A survey of algebraic unitary codes

Oggier, Frederique

2009

Oggier, F. (2009). A survey of algebraic unitary codes. International Workshop on Coding and Cryptology, 5557, (pp.171-187).

<https://hdl.handle.net/10356/91207>

https://doi.org/10.1007/978-3-642-01877-0_15

International Workshop on Coding and Cryptology (2009) @ copyright 2009 Springer. The original publication is available at
<http://www.springer.com/computer/foundations/book/978-3-642-01813-8>

Downloaded on 26 Apr 2023 18:55:27 SGT

A Survey of Algebraic Unitary Codes

Frédérique Oggier *

Division of Mathematical Sciences,
School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore
`frederique@ntu.edu.sg`

Abstract. This survey paper gives an overview of algebraic unitary codes. It describes the coding problem involved, and present several algebraic approaches yielding interesting constructions, as well as the latest bounds.

1 Introduction

The problem addressed in the design of unitary codes can be summarized shortly: find a family $\mathcal{C}$ of $n \times n$ unitary matrices such that

$$\zeta(\mathcal{C}) = \min_{U \neq U' \in \mathcal{C}} \frac{1}{2} |\det(U - U')|^{1/n} \quad (1)$$

is maximized. The above quantity is called the *diversity product*, and it of course depends on both the dimension n and the cardinality of the code $\mathcal{C}$, that we denote by L . When the diversity product is non-zero, the family $\mathcal{C}$ is called *fully diverse*. We call $R = \frac{1}{n} \log_2(L)$ the rate of the code $\mathcal{C}$.

Similarly to classical coding theory, this question originates from an engineering problem, namely the design of so-called non-coherent differential space-time coding, that is coding over a wireless channel with several antennas with no knowledge of the channel at the receiver (the interested reader may refer for example to [5, 7] for more details of the engineering problem).

Over the last decade, engineers and mathematicians have tried to provide code constructions using many different approaches. In this survey paper, we focus on algebraic constructions, and present an overview of the algebraic techniques tried so far, as well as some of the best unitary codes and bounds available in the literature.

2 Diagonal codes

The easiest case one can think of is likely to be families of diagonal matrices. They have been investigated in the first papers [5, 7, 8], and are usually called *cyclic codes*.

* The work of Frédérique Oggier is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03.

Let ζ be a primitive L th root of unity. An $n \times n$ cyclic code $\mathcal{C}$ is given by

$$\mathcal{C} = \left\{ \left(\begin{pmatrix} \zeta^{u_1} & 0 & \dots & 0 \\ 0 & \zeta^{u_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \zeta^{u_n} \end{pmatrix} \right)^l \mid l = 0, \dots, L-1 \right\},$$

where $u_1, \dots, u_n$ are integers L between 0 and $L-1$.

Example 1. [Cyclic code with $n = 2$, $L = 8$.] Let ζ_8 be a primitive 8th root of unity. If $(u_1, u_2) = (1, 3)$, a 2×2 cyclic code is given by

$$\mathcal{C} = \left\{ \left(\begin{pmatrix} \zeta_8 & 0 \\ 0 & \zeta_8^3 \end{pmatrix} \right)^l \mid l = 0, \dots, 7 \right\}.$$

We have a diversity product $\zeta(\mathcal{C})$ of 0.5946.

Given the cardinality L , the code design consists of choosing $u_1, \dots, u_n$ relatively prime to L in order to maximize the diversity product as defined in (1). In particular, it has to be non-zero. In [5, 7, 8], the authors resort to exhaustive computer search to find optimal $u_1, \dots, u_n$. Some examples of such codes are reported in Table 1. Note that computer search is restricted to rather small n , and values for $n \geq 6$ have been generated randomly.

Table 1. Some cyclic codes with high diversity product.

n	L	R	$\zeta(\mathcal{C})$	$u_1, \dots, u_n$
2	8	1.5	0.5946	(1, 3)
3	63	1.99	0.3301	(1, 17, 26)
4	16	1	0.5453	(1, 3, 5, 7)
4	256	2	0.2208	(1, 25, 97, 107)
5	32	1	0.4095	(1, 5, 7, 9, 11)
6	4096	2	0.1428	(1, 599, 623, 1445, 1527, 1715)
7	128	1	0.3487	(1, 13, 17, 27, 29, 45, 49)
7	16384	2	0.1213	(1, 1875, 5207, 5551, 7687, 7827, 9013)

A natural way to give some structure (and to ensure fully diverse codes) is to use cyclotomic fields. As above, $\zeta_L = \zeta$ is a primitive L th root of unity, and let $F = \mathbb{Q}(\zeta_L)$ be its corresponding cyclotomic field. Assume that F has a subfield K such that F/K is cyclic of degree n , with Galois group generated by σ . We

consider cyclic codes $\mathcal{C} = \mathcal{C}(F/K, L, n)$ of the form

$$\mathcal{C} = \left\{ \left(\begin{pmatrix} \sigma(\zeta) & 0 & \dots & 0 \\ 0 & \sigma^2(\zeta) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma^n(\zeta) \end{pmatrix} \right)^l \mid l = 0, \dots, L-1 \right\}.$$

It is then easy to give a closed form expression for the diversity product.

Lemma 1. *The diversity product of a cyclic code $\mathcal{C}(F/K, L, n)$ is given by*

$$\frac{1}{2} \min_{l \neq l'} |\det(U^l - U^{l'})|^{1/n} = \frac{1}{2} \min_{l \neq l'} |N_{F/K}(1 - \zeta^{l'-l})|^{1/n}. \quad (2)$$

Proof. We have that

$$\det(U^l - U^{l'}) = \prod_{i=1}^n (\sigma^i(\zeta)^l - \sigma^i(\zeta)^{l'}) = \prod_{i=1}^n \sigma^i(\zeta^l - \zeta^{l'}) = N_{F/K}(\zeta^l - \zeta^{l'})$$

by definition of the norm $N_{F/K}$. Now

$$N_{F/K}(\zeta^l - \zeta^{l'}) = N_{F/K}(\zeta^l) N_{F/K}(1 - \zeta^{l'-l}),$$

so that

$$|\det(U^l - U^{l'})|^2 = |N_{F/K}(1 - \zeta^{l'-l})|^2$$

since $|N_{F/K}(\zeta^l)|^2 = 1$. $\square$

If $\mathbb{Q}(\zeta_L)$ contains a quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$ such that $\mathbb{Q}(\zeta_L)/\mathbb{Q}(\sqrt{-d})$ is cyclic, with d some positive square free integer, then we can consider the code $\mathcal{C}(\mathbb{Q}(\zeta_L)/\mathbb{Q}(\sqrt{-d}), L, \varphi(L)/2)$, where φ denotes the Euler totient function.

Lemma 2. *The diversity product of the code $\mathcal{C}(\mathbb{Q}(\zeta_L)/\mathbb{Q}(\sqrt{-d}), L, \varphi(L)/2)$ is given by*

$$\frac{1}{2} \min_{l \neq l'} |\det(U^l - U^{l'})|^{1/n} = \frac{1}{2} |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta)|^{1/2\varphi(L)}.$$

Proof. We have that

$$\min_{l \neq l'} |\det(U^l - U^{l'})|^2 = |N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-d})}(1 - \zeta)|^2 = |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta)|,$$

by considering the norm of $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$. $\square$

We notice that when $L = 8$ (with $\mathbb{Q}(\zeta_8)/\mathbb{Q}(i)$, $\zeta(\mathcal{C}) = 0.5946$) and $L = 16$ (with $\mathbb{Q}(\zeta_{16})/\mathbb{Q}(i)$, $\zeta(\mathcal{C}) = 0.5453$), we get the same diversity product as for cyclic codes. Actually, we even get the same construction (the code based on a cyclotomic extension with $L = 8$ is indeed the same code as in Example 1).

Apart finding in a different way known constructions, many other codes can be obtained with this technique [15], see Table 2 for some examples.

Table 2. Some codes based on cyclotomic extensions and their parameters: $n = 2$ and larger L , and $n = 8$.

n	L	R	$\zeta(\mathcal{C})$	σ
2	32	2.5	0.19509	$\zeta \mapsto \zeta^{15}$
2	64	3	0.09802	$\zeta \mapsto \zeta^{31}$
2	35	2.56	0.21442	$\zeta \mapsto \zeta^6$
2	63	2.98	0.13914	$\zeta \mapsto \zeta^8$
8	256	1	0.098017	$\zeta \mapsto \zeta^7$
8	255	0.99	0.30688	$\zeta \mapsto \zeta^{15}$

3 Representation of finite fixed point free groups

In order to go beyond diagonal matrices, the seminal paper [19] has looked at unitary representations of finite groups. If the code $\mathcal{C}$ is a group of unitary matrices, we have that

$$|\det(U' - U'')| = |\det(I - U)|$$

for $U = U'^{-1}U'' \in \mathcal{C}$, and in order to have a fully diverse code $\mathcal{C}$, we need to make sure that U has no eigenvalue at 1. Representations with no eigenvalue at 1 have been well studied, and are called *fixed point free representations*. A group is called *fixed point free* if it has a fixed point free representation. A complete classification of finite groups that are fixed point free is given in [19], based on the work of Zassenhaus, who has given an almost complete classification.

For Abelian groups, their irreducible representations are one-dimensional, that is they are characters of the group (characters are multiplicative mappings from the group to complex roots of unity). Furthermore, a character is fixed point free if and only if it is injective (or primitive). Thus for the particular case of a cyclic group $\langle \sigma \rangle$ of order L , its fixed point free characters are exactly those which map a generator of the group to a primitive L th root of unity. More precisely, primitive characters χ_u are given by $\chi_u(\sigma^l) = e^{2i\pi ul/L}$, $u = 0, \dots, L-1$, with u and L coprime. An n -dimensional representation Δ of G is given by a direct sum of n characters

$$\Delta(\sigma^l) = \begin{pmatrix} \zeta^{u_1 l} & 0 & 0 \\ 0 & \zeta^{u_2 l} & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \zeta^{u_n l} \end{pmatrix}, \quad \zeta = \zeta_L = e^{2i\pi/L}.$$

It is interesting to note that we are back to the cyclic code constructions of Section 2. Now a more general Abelian group G is fixed point free if and only if it has a primitive character, that is, if and only if one can embed an isomorphic copy of G in the non-zero complex numbers. This means that G has to be

cyclic, which shows that one has to consider non-Abelian groups to get new code constructions.

Let us give one example of representation of a family of fixed point free non-Abelian groups (it is proved in [19] that this is the only family with odd orders, and with irreducible representations of odd dimension n). Let r, m be two positive integers, and define n to be the order of $r \pmod{m}$, i.e., n is the smallest positive integer such that $r^n \equiv 1 \pmod{m}$. Set $t = m / \gcd(r-1, m)$. Consider the groups given by generators and relations as follows:

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

An n -dimensional representation Δ is given by

$$\Delta(G_{m,r}) = \{\Delta(\sigma)^l \Delta(\tau)^k \mid l = 0, \dots, m-1, k = 0, \dots, n-1\},$$

with

$$\Delta(\tau) = \begin{pmatrix} 0 & 0 & 0 & \zeta_m^t \\ 1 & 0 & 0 & 0 \\ 0 & 1 & \ddots & \vdots \\ 0 & \ddots & & \\ 0 & & 1 & 0 \end{pmatrix}^T, \quad \Delta(\sigma) = \begin{pmatrix} \zeta_m & 0 & 0 \\ 0 & \zeta_m^r & 0 \\ \vdots & & \ddots \\ 0 & 0 & \zeta_m^{r^{n-1}} \end{pmatrix}.$$

Example 2 (FPF group code with $n = 3$, $L = 63$.) Take $n = 3$, $r = 4$ and $m = 21$. We have the fixed point free group $G_{21,4}$. We get the family of 63 unitary matrices $E^i D^j$, where

$$D = \begin{pmatrix} \zeta_{21} & 0 & 0 \\ 0 & \zeta_{21}^4 & 0 \\ 0 & 0 & \zeta_{21}^{16} \end{pmatrix}, \quad E = \begin{pmatrix} 0 & 0 & \zeta_{21}^7 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

The diversity product is $\zeta(\Delta) = 0.3851$.

Since the matrices obtained via the representation of $G_{m,r}$ are doubly-banded, it is possible to compute explicitly their diversity product.

Lemma 3. [19, p.18] *For any fixed point free representation Δ of $G_{m,r}$, we have*

$$\zeta(\Delta) = \frac{1}{2} \min_{0 \leq l \leq m-1, 0 \leq k \leq n-1} \left| \prod_{j=1}^q \left(1 - \zeta_m^{\frac{k}{q} t + l r^{j-1} \frac{r^n - 1}{r^q - 1}} \right) \right|^{1/n}, \quad q = \gcd(n, k).$$

Examples of code constructions based on $G_{m,r}$ and their diversity product are given in Table 3.

Table 3. Some FPF group codes and their parameters.

n	L	R	$\zeta(\Delta)$	$G_{m,r}$
3	63	1.99	0.3851	$G_{21,4}$
3	513	3	0.1353	$G_{171,64}$
5	1025	2	0.1679	$G_{205,16}$
5	1021125	3.99	0.0037	$G_{204205,21}$
7	16513	2	0.0955	$G_{2359,8}$
9	513	1	0.3610	$G_{57,4}$

4 The Cayley transform

As we have already seen through the previous sections, the diversity product is a quantity rather difficult to evaluate. In order to get families of codes with high cardinality, the focus on the diversity product has been relaxed in [4], where Cayley codes have been proposed, based on the Cayley transform that maps the space of (skew)Hermitian matrices to the manifold of unitary matrices.

Let A be a Hermitian matrix, hence iA is automatically skew-Hermitian. The Cayley transform of iA is given by

$$U = (I + iA)^{-1}(I - iA).$$

It is easy to check that U is unitary. The Cayley transform of iA is preferred since all its eigenvalues are strictly imaginary, thus different from 1, so that the inverse of $I + iA$ always exists.

The cardinality of the unitary code $\mathcal{C}$ depends on the choice of the Hermitian matrices. Each matrix A is represented in a basis of Hermitian matrices

$$A = \sum_{q=1}^Q \alpha_q A_q,$$

where $\alpha_1, \dots, \alpha_Q \in \mathbb{R}$ are chosen from a set $\mathcal{S}$ with r possible values, and where A_q are fixed $n \times n$ Hermitian matrices. Let $L = 2^{RM} = r^Q$ be the cardinality of the code. The rate of a Cayley code is given by

$$R = \frac{Q}{M} \log_2 r.$$

At this point, one should choose Q , the Hermitian basis matrices $\{A_q\}$, and the set $\mathcal{S}$ from which each α_q is picked in order to optimize the diversity product (1). Arguing that at high rate this may become quickly intractable, the approach of [4] consists of optimizing a mutual information criterion instead. This leads to a probabilistic characterization of the best parameters. The matrices $A_1, \dots, A_Q$ are chosen at random such that U is isotropically distributed (an isotropically distributed unitary matrix has a probability density function which is invariant

to pre- and post- multiplication by an arbitrary unitary matrix). Consequently, it is shown that the optimal distribution on A is

$$p(A) = \frac{2^{n^2-n}(n-1)! \cdots 1!}{\pi^{n(n+1)/2}} \frac{1}{\det(I + A^2)^n}.$$

The above probability density function is a generalization of the scalar Cauchy distribution, which is why A is said to be Cauchy distributed. Finally, using Cauchy matrices is shown to imply that a good choice for the scalars $\alpha_1, \dots, \alpha_Q$ is to take them scalar Cauchy distributed.

An alternative approach to Cayley codes has been proposed in [14], where fully diverse Cayley codes have been built. In parallel to the work on unitary codes, progresses have been made in another area of coding theory, where division algebras have been introduced [18] as a mean to design fully diverse codes (which typically are not unitary). Let us first explain how this is done in general (see [18]), before getting back to the particular construction of interest here.

Let L/K be a Galois extension of degree n such that its Galois group $G = \text{Gal}(L/K)$ is cyclic, with generator σ .

Definition 1. Choose a non-zero element $\gamma \in K$. We construct a non-commutative algebra, denoted by $\mathcal{A} = (L/K, \sigma, \gamma)$, as follows:

$$\mathcal{A} = L \oplus eL \oplus \dots \oplus e^{n-1}L$$

such that e satisfies

$$e^n = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda) \text{ for } \lambda \in L.$$

Such an algebra is called a cyclic algebra.

It is a right vector space over L , and as such has dimension $(\mathcal{A} : L) = n$.

Cyclic algebras have been considered for coding applications since they naturally provide families of matrices as follows. Since each $x \in \mathcal{A}$ is expressible as

$$x = x_0 + ex_1 + \dots + e^{n-1}x_{n-1}, \quad x_i \in L \text{ for all } i,$$

there is a correspondence between $x \in \mathcal{A}$ and the matrix of left multiplication by x given by

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \dots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix}. \quad (3)$$

Example 3 (Cyclic algebra of dimension 2.). For $n = 2$, we have

$$\mathcal{A} = L \oplus eL$$

such that e satisfies

$$e^2 = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda) \text{ for } \lambda \in L.$$

Now, an element $x \in \mathcal{A}$ can be written $x = x_0 + ex_1$. Let us compute the multiplication by x of any element $y \in \mathcal{A}$.

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0y_0 + x_0ey_1 + ex_1y_0 + ex_1ey_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + \gamma\sigma(x_1)y_1, \end{aligned}$$

since $e^2 = \gamma$ and using the non-commutative rule $\lambda e = e\sigma(\lambda)$. In matrix form in the basis $\{1, e\}$, this yields

$$xy = \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}.$$

There is thus a correspondence

$$x = x_0 + ex_1 \in \mathcal{A} \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}. \quad (4)$$

Cyclic algebras provide us with a family $\mathcal{C}$ of matrices of the form (3), which is clearly linear (since σ is). Thus

$$\det(X' - X'') = \det(X), \quad \mathbf{0} \neq X \in \mathcal{C}, \text{ for all } X' \neq X'' \in \mathcal{C},$$

so that the diversity product (1) simplifies to

$$\zeta(\mathcal{C}) = \frac{1}{2} \min_{X \neq \mathbf{0}} |\det(X)|^{1/n}, \quad X \in \mathcal{C}.$$

If now the cyclic algebra we consider is also a division algebra, that is, by definition, that every element in $\mathcal{A}$ is invertible, this guarantees that $\zeta(\mathcal{C}) > 0$.

In order to know whether a cyclic algebra is a division algebra, the following criterion is useful.

Proposition 1. [16] *The algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree n is a division algebra if the smallest positive integer t such that γ^t is the norm of some element in L is n .*

We now show how the general theory exposed above can be used for constructing fully diverse Cayley codes [14]. Let us give an example of constructions of a 2×2 Cayley code built on a cyclic division algebra. Let us first note that for the families of unitary matrices U to be fully diverse, it is equivalent to have the Hermitian matrices A to be fully diverse, which we can find inside any cyclic division algebra.

Let us thus take the cyclic division algebra $\mathcal{A} = (\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \sigma, i)$, where $\sigma : \sqrt{5} \mapsto -\sqrt{5}$ and $\mathbb{Q}(i, \sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}(i)\}$. Let $x \in \mathcal{A}$,

$$x = x_0 + ex_1, \quad x_0, x_1 \in \mathbb{Q}(i, \sqrt{5}).$$

From the matrix representation (4), it is easy to find a subset of Hermitian matrices. Since an arbitrary $n \times n$ Hermitian matrix is parameterized by n^2 real variables, we are free to choose any $Q \leq n^2$ basis matrices. Let us choose $Q = n^2 = 4$. Set $\theta = \frac{1+\sqrt{5}}{2}$, and recall that here $\gamma = i$.

A suitable Hermitian matrix X is given by

$$a_0 I_2 + b_0 \begin{pmatrix} \theta & 0 \\ 0 & 1 - \theta \end{pmatrix} + s \begin{pmatrix} 0 & 1 - \theta - i\theta \\ i\theta + (1 - \theta) & 0 \end{pmatrix} + t \begin{pmatrix} 0 & -\theta + i(1 - \theta) \\ -i(1 - \theta) - \theta & 0 \end{pmatrix}.$$

The coefficients a_0, b_0, s, t belongs to $\mathbb{Q}$ since $\mathcal{A}$ is defined over a number field. We thus need $\mathcal{S} \subset \mathbb{Q}$.

We finally get a basis of four matrices

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 - \theta - i\theta \\ i\theta + (1 - \theta) & 0 \end{pmatrix}, \begin{pmatrix} \theta & 0 \\ 0 & 1 - \theta \end{pmatrix}, \begin{pmatrix} 0 & -\theta + i(1 - \theta) \\ -i(1 - \theta) - \theta & 0 \end{pmatrix} \right\},$$

yielding a fully-diverse 2×2 Cayley code.

Values of diversity products are not available for Cayley codes. Note that Cayley codes are the constructions allowing the highest rates. For example, a code for $n = 8$ has been built [4], with a rate of 16, which means that $L = |\mathcal{C}| = 2^{128}$, which is roughly $3.4 \cdot 10^{38}$. By comparison, codes based on cyclotomic fields (see Section 2) are available at rate 1 (256 matrices) but with guaranteed diversity product 0.098017, while the highest rate obtained for codes based on the representation of $G_{m,r}$ (Section 3) is 3.99 in dimension 4, for a diversity product of 0.0037.

5 Representation of Lie groups

In Section 3, we have briefly discussed how representation of finite groups could help approaching the problem of designing unitary codes. However, in considering finite groups, the cardinality of the code is naturally bounded by the order of the group. This naturally leads to infinite groups and the representation of Lie groups, in order to increase the cardinality of the unitary codes.

This line of research started with a negative result [6]: The only fixed point free Lie groups are $U(1)$, the unitary group of dimension 1, and $SU(2)$, the special unitary group of dimension 2. Furthermore, their only fixed point free irreducible representation are 1- and 2- dimensional, respectively.

To pursue further, one had to relax the condition of being fixed point free, and consider Lie groups of rank 2. The rank of a Lie group equals the maximum

number of commuting basis elements of its Lie algebra. The motivation lies in the fact that if a Lie algebra has rank n , then it has at least one element with $n - 1$ eigenvalues at 1. Thus the lower the rank of a Lie group, the more likely to find a subset which is fully-diverse. In particular, fixed point free Lie groups have rank 1. There are three Lie groups of rank 2: the Lie group of unit determinant 3×3 unitary matrices $SU(3)$, the Lie group of 4×4 unitary symplectic matrices $Sp(2)$, and one exceptional Lie group $\mathcal{G}_2$. Both $Sp(2)$ and $SU(3)$ have already been studied in the literature.

In [10], the symplectic group $Sp(2)$ is used for building 4-dimensional unitary codes. Let us first recall the definition of a symplectic group.

Definition 2. *The n th order symplectic group $Sp(n)$ is the set of $2n \times 2n$ complex matrices S obeying*

1. *the unitary condition $S^*S = SS^* = I_{2n}$*
2. *the symplectic condition $S^t J_{2n} S = J_{2n}$, where*

$$J_{2n} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

The symplectic group $Sp(n)$ can be parameterized as follows:

Theorem 1. [10] *A matrix S belongs to $Sp(n)$ if and only if it can be written as*

$$S = \begin{pmatrix} U \Sigma_A V & U \Sigma_B \bar{V} \\ -\bar{U} \Sigma_B V & \bar{U} \Sigma_A \bar{V} \end{pmatrix}$$

where U and V are $n \times n$ unitary matrices, and $\Sigma_A = \text{diag}(\cos \theta_1, \dots, \cos \theta_n)$, $\Sigma_B = \text{diag}(\sin \theta_1, \dots, \sin \theta_n)$, with $\theta_1, \dots, \theta_n \in [0, \pi/2]$.

Let $\Sigma_A = \Sigma_B = \frac{1}{\sqrt{2}} I_2$ and consider the code given by

$$\mathcal{C}_{P,Q,\theta} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} UV & U\bar{V} \\ -\bar{U}V & \bar{U}\bar{V} \end{pmatrix}, 0 \leq k, l \leq P, 0 \leq m, n \leq Q \right\}$$

where

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\frac{2\pi k}{P}} & e^{i\frac{2\pi l}{P}} \\ -e^{-i\frac{2\pi l}{P}} & e^{-i\frac{2\pi k}{P}} \end{pmatrix}, V = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i(\frac{2\pi m}{Q} + \theta)} & e^{i(\frac{2\pi n}{Q} + \theta)} \\ -e^{-i(\frac{2\pi n}{Q} + \theta)} & e^{-i(\frac{2\pi m}{Q} + \theta)} \end{pmatrix}.$$

Concerning the diversity product (1) of this code, it is proved that there exists a θ such that the code is fully diverse if and only if P and Q are coprime.

In [9], 3-dimensional unitary codes have been obtained based on the special unitary group $SU(3)$, that is the group of 3×3 unitary matrices U such that $\det(U) = 1$. Similarly to $Sp(2)$, we start with a parameterization of $SU(3)$.

Theorem 2. *A matrix U belongs to $SU(3)$ if and only if it can be written*

$$U = \begin{pmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Phi \end{pmatrix} \begin{pmatrix} \sqrt{1-|\alpha|^2} & 0 & \bar{\alpha} \\ 0 & 1 & 0 \\ -\alpha & 0 & \sqrt{1-|\alpha|^2} \end{pmatrix} \begin{pmatrix} \Psi & \mathbf{0}_{21} \\ \mathbf{0}_{12} & 1 \end{pmatrix}$$

where $\Phi, \Psi \in SU(2)$ and α is a complex scalar such that $|\alpha| \leq 1$.

In order to get fully diverse codes, the above parametrization is further refined, with U written as

$$\underbrace{\begin{pmatrix} e^{i\theta} & 0 & 0 \\ 0 & \phi_{11} & \phi_{12}e^{-i\theta} \\ 0 & -\bar{\phi}_{12} & \bar{\phi}_{11}e^{-i\theta} \end{pmatrix}}_{A_{\phi,\theta}} \begin{pmatrix} \sqrt{1-|\alpha|^2}e^{-i(\theta+\xi)} & 0 & \bar{\alpha}e^{-i(\theta-\xi)} \\ 0 & 1 & 0 \\ -\alpha e^{i(\theta-\xi)} & 0 & \sqrt{1-|\alpha|^2}e^{i(\theta+\xi)} \end{pmatrix} \underbrace{\begin{pmatrix} \psi_{11}e^{-i\xi} & \psi_{12}e^{-i\xi} & 0 \\ -\bar{\psi}_{12} & \bar{\psi}_{11} & 0 \\ 0 & 0 & e^{i\xi} \end{pmatrix}}_{B_{\psi,\xi}}$$

where θ, ξ are any real angles in $[0, 2\pi)$. A first family of codes is obtained by setting the middle matrix to be the identity matrix I_3 , and by choosing the matrices Φ and Ψ to be

$$\Phi = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{2i\pi \frac{p}{P}} & e^{2i\pi \frac{q}{Q}} \\ -e^{-2i\pi \frac{q}{Q}} & e^{-2i\pi \frac{p}{P}} \end{pmatrix}, \quad \Psi = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{2i\pi \frac{r}{R}} & e^{2i\pi \frac{s}{S}} \\ -e^{-2i\pi \frac{s}{S}} & e^{-2i\pi \frac{r}{R}} \end{pmatrix},$$

where P, Q, R, S are positive integers. We thus obtain $U = A_{\phi,\theta}B_{\psi,\xi} = A_{p,q,\theta}B_{r,s,\xi}$, but despite the simplifications made, fully diverse codes still cannot be guaranteed without asking some dependency among the parameters. A linear dependency is proposed:

$$\theta_{p,q} = 2\pi \left(\frac{p}{P} - \frac{q}{Q} \right), \quad \xi_{r,s} = 2\pi \left(\frac{r}{R} - \frac{s}{S} \right).$$

Finally, the code

$$\mathcal{C} = \{A_{p,q}B_{p,q} \mid p \in (0, P], q \in (0, Q], r \in (0, R], s \in (0, S]\}$$

is proved to be fully diverse if P, Q are coprime, and R, S are coprime.

Table 4. Some $SU(3)$ group codes and their parameters.

(P, Q, R, S)	Rate	$\zeta(\mathcal{C})$
(5,7,3,1)	2.2381	0.2133
(5,7,9,1)	2.7664	0.1714
(7,9,11,1)	3.1456	0.0961
(3,7,5,11)	3.3912	0.0803
(5,9,7,11)	3.9195	0.0510
(7,11,9,13)	4.3791	0.0316

Examples of code constructions based on $SU(3)$ and their diversity product are given in Table 4.

6 Cyclic division algebras

Cyclic division algebras have become a popular algebraic tool to get families of fully diverse codes [18]. However, in order to use cyclic algebras for unitary codes, one needs to understand how to find suitable unitary elements.

As a motivation to consider cyclic division algebras, we first show how the codes obtained from the representation of the groups $G_{m,r}$ (see Section 3) can be found by looking at suitable cyclic algebras.

Let r, m be two positive integers, and define n to be the order of $r \pmod{m}$, i.e., n is the smallest positive integer such that $r^n \equiv 1 \pmod{m}$. Set $t = m/\gcd(r-1, m)$. Consider the cyclotomic field $L = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m th root of unity. It is of degree $\varphi(m)$ over $\mathbb{Q}$ (φ is the Euler totient function).

Proposition 2. *Let $\sigma : \zeta_m \mapsto \zeta_m^r$. There exists a field extension K such that $\mathbb{Q}(\zeta_m)$ is a cyclic extension of K of degree n and $\zeta_m^t \in K$.*

Proof. Since $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, $r^n \equiv 1 \pmod{m}$ implies that there is a cyclic subgroup of order n in $(\mathbb{Z}/m\mathbb{Z})^*$, which means that $\mathbb{Q}(\zeta_m)/K$ is cyclic of order n . This subgroup of order n is generated by $\sigma : \zeta_m \mapsto \zeta_m^r$.

What is left to prove is that $\zeta_m^t \in K$, i.e., that ζ_m^t is fixed by σ . But

$$\sigma(\zeta_m^t) = \zeta_m^t \iff t(r-1) \equiv 0 \pmod{m},$$

which is satisfied since $t(r-1) = m(r-1)/\gcd(r-1, m)$ and clearly $\gcd(r-1, m) \mid r-1$. $\square$

We therefore consider the cyclic algebra $\mathcal{A} = (\mathbb{Q}(\zeta_m)/K, \sigma, \zeta_m^t)$. The matrix representation of the element e of $\mathcal{A}$ such that $e^n = \zeta_m^t$ is thus (see Section 4)

$$E = \begin{pmatrix} 0 & 0 & 0 & \zeta_m^t \\ 1 & 0 & 0 & 0 \\ 0 & 1 & \ddots & \vdots \\ 0 & \ddots & & \\ 0 & & 1 & 0 \end{pmatrix},$$

while the one of $\zeta_m \in L$ is given by

$$D = \begin{pmatrix} \zeta_m & 0 & 0 \\ 0 & \zeta_m^r & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \zeta_m^{r^{n-1}} \end{pmatrix}.$$

Since $\zeta_m^k \overline{\zeta_m^k} = 1$ for any integer k , the matrices E^i , $i = 0, \dots, n-1$ and D^j , $j = 0, \dots, m-1$ are unitary. Thus the set $E^i D^j$ yields a family of $nm-1$ unitary matrices, which is easily recognizable as being similar to the representation of the groups $G_{m,r}$.

In order to identify unitary matrices, one can endow suitable cyclic algebras with a unitary involution. Let us consider the cyclic algebra $\mathcal{A} = (L/K, \sigma, \gamma)$.

Proposition 3. [12, 13] Let $\alpha_L : L \rightarrow L$ be a (non-trivial) involution on L such that α_L commutes with all elements of $\text{Gal}(L/K)$. Let $\alpha : \mathcal{A} \rightarrow \mathcal{A}$ such that

$$\alpha(x_0 + ex_1 + \dots + e^{n-1}x_{n-1}) = \alpha_L(x_0) + e^{-1}\sigma^{-1}(\alpha_L(x_1)) + \dots + e^{-(n-1)}\sigma^{-(n-1)}(\alpha_L(x_{n-1})).$$

Then α defines an involution on $\mathcal{A}$ if and only if $\gamma\alpha_L(\gamma) = 1$.

This involution can be extended to the algebra $\mathcal{A} \otimes_K L \cong \mathcal{M}_n(L)$, and it can be showed that if α_L is the complex conjugation, then the extension of α to $\mathcal{M}_n(L)$ corresponds to the Hermitian conjugation. In other words, unitary matrices in $\mathcal{M}_n(L)$ correspond to elements $x \in \mathcal{A}$ such that $x\alpha(x) = x\alpha(x) = 1$.

A family of such elements can be found by restriction to commutative subfields of $\mathcal{A}$ as follows.

Proposition 4. Let $\mathcal{A} = (L/K, \sigma, \gamma)$ be a cyclic division algebra. Let $x \in \mathcal{A}^*$ such that $x\alpha(x) = 1$, $x \notin K$. Then there exists $u \in \mathcal{A}^*$ such that $u\alpha(u) = \alpha(u)u$ and $x = u\alpha(u)^{-1} = \alpha(u)^{-1}u$.

Proof. Let $x \in \mathcal{A}^*$ such that $x\alpha(x) = 1$. Let M denote the subfield of $\mathcal{A}$ generated by K and x . It is commutative and satisfies that $\alpha(M) = M$, since $\alpha(K) = K$ and $\alpha(x) = x^{-1}$. Thus

$$M^\alpha = \{y \in M \mid \alpha(y) = y\},$$

the subfield fixed by α is well-defined. Since $M^\alpha \neq M$ ($x \neq \pm 1$), M/M^α is a quadratic extension with Galois group $\text{Gal}(M/M^\alpha) = \{Id_M, \alpha|_M\}$. The condition $x\alpha(x) = 1$ is here translated into $N_{M/M^\alpha}(x) = 1$. By the corollary of Hilbert 90 Theorem that exactly characterizes elements of norm 1 in cyclic extension, there exists $u \in M^*$ such that $x = u/\alpha(u)$. $\square$

We thus get the following recipe. Take a commutative subfield $M \neq K$ of $\mathcal{A}$ such that $\alpha(M) = M$ but with $y \in M$ such that $\alpha(y) \neq y$, so that M^α is not M itself. Take $u \in M^*$ and compute $x = u/\alpha(u)$. The element $x \in \mathcal{A}$ will satisfy $x\alpha(x) = 1$.

Example 4. Let $K = \mathbb{Q}(\zeta_3)$ and $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_3)$ be the compositum of $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_7)$. We have $\text{Gal}(L/\mathbb{Q}(\zeta_3)) = \langle \sigma \rangle$, with $\sigma : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$. Let $\mathcal{A} = (\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_3)/\mathbb{Q}(\zeta_3), \sigma, \zeta_3)$ be the corresponding cyclic division algebra. The involution α on $\mathcal{A}$ is given by

$$\begin{aligned} \alpha : \mathcal{A} &\rightarrow \mathcal{A} \\ x_0 + ex_1 + e^2x_2 &\mapsto \alpha_L(x_0) + e\zeta_3^2\sigma(\alpha_L(x_2)) + e^2\zeta_3^2\sigma^2(\alpha_L(x_1)), \end{aligned}$$

where $\alpha_L(b_0 + b_1\zeta_3) = b_0 + b_1\zeta_3^2$. We look for subfields M of $\mathcal{A}$, which possess a quadratic subfield M/M^α fixed by α . For example, consider $K(e)$, with minimal polynomial $\chi_e(X) = X^3 - \zeta_3$. Thus $K(e) = \mathbb{Q}(\zeta_9)$. Since $\alpha(e) = e^{-1}$, we have that $\alpha(\zeta_9) = \zeta_9^{-1}$ and α is the complex conjugation on $K(e) = \mathbb{Q}(\zeta_9)$. Its maximal

real subfield $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ is fixed by α . We now build unitary matrices in the commutative subfield $\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)$ of $\mathcal{A}$.

Take for example the element

$$\begin{aligned} y &= 1 + \zeta_9 + \zeta_9^3 + \zeta_9^5 \in \mathbb{Q}(\zeta_9) \\ &= (1 + \zeta_3) + e + e^2\zeta_3 \in \mathcal{A} \end{aligned}$$

As a matrix, y can be represented as

$$Y = \begin{pmatrix} 1 + \zeta_3 & \zeta_3^2 & \zeta_3 \\ 1 & 1 + \zeta_3 & \zeta_3^2 \\ \zeta_3 & 1 & 1 + \zeta_3 \end{pmatrix}.$$

We have

$$\begin{aligned} \alpha(y) &= -\zeta_9^2 - \zeta_9^3 + \zeta_9^4 - \zeta_9^5 \in \mathbb{Q}(\zeta_9) \\ &= -\zeta_3 + e\zeta_3 + e^2\zeta_3^2 \in \mathcal{A} \end{aligned}$$

Again, as a matrix, $\alpha(y)$ can be represented as

$$\begin{pmatrix} -\zeta_3 & 1 & \zeta_3^2 \\ \zeta_3 & -\zeta_3 & 1 \\ \zeta_3^2 & \zeta_3 & -\zeta_3 \end{pmatrix}$$

which can be checked to be Y^* . We have

$$x = y/\alpha(y) = \frac{1}{19}(-10 + 16\zeta_9 + \zeta_9^2 - 4\zeta_9^3 + 14\zeta_9^4 + 8\zeta_9^5),$$

which has norm 1. Clearly $x\alpha(x) = 1$ and the matrix $Y(Y^*)^{-1}$ is unitary. This can be easily verified, since

$$Y(Y^*)^{-1} = \begin{pmatrix} -0.421 - 0.182i & 0.473 + 0.638i & -0.157 + 0.36i \\ -0.236 - 0.319i & -0.421 - 0.182i & 0.473 + 0.638i \\ -0.789 + 0.09i & -0.236 - 0.319i & -0.421 - 0.182i \end{pmatrix}^t.$$

A few examples of codes obtained using this technique are illustrated in dimension 3 in Table 5.

Table 5. Some cyclic algebra codes in dimension 3 and their parameters.

$ \mathcal{C} $	R	$\zeta(\mathcal{C})$
63	1.9924	0.38508
126	2.3258	0.29658
441	2.9282	0.18898
819	3.2259	0.06442

In a different approach, note that cyclic algebras of degree 3 have been further studied in [1].

7 Some other constructions

Apart the Cayley codes, which have been presented because they provide efficient unitary codes despite the lack of understanding of their diversity product, all the constructions presented are part of the same story: cyclic codes are a particular case of fixed point free group codes, which are themselves either a particular case of cyclic algebra codes, or can be generalized towards infinite groups like Lie group codes. Below can be found a few other constructions, the list does not pretend to be exhaustive.

The case of 2×2 codes. Many constructions have been proposed for the simple case of 2×2 matrices, and in [11], a systematic parameterization has been done in order to get the highest possible diversity product.

Number fields. Constructions in dimension up to 11 have been proposed based on number fields in [20].

8 Bounds

We have seen several methods to build unitary codes with good diversity product. A natural question to address at this point is, given a cardinality L of $n \times n$ unitary matrices, what is the best possible diversity product, and vice versa, given a diversity product, what is the best possible cardinality L . This question has been addressed by different authors (for example [3, 2]).

The latest (and tightest) bounds have been given in [2], based on linear programming bound techniques:

Theorem 3. [2] *Let $\mathcal{C}$ be a unitary code with diversity product $\zeta(\mathcal{C})$, the following upper bounds hold :*

$$\begin{aligned} |\mathcal{C}| &\leq \frac{2\zeta(\mathcal{C})^2}{2\zeta(\mathcal{C})^2-1} && \text{if } \zeta(\mathcal{C})^2 > \frac{1}{2} \\ |\mathcal{C}| &\leq \frac{8n\zeta(\mathcal{C})^2}{4n\zeta(\mathcal{C})^2-(2n-1)} && \text{if } \zeta(\mathcal{C})^2 > \frac{2n-1}{4n}, \quad n \geq 3 \\ |\mathcal{C}| &\leq \frac{8\zeta(\mathcal{C})^6+4\zeta(\mathcal{C})^4+8\zeta(\mathcal{C})^2}{8\zeta(\mathcal{C})^6-\frac{1}{4}} && \text{if } \zeta(\mathcal{C})^2 \geq \frac{1}{2}, \quad n = 2. \end{aligned}$$

In [2], the authors determine upper bounds for $\zeta(\mathcal{C})$ given L , and simultaneously compute these bounds numerically. A few numerical values in dimension 2 and 3 are given in Table 6.

To conclude, let us compare these bounds with some best known codes.

- For $n = 2$ and $L = 24$: the bound predicts $\zeta(\mathcal{C}) \geq 0.57304$, while the best known code is a fixed point free group code, with $\zeta(\mathcal{C}) = 0.5$.
- For $n = 2$ and $L = 48$: we have a bound of $\zeta(\mathcal{C}) \geq 0.4989$, while the best known code is again a fixed point free group code, with $\zeta(\mathcal{C}) = 0.3868$.

Table 6. Bounds on the diversity product in dimension 2 and 3

n	L	$\zeta(\mathcal{C})$
2	24	0.5730
2	48	0.4989
2	80	0.4504
2	100	0.4301
3	24	0.6431
3	48	0.5942
3	80	0.5628
3	100	0.5482

- One more value of comparison for $n = 2$ is that for $L = 80$, the bound yields 0.4504, while even for $L = 75$, the best parameterized code [11] has a diversity product of 0.3535.
- For $n = 3$, a construction from number fields [20] gives 0.4845 for $L = 57$. Other code constructions are quite far from the bound. For example, for $L = 60$, $SU(3)$ codes give a diversity of 0.2977, while we have a fixed point free group yielding 0.3851 for $L = 63$.

9 Open problems

Despite a fair amount of effort and imagination, the problem of designing good unitary codes is far from being solved. Many techniques have been investigated, yielding nice constructions with good parameters. However, the best codes are still to be found. It can be seen from the known bounds that there is a relatively big gap between the bounds and the known constructions, suggesting that there is still work to be done, to either tighten the bounds, or construct better codes. One of the difficulties of this problem is the fact that the main design criterion, the diversity product, is generally difficult to evaluate.

References

1. J. Abarbanel, A. Averbuch, S. Rosset, J. Zlotnick, “Unitary non-group STBC codes from cyclic algebras”, *IEEE Trans. Inform. Theory*, vol. 52, pp. 3903-3912, Sept. 2006.
2. J. Creignou, H. Diete, “Linear programming bounds for unitary space time codes”, *Proceedings of International Symposium on Information Theory (ISIT)*, Toronto, 2008.
3. G. Han, J. Rosenthal, “Unitary Space-Time Constellation Analysis : An Upper Bound for the Diversity”, *IEEE Trans. Inform. Theory*, vol. 52, n. 10, pp. 4713-4721, Oct. 2006.
4. B. Hassibi and B. Hochwald, “Cayley Differential Unitary Space-Time Codes”, *IEEE Trans. on Information Theory*, vol. 48, June 2002.

5. B. Hochwald and W. Sweldens, "Differential unitary space time modulation", *IEEE Trans. Commun.*, vol. 48, Dec. 2000.
6. B. Hassibi and M. Khorrami, "Fully-diverse multiple-antenna signal constellations and fixed-point free Lee groups", *Proceedings of International Symposium on Information Theory (ISIT)*, Washington DC, 2001. Full version available online at mars.bell-labs.com/cm/ms/what/mars/papers/lie/lie.ps
7. B. Hughes, "Differential space-time modulation," *IEEE Trans. Inform. Theory*, vol 46, Nov. 2000.
8. B. L. Hughes, "Optimal space-time constellations from groups", *IEEE Trans. Inform. Theory*, vol. 49, pp. 401-410, Feb. 2003.
9. Y. Jing, B. Hassibi, "Three-Transmit-Antenna Space-Time Codes Based on $SU(3)$ ", *IEEE Trans. Signal Processing*, vol. 53, no 10, Oct. 2005.
10. Y. Jing, B. Hassibi, "Design of full-diverse multiple-antenna codes based on $Sp(2)$ ", *IEEE Trans. on Information Theory*, vol. 50, no 11, Nov. 2004.
11. Xue-Bin Liang and Xiang-Gen Xia, "Unitary Signal Constellations for Differential Space-Time Modulation With Two Transmit Antennas: Parametric Codes, Optimal Designs, and Bounds," *IEEE Trans. on Inform. Theory*, vol. 48, no.8, August 2002.
12. F. Oggier, E. Lequeu, "Families of unitary matrices achieving full diversity", *Proceedings of the International Symposium on Information Theory (ISIT)*, Adelaide, 2005.
13. F. Oggier, "Cyclic Algebras for Noncoherent Differential Space-Time Coding", *IEEE Transactions on Information Theory*, vol. 53, no. 9, September 2007.
14. F. Oggier, B. Hassibi, "Algebraic Cayley differential Space-Time Codes", *IEEE Transactions on Information Theory*, vol. 53, no. 5, May 2007.
15. F. Oggier, "Design of Algebraic Cyclic Codes", *Proceedings of the Information Theory Workshop (ITW)*, Porto, 2008.
16. R. S. Pierce, "Associative Algebras," Springer-Verlag, New York, 1982.
17. I. Reiner, "Maximal Orders", Academic Press, 1975.
18. B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596– 2616, October 2003.
19. A. Shokrollahi, B. Hassibi, B. M. Hochwald, W. Sweldens, "Representation Theory for High-Rate Multiple-Antenna Code Design", *IEEE Trans. Information Theory*, vol. 47, no 6, Sept. 2001.
20. C. Xing, "Constructions of unitary space-time codes from number fields", preprint.