Construction of Space-Time Block Codes from a Decoding Point of View

Kenneth Tay
Junior Independent Work
Fall 2008
Advisor: Prof. Robert Calderbank
Dept. of Mathematics
Princeton University

January 9, 2009

Abstract

Perfect space-time block codes (STBCs) were first introduced by Oggier et al. to have full rate, full diversity and non-vanishing determinant. These perfect STBCs were constructed with the use of cyclic division algebras. Sirianunpiboon et al. present a decoding algorithm for STBCs with essentially Maximum Likelihood (ML) performance along with an identity which, when satisfied by the STBC, makes decoding via this algorithm computationally easier. The aim of this work is to develop STBCs from the point of view of the decoder i.e. finding STBCs that satisfy the identity given by Sirianunpiboon et al.

1 Introduction

Coding theory was developed to address the problem of transmitting information accurately over noisy channels. When an antenna sends a signal to

a receiver, it gets distorted due to a variety of reasons e.g. attenuation. The receiver faces the challenge of recovering the original signal given the received signal. Coding theory addresses this in a number of ways. The most common solution is for the sender to send signals from a certain codebook (the signals are called "codewords"). The codewords are chosen such that they are "far apart" in terms of a certain notion of distance. The receiver then decodes the received signal as the codeword in the codebook that it is "closest" to. The receiver's algorithm is also known as "maximum likelihood decoding".

When coding theory was first developed, the codewords used were vectors, but in 1998 Tarokh et al. proposed a system called "space-time coding" [6]. In this system, the reliability of the information sent could be increased by either using multiple communication channels with different characteristics (also known as a "diversity scheme"), or by employing multiple antennas at both the transmitter and the receiver (also known as the "multiple-input multiple-output (MIMO) system"). In both these schemes, the codewords used are matrices.

The first space-time block code (STBC) that was published was the Alamouti scheme, published in 1998 [1]. Since then, many STBCs have been constructed with the use of algebraic objects, most notably via division algebras. In 2007, Oggier et al. published a paper detailing how cyclic division algebras could be used to construct such codes, as well as detailing examples of perfect STBCs for two to six antennas [4]. In 2008, Sirianunpiboon et al. published a paper presenting a fast essentially maximum likelihood decoding algorithm for the Golden Code (a 2×2 perfect STBC) [5]. Howard et al. noticed that if an STBC satisfied a certain identity, that made the STBC more desirable in terms of the availability of a faster decoding algorithm [3].

The aim of this paper is to develop STBCs that satisfy the identity given in [3] that hopefully have other desirable properties as well.

The rest of the paper is organized as follows. Section 2 gives an overview of the MIMO system and the definition of an STBC along with some properties that make an STBC more desirable. Section 3 gives a short overview of the work of Oggier et al. [4], Sirianunpiboon et al. [5] and Howard et al. [3], which provides the background for this work. In section 3 we also present a generalization of the identity given in [3] (which we henceforth call the "decoding identity"). The goal of section 4 is to use the background

provided in section 3 to derive necessary and sufficient conditions for an STBC to satisfy the decoding identity. Section 5 provides an $n \times n$ STBC which satisfies the conditions laid out in section 4, along with some analysis. Findings and future directions for research are summarized in the conclusion, in section 6.

Note: Throughout this paper, we will let I_k denote the $k \times k$ identity matrix, and $\zeta_k = e^{\frac{2\pi i}{k}}$.

2 An Introduction to Space-Time Block Codes (STBCs)

Refer to [2] or [4] for a more complete introduction to STBCs.

2.1 The Multiple-Input Multiple-Output System

In one time segment, a single transmit antenna sends one signal, which is modeled as a complex number $x \in \mathbb{C}$. The signal travels to the antenna at the receiver through some channel. While passing through the channel the signal gets distorted, and this is modeled by multiply x by some $h \in \mathbb{C}$, which is known as the "channel gain" or "fade coefficient". Finally the signal picks up some noise z at the receiver itself, assumed to be additive noise. As such, the received signal is $y = hx + z$.

Now consider a system with n_t transmit antennas and n_r receive antennas. If we let h_{ij} denote the channel gain between the jth transmit and ith receive antennas, then the received signal at the ith receive antenna is

$$y_i = \sum_{j=1}^{n_t} h_{ij} x_j + z_i,$$

where z_i is the additive noise at the ith receive antenna, often modeled as a complex Gaussian variable with zero mean.

If, in addition, we assume that the channel is "quasi-static", i.e. the channel gains h_{ij} remain essentially constant over T time segments, we can use matrix

notation to express the received signals at all the receive antennas over T time segments:

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \mathbf{X}_{n_t \times T} + \mathbf{Z}_{n_r \times T}.$$

2.2 Space-Time Block Codes

Definition 2.1. A space-time block code (STBC) is a finite set $\mathcal{C}$ of $n_t \times T$ complex matrices $\mathbf{X}$ (with n_t, T and $\mathbf{X}$ as defined in the previous section).

The entries of a codeword $\mathbf{X} \in \mathcal{C}$ are usually chosen from a finite subset of the complex numbers, called a "signal constellation" $S \subset \mathbb{C}$. Common constellations are the M-QAM constellations (M points in the $\mathbb{Z}[i]$ lattice arranged in a square about the origin), and the M-HEX constellations (M points from the $\mathbb{Z}[\zeta]$ lattice, where $\zeta = e^{\frac{2\pi i}{3}}$).

The definition above allows a wide range of subsets of $\mathbb{C}$ to form STBCs. However, for STBCs to be useful in reality, they must have some sort of algebraic structure. Often, it is useful for the codebook $\mathcal{C}$ to be part of a subring of $\mathrm{GL}_n(\mathbb{C})$. As such, the following approach is often taken: we look for an infinite code $\mathcal{C}_\infty \subseteq \mathbb{C}$ with desirable properties, then we choose $\mathcal{C}$ to be a finite subgroup of $\mathcal{C}_\infty$.

In this paper, we will only be concerned with square STBCs, i.e. $n_t = T$.

There are several properties that make STBCs more desirable: [2] and [4] list some of them. We only provide the two that are relevant to this work:

1. **Full diversity.** For square STBCs, full diversity is obtained if the determinant of the difference of any two distinct codewords is nonzero, i.e.
$$\mathbf{X}_i \neq \mathbf{X}_j \in C \quad \Rightarrow \quad \det(\mathbf{X}_i - \mathbf{X}_j) \neq 0.$$
2. **Minimum determinant.** The coding gain for an STBC is given by the minimum determinant
$$\min_{\mathbf{X}_i \neq \mathbf{X}_j \in C} |\det(\mathbf{X}_i - \mathbf{X}_j)|^2.$$
A larger minimum determinant makes an STBC more desirable.

3 Overview of Previous Work Done

3.1 Construction of STBCs from Cyclic Division Algebras

[4] details the construction of perfect STBCs with the use of cyclic division algebras. The Golden code was presented as a worked example of such an STBC.

It was noticed that $\{1, \tau\}$ (where $\tau = \frac{1+\sqrt{5}}{2}$) was a $\mathbb{Z}[i]$-basis for $\mathcal{O}_L$, where $L = \mathbb{Q}(i, \sqrt{5})$. As such, a 2×2 STBC could be constructed using the extension $L/\mathbb{Q}(i)$, with codewords of the form

$$\begin{pmatrix} a & c \\ ic & a \end{pmatrix} + \begin{pmatrix} \tau & \\ & \sigma(\tau) \end{pmatrix} \begin{pmatrix} b & d \\ id & b \end{pmatrix} = \begin{pmatrix} a & c \\ ic & a \end{pmatrix} + \begin{pmatrix} \tau & \\ & \mu \end{pmatrix} \begin{pmatrix} b & d \\ id & b \end{pmatrix}$$

where σ is the generator of $\mathrm{Gal}(L/\mathbb{Q}(i))$, and $\mu = \frac{1-\sqrt{5}}{2}$.

This construction can be generalized to obtain $n \times n$ codewords: Let L/K be a Galois extension of degree n such that its Galois group is cyclic, with generator σ. Let $\gamma \in K$ be non-zero such that $0 \neq \gamma, \gamma^2, \ldots, \gamma^{n-1} \in K$ are not a norm of some element of L. Then the set of matrices

$$\begin{pmatrix} x_1 & \gamma\sigma(x_n) & \gamma\sigma^2(x_{n-1}) & \ldots & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \gamma\sigma^2(x_n) & \ldots & \gamma\sigma^{n-1}(x_3) \\ \vdots & & \vdots & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \ldots & \gamma\sigma^{n-1}(x_n) \\ x_n & \sigma(x_{n-1}) & \sigma^2(x_{n-2}) & \ldots & \sigma^{n-1}(x_1) \end{pmatrix}^T,$$

with $x_1, \ldots, x_n \in L$ form an STBC.

Now, let us assume that $x_1, \ldots, x_n \in \mathcal{O}_L$. Let $\{\theta_{11}, \theta_{21}, \ldots, \theta_{n1}\}$ be an integral basis for $\mathcal{O}_L$. For $i = 1, \ldots, n$, let

$$x_i = \sum_{k=1}^{n} \theta_{k1} x_{ki},$$

with the x_{ki}'s in $\mathcal{O}_K$. If for each $i = 1, \ldots, n$ and $j = 1, \ldots, n$, we let $\theta_{ij} = \sigma^{j-1}(\theta_{i1})$, then

$$\begin{aligned}
\sigma^{j-1}(x_i) &= \sigma^{j-1}\left(\sum_{k=1}^{n} \theta_{k1} x_{ki}\right) \\
&= \sum_{k=1}^{n} \sigma^{j-1}(\theta_{k1} x_{ki}) \\
&= \sum_{k=1}^{n} x_{ki} \sigma^{j-1}(\theta_{k1}) \quad \text{(as the } x_{ki}\text{'s lie in the base field)} \\
&= \sum_{k=1}^{n} \theta_{kj} x_{ki}.
\end{aligned}$$

As such, we can write the codewords in the following form:

$$\begin{aligned}
\mathbf{X} &= \begin{pmatrix}
\sigma^0(x_1) & \sigma^0(x_2) & \sigma^0(x_3) & \ldots & \sigma^0(x_n) \\
\gamma\sigma^1(x_n) & \sigma^1(x_1) & \sigma^1(x_2) & \ldots & \sigma^1(x_{n-1}) \\
\gamma\sigma^2(x_{n-1}) & \gamma\sigma^2(x_n) & \sigma^2(x_1) & \ldots & \sigma^2(x_{n-2}) \\
\vdots & \vdots & \vdots & & \vdots \\
\gamma\sigma^{n-1}(x_2) & \gamma\sigma^{n-1}(x_3) & \gamma\sigma^{n-1}(x_4) & \ldots & \sigma^{n-1}(x_1)
\end{pmatrix} \\
&= \sum_{i=1}^{n} \begin{pmatrix}
\theta_{i1}x_{i1} & \theta_{i1}x_{i2} & \theta_{i1}x_{i3} & \ldots & \theta_{i1}x_{in} \\
\gamma\theta_{i2}x_{in} & \theta_{i2}x_{i1} & \theta_{i2}x_{i2} & \ldots & \theta_{i2}x_{i(n-1)} \\
\gamma\theta_{i3}x_{i(n-1)} & \gamma\theta_{i3}x_{in} & \theta_{i3}x_{i1} & \ldots & \theta_{i3}x_{i(n-2)} \\
\vdots & \vdots & \vdots & & \vdots \\
\gamma\theta_{in}x_{i2} & \gamma\theta_{in}x_{i3} & \gamma\theta_{in}x_{i4} & \ldots & \theta_{in}x_{i1}
\end{pmatrix} \\
&= \sum_{i=1}^{n} \begin{pmatrix}
\theta_{i1} & & & & \\
& \theta_{i2} & & & \\
& & \theta_{i3} & & \\
& & & \ddots & \\
& & & & \theta_{in}
\end{pmatrix} \begin{pmatrix}
x_{i1} & x_{i2} & x_{i3} & \ldots & x_{in} \\
\gamma x_{in} & x_{i1} & x_{i2} & \ldots & x_{i(n-1)} \\
\gamma x_{i(n-1)} & \gamma x_{in} & x_{i1} & \ldots & x_{i(n-2)} \\
\vdots & \vdots & \vdots & & \vdots \\
\gamma x_{i2} & \gamma x_{i3} & \gamma x_{i4} & \ldots & x_{i1}
\end{pmatrix}.
\end{aligned}$$

3.2 The Decoding Identity for the Golden Code

[5] analyzes two different decoding algorithms for the Golden code: exact ML decoding and a quadratic algorithm that gives essentially ML performance. We give a quick sketch of the process, placing emphasis on the parts which will be relevant to this paper.

Codewords from the Golden Code have the following form:

$$\begin{pmatrix} x_1 & x_3 \\ ix_3 & x_1 \end{pmatrix} + \begin{pmatrix} \tau & \\ & \mu \end{pmatrix} \begin{pmatrix} x_2 & x_4 \\ ix_4 & x_2 \end{pmatrix},$$

with $\tau = \frac{1+\sqrt{5}}{2}, \tau\mu = -1$. The view at the receiver is given by

$$(r_{11}, r_{12}) = (x_1, x_3) \begin{pmatrix} h_{11} & h_{21} \\ ih_{21} & h_{11} \end{pmatrix} + (x_2, x_4) \begin{pmatrix} h_{11}\tau & h_{21}\mu \\ ih_{21}\mu & h_{11}\tau \end{pmatrix} + (n_{11}, n_{12}),$$

$$(r_{21}, r_{22}) = (x_1, x_3) \begin{pmatrix} h_{12} & h_{22} \\ ih_{22} & h_{12} \end{pmatrix} + (x_2, x_4) \begin{pmatrix} h_{12}\tau & h_{22}\mu \\ ih_{22}\mu & h_{12}\tau \end{pmatrix} + (n_{21}, n_{22}),$$

where n_{11}, n_{12}, n_{21} and n_{22} are complex Gaussian random variables with zero mean and covariance $2\sigma^2 I_2$, modeling noise in the channels.

For simplicity, introduce the following matrices:

$$h = \begin{pmatrix} h_{11} & h_{21} \\ ih_{21} & h_{11} \end{pmatrix}, \quad \tilde{h} = \begin{pmatrix} h_{11}\tau & h_{21}\mu \\ ih_{21}\mu & h_{11}\tau \end{pmatrix}$$

$$g = \begin{pmatrix} h_{12} & h_{22} \\ ih_{22} & h_{12} \end{pmatrix}, \quad \tilde{g} = \begin{pmatrix} h_{12}\tau & h_{22}\mu \\ ih_{22}\mu & h_{12}\tau \end{pmatrix}$$

$$H = (h, g), \quad \tilde{H} = (\tilde{h}, \tilde{g})$$

Let $\mathbf{s} = (x_1, x_3),\ \mathbf{c} = (x_2, x_4)$. Then the likelihood function of $\mathbf{s}$ and $\mathbf{c}$ given the received signal $\mathbf{r}$ is given by

$$p(\mathbf{r}|\mathbf{s}, \mathbf{c}) \propto \exp\left(-\frac{1}{2\sigma^2} ||\mathbf{r} - \mathbf{s}H - \mathbf{c}\tilde{H}||^2 \right).$$

Taking the prior distribution of the symbols $\mathbf{s}$ and $\mathbf{c}$ to be uniform on the constellation $\mathcal{C}$ from which we draw our x_i's, we have the ML estimate given by:

$$(\hat{\mathbf{s}}, \hat{\mathbf{c}}) = \underset{\mathbf{s},\mathbf{c} \in C^2}{\operatorname{argmax}} p(\mathbf{r}|\mathbf{s}, \mathbf{c}).$$

In essence, exact ML decoding looks at the likelihood function $p(\mathbf{r}|x_1, X)$, where $X = (x_2, x_3, x_4)$. This likelihood is maximized with respect to x_1, given X, giving maximizer $\hat{x}_1(X)$. Then, the resulting partially optimized likelihood is maximized with respect to X, to give maximizer $\hat{X}$. The exact ML solution is obtained: $(x_1, x_2, x_3, x_4) = (\hat{x}_1(\hat{X}), \hat{X})$. This algorithm is $O(N^3)$, where N is the size of the QAM constellation that is in use.

The details for the quadratic algorithm that gives essentially ML performance are complicated and largely irrelevant to this paper. Instead of looking at the likelihood function $p(\mathbf{r}|x_1, X)$, this algorithm looks at the likelihood function $p(\mathbf{r}|\mathbf{s}, \mathbf{c})$ and performs roughly the same steps as the exact ML decoding algorithm.

It can be verified for the Golden Code that $HH^\dagger + \tilde{H}\tilde{H}^\dagger$ is a multiple of the identity. This is the decoding identity that makes the quadratic algorithm work well. We wish to study this decoding identity and find STBCs that satisfy this particular identity.

We conclude this subsection with a lemma that will be useful in understanding the identity above.

Lemma 3.1. $HH^\dagger + \tilde{H}\tilde{H}^\dagger$ is a multiple of $I_2 \Leftrightarrow hh^\dagger + \tilde{h}\tilde{h}^\dagger$ is a multiple of I_2.

Proof. Note that $HH^\dagger + \tilde{H}\tilde{H}^\dagger = (hh^\dagger + \tilde{h}\tilde{h}^\dagger) + (gg^\dagger + \tilde{g}\tilde{g}^\dagger)$. As the h_{ij}'s are to be viewed as indeterminates and $hh^\dagger + \tilde{h}\tilde{h}^\dagger$ and $gg^\dagger + \tilde{g}\tilde{g}^\dagger$ involve different h_{ij}'s in their expressions, it means that

$$HH^\dagger + \tilde{H}\tilde{H}^\dagger \text{ multiple of } I \Rightarrow hh^\dagger + \tilde{h}\tilde{h}^\dagger \text{ multiple of } I, gg^\dagger + \tilde{g}\tilde{g}^\dagger \text{ multiple of } I.$$

However, h ($\tilde{h}$ resp.) looks exactly the same as g ($\tilde{g}$ resp.), except the indeterminates have been switched: h_{11} and h_{21} in h have been replaced with h_{12} and h_{22} in g. This means that

$$hh^\dagger + \tilde{h}\tilde{h}^\dagger \text{ multiple of } I \Leftrightarrow gg^\dagger + \tilde{g}\tilde{g}^\dagger \text{ multiple of } I.$$

Thus,

$$hh^\dagger + \tilde{h}\tilde{h}^\dagger \text{ multiple of } I \Leftrightarrow HH^\dagger + \tilde{H}\tilde{H}^\dagger \text{ multiple of } I.$$

□

3.3 The Decoding Identity for an $n \times n$ Code

[3] walks through the same process as [5] for a 3×3 perfect STBC instead of the Golden code. Let H_1, H_2, H_3 be the 3×3 analogues for H and $\tilde{H}$ of the Golden code. It was noted that the identity

$$H_1 H_1^\dagger + H_2 H_2^\dagger + H_3 H_3^\dagger = kI_3,$$

where k is a constant, formed the basis for the fast decoding algorithm presented later in the paper.

We call the natural extension of this identity to the $n \times n$ case the "decoding identity":

$$\sum_{i=1}^{n} H_i H_i^\dagger = kI_n \tag{1}$$

where k is some constant, and the H_i's are the $n \times n$ analogues of H and $\tilde{H}$ of the Golden code.

Next, we derive explicit expressions for the n-dimensional analogues of h and $\tilde{h}$ (we do not need to do so for the n-dimensional analogues of H and $\tilde{H}$, as we will see later). Ignoring noise, the view at the transmitter for the first receiver is:

$$(r_{11}, r_{12}, \ldots, r_{1n}) = (h_{11}, h_{21}, \ldots, h_{n1}) \sum_{i=1}^{n} \begin{pmatrix} \theta_{i1} & & & \\ & \theta_{i2} & & \\ & & \ddots & \\ & & & \theta_{in} \end{pmatrix} \begin{pmatrix} x_{i1} & x_{i2} & \ldots & x_{in} \\ \gamma x_{in} & x_{i1} & \ldots & x_{i(n-1)} \\ \gamma x_{i(n-1)} & \gamma x_{in} & \ldots & x_{i(n-2)} \\ \vdots & \vdots & & \vdots \\ \gamma x_{i2} & \gamma x_{i3} & \ldots & x_{i1} \end{pmatrix}$$

$$= \sum_{i=1}^{n} (\theta_{i1} h_{11}, \theta_{i2} h_{21}, \ldots, \theta_{in} h_{n1}) \begin{pmatrix} x_{i1} & x_{i2} & \ldots & x_{in} \\ \gamma x_{in} & x_{i1} & \ldots & x_{i(n-1)} \\ \gamma x_{i(n-1)} & \gamma x_{in} & \ldots & x_{i(n-2)} \\ \vdots & \vdots & & \vdots \\ \gamma x_{i2} & \gamma x_{i3} & \ldots & x_{i1} \end{pmatrix},$$

At the receiver itself, we have:

$$(r_{11}, r_{12}, \ldots, r_{1n}) = \sum_{i=1}^{n} (x_{i1}, x_{i2}, \ldots, x_{in}) \begin{pmatrix} \theta_{i1}h_{11} & \theta_{i2}h_{21} & \ldots & \theta_{in}h_{n1} \\ \gamma\theta_{in}h_{n1} & \theta_{i1}h_{11} & \ldots & \theta_{i(n-1)}h_{(n-1)1} \\ \gamma\theta_{i(n-1)}h_{(n-1)1} & \gamma\theta_{in}h_{n1} & \ldots & \theta_{i(n-2)}h_{(n-2)1} \\ \vdots & \vdots & & \vdots \\ \gamma\theta_{i2}h_{21} & \gamma\theta_{i3}h_{31} & \ldots & \theta_{i1}h_{11} \end{pmatrix}.$$

As such, the analogues of h and $\tilde{h}$ for the $n \times n$ case are

$$h_i = \begin{pmatrix} \theta_{i1}h_{11} & \theta_{i2}h_{21} & \ldots & \theta_{in}h_{n1} \\ \gamma\theta_{in}h_{n1} & \theta_{i1}h_{11} & \ldots & \theta_{i(n-1)}h_{(n-1)1} \\ \gamma\theta_{i(n-1)}h_{(n-1)1} & \gamma\theta_{in}h_{n1} & \ldots & \theta_{i(n-2)}h_{(n-2)1} \\ \vdots & \vdots & & \vdots \\ \gamma\theta_{i2}h_{21} & \gamma\theta_{i3}h_{31} & \ldots & \theta_{i1}h_{11} \end{pmatrix}, \quad \text{for } i = 1, 2, \ldots, n.$$

Notice that the relevant expressions for the other receivers are almost exactly the same, and only differ from each other in the same way that h and g differed for the Golden code (i.e. the labels of the indeterminates were switched). As such, (1) can be reduced to

$$\sum_{i=1}^{n} h_i h_i^{\dagger} = kI_n, \quad k \text{ constant.} \tag{2}$$

The proof of this reduction is similar to the proof of Lemma 3.1. We will refer to both (1) and (2) as the "decoding identity". There will be no confusion as the two equations are equivalent.

4 Finding Conditions on STBCs satisfying the Decoding Identity

In this section we want to find necessary and sufficient conditions for STBCs to satisfy the decoding identity. Following [4], we seek to find STBCs satis-

fying the decoding identity of the form

$$\sum_{i=1}^{n} \begin{pmatrix} \theta_{i1} & & & & \\ & \theta_{i2} & & & \\ & & \theta_{i3} & & \\ & & & \ddots & \\ & & & & \theta_{in} \end{pmatrix} \begin{pmatrix} x_{i1} & x_{i2} & x_{i3} & \dots & x_{in} \\ \gamma x_{in} & x_{i1} & x_{i2} & \dots & x_{i(n-1)} \\ \gamma x_{i(n-1)} & \gamma x_{in} & x_{i1} & \dots & x_{i(n-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ \gamma x_{i2} & \gamma x_{i3} & \gamma x_{i4} & \dots & x_{i1} \end{pmatrix}.$$

Unlike [4], however, we do not place any restrictions on the θ_{ij}'s and on γ, i.e. the only restriction we have is that $\gamma, \theta_{ij} \in \mathbb{C} \setminus \{0\}$, for $i, j = 1, \dots, n$.

Let $\mathbf{H} = \sum_{i=1}^{n} h_i h_i^{\dagger}$. Consider the diagonal entries of $\mathbf{H}$. For $j = 1, 2, \dots, n$,

$$\begin{aligned} (h_i h_i^{\dagger})_{jj} &= (|\theta_{i1} h_{11}|^2 + |\theta_{i2} h_{21}|^2 + \cdots + |\theta_{i(n+1-j)} h_{(n+1-j)1}|^2) \\ &\quad + |\gamma|^2 (|\theta_{i(n+2-j)} h_{(n+2-j)1}|^2 + \cdots + |\theta_{in} h_{n1}|^2) \quad \text{for } i = 1, \dots, n, \\ (\mathbf{H})_{jj} &= \sum_{i=1}^{n} (h_i h_i^{\dagger})_{jj} \\ &= \left(|h_{11}|^2 \sum_{i=1}^{n} |\theta_{i1}|^2 + \cdots + |h_{(n+1-j)1}|^2 \sum_{i=1}^{n} |\theta_{i(n+1-j)}|^2 \right) \\ &\quad + \left(|h_{(n+2-j)1}|^2 |\gamma|^2 \sum_{i=1}^{n} |\theta_{i(n+2-j)}|^2 + \cdots + |h_{n1}|^2 |\gamma|^2 \sum_{i=1}^{n} |\theta_{in}|^2 \right). \end{aligned}$$

In order for $\mathbf{H}$ to be a multiple of the identity, we must have $(\mathbf{H})_{jj}$ equal for all j. As the h_{i1}'s are indeterminates, we must have the coefficients of each $|h_{i1}|^2$ be the same in each of $(\mathbf{H})_{jj}$. In particular, considering the coefficient of $|h_{n1}|^2$ in $(\mathbf{H})_{11}$ and $(\mathbf{H})_{nn}$, we have

$$\sum_{i=1}^{n} |\theta_{in}|^2 = |\gamma|^2 \sum_{i=1}^{n} |\theta_{in}|^2 \quad \Rightarrow \quad |\gamma| = 1 \text{ (as } \theta_{ij}\text{'s are non-zero).}$$

It is clear that $|\gamma| = 1$ guarantees that the diagonal entries of $\mathbf{H}$ are all equal. As such, we have the following lemma:

Lemma 4.1. Diagonal entries of $\mathbf{H}$ are all equal $\Leftrightarrow |\gamma| = 1$.

From now on, assume that $|\gamma| = 1$. Introduce the matrix

$$Z = \begin{pmatrix} 0 & I_{n-1} \\ \gamma & 0 \end{pmatrix} = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ \gamma & & & & \end{pmatrix}.$$

Z has two properties that we will find useful:

1. Z is unitary i.e. $Z^{-1} = Z^\dagger$.
2. $Z^n = \gamma I_n$.

The first property is clear from inspection. Below is the proof for the second property.

Proof. Let Z be the matrix representation of some linear transformation T acting from V to V, where V is some n-dimensional vector space, with respect to basis $\{a_1, \ldots, a_n\}$. Then for each $i = 1, \ldots, n$,

$$\begin{aligned} T^n(a_i) &= T^{n-i+1}(T^{i-1}(a_i)) \\ &= T^{n-i+1}(a_1) \\ &= T^{n-i}(\gamma a_n) \\ &= \gamma a_i. \end{aligned}$$

The conclusion follows immediately. □

Using the fact that $Z^\dagger = Z^{-1}$, for each i, we have:

$$\begin{aligned} h_i &= \theta_{i1} h_{11} I + \theta_{i2} h_{21} Z + \cdots + \theta_{in} h_{n1} Z^{n-1}, \\ h_i^\dagger &= \bar{\theta}_{i1} \bar{h}_{11} I + \bar{\theta}_{i2} \bar{h}_{21} Z^{-1} + \cdots + \bar{\theta}_{in} \bar{h}_{n1} Z^{-(n-1)}, \end{aligned}$$

Now, using $I = \gamma^{-1}Z^n$, for $i = 1, \ldots, n$,

$$\begin{aligned} h_i h_i^\dagger = &(|\theta_{i1}|^2|h_{11}|^2 + |\theta_{i2}|^2|h_{21}|^2 + \cdots + |\theta_{in}|^2|h_{n1}|^2)I \\ &+ (\bar{\theta}_{i1}\theta_{i2}\bar{h}_{11}h_{21} + \bar{\theta}_{i2}\theta_{i3}\bar{h}_{21}h_{31} + \cdots + \bar{\theta}_{i(n-1)}\theta_{in}\bar{h}_{(n-1)1}h_{n1} + \gamma^{-1}\bar{\theta}_{in}\theta_{i1}\bar{h}_{n1}h_{11})Z \\ &+ (\bar{\theta}_{i1}\theta_{i3}\bar{h}_{11}h_{31} + \cdots + \bar{\theta}_{i(n-2)}\theta_{in}\bar{h}_{(n-2)1}h_{n1} + \gamma^{-1}\bar{\theta}_{i(n-1)}\theta_{i1}\bar{h}_{(n-1)1}h_{11} + \gamma^{-1}\bar{\theta}_{in}\theta_{i2}\bar{h}_{n1}h_{21})Z^2 \\ &\ \vdots \\ &+ (\bar{\theta}_{i1}\theta_{in}\bar{h}_{11}h_{n1} + \gamma^{-1}\bar{\theta}_{i2}\theta_{i1}\bar{h}_{21}h_{11} + \cdots + \gamma^{-1}\bar{\theta}_{in}\theta_{i(n-1)}\bar{h}_{n1}h_{(n-1)1})Z^{n-1}. \end{aligned}$$

First, note that when we sum up $h_i h_i^\dagger$ over i, we are just adding summation signs, from 1 to n, in front of each coefficient of Z^k (k from 0 to $n-1$). Second, note that for any i and j such that $0 \leq i, j \leq n-1$, $i \neq j$, $\nexists\, p, q$ such that both $(Z^i)_{pq}$ and $(Z^j)_{pq}$ are nonzero. This means that in order for the off-diagonal entries of $\mathbf{H}$ to all be zero, we must have the coefficient of Z^k in the Z-expansion of $\mathbf{H}$ equal to zero for $k = 1, \ldots, n$. Finally, as the $\bar{h}_{i1}h_{j1}$'s are considered indeterminates, in order for $\mathbf{H}$ to be a multiple of the identity, we must have

$$\sum_{i=1}^{n} \bar{\theta}_{ij}\theta_{ik} = 0 \quad \forall\, j \neq k. \tag{3}$$

The converse is trivially true. In summary, we have the following theorem:

Theorem 4.2.

$$\mathbf{H} \text{ a multiple of the identity} \quad \Leftrightarrow \quad \begin{cases} |\gamma| = 1 \\ \sum_{i=1}^{n} \bar{\theta}_{ij}\theta_{ik} = 0 \quad \forall\, j \neq k. \end{cases}$$

5 Example of an STBC satisfying the Decoding Property

We present an STBC that satisfies the right-hand side of Theorem 4.2 is a particularly nice way.

Let $\zeta = e^{\frac{2\pi i}{n}}$. For $j = 1, \ldots, n$, and $k = 1, \ldots, n$, let

$$\theta_{jk} = \alpha_j \zeta^{(j-1)(k-1)},$$

with $\alpha_j \in \mathbb{C}, |\alpha_j| = M$ for all j, for some $M \in \mathbb{R}^+$.

Claim 5.1. An STBC with θ_{jk}'s as defined above, and with any $\gamma \in \mathbb{C}$ such that $|\gamma| = 1$, satisfies the right-hand side of Theorem 4.2, and hence satisfies the decoding identity.

Proof. We only have the prove the second condition on the right-hand side i.e. the condition involving the θ_{jk}'s.

For any j and k such that $j \neq k$,

$$\begin{aligned}
\sum_{i=1}^{n} \bar{\theta}_{ij}\theta_{ik} &= \sum_{i=1}^{n} \overline{\alpha_i \zeta^{(i-1)(j-1)}} \cdot \alpha_i \zeta^{(i-1)(k-1)} \\
&= \sum_{i=1}^{n} (\bar{\alpha}_i \cdot \alpha_i) \zeta^{(i-1)(1-j)} \zeta^{(i-1)(k-1)} \\
&= \sum_{i=1}^{n} M^2 (\zeta^{k-j})^{i-1} \qquad (\text{as } |\alpha_i| = M \text{ for all } i) \\
&= 0 \qquad (\text{as } k-j \neq 0 \text{ and } \zeta^{k-j} \text{ is an } n^{\text{th}} \text{ root of unity} \neq 1).
\end{aligned}$$

□

Some remarks regarding the proof above are in order:

1. The proof above did not require any restrictions on the α_i's except that they are all of the same length. If we require $\theta_{1j} = 1$ for all j, set $\alpha_1 = 1$.

2. The proof above would still work if $\zeta = e^{\frac{2\pi i}{n}}$ is replaced with any primitive n^{th} root of unity. (3) would not hold if we replaced ζ with an n^{th} root of unity that does not generate all n^{th} roots of unity (i.e. a non-primitive n^{th} root of unity).

3. The solution above has been constructed such that the proof of it sat-

isfying (3) is straightforward. For this solution, for all j,

$$\begin{aligned}
\bar{\theta}_{j1}\theta_{j2} = \bar{\theta}_{j2}\theta_{j3} = \cdots = \bar{\theta}_{jn}\theta_{j1} &= \zeta^{j-1} \\
\bar{\theta}_{j1}\theta_{j3} = \bar{\theta}_{j2}\theta_{j4} = \cdots = \bar{\theta}_{jn}\theta_{j2} &= \zeta^{2(j-1)} \\
\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad & \vdots \\
\bar{\theta}_{j1}\theta_{jn} = \bar{\theta}_{j2}\theta_{j1} = \cdots = \bar{\theta}_{jn}\theta_{j(n-1)} &= \zeta^{(n-1)(j-1)}.
\end{aligned}$$

A natural question to ask is whether there are other codes which satisfy (3) and having $|\gamma| = 1$. The answer is yes: for instance, the 3×3 STBC presented in [3] and [4] is one such code.

5.1 Bounding $\det(\mathbf{X}_i - \mathbf{X}_j)$ from Below

A technique used in [4] to show that $\det(\mathbf{X}_i - \mathbf{X}_j)$ is bounded from below was to show that for any codeword $\mathbf{X} \in \mathcal{C}$, $\det \mathbf{X}$ lay in the integer ring of a field. As such, if the code is fully diverse (i.e. $\mathbf{X} \neq \mathbf{0} \Rightarrow \det \mathbf{X} \neq 0$), a bound on $\det(\mathbf{X}_i - \mathbf{X}_j)$ from below follows immediately.

In this section, we wish to find a cyclic extension E/F of degree n, α_i's and γ such that for all $\mathbf{X} \in \mathcal{C}$, $\det \mathbf{X}$ lies in $\mathcal{O}_F$ whenever the x_{ij}'s all lie in $\mathcal{O}_F$.

We begin by proving the following lemma:

Lemma 5.2. Let $n \geq 2$. Then, for $a_{ij} \in \mathbb{C}$ for $i, j = 1, \ldots, n$, and $\gamma \in \mathbb{C}$,

$$\det \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1(n-1)} & a_{1n} \\ \gamma a_{21} & a_{22} & \ldots & a_{2(n-1)} & a_{2n} \\ \gamma a_{31} & \gamma a_{32} & \ldots & a_{3(n-1)} & a_{3n} \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma a_{n1} & \gamma a_{n2} & \ldots & \gamma a_{n(n-1)} & a_{nn} \end{pmatrix} = \det \begin{pmatrix} a_{22} & a_{23} & \ldots & a_{2n} & a_{21} \\ \gamma a_{32} & a_{33} & \ldots & a_{3n} & a_{31} \\ \gamma a_{42} & \gamma a_{43} & \ldots & a_{4n} & a_{41} \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma a_{12} & \gamma a_{13} & \ldots & \gamma a_{1n} & a_{11} \end{pmatrix}.$$

Proof.

$$\det\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \gamma a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ \gamma a_{(n-1)1} & \gamma a_{(n-1)2} & \dots & a_{(n-1)n} \\ \gamma a_{n1} & \gamma a_{n2} & \dots & a_{nn} \end{pmatrix} = (-1)^{n-1}\det\begin{pmatrix} \gamma a_{21} & a_{22} & \dots & a_{2(n-1)} & a_{2n} \\ \gamma a_{31} & \gamma a_{32} & \dots & a_{3(n-1)} & a_{3n} \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma a_{n1} & \gamma a_{n2} & \dots & \gamma a_{n(n-1)} & a_{nn} \\ a_{11} & a_{12} & \dots & a_{1(n-1)} & a_{1n} \end{pmatrix}$$

$$= (-1)^{2(n-1)}\det\begin{pmatrix} a_{22} & a_{23} & \dots & a_{2n} & \gamma a_{21} \\ \gamma a_{32} & a_{33} & \dots & a_{3n} & \gamma a_{31} \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma a_{n2} & \gamma a_{n3} & \dots & a_{nn} & \gamma a_{n1} \\ a_{12} & a_{13} & \dots & a_{1n} & a_{11} \end{pmatrix}$$

$$= \det\begin{pmatrix} a_{22} & a_{23} & \dots & a_{2n} & \gamma a_{21} \\ \gamma a_{32} & a_{33} & \dots & a_{3n} & \gamma a_{31} \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma a_{n2} & \gamma a_{n3} & \dots & a_{nn} & \gamma a_{n1} \\ a_{12} & a_{13} & \dots & a_{1n} & a_{11} \end{pmatrix}$$

$$\text{Let } A = \begin{pmatrix} a_{22} & a_{23} & \dots & a_{2n} & a_{21} \\ \gamma a_{32} & a_{33} & \dots & a_{3n} & a_{31} \\ \gamma a_{42} & \gamma a_{43} & \dots & a_{4n} & a_{41} \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma a_{12} & \gamma a_{13} & \dots & \gamma a_{1n} & a_{11} \end{pmatrix}, B = \begin{pmatrix} a_{22} & a_{23} & \dots & a_{2n} & \gamma a_{21} \\ \gamma a_{32} & a_{33} & \dots & a_{3n} & \gamma a_{31} \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma a_{n2} & \gamma a_{n3} & \dots & a_{nn} & \gamma a_{n1} \\ a_{12} & a_{13} & \dots & a_{1n} & a_{11} \end{pmatrix}.$$

Notice that each a_{ij} is in the same cell for A and B. Recall the formula

$$\det X = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}.$$

We have

$$\det A = \sum_{\sigma \in S_n} \gamma_\sigma^A \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)},$$

$$\det B = \sum_{\sigma \in S_n} \gamma_\sigma^B \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)},$$

where γ_σ^A (γ_σ^B resp.) is γ to the power of the number of times γ appears in the permutation matrix of σ for A (B resp.). We just have to show that for all σ, $\gamma_\sigma^A = \gamma_\sigma^B$.

Note that for $2 \le i, j \le n$,

$$(a_{ij} \text{ has a } \gamma \text{ before it in A}) \Leftrightarrow (a_{ij} \text{ has a } \gamma \text{ before it in B}).$$

If a_{11} is in the permutation matrix, there is no γ before a_{11} in both A and B. If a_{1j} is in the permutation matrix for some $j > 1$, a_{k1} must be in the permutation matrix for some $k > 1$ (and vice versa). Between the two of them they have one γ before them. As such, $\gamma_\sigma^A = \gamma_\sigma^B$ for all $\sigma \in S_n$. Thus $\det A = \det B$. □

Let the generator of the Galois group of E/F be σ. Then $\det \mathbf{X}$ lies in $\mathcal{O}_F$ if and only if $\det \mathbf{X} = \sigma \det \mathbf{X}$. An easy way to do this is to have, for all $x_{ij} \in \mathcal{O}_F$,

$$\begin{aligned}
\sigma(\alpha_1 x_{1j} + \alpha_2 x_{2j} + \cdots + \alpha_n x_{nj}) &= \alpha_1 x_{1j} + \alpha_2 \zeta x_{2j} + \cdots + \alpha_n \zeta^{n-1} x_{nj} \quad \forall j, \\
\sigma(\alpha_1 x_{1j} + \alpha_2 \zeta x_{2j} + \cdots + \alpha_n \zeta^{n-1} x_{nj}) &= \alpha_1 x_{1j} + \alpha_2 \zeta^2 x_{2j} + \cdots + \alpha_n \zeta^{2(n-1)} x_{nj} \quad \forall j, \\
&\vdots \\
\sigma(\alpha_1 x_{1j} + \alpha_2 \zeta^{n-1} x_{2j} + \cdots + \alpha_n \zeta^{(n-1)^2} x_{nj}) &= \alpha_1 x_{1j} + \alpha_2 x_{2j} + \cdots + \alpha_n x_{nj} \quad \forall j, \\
\gamma \in F, \alpha_1, \ldots, \alpha_n \in \mathcal{O}_E.&
\end{aligned}$$

We can then apply Lemma 5.2 to get $\det \mathbf{X} = \sigma \det \mathbf{X}$. (The above is sufficient is because $\sigma \det(\mathbf{X}_{ij}) = \det(\sigma(\mathbf{X}_{ij}))$.)

There is a natural choice in order for the above identities to be satisfied. Let $E = \mathbb{Q}(\zeta_{n^2})$, $F = \mathbb{Q}(\zeta_n)$, σ such that $\sigma(\zeta_{n^2}) = \zeta_{n^2}^{n+1}$, $\alpha_k = \zeta_{n^2}^{k-1}$ for $k = 1, \ldots, n$, $\gamma = \zeta_n$. We can apply Lemma 5.2 to get the result that $\det \mathbf{X}$ is invariant under σ.

It remains to show that σ generates $\mathrm{Gal}(E/F)$. The proof is given below.

Proof. Consider the fields $\mathbb{Q} \subset \mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_{n^2})$. Extensions $\mathbb{Q}(\zeta_{n^2})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ are Galois extensions with Galois groups $(\mathbb{Z}/n^2\mathbb{Z})^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ respectively. Let Galois extension $\mathbb{Q}(\zeta_{n^2})/\mathbb{Q}(\zeta_n)$ have Galois group H. Then

$$(\mathbb{Z}/n^2\mathbb{Z})^\times / H = (\mathbb{Z}/n\mathbb{Z})^\times.$$

Let $\phi : (\mathbb{Z}/n^2\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\phi(a \pmod{n^2}) = a \pmod{n}$. Then clearly ϕ is a homormophism of groups, and

$$\ker(\phi) = \{kn + 1 \pmod{n^2} | k = 0, \ldots, n-1\}$$

which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Thus $H \cong \ker(\phi) \cong \mathbb{Z}/n\mathbb{Z}$. Note that $\sigma(\zeta_{n^2}^{kn+1}) = \zeta_{n^2}^{(k+1)n+1}$. This means that $\langle\sigma\rangle$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Thus $\langle\sigma\rangle \cong H$. □

Signal constellations are usually not drawn from the lattice $\mathbb{Z}[\zeta_n]$ for general n. However, if $3|n$ or $4|n$, we have $\mathbb{Z}[\zeta_3] \subset \mathbb{Z}[\zeta_n]$ or $\mathbb{Z}[\zeta_4] \subset \mathbb{Z}[\zeta_n]$, in which case we can limit our symbols to QAM- or HEX- symbols.

5.2 $\det \mathbf{X}$ for the 3×3 Codeword

We calculate the determinant for the case of $n = 3$. Write the codewords as

$$\mathbf{X} = \begin{pmatrix} x_1 + \zeta_9 x_2 + \zeta_9^2 x_3 & y_1 + \zeta_9 y_2 + \zeta_9^2 y_3 & z_1 + \zeta_9 z_2 + \zeta_9^2 z_3 \\ \zeta_9^3(z_1 + \zeta_9^4 z_2 + \zeta_9^8 z_3) & x_1 + \zeta_9^4 x_2 + \zeta_9^8 x_3 & y_1 + \zeta_9^4 y_2 + \zeta_9^8 y_3 \\ \zeta_9^3(y_1 + \zeta_9^7 y_2 + \zeta_9^{14} y_3) & \zeta_9^3(z_1 + \zeta_9^7 z_2 + \zeta_9^{14} z_3) & x_1 + \zeta_9^7 x_2 + \zeta_9^{14} x_3 \end{pmatrix},$$

with $x_i, y_i, z_i \in \mathbb{Z}[\zeta_3]$. Then

$$\begin{aligned} \det \mathbf{X} = {} & (x_1^3 + \zeta_3 x_2^3 + \zeta_3^2 x_3^3) + (\zeta y_1^3 + \zeta_3^2 y_2^3 + y_3^3) + (\zeta_3^2 z_1^3 + z_2^3 + \zeta_3 z_3^3) \\ & + 3(1 + \zeta_3^2) x_1 x_2 x_3 + 3(\zeta_3 + 1) y_1 y_2 y_3 + 3(\zeta_3^2 + \zeta_3) z_1 z_2 z_3 \\ & - 3(x_1 y_3 z_2 + x_2 y_1 z_3 + x_3 y_2 z_1) \\ & - 3\zeta_3(x_1 y_2 z_3 + x_2 y_3 z_1 + x_3 y_1 z_2) \\ & - 3(\zeta_3 x_1 y_1 z_1 + \zeta_3^2 x_2 y_2 z_2 + x_3 y_3 z_3). \end{aligned}$$

If $\det \mathbf{X} \neq 0$ whenever $\mathbf{X} \neq \mathbf{0}$, then, together with the results from Section 5.1, we would get a positive lower bound on $\det(\mathbf{X}_i - \mathbf{X}_j)$. Unfortunately, when all the x_i, y_i, z_i are zero except x_1 and y_3, and when $x_1 = -y_3$, we have $\det \mathbf{X} = 0$.

5.3 Linear Combinations of STBCs

Due to the additivity and multiplicativity of the automorphism σ, if we have 2 codebooks $\mathcal{C}_1$ and $\mathcal{C}_2$ such that for any $\mathbf{X} \in \mathcal{C}_1$ and any $\mathbf{Y} \in \mathcal{C}_2$, the equations on page 17 hold, then those same equations will hold as well for $\mathbf{X}+\mathbf{Y}$. This means that once we have some STBCs that satisfy the equations on page 17, they generate a space of solutions to those equations via linear combinations. We can then look for STBCs with non-vanishing determinant from this space.

6 Conclusion

Cyclic division algebras provide a beautiful way to prove the non-vanishing property of the determinant for an STBC by relating each non-zero codeword with a non-zero element of a cyclic division algebra, which is invertible. The computation of a general $n \times n$ determinant is not straightforward, and working with another algebraic object helps us to obtain results on the determinant via an indirect route.

This paper has attempted to develop STBCs with desirable properties (i.e. the decoding property and non-vanishing determinant) directly from the determinant. In the final section of the paper it was noted that while the solution provided in Section 5 does not always produce STBCs with non-vanishing determinant, it is possible that a linear combination of these STBCs would produce an STBC with non-vanishing determinant. Also, in this paper we have only dealt with a narrow scope of solutions that satisfy the identities in Theorem 4.2. There are several other solutions that are important that were not analyzed (e.g. the 3×3 STBC in [3]. This is a direction where future research could be conducted.

Acknowledgements

I would like to thank my advisor, Prof. Robert Calderbank, for his guidance, understanding, and continual support throughout this project.

References

[1] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Select Areas in Communications*, 16:8, 1998.

[2] A. O. F. Hendrickson, "Space-time block codes from cyclic division algebras: An Introduction," available at "http://www.math.wisc.edu/ boston/hendrickson.pdf," 2004.

[3] S. D. Howard, S. Sirianunpiboon and A. R. Calderbank, "Low complexity essentially maximum likelihood decoding of perfect space-time block codes," *Proc. IEEE ICASSP, Taipei, Taiwan*, 2009.

[4] F. Oggier, J.-C. Belfiore and E. Viterbo, "Cyclic division algebras: A tool for space-time coding," *Foundations and Trends in Communications and Information Theory*, 4:1, 2007.

[5] S. Sirianunpiboon, A. R. Calderbank and S. D. Howard, "Fast essentially maximum likelihood decoding of the golden code," *submitted to IEEE Trans. Information Theory*, 2008.

[6] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Information Theory*, 44:2, 1998.

Pledge

This paper represents my own work in accordance with university regulations.

Kenneth Tay