k ($N_{\mathbb{K}/\mathbb{F}}(1) = 1^n = 1$). Thus $\mathbf{D}$ can only be a division algebra for n ≤ 6. From this meager information we get:

γ	smallest k	possible n	$\mathbb{F}$
-1	2	2	$\mathbb{Q}(\sqrt{-d})$
$\pm i$	4	2,3,4	$\mathbb{Q}(i)$
j, j^2	3	2,3	$\mathbb{Q}(j)$
$-j$, $-j^2$	6	2,3,4,5,6	$\mathbb{Q}(j)$

(8)

If n = 5, by (8) γ would have to be $-j$ or $-j^2$, and $\mathbb{F}$ would be $\mathbb{Q}(j)$. However, $1 + j$ lies inside $\mathbb{F}$ (and hence any extension thereof). Thus the relative norm (from $\mathbb{K}$ to $\mathbb{F}$) of $j + 1$ is $(1 + j)^5 = -j$, and that of $j^2 + 1$ is $-j^2$. Thus our only choices for γ are norms,

preventing **D** from being a division algebra and any code constructed from **D** from being fully diverse. There can be no PSTBC for 5 antennas.

Now that we have shown which PSTBCs are prevented from existing, let's show that what went wrong for n=5 does not always happen for other numbers of antennas; we can actually choose $\mathbb{F}$, γ, $\mathbb{K}$ so that we get a fully diverse infinite code (i.e γ is not a relative norm from $\mathbb{K}$ to $\mathbb{F}$). Later, we'll go into how the choice of $\mathcal{I}$ is made.

n=2

For 2 antennas we'll reproduce here what [2] call the *Golden Code*. This name refers to the use of $\theta = \frac{1+\sqrt{5}}{2}$, known as the *Golden Number*, in the construction of the code. Let $\mathbb{F} = \mathbb{Q}(i)$, $\mathbb{K} = \mathbb{F}(\theta) = \mathbb{Q}(i, \sqrt{5})$. Since θ has minimal polynomial $x^2 - x - 1$ over $\mathbb{Q}$, $[\mathbb{Q}(\theta) : \mathbb{Q}] = 2$. Also, $\mathbb{Q}(\theta) \subset \mathbb{R}$, so the minimal polynomial of i, $x^2 + 1$, remains irreducible over $\mathbb{Q}(\theta)$. Thus, $[\mathbb{K} : \mathbb{Q}] = 4$, which implies that $[\mathbb{K} : \mathbb{Q}(\theta)] = 2$. We then have $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$ and $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i][\theta] = \{a + b\theta | a, b \in \mathbb{Z}[i]\}$.

claim: $\gamma = i$ is not a relative norm from $\mathbb{K}$ to $\mathbb{F}$

proof: Let $z \in \mathbb{K}$: $z = a + b\sqrt{5}$ with $a, b \in \mathbb{F}$. Its relative norm is

$$N_{\mathbb{K}/\mathbb{F}}(z) = (a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2$$

To show that $a^2 + 5b^2 = i$ has no solutions in $\mathbb{Q}(i)$, we'll first embed $\mathbb{Q}(i)$ in $\mathbb{Q}_5$. We'll then show that the existence of solutions in $\mathbb{Q}_5$ is determined by the existence of solutions in $\mathbb{Z}/5$ which we can determine explicitly.

To show that this embedding can be accomplished, we need $i \in \mathbb{Z}_5$. This is true if $x^2 + 1$, the minimal polynomial of i has roots in $\mathbb{Z}_5$. By *Hensel's Lemma*, we only need to find roots in $\mathbb{Z}/5$. But this is obvious: $(2)^2 + 1 \equiv 0 \pmod 5$. Thus, i maps to $y + 5x$ where $x, y \in \mathbb{Z}_5$ and $y^2 = -1$. Now we can naturally think of $\mathbb{Q}(i)$ sitting inside of $\mathbb{Q}_5$ and so consider a, b to be in $\mathbb{Q}_5$.

If such a, b exist, in terms of the 5-adic valuation we have

$$\nu_5(a^2 - 5b^2) = \nu_5(y + 5x) = 0 \tag{9}$$

where we have the equality on the right since 5 cannot divide $x + 5y$ when y is a unit and $x \in \mathbb{Z}_5$. Since the left side of (9) $= \min\{2\nu_5(a), 2\nu_5(b) + 1\}$,

a must be in $\mathbb{Z}_5$, and then so must b.
Now we can once more use *Hensel's Lemma* to say that the existence of $\mathbb{Z}_5$ solutions to

$$a^2 - 5b^2 = y + 5x \tag{10}$$

is tantamount to the existence of solutions in $\mathbb{Z}/5$. If we reduce this equation mod 5, we get $a^2 \equiv y \pmod 5$. However, since $y^2 = -1$, $y \pmod 5$ must be 2 which has no square root mod 5. Thus there are no solutions to (7) and so i cannot be a relative norm.

• In designing an infinite *P*erfect Code for 2 antennas we are not restricted to the Golden Code. The same construction will work, word for word, if we choose θ to be $\frac{1+\sqrt{p}}{2}$ where p is a prime $\equiv 5 \pmod 8$. In fact, only the very last step in the proof of that i is not a relative norm (that $a^2 \equiv y \pmod 5$ implies no solutions to $a^2 + 5b^2 = y + 5x$) depends on more than $p \equiv 1 \pmod 4$.

n=3

The choice for $\mathbb{F}$, $\mathbb{K}$, γ is similar for other numbers of antennas. For n=3, let $\mathbb{F} = \mathbb{Q}(j)$, $\mathbb{K} = \mathbb{F}(\theta)$ where $\theta = \zeta_7 + \zeta_7^{-1} = 2cos(\frac{2\pi i}{7})$ and $\gamma = j$. In order to show that **D** is a division algebra, we need to show j, j^2 are not relative norms. This is considerably more involved than for the case of 2 antennas. Details are given on p.22, 29, 30 of [7]

n=4

For n=4, let $\mathbb{F} = \mathbb{Q}(i)$, $\mathbb{K} = \mathbb{F}(\theta)$ where $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2cos(\frac{2\pi i}{15})$ and $\gamma = i$. In order to show that **D** is a division algebra, we need to show that γ, γ^2, $\gamma^3 = \pm i$, -1 are not relative norms. Details are given on p.20, 30,31 of [7]

n=6

For n=6, let $\mathbb{F} = \mathbb{Q}(j)$, $\mathbb{K} = \mathbb{F}(\theta)$ where $\theta = \zeta_{28} + \zeta_{28}^{-1} = 2cos(\frac{2\pi i}{28})$ and $\gamma = -j$. In order to show that **D** is a division algebra, we need to show γ, γ^2, γ^3, $\gamma^4 = \pm j$, $\pm j^2$ and -1 are not relative norms. Details are given on p.24, 31, 32 of [7]

Shaping and $\mathcal{I}$

We now have a division algebra **D** for 2, 3, 4 and 6 antennas. Each **D** corresponds to an infinite code $\mathcal{C}_\infty$ via the matrix representation shown earlier. We obtain the *P*erfect Code as a subset of $\mathcal{C}_\infty$ by restricting the x_i to be in an ideal $\mathcal{I}$ of $\mathcal{O}_\mathbb{K}$ and specifying a normalizing constant c:

$$\mathcal{C}_{\mathcal{I}} = \left\{ \mathbf{x} = c \begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \sigma(x_1) & \dots & \sigma(x_{n-2}) \\ \vdots & & & \ddots & \vdots \\ \gamma\sigma(x_2) & \gamma\sigma(x_3) & \gamma\sigma(x_4) & \dots & \sigma^{n-2}(x_1) \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \gamma\sigma^{n-1}(x_3) & \dots & \sigma^{n-1}(x_0) \end{pmatrix} \middle| x_i \in \mathcal{I} \subset \mathcal{O}_{\mathbb{K}}, c \in \mathbb{K} \right\} \tag{11}$$

The second major engineering requirement for a *P*erfect Code, **shaping**, concerns which ideal of $\mathcal{O}_{\mathbb{K}}$ is chosen. Basically, in order for the code to be energy efficient, we want the ideal from which it is derived to have the simplest "shape" as possible. What is meant by "shape" should become clear presently.

We can think of $\mathcal{O}_{\mathbb{K}}$ as a lattice in $\mathbb{C}^n$ as follows. In each case above,

$$\mathcal{O}_{\mathbb{K}} = \{a_1 + a_2\theta + \ldots + a_n\theta^{n-1} | a_i \in \mathcal{O}_{\mathbb{F}}\} \tag{12}$$

where $\mathbb{F} = \mathbb{Q}(i)$ for n=2,4 and $\mathbb{Q}(j)$ for n=3,6. We say that $\mathcal{O}_{\mathbb{K}}$ has basis $\{1, \theta, \ldots, \theta^{n-1}\}$ over $\mathcal{O}_{\mathbb{F}}$. Recall that $Gal(\mathbb{K}/\mathbb{F}) = <\sigma> \simeq \mathbb{Z}/n$, and define an embedding:

$$\begin{aligned} \varphi : &\mathcal{O}_{\mathbb{K}} \longmapsto \mathbb{C}^n \\ &x \longmapsto \varphi(x) = (x, \sigma(x), \ldots, \sigma^{n-1}(x)) \end{aligned} \tag{13}$$

The image of this embedding is a lattice in $\mathbb{C}^n$ with basis φ(basis of $\mathcal{O}_{\mathbb{K}}$). For every ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{K}}$ we can restrict the embedding to provide a lattice $\Lambda(\mathcal{I})$ with basis φ(basis of $\mathcal{I}$). *Note*: every such ideal has an integral basis over $\mathcal{O}_{\mathbb{F}}$. More specifically, suppose $\mathcal{I}$ has basis $\{\beta_k\}_{k=1}^n$. Then $\{\varphi(\beta_k)\}$ is a collection of n vectors in $\mathbb{C}^n$. We form a matrix M with the $\varphi(\beta_k)$ as columns so that the l, kth entry is $\sigma^{l-1}(\beta_k)$:

$$M = c \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ \sigma(\beta_1) & \sigma(\beta_2) & \dots & \sigma(\beta_n) \\ \vdots & & \ddots & \vdots \\ \sigma^{n-1}(\beta_1) & \sigma^{n-1}(\beta_2) & \dots & \sigma^{n-1}(\beta_n) \end{pmatrix} \tag{14}$$

Next we form the Hermitian Transpose of M, M^*:

$$M^* = \overline{c} \begin{pmatrix} \overline{\beta}_1 & \sigma(\overline{\beta}_1) & \dots & \sigma^{n-1}(\overline{\beta}_1) \\ \overline{\beta}_2 & \sigma(\overline{\beta}_2) & \dots & \sigma^{n-1}(\overline{\beta}_2) \\ \vdots & & \ddots & \vdots \\ \overline{\beta}_n & \sigma(\overline{\beta}_n) & \dots & \sigma^{n-1}(\overline{\beta}_n) \end{pmatrix} \tag{15}$$

where the bar denotes the nontrivial automorphism of $\mathbb{F}$ over $\mathbb{Q}$. For $\mathbb{F} = \mathbb{Q}(i)$, the map is given by $i \mapsto -i$, and for $\mathbb{F} = \mathbb{Q}(j)$, $j \mapsto j^2$.

$G = M^*M$ is called the *Gram Matrix*. Its l, kth entry is

$$|c|^2 \sum_{m=1}^{n-1} \sigma^m(\beta_l \overline{\beta}_k) = |c|^2 Tr_{\mathbb{K}/\mathbb{F}}(\beta_l \overline{\beta}_k) \tag{16}$$

The computation of G is instrumental in determining whether we've chosen $\mathcal{I}$ so that $\Lambda(\mathcal{I})$ is a rotated, scaled version of $\Lambda(\mathcal{O}_\mathbb{F})$: $\mathbb{Z}[i]^n$ (for n=2,4) and $\mathbb{Z}[j]^n$ (for n=3,6). This is what we meant earlier by the correct "shape". This criterion is turn equivalent to asking if $G = c^2 Id$. In this situation, we say there is no shaping loss in the signal constellation. In order for the codes we defined above to be perfect, for each we need an ideal $\mathcal{I}$ with basis $\{\beta_k\}_{k=1}^n$ and a c so that

$$|c|^2 Tr_{\mathbb{K}/\mathbb{F}}(\beta_l \overline{\beta}_k) = \delta_{lk} \tag{17}$$

Before proceeding to a proof that a particular $\mathcal{I}$ satisfies the shaping constraint, let's look at the heuristics that would permit us to guess what $\mathcal{I}$ is. The key here is the relation between the volume of a fundamental region of the lattice, the discriminant of a field and the norm of an ideal. First, we want our lattice to have the same volume as a scaled version of $\Lambda(\mathcal{O}_\mathbb{F})$. For some k we have:

$$vol(\Lambda(\mathcal{I})) = vol(\Lambda(\mathcal{O}_\mathbb{F})) = \begin{cases} k^{2n} & if \quad \mathcal{O}_\mathbb{F} = \mathbb{Q}(i) \\ (k^2 \frac{\sqrt{3}}{2})^n & if \quad \mathcal{O}_\mathbb{F} = \mathbb{Q}(j) \end{cases} \tag{18}$$

Furthermore,

$$vol(\Lambda(\mathcal{I})) = \mathcal{N}(\mathcal{I}) vol(\Lambda(\mathcal{O}_\mathbb{K})) \tag{19}$$

$$vol(\Lambda(\mathcal{O}_{\mathbb{K}})) = 2^{-n}\sqrt{|d_{\mathbb{K}}|} \tag{20}$$

where $\mathcal{N}(\mathcal{I})$ is the norm of $\mathcal{I}$ and $d_{\mathbb{K}}$ is the absolute discriminant of $\mathbb{K}$.

Guessing $\mathcal{I}$ for n=2 *The Golden Code*

Recall $\mathbb{K} = \mathbb{F}(\theta) = \mathbb{Q}(i, \sqrt{5})$ where $Gal(\mathbb{K}/\mathbb{F}) =< \sigma > \simeq \mathbb{Z}/n$ with σ given by $\sqrt{5} \mapsto -\sqrt{5}$. $d_{\mathbb{K}} = 2^4 5^2$ so (20) becomes

$$vol(\Lambda(\mathcal{O}_{\mathbb{K}})) = 5$$

While (18) gives us that $vol(\Lambda(\mathcal{I})) = k^2$. Putting these together with (19) we get

$$k^2 = 5\mathcal{N}(\mathcal{I})$$

And so we look in $\mathcal{O}_{\mathbb{K}}$ for an ideal with norm 5. Since $5 \equiv 1 \pmod 4$, 5 splits in $\mathbb{Z}[i]$, and since $d_{\mathbb{Q}(\theta)} = 5$, 5 ramifies in $\mathcal{O}_{\mathbb{Q}(\theta)}$. This means that as an ideal in $\mathcal{O}_{\mathbb{K}}$, $(5) = (\mathcal{I}_1)^2(\mathcal{I}_2)^2$. Upon inspection, we find

$$\mathcal{I}_1 = (\alpha) = (1 + i - i\theta) \tag{21}$$

$$\mathcal{I}_2 = (\sigma(\alpha)) = (1 + i - i\sigma(\theta)) \tag{22}$$

$$\mathcal{N}(\mathcal{I}_1) = N_{\mathbb{K}/\mathbb{Q})}(\alpha) = \mathcal{N}(\mathcal{I}_2) = N_{\mathbb{K}/\mathbb{Q}}(\sigma(\alpha)) = 5 \tag{23}$$

Verification of the shape of $\mathcal{I}$

Next, we verify that (17) holds for $\mathcal{I} = (\alpha)$.

claim: $\mathbf{\Lambda}(\alpha) = (\sqrt{\mathbf{5}}\mathbb{Z}[\mathbf{i}])^{\mathbf{2}}$
proof: (α) has basis $\{\alpha, \alpha\sigma\}$ over $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i]$. $\overline{\alpha} = \overline{1 + i - i\theta} = 1 - i + i\theta$.

$\alpha\overline{\alpha} = (1 + i - i\theta)(1 - i + i\theta) = \frac{5}{2} - \frac{\sqrt{5}}{2}$

$\alpha\overline{\alpha\theta} = \alpha\theta\overline{\alpha} = \alpha\overline{\alpha}\theta = \frac{3\sqrt{5}}{2}$

$\alpha\theta\overline{\alpha\theta} = \alpha\overline{\alpha}\theta^2 = \alpha\overline{\alpha}(\theta + 1) = \frac{5}{2} - \frac{\sqrt{5}}{4}$

Thus

$Tr_{\mathbb{K}/\mathbb{F}}(\alpha\overline{\alpha}) = Tr_{\mathbb{K}/\mathbb{F}}(\alpha\theta\overline{\alpha\theta}) = 5$

$Tr_{\mathbb{K}/\mathbb{F}}(\alpha\overline{\alpha\theta}) = Tr_{\mathbb{K}/\mathbb{F}}(\alpha\theta\overline{\alpha}) = 0$

Hence $G = 5Id$. Thus $\Lambda(\alpha)$ is a rotated version of $(\mathbb{Z}[i])^2$, scaled by $\sqrt{5}$. We choose our normalizing constant to be $\frac{1}{\sqrt{5}}$ and have verified

$$\mathcal{C}_{(\alpha)} = \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} x_0 & x_1 \\ i\sigma(x_0) & \sigma(x_1) \end{pmatrix} \middle| x_i \in (\alpha) \right\} \qquad \text{is a } \textit{P}\text{erfect Code} \qquad (24)$$

We can rewrite this *Golden Code* as

$$\mathcal{C}_{(\alpha)} = \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(a+b\theta) & \alpha(c+d\theta \\ i\sigma(\alpha)(c+d\sigma(\theta)) & \sigma(\alpha)(a+b\sigma(\theta)) \end{pmatrix} \middle| a, b \in \mathbb{Z}[i] \right\} \qquad (25)$$

Other numbers of Antennas

The heuristics for finding such an $\mathcal{I}$ are similar for n = 3,4 and 6, but verification becomes more complex. For n = 6, the ideal chosen is no longer principal (i.e. generated by a single element), and so this makes even finding the right basis a difficult matter. See [7] for details.

Conclusion

Above, we have outlined the construction of Space-Time Block Codes that satisfy both the strict rank criterion and the cubic shaping constraint as the spectral efficiency increases. These codes thus maximize the diversity and coding advantages postulated by a MIMO system. Moreover, these codes deserve the name *P*erfect in that the requirements postulated from the engineering side fit so nicely certain number theoretic properties encountered in the algebraic construction of the codes. Their applicability however is limited, like all STBCs, in that they are postulated for flat fading Rayleigh channels where all channel coefficients are known.

> This model is valid for the case when the delay spread is small enough compared to the symbol duration. As we discuss earlier, if the delay spread is comparable or larger than the symbol duration, the channel will distort the signal resulting in what is known as frequency-selective channels. The channel response is no longer constant and not all frequency components fade simultaneously. In this case, the delayed paths overlap will cause intersymbol interference (ISI) p. 5 in [6]

It has been shown that the diversity gain of STBCs can be preserved under these circumstances, but the coding advantage is another story. Linear ML decoding is not possible in the presence of frequency selectivity at the channel; the transition from 4 to 5 enabled by linear decoding is only possible if we can assume that the channels fade independently [3], [5]. One possible solution is to employ a channel equalizer along with the space-time decoder. Yet, "the nonlinear and noncausal nature of the [STB] code makes the use of classical equalization methods a challenging problem" p. 291 in [5]. One approach has been to combine the Alamouti STBC with OFDM. OFDM is applied to convert the frequency selective channel into into a set of independent parallel frequency-flat subchannels. The Alamouti scheme is then applied to successive subcarriers. Unfortunately this strategy is expensive computationally at the receiver.

One hope for these MIMO systems and STBCs is that they could help to resolve the bottleneck of traffic capacity in current and future wireless applications. And for low-power, peer-to-peer and multiple-access applications, ultra-wideband transmissions have demonstrated several advantages. One would like to see the two marry happily. In some ways, this is the case. UWB communications are rather sensitive to timing jitter, something that is alleviated by MIMO systems [9]. But other aspects present natural difficulties. For example, in UWB transmission, the inverse bandwidth is not large in comparison to the delay spread; the receiver cannot resolve the different subpaths that the signal takes because they arrive within too short a time of one another. This leaves us in the frequency selective situation above [6]. It is unclear what will become the dominant coding strategy in these UWB applications, but it seems unlikely anything so *P*erfect as the PSTBCs will emerge.

References

[1] S. Alamouti. A simple transmit diversity technique for wireless communications. *IEEE Journal on Selected Areas in Communications*, 16:1451–1458, Oct 1998.

[2] J.-C. Belfiore, G. Rekaya, and E. Viterbo. The goldencode: A 2 x 2 full-rate space-time code with non-vanishing determinants. 2004.

[3] M. O. Damen, A. Tewfik, and J. C. Belfiore. A construction of a space-time code based on number theory. *IEEE Trans. Inform. Theory*, 48:753–760, Mar 2002.

[4] A. FrÖlich and M. Talylor. *Algebraic Number Theory*. Cambridge University Press, 1991.

[5] D. Gesbert, M. Shafi, D. shan Shiu, P. J. Smith, and A. Naguib. From theory to practice: An overview of mimo space–time coded wireless systems. *IEEE Journal on Selected Areas in Communications*, 21(3):281–302, Apr 2003.

[6] K. Hao. Untitled draft. 2004.

[7] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo. Perfect space time block codes. 2004.

[8] L. Poo. Space-time coding for wireless communication: A survey.

[9] L. Yang and G. B. Giannakis. Analog space-time coding for multi-antenna ultra-wideband transmissions. *IEEE Trans. on Communications*, 52(3):507–517, Mar 2004.