Unitary non-group STBC from cyclic algebras

Joseph Abarbanel[1], Amir Averbuch[2]

Shmuel Rosset[1], Joseph Zlotnick[3]

[1]School of Mathematical Sciences

[2]School of Computer Science

[3]Department of Electrical Engineering - Systems, Faculty of Engineering,

Tel Aviv Univeristy, Tel Aviv 69978, Israel

Abstract

Space Time Block Codes (STBC) are designed for Multiple Input - Multiple Output (MIMO) channels. In order to avoid errors, Single Input Single Output (SISO) fading channels require long coding blocks and interleavers that result in high delays. If one wishes to increase the data rate it is necessary to take advantage of space diversity.

Early STBC, that where developed by Alamouti [7] for known channels and by Tarokh [6] for unknown channels, have been proven to increase the performance of channels characterized by Rayleigh fading. Codes that are based on division algebras have by definition non-zero diversity and therefore are suitable for STBC in order to achieve high rates at low Symbol to Noise Ratio (SNR). This work presents new high diversity group based STBCs with improved performance both in known and unknown channels. We describe two new sets of codes for multiple antenna communication. The first set is a set of 'superquaternions' and improves considerably on the Alamouti codes. It is based on the mathematical fact that "normalized" integral quaternions are very well distributed over the unit sphere in 4 dimensional Euclidean space. The second set of codes gives arrays of 3 by 3 unitary matrices with full diversity. Here the idea is to use cosets of finite subgroups of division algebras that are 9 dimensional over their center, which is a finite cyclotomic extension of the field of rational numbers. It is shown that these codes outperform Alamouti and G_{mr}.

1 Introduction

Multiple antenna wireless communication is known to be a promising solution to the problem of increasing data rates without increasing the transmission power. It has been established in many recent publications ([1]) that differential unitary space time transmissions are very well suited for unknown continuously varying Rayleigh flat fading channels.

The design of such codes is comprised of a set of L unitary $M \times M$ matrices, where M is the number of transmission antennae. In most cases L is of the form 2^{RM} where R is the transmission rate. The principal criterion for the quality of such sets is its so called diversity

$$\min\{\frac{1}{2}\sqrt[M]{|\det(A-B)|}\}$$

where A, B are distinct members of the set. The set is said to have *full* diversity if this number is positive.

Recent effort has concentrated on the development of sets which are groups. For example the exhaustive paper [3] characterizes the class of sets of unitary matrices that have full diversity and form a group. In this paper our approach has been to look at sets of matrices inside division algebras that are finite dimensional over the field of rational numbers $\mathbb{Q}$. The basic motivation was that any set of non-zero elements of a division algebra is assured to have full diversity.

The first division algebra that comes to mind is the classical ring of Hamilton's quaternions. This is a four dimensional algebra over $\mathbb{Q}$ and its tensor product with $\mathbb{R}$ is also a division algebra (this is the celebrated algebra discovered by Hamilton, later shown by Frobenius to be unique.) In fact Alamouti's renowned method ([7]) employs quaternions in disguise. We investigate sets of quaternion elements, called "super-quaternions", that are "layers" in a very interesting infinite group that seems to be a new object. Our results were already an improvement over existing methods.

Trying to extend our search to the 3-dimensional case, i.e. algebras which are finite dimensional over $\mathbb{Q}$ and are 9-dimensional over their center, we developed a completely new method to create sets of 3×3 unitary matrices with good diversity qualities. Our simulations show that our codes outperform all known codes. Our method is based on taking cosets of known finite groups inside the multiplicative group of the division algebra. The heart of the method is its choice of "good" coset representatives. This is an elaborate scheme. Fortunately, in dimension 3 this scheme involves solving some linear equations. Trying to extend our considerations to degree 4 leads to a set of quadratic equations that seem harder to solve.

An additional aspect of our development in dimension 3 is that assuring unitarity in this dimension is non-trivial. This is in contrast with the 2 dimensional case in which unitarity is easily achieved: every element of norm 1 is automatically unitary.

2 Extensions of the Quaternion Groups

This section presents new codes, that are based on extensions of the quaternion groups.

2.1 Super Quaternion sets

The quaternion algebra, developed by Hamilton, is the 4 dimensional algebra over the real numbers with basis

$$\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$$

and the familiar rules of multiplication:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \ \mathbf{ij} = -\mathbf{ji} = \mathbf{k}.$$

The 8 quaternions

$$\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$$

form a group, the renowned quaternion group. The quaternion algebra has a 2 dimensional complex representation, i.e. an embedding in $M_2(\mathbb{C})$, in which to the elements $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ correspond the matrices

$$Q_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad Q_{\mathbf{i}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad Q_{\mathbf{j}} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad Q_{\mathbf{k}} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

The set $\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ is a group of order 8 and thus our representation has eight matrices. We denote the quaternion group of order 8 by $\mathbb{H}_2$. If the transmission rate is $R = \log_2 8/2$ then the diversity product (to be defined below) is $\zeta_{\mathbb{H}_2} = 0.7071$.

We now define the *super-quaternion* group as

$$S\mathbb{H} \ = \ \left\{ \frac{x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}}{\sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}} \ \mid 0 < x_1^2 + x_2^2 + x_3^2 + x_4^2, \ x_i \in \mathbb{Z} \right\}.$$

It is easy to see that $S\mathbb{H}$ is a group. It is of course an infinite group, and is a kind of lattice in $SU(2)$. How does this group look like? The integral solutions of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1, \ x_i \in \mathbb{Z}$$

are simply the eight elements of the quaternion group $\mathbb{H}$. For each prime integer p let

$$S\mathbb{H}(p) \;=\; \left\{ \frac{x_1 + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k}}{\sqrt{x_1^2+x_2^2+x_3^2+x_4^2}} \mid x_1^2+x_2^2+x_3^2+x_4^2 \text{ a power of } p \right\}.$$

It is clear that each $S\mathbb{H}(p)$ is a subgroup. It can be shown that an element of $S\mathbb{H}$, whose denominator is divisible by $p_1, \ldots, p_k$, is an almost unique product of elements of $S\mathbb{H}(p_1), \ldots, S\mathbb{H}(p_k)$ ([8, 9]).

We define the n-th layer of our group as the set of all quaternions of the form

$$L_n \triangleq \left\{ \frac{x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}}{\sqrt{n}} : \sum x_i^2 = n, \quad x_i \in \mathbb{Z} \right\} \tag{2.1}$$

where x_0, x_1, x_2, x_3 are relatively prime integers such that $\sum x_i^2 = n$. It may well be empty. For example L_8 is empty because in every integer solution of the equation $x_0^2+x_1^2+x_2^2+x_3^2 = 8$ the numbers x_0, x_1, x_2, x_3 are all even so there is no solution in which the greatest common divisor is 1. But it follows from a famous formula of Jacobi that if p is an odd prime number then the size of L_{p^n} is $p^{n-1}(p+1)$.

We use the union of layers to generate sets of matrices. Thus we define

$$S_n \;=\; \left\{ \frac{x_1 I + x_2 Q_{\mathbf{i}} + x_3 Q_{\mathbf{j}} + x_4 Q_{\mathbf{k}}}{\sqrt{x_1^2+x_2^2+x_3^2+x_4^2}} \;\middle|\; \begin{array}{l} 0 < x_1^2+x_2^2+x_3^2+x_4^2 \le n, \\ x_i \in \mathbb{Z} \end{array} \right\}. \tag{2.2}$$

The matrices in S_n are unitary. Indeed, if q is a linear combination of matrices in S_2, $q = x_1 Q_1 + x_2 Q_{\mathbf{i}} + x_3 Q_{\mathbf{j}} + x_4 Q_{\mathbf{k}}$, and $\bar{q}$ is the conjugate transpose matrix, then $\bar{q} = x_1 Q_1 - x_2 Q_{\mathbf{i}} - x_3 Q_{\mathbf{j}} - x_4 Q_{\mathbf{k}}$ then $q\bar{q} = \|q\|^2 = (x_1^2+x_2^2+x_3^2+x_4^2)Q_1 = kI$. Therefore, all the elements in S_n are normalized by $\frac{1}{\sqrt{k}}$ and they become unitary matrices. S_n is the disjoint union of the layers $L_1, \ldots, L_n$.

In this case, L_1 is Q_2 in Eq. 2.1 and it has eight elements. The calculation of the number of elements in each layer (which is the number of solutions to Eq. 2.2), shows that $|L_2| = 24$, $|L_3| = 32$, $|L_4| = 24$, etc.

By examining the layers L_i of the super quaternion, we observe that in some cases the same matrix element can exist in more than one layer. If $(x_1, ..., x_n)$ is in layer L_i, then $(\alpha x_1, \alpha x_2, ..., \alpha x_n)$ must be in layer $L_{\alpha^2 i}$, and since the elements are normalized, the matrices are equal. Therefore, for $\alpha > 1$ we have $L_i \subseteq L_{\alpha^2 i}$. For example, the element $Q_a \in L_1$ (the solution $(1,0,0,0)$), is equal to element $2Q_a/\sqrt{4} \in L_4$ (the solution $(2,0,0,0)$). To eliminate the duplicate elements, we have to reduce these solutions in order to calculate correctly S_n and its diversity product (gcd of all x_i is 1).

2.2 Super Quaternion diversity

In this section we present the diversity of the Super Quaternion structure.

First we calculate the diversity of the commonly used orthogonal design for comparison. For each couple of constellation symbols S_1, S_2 we transmit the matrix

$$C_{S_1S_2} = \begin{pmatrix} S_1 & S_2 \\ -S_2^* & S_1^* \end{pmatrix}.$$

The diversity is defined by

$$\zeta = \frac{1}{2} \min det(C_{S_1S_2} - C_{S_1'S_2'})|^{\frac{1}{m}} = \frac{1}{2} \min \sqrt{|S_1 - S_1'|^2 + |S_2 - S_2'|^2}$$

where the min is over all the codewords $C_{S_1S_2}$ and $C_{S_1'S_2'}$. Without loss of generality, we can assume that $S_1 \neq S_1'$. In this case, we minimize the expression above by choosing $S_2 = S_2'$. We can write ζ as:

$$\zeta = \frac{1}{2} min|S_1 - S_1'| = \frac{1}{2} min|(S_1 - S_1')S_1^* / |S_1|\,| = \frac{1}{2} min\,||S_1| - S_1'S_1^* / |S_1||\,. \tag{2.3}$$

Let $S_1 = \frac{1}{\sqrt{2}} e^{2k\pi i/n}, S_1' = \frac{1}{\sqrt{2}} e^{2k'\pi i/n}$ for $n - PSK$ code (the normalization by $\frac{1}{\sqrt{2}}$ aims to maintain transmit power of 1).

$$\zeta = \frac{1}{2} \min_{k \neq k'} \frac{1}{\sqrt{2}} |1 - e^{2(k'-k)\pi i/n}|. \tag{2.4}$$

$$\begin{aligned} &|1 - e^{2(k'-k)\pi i/n}|^2 = |1 - e^{2k''\pi i/n}|^2 \\ &= (1 - \cos(2k''\pi/n))^2 + (\sin(2k''\pi/n))^2 \\ &= 2(1 - \cos(2k''\pi/n)) = 4\sin^2(k''\pi/n). \end{aligned} \tag{2.5}$$

Substituting Eq. 2.5 in Eq. 2.4 we have

$$\begin{aligned} \zeta &= \frac{1}{2} \min_{k \neq k'} \frac{1}{\sqrt{2}} |1 - e^{2(k'-k)\pi i/n}| = \frac{1}{2} \min_{k'' \neq 0} \frac{1}{\sqrt{2}} |2\sin(k''\pi/n)| \\ &= \frac{1}{\sqrt{2}} \min_{k'' \neq 0} |\sin(k''\pi/n)| = \frac{1}{\sqrt{2}} \sin(\pi/n). \end{aligned}$$

Table 1 summarizes the diversity of some of the new quaternion structures:

R	L	M	ζ	Diversity bound (Eq. 4.12)	Group structure
2.5	32	2	0.3827	0.53	S_2
3	64	2	0.3029	0.42	S_3
3.161	80	2	0.2588	0.39	S_4
3.5	128	2	0.1602	0.3332	S_5
3.904	224	2	0.1602	0.2762	S_6
4.085	288	2	0.1602	0.2542	$S_7 = S_8$
4.292	384	2	0.1374	0.2308	S_9
4.522	528	2	0.0709	0.2076	S_{10}
2.5	32	2	0.4082	0.53	L_3
2.29	24	2	0.5	0.5808	L_2
2.79	48	2	0.3827	0.4638	$Q_2 \cup L_2 \cup L_4 = S\mathbb{H}(2)$

Table 1: Super-quaternion structures (diversity products ζ, transmission rate R, size of the constellation L, M number of antennas) and the diversity upper bound computed by Eq. 4.12

For comparison, the quaternion groups Q_2, Q_4 and Q_5 diversity (from [3]) are shown in table 2:

R	L	M	ζ	Group structure
1.5	8	2	0.7071	Quaternion group Q_2
2.5	32	2	0.1951	Quaternion group Q_4
3	64	2	0.0951	Quaternion group Q_5

Table 2: Quaternion groups and their diversity products ζ, transmission rate R, size of the constellation L and M the number of antenna - from [3].

We can see that the codes in Table 1 that are proposed in this paper outperform the ζ values in Table 2 with the same R. Generally, the diversity is in opposite ratio to the rate, though as it may be seen from Table 1 the diversity also depends on the specific unions, that may achieve better diversity for a given rate.

2.2.1 Quaternion Group Example

In Q_2 there are eight code words (eight matrices):

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The rate for this code is $\frac{1}{2}log_2(8) = 1.5$ bits per channel use. The diversity of this code is $\zeta\{Q_2\} = 0.707$, which is equal to the diversity of Orthogonal Design [7] code for BPSK constellation that has a mere 1 bit per channel use rate.

Figure 1 describes the Quaternion group constellation for rate 1.5.

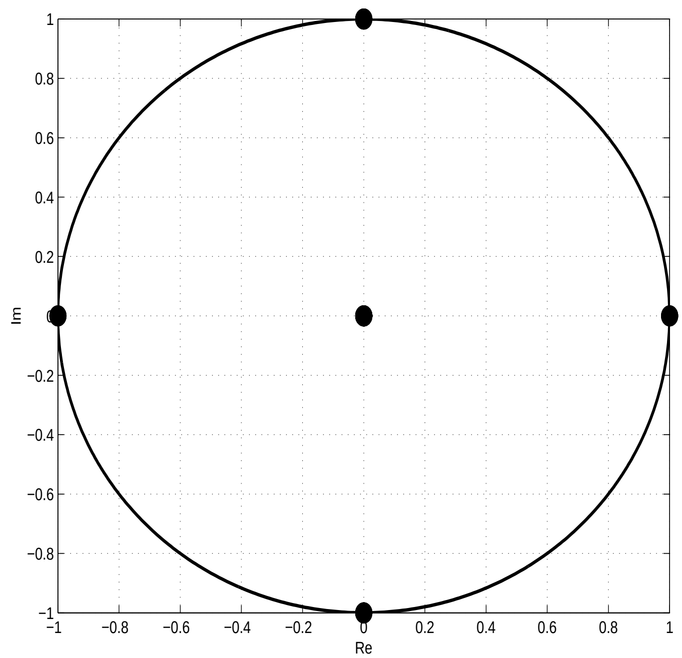

Figure 1: A Quaternion group constellation for rate 1.5

2.2.2 Super Quaternion Set Example

The Super Quaternion set $Q_2 \cup L_2 \cup L_4$ contains 48 code words and is infact the group $S\mathbb{H}(2)$. The rate of this code is 2.7925 and the code diversity is 0.3827. By applying Orthogonal Design to 6-PSK we get merely a 0.3536 diversity for a lesser rate of 2.585.

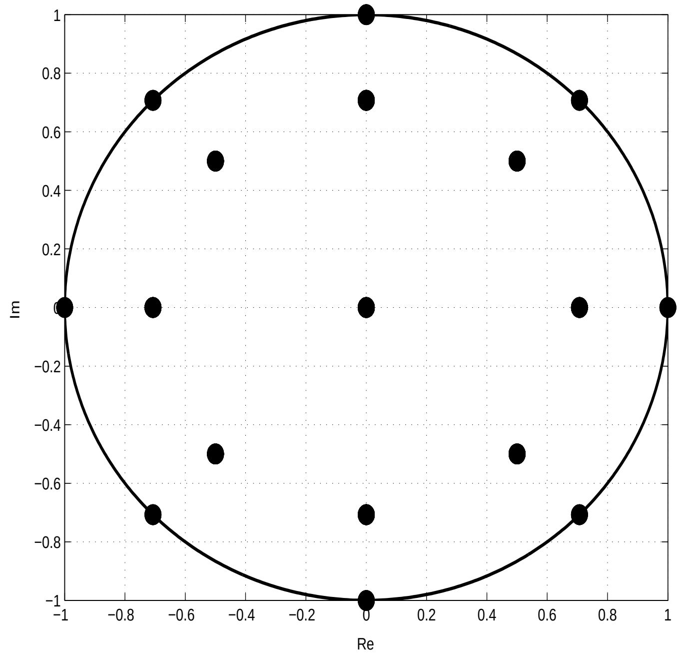

Figure 2: A Super Quaternion constellation of the set $Q_2 \cup L_2 \cup L_4$ for rate 2.8

3 Unitary 3×3 matrices from certain cyclic algebras

In our efforts to find good sets of 3×3 unitary matrices, we investigate "cyclic algebras" which are defined below. Let K/k be a cyclic Galois extension of dimension n, so that its Galois group is cyclic of order n. Let σ be a generator of the Galois group. Assume that $0 \neq \gamma \in k$. The cyclic algebra associated with this data is defined, as a left K vector space, as

$$K \oplus Kb \oplus \cdots \oplus Kb^{n-1}.$$

The multiplication is defined by the following equations: $b^n = \gamma$ and $ba = \sigma(a)b \quad \forall a \in K$. We will denote such an algebra as $(K/k, \gamma)$.

Let m, r be relatively prime integers, and let n be the order of r in the multiplicative group $(\mathbb{Z}/(m))^\star$. Let $s = (r-1, m)$ and $t = m/s$. Suppose that $(n,t) = 1$ and $n|s$. We can now define a central simple algebra over $\mathbb{Q}$. This algebra is constructed by taking the cyclotomic extension, K, generated by the roots of unity of order m. The Galois group of this extension is the multiplicative group $(\mathbb{Z}/(m))^\star$, and r defines a cyclic subgroup of order n in the Galois group, whose generator is an automorphism, σ, which raises roots of unity to the r-th power. The center of our algebra will be the fixed subfield of this automorphism, k, and σ is a generator of the Galois group of the extension K/k. Let ξ be a primitive root of unity of order m. The algebra is defined as the cyclic algebra $A_{m,r} = (K/k, \xi^t)$.

For certain values of m, r, $A_{m,r}$ is a division algebra, for instance $(m, r) = (21, 4)$. The precise conditions are quite complicated, and are spelled out completely in [2].

There is a natural embedding of this algebra in $M_n(\mathbb{C})$, which comes from the regular representation of the algebra as a left vector space of dimension n over K. Explicitly, the element $a_0 + a_1 b + a_2 b^2 + \cdots + a_{n-1} b^{n-1}$ maps to

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ \gamma\sigma(a_{n-1}) & \sigma(a_0) & \sigma(a_1) & \cdots & \sigma(a_{n-2}) \\ \gamma\sigma^2(a_{n-2}) & \gamma\sigma^2(a_{n-1}) & \sigma^2(a_0) & \cdots & \sigma^2(a_{n-3}) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \gamma\sigma^{n-1}(a_1) & \gamma\sigma^{n-1}(a_2) & \gamma\sigma^{n-1}(a_3) & \cdots & \sigma^{n-1}(a_{n-2}) \end{pmatrix}.$$

We now wish to find "unitary" elements in the algebra we have defined. The definition will depend on an anti-automorphism, τ, of the algebra, which corresponds to taking the conjugate transpose of a matrix. The "unitary" elements will be those such that $\tau(x) = x^{-1}$. The field K will be invariant under τ. Thus, it is enough to define τ on a primitive root of unity, and we take $\tau(\xi) = \xi^{-1}$. This is simply the restriction of complex conjugation to K under a fixed embedding of K in $\mathbb{C}$. It remains to define τ on b, and since b should be unitary, we must have $\tau(b) = b^{-1} = \gamma^{-1} b^{n-1}$. From the requirement τ be an anti-automorphism, this defines τ completely, and it is easy to see that it is well defined. Note that on elements of K, σ and τ commute and that $\tau^2 = id$.

We are now in a position to find many unitary $n \times n$ matrices that have positive diversity, since all the elements we find will be in a division algebra. In fact, we will need to divide by square roots. If n is odd, then adding a square root of a rational number cannot split the algebra, hence we will still have a division algebra.

When looking for unitary elements, we are looking for

$$x = \sum_{i=0}^{n-1} a_i b^i$$

where $a_i \in K$. Note that $\tau(x) = \tau(a_0) + \sum_{i=1}^{n-1} \gamma^{-1} \sigma^i(\tau(a_{n-i})) b^i$. Now, we require $x\tau(x) = 1 \in K$. If $z = x\tau(x)$ then let $z = \sum_{i=0}^{n-1} \alpha_i b^i$. It is easy to see that $\tau(z) = z$ so we get $\alpha_0 = \tau(\alpha_0)$ and $\alpha_i = \gamma^{-1}\sigma^i(\tau(\alpha_{n-i}))$. For instance, if $n = 3$, the equation $x\tau(x) = 1$ is really just two (and not three) equations, because if $\alpha_1 = 0$ then automatically $\alpha_2 = 0$.

We now specialize to the case with the case $n = 3$, let us consider the case where a_0, a_1 are known, and are in our extended algebra. In this case we get

$$x\tau(x) = (a_0 + a_1 b + a_2 b^2)(\tau(a_0) + \gamma^{-1}\sigma(\tau(a_2))b + \gamma^{-1}\sigma^2(\tau(a_1))b^2) =$$

$$= (a_0\tau(a_0) + a_1\tau(a_1) + a_2\tau(a_2)) + (\gamma^{-1}a_0\sigma(\tau(a_2)) + a_1\sigma(\tau(a_0)) + \gamma^{-1}\sigma(\tau(a_1)a_2))b + \alpha_2 b^2$$

so there are really only two equations, the second of which is of the form

$$\alpha\sigma(\tau(a_2)) + \beta a_2 = \delta$$

where $\alpha = \gamma^{-1}a_0, \beta = \gamma^{-1}\sigma(\tau(a_1)), \delta = -a_1\sigma(\tau(a_0))$, and in particular $\alpha, \beta, \delta \in K$.

Since K is a vector space over $\mathbb{Q}$ of dimension $\varphi(m)$, we get $\varphi(m)$ linear equations in the $\varphi(m)$ coordinates of a_2 as an element in K.

Thus, given $a_0, a_1 \in K$, we check if there are solutions to the linear set of equations. For each solution, a_2, we calculate

$$a_0\tau(a_0) + a_1\tau(a_1) + a_2\tau(a_2) = s(a_0, a_1, a_2) \in K.$$

We divide all three values by $\sqrt{s(a_0, a_1, a_2)}$, to get a unitary matrix. Note, that to calculate $\sigma(\sqrt{s})$ we can simply take $\sqrt{\sigma(s)}$.

If a_0, a_1 are rational, it can be seen that if $a_0^2 \neq a_1^2$ then there is a solution. Indeed, if we set $a_2 = x\gamma + y\gamma^{-1}$, we have $\sigma(a_2) = a_2$ and $\tau(a_2) = y\gamma + x\gamma^{-1}$. The equation becomes

$$\gamma^{-1}a_0(y\gamma + x\gamma^{-1}) + \gamma^{-1}a_1(x\gamma + y\gamma^{-1}) = -a_0 a_1.$$

Thus, we have in fact two equations $a_0 y + a_1 x = -a_0 a_1$ and $a_1 y + a_0 x = 0$. There is one solution, and it is $x = \frac{a_0 a_1^2}{a_0^2 - a_1^2}, y = -\frac{a_0^2 a_1}{a_0^2 - a_1^2}$.

For $n > 3$ a similar procedure gives n equations, which are actually $\lceil \frac{n+1}{2} \rceil$ equations. If we fix, as above, the value of $a_0, a_1, \ldots, a_{n-2}$ we get, disregarding the equation for the coefficient of b^0, at least two equations, involving only a_{n-1}. Thus we have at least $2\varphi(m)$, where $\varphi(m)$ denotes Euler's totient function, equations in the $\varphi(m)$ coordinates of a_{n-1}. Since the system of equations is overdetermined, this procedure has very little chance of working. On the other hand, if more than one a_i variable is left unknown, the equations become quadratic, and this seems much more difficult to solve. Thus, the ideas of this section seem to be restricted to the case $n \leq 3$. Note that for $n = 2$ the same procedure can be used.

4 Rate Bound for 2-transmit Diversity

This section presents general bounds for 2-transmit diversity both for the case of orthogonal design and the specific case of unitary design.

4.1 Isometry to $\mathbb{R}^4$

Let M_2 be a set of orthogonal matrices of the form $m_2 = \begin{pmatrix} S_1 & S_2 \\ -S_2^* & S_1^* \end{pmatrix}$ for each $m_2 \in M_2$ S_1 and S_2 are some complex symbols. We define the following isometry

$$g : M_2 \longrightarrow \mathbb{R}^4 \tag{4.1}$$

Assume $S_1 = a + bi$ and $S_2 = c + di$. Then, $g(m_2) = (a, b, c, d)$. It is easy to see that g is an isometry if we define the distance between two matrices $m_2, m_2^{'}$ in M_2 to be

$$d(m_2, m_2^{'}) = \frac{1}{2}\sqrt{det(|m_2 - m_2^{'}|)} \tag{4.2}$$

and the distance between two vectors in $\mathbb{R}^4$ to be half the Euclidian distance:

$$d((a, b, c, d), (a', b', c', d')) = \frac{1}{2}\sqrt{(a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2}. \tag{4.3}$$

The minimal distance among the matrices in M_2, according to Eq. 4.2, is the diversity of M_2 by definition.

4.2 Orthogonal Design

Assume we have a set of n vectors $\{(a_i, b_i, c_i, d_i)\}_{i=1}^n$ with minimal distance (diversity) ζ, and maximal norm A (distance from (0,0,0,0)) How the parameters n, ζ and A are related ?

Every vector $\{(a_i, b_i, c_i, d_i)\}$ is surrounded by a 4-dimensional ball of radius $\zeta/2$ that does not contain other vectors. The volume of this ball is $\frac{\pi^2}{2}\zeta^4$. Since all the vectors have at most norm A, all the balls that are defined by the volume $\frac{\pi^2}{2}\zeta^4$, are confined within the ball of radius $A + \zeta/2$, which has the volume

$$\frac{\pi^2}{2}(2A + \zeta)^4. \tag{4.4}$$

It follows that

$$n \leq \frac{\frac{\pi^2}{2}(2A + \zeta)^4}{\frac{\pi^2}{2}\zeta^4} = \left(\frac{2A + \zeta}{\zeta}\right)^4.$$

Given a maximal transmit power of a matrix of $m_2 \in M_2$, i.e. $max\{det(m_2)|m_2 \in M_2\} = P$, and a minimal diversity ζ, then the maximal number of matrices in M_2 is

$$n \leq \left(\frac{\sqrt{P}+\zeta}{\zeta}\right)^4 \tag{4.5}$$

and the maximal rate is

$$R_{max} \leq 2(log_2(\sqrt{P}+\zeta) - log_2(\zeta)). \tag{4.6}$$

4.3 Unitary Design

For unitary matrices a tighter bound can be found. Since unitary matrices have determinant 1, the isometry of a unitary set of matrices to $\mathbb{R}$, is equivalent to placing vectors on the envelope of a 4-dimensional sphere, whose volume is $\frac{\pi^2}{2}\zeta^4$. The 'area' of this envelope is

$$\frac{d}{dx}\left(\frac{\pi^2}{2}x^4\right)_{x=1} = 2\pi^2 \tag{4.7}$$

In order to calculate the free space around each vector on the envelope of the four dimensional sphere we change variables:

$$\begin{array}{ll} x \triangleq R\cos(\gamma)\cos(\theta)\cos(\varphi) & y \triangleq R\cos(\gamma)\cos(\theta)\sin(\varphi) \\ z \triangleq R\cos(\gamma)\sin(\theta) & w \triangleq R\sin(\gamma). \end{array} \tag{4.8}$$

The absolute value of the Jacobian of these variables is:

$$\begin{aligned} &\left|\begin{array}{cccc} \cos(\gamma)\cos(\theta)\cos(\varphi) & \cos(\gamma)\cos(\theta)\sin(\varphi) & \cos(\gamma)\sin(\theta) & \sin(\gamma) \\ -R\sin(\gamma)\cos(\theta)\cos(\varphi) & -Rsin(\gamma)\cos(\theta)\sin(\varphi) & -Rsin(\gamma)\sin(\theta) & R\cos(\gamma) \\ -R\cos(\gamma)\sin(\theta)\cos(\varphi) & -R\cos(\gamma)\sin(\theta)\sin(\varphi) & R\cos(\gamma)\cos(\theta) & 0 \\ R\cos(\gamma)\cos(\theta)\sin(\varphi) & -R\cos(\gamma)\cos(\theta)\cos(\varphi) & 0 & 0 \end{array}\right| \\ = \quad & R^3\cos^2(\gamma)\cos(\theta). \end{aligned} \tag{4.9}$$

Without loss of generality we calculate the free space around the vector $\vec{r_0} = (w_o, x_0, y_0, z_0)$, (equivalently defined by R_0, γ_0, θ_0 and φ_0) on the w axis, i.e. $w_0 = 1, \quad x_0 = y_0 = z_0 = 0$ or in our new coordinates $R_0 = 1, \quad \gamma_0 = \pi/2$.

For diversity ζ we calculate the free three-dimensional area around $\vec{r_0}$ by integrating over the envelope of the sphere and over the vectors within distance smaller than $\zeta/2$ (by saying distance we mean the definition in Eq. 4.3). The vector $\vec{r}$ on the sphere satisfies:

$$d(\vec{r}, \vec{r_0}) = \frac{1}{2}\sqrt{x^2+y^2+z^2+(w-1)^2} = \frac{1}{2}\sqrt{2-2w} = \frac{1}{2}\sqrt{2-2\sin(\gamma)}.$$

The free 'area' is therefore confined to

$$d(\vec{r},\vec{r_0}) = \frac{1}{2}\sqrt{2-2\sin(\gamma)} \leq \zeta/2$$
$$\sin(\gamma) \geq 1-\frac{1}{2}\zeta^2$$
$$\gamma \geq arcsin\left(1-\frac{\zeta^2}{2}\right).$$

Now, we can calculate the free 'area' around $\vec{r_0}$:

$\int\int\int_{d(\vec{r},\vec{r_0})\leq\zeta/2} R^3\cos^2(\gamma)\cos(\theta)d\gamma d\theta d\varphi = \int\int\int_{\gamma\geq arcsin\left(1-\frac{\zeta^2}{2}\right)}\cos^2(\gamma)\cos(\theta)d\gamma d\theta d\varphi =$
$\int_0^{2\pi}d\varphi\int_{\frac{-pi}{2}}^{\frac{pi}{2}}\cos(\theta)d\theta\int_{arcsin\left(1-\frac{\zeta^2}{2}\right)}^{\frac{pi}{2}}\cos^2(\gamma)d\gamma = 2\pi\cdot\sin(\theta)|_{-\pi/2}^{\pi/2}\cdot\int_{arcsin\left(1-\frac{\zeta^2}{2}\right)}^{\frac{pi}{2}}(\frac{1}{2}(1+\cos(2\gamma))d\gamma =$
$2\pi\left[\frac{\pi}{2}-arcsin\left(1-\frac{\zeta^2}{2}\right)-\frac{1}{2}sin(2arcsin\left(1-\frac{\zeta^2}{2}\right))\right].$

Using the identity:

$$\sin(2arcsinx) = 2\sin(arcsinx)\cos(arcsinx) = 2x\sqrt{1-x^2}$$

we get that the free 'area' is:

$$\begin{aligned}&\int\int\int d(\vec{r},\vec{r_0})\leq\zeta/2R^3\cos^2(\gamma)\cos(\theta)d\gamma d\theta d\varphi\\ &= 2\pi\left[\frac{\pi}{2}-arcsin\left(1-\frac{\zeta^2}{2}\right)-\zeta\left(1-\frac{\zeta^2}{2}\right)\sqrt{1-\frac{\zeta^2}{4}}\right].\end{aligned}\tag{4.10}$$

The size of a unitary constellation with diversity ζ according to Eqs. 4.7 and 4.10 is smaller than

$$n \leq \frac{\pi}{\frac{\pi}{2}-arcsin\left(1-\frac{\zeta^2}{2}\right)-\zeta\left(1-\frac{\zeta^2}{2}\right)\sqrt{1-\frac{\zeta^2}{4}}}.\tag{4.11}$$

and the maximal achieved rate is

$$R_{max} \leq \frac{1}{2}\left(log_2(\pi)-log_2(\frac{\pi}{2}-arcsin\left(1-\frac{\zeta^2}{2}\right)-\zeta\left(1-\frac{\zeta^2}{2}\right)\sqrt{1-\frac{\zeta^2}{4}})\right).\tag{4.12}$$

Examples:

1. The Super Quaternion group $Q_2\cup L_2\cup L_4$ has diversity $\zeta = 0.3827$ and rate $R = 2.79$, while the bound on the rate of a set with diversity $\zeta = 0.3827$ is $R_{max} \leq 3.2$.

2. The Super Quaternion set S_8 has diversity $\zeta = 0.1602$ and rate $R = 4$, while the bound on the rate of a set with such diversity is $R_{max} \leq 5$.

5 Finding good cosets in dimension 3

In this section $n = 3$. Our purpose here to exhibit good coset extensions of some $G_{m,r}$ groups, i.e. sets of the form $a \cdot G_{m,r}$, with a in the algebra, that are disjoint from each other. Using the terminology in section 3, we know that there is an infinite number of unitary matrices we can try, simply by taking a_0, a_1 to be rational. In fact, if we take $a_0 = 1$ and a_1 very small, we will get a unitary matrix that is very close to being the identity. This gives us the ability to make small "changes" to elements of the algebra.

We can now describe two different methods for trying to find cosets. In the first method, we construct a number of elements of the algebra in the way described above. We then simply take random multiplications of these elements. For each new element we get we check the diversity against the set of matrices we have so far. It is easy to see that this will be the diversity of the entire coset. We do this many times, and choose the coset that has the best diversity.

The second method is to construct a set of matrices that are close to the identity. One way to do this is to take $a_0 = 1$, and for each basis element of K over $\mathbb{Q}$ and each of the three elements of the first row of the matrix, we add a small rational multiple of this basis element. We can decrease this multiple as we go along, so that we make smaller and smaller changes. If we have a set of matrices, and a trial matrix, we try changing it "slightly" in all directions, and take the best one. If we can no longer improve, we decrease the multiple and try again. We can also try to add two or more cosets at a time, and try changes in one or more of the matrices. So far, when attempting to add two cosets, the best method seems to be taking two additional elements and trying to change both of them slowly.

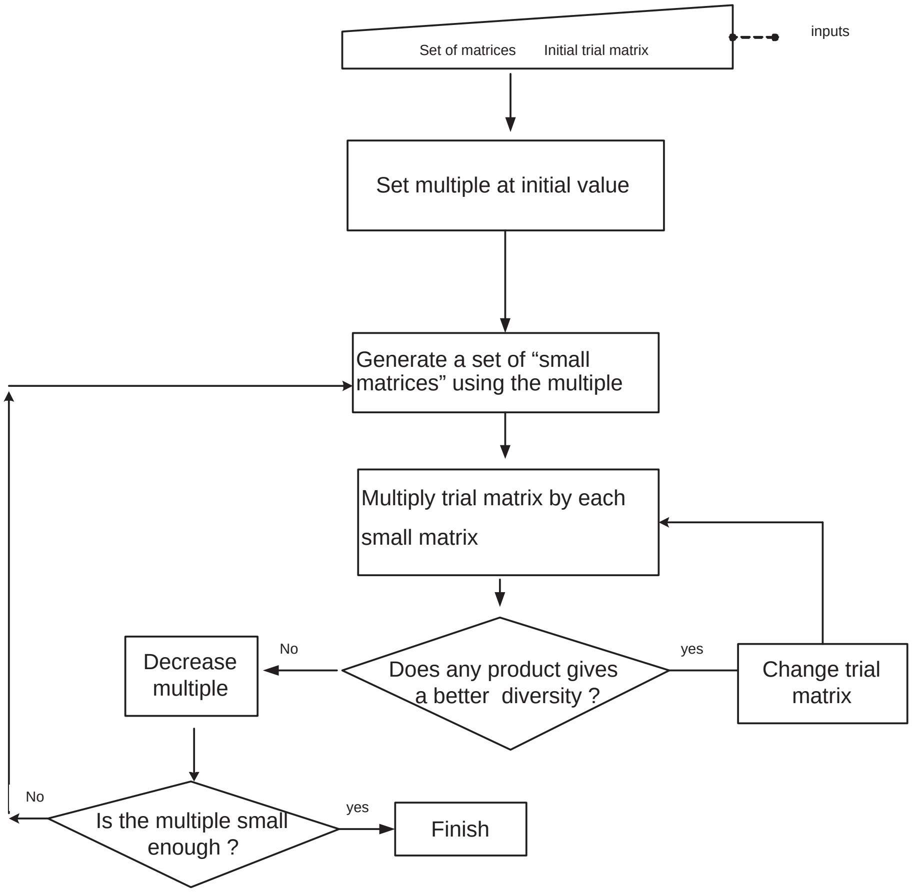

Figure 3: Flow chart for the coset computation

6 Results

6.1 Results of Super Quaternion structures

Due to the orthogonal design of the Super Quaternion structure, the Super Quaternion codes can be implemented over unknown channels as well as known channels. The two following graphs show Super Quaternion performance compared to orthogonal design over known and unknown channels. At rate 4 it can be seen than Super Quaternion design outperforms the Orthogonal design [7] by almost 2 dB at high SNR.

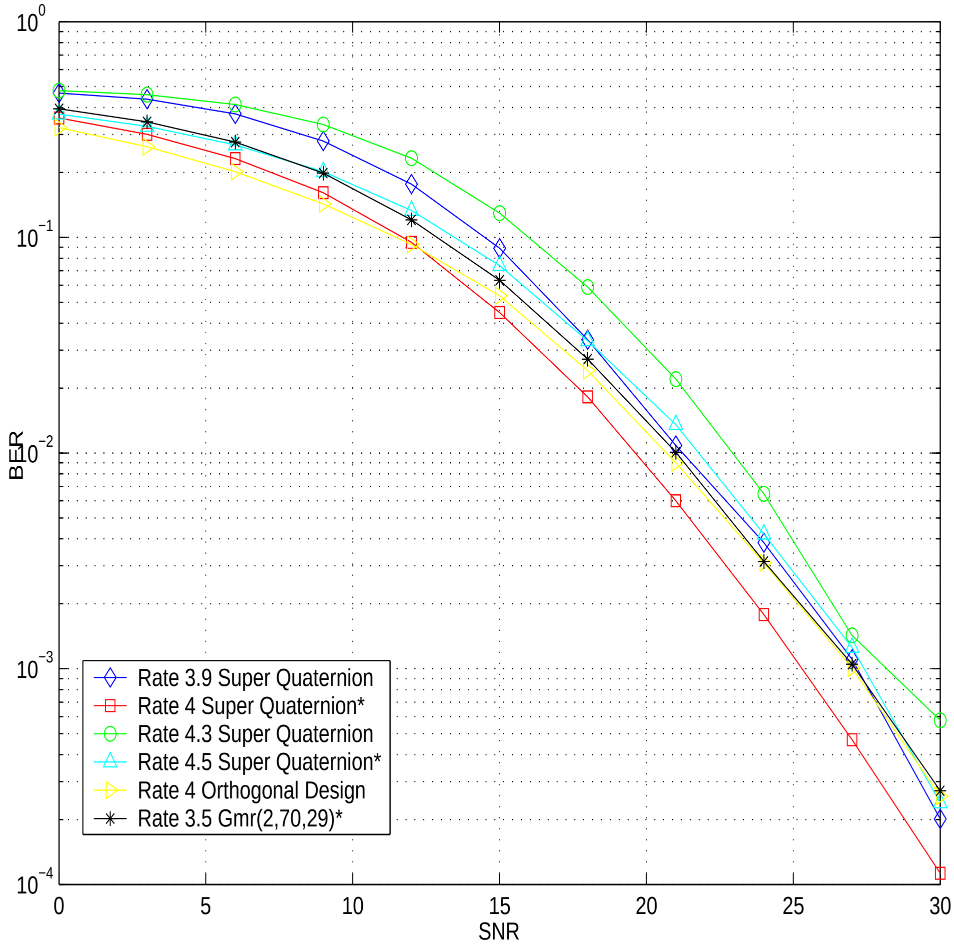

Figure 4: Comparison of Super Quaternion to other codes at high rates over known channels. * marks codes that where concatenated to whole rate for bit allocation

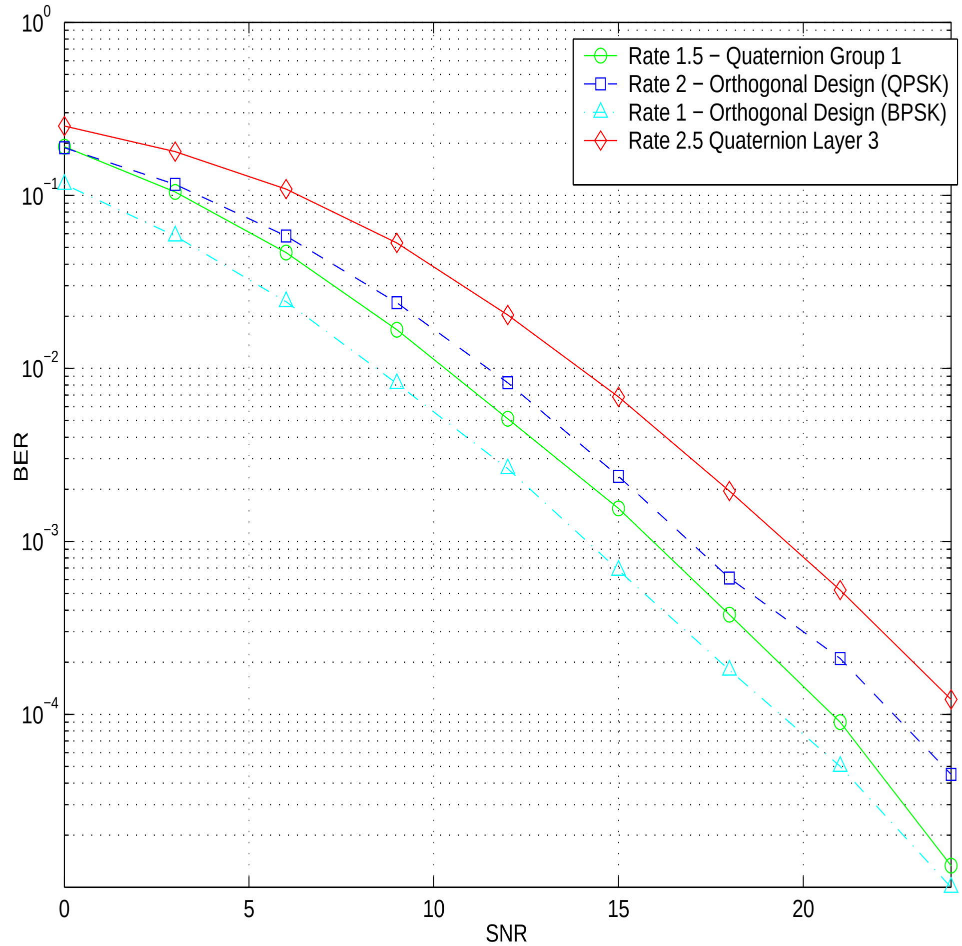

Figure 5: Comparison of Super Quaternion and Alamouti [7] Orthogonal design over known channels (the codes are available at different rates)

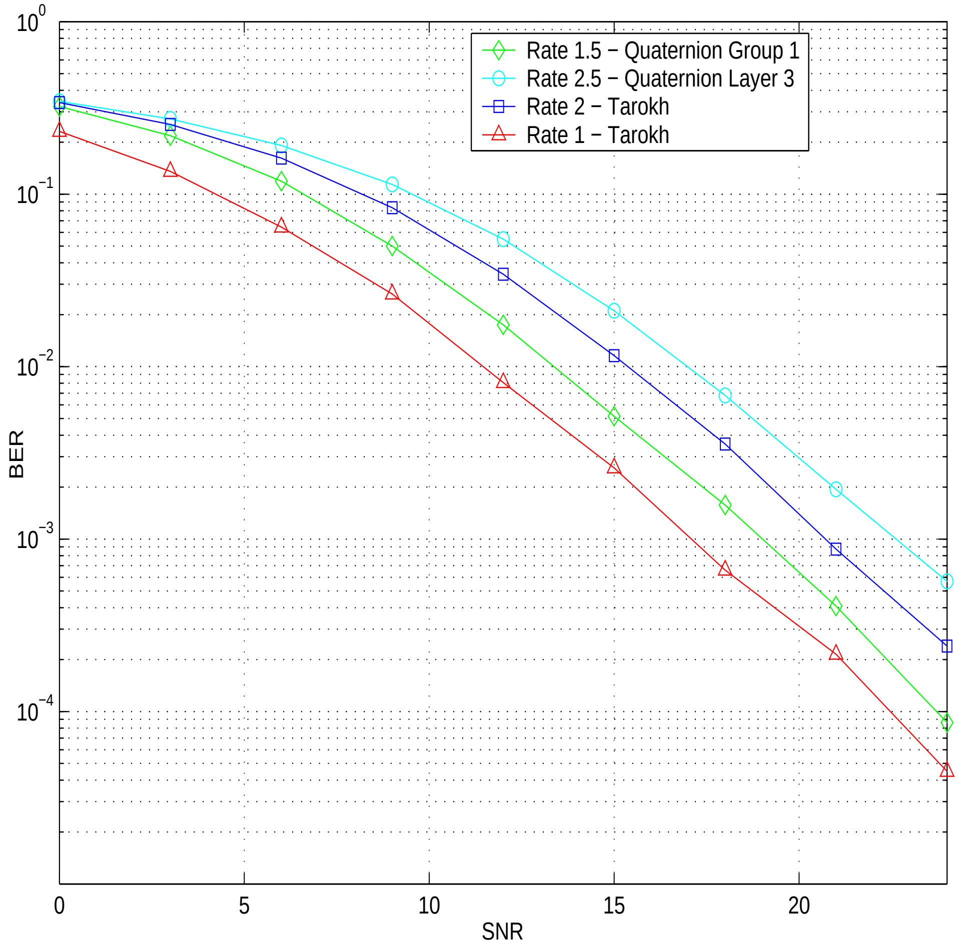

Figure 6: Comparison between the Super Quaternion and Tarokh [6] Orthogonal design over unknown channels (the codes are available at different rates)

6.2 Results of coset search

When attempting to find a good set of 512 3×3 unitary matrices, using the $G_{m,r}$ groups, the best diversity we can get is 0.184, for $m = 186, r = 25$ (there are actually 558 matrices, but for practical purposes it is often best to take a power of 2 number of matrices). However, when taking $m = 63, r = 37$ and adjoining two additional cosets (using the second method mentioned above, adding both cosets at the same time), we achieve a diversity of 0.224. When running simulations of error rates compared to SNR, we see that around an error rate of 10^{-2}, the new set has an SNR that is better by almost $1dB$ than the best $G_{m,r}$ group.

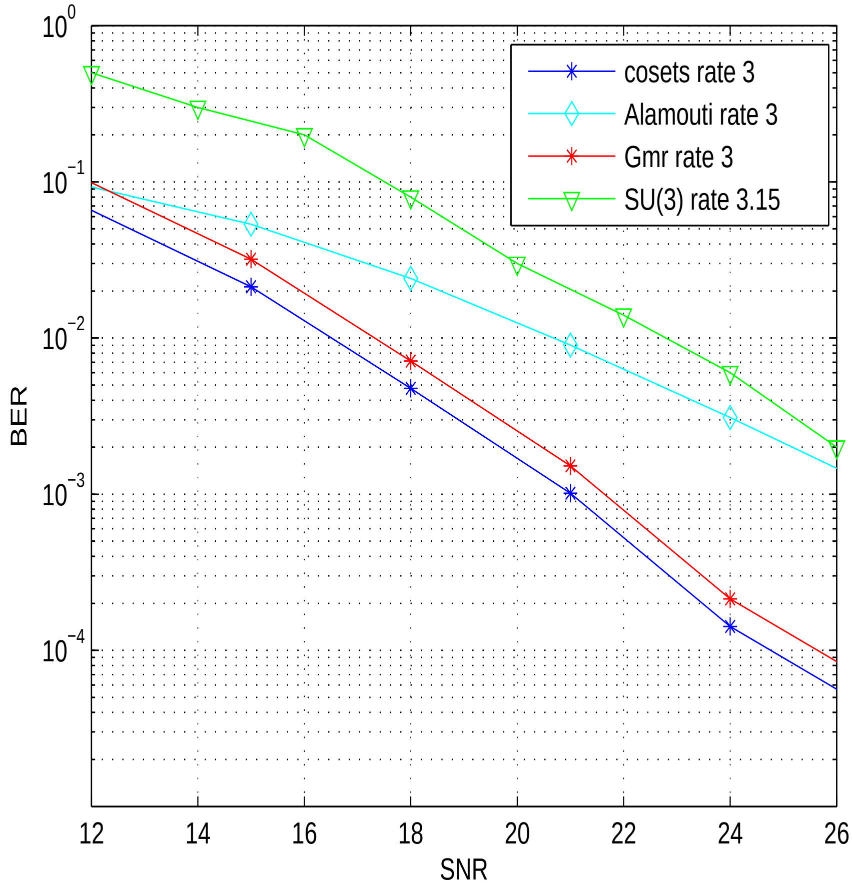

Figure 7: Comparison of rate 3 cosets over known channels to Gmr, Alamouti and SU(3) ([4]) performance

7 Conclusion

We propose new STBC that are based on division algebras. They achieve high rates at low Symbol to Noise Ratio (SNR). This work presents improved performance both in known and unknown channels. We describe two new sets of codes. The first set is a set of 'superquaternions' that improves considerably on the Alamouti codes. It is based on the mathematical fact that "normalized" integral quaternions are very well distributed over the unit sphere in 4 dimensional Euclidean space. The second set of codes gives arrays of 3 by 3 unitary matrices with full diversity. Here the idea is to use cosets of finite subgroups of division algebras that are 9 dimensional over their center, which is a finite cyclotomic extension of the field of rational numbers. It is shown that these codes outperform Alamouti and G_{mr}.

In the future, we intend to extend our techniques and develop codes for 4 transmit antennas.

References

[1] Gesbert D., Shafi M., Shiu D., Smith P. and Naguib A., *From Theory to Practice: An Overview of MIMO SpaceTime Coded Wireless Systems* IEEE J. on Selected Areas in Communications, **21(3)** (2003), 281-302.

[2] S. A. Amitsur, *Finite Subgroups of Division Rings*, Trans. Amer. Math. Soc. **80** (1955) 361–386.

[3] B. Hassibi, B. M. Hochwald, A. Shokrollahi, W. Sweldens, *Representation Theory for High-Rate Multiple-Antenna Code Design*, IEEE Trans. Inform. Theory **47** (2001), no. 6, 2335–2367.

[4] Y. Jing, B. Hassibi, *Three-transmit-antenna space-time codes based on* $SU(3)$, IEEE Trans. on Signal Processing, **53**(10) 2005, 3688 - 3702.

[5] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Hamburg, **11** (1936) 187–220.

[6] Vahid Tarokh. *A Differential Detection Scheme for Transmit Diversity*, IEEE Journal on Select Areas in Communications, Vol. 18, No. 7, July 2000.

[7] Siavash M. Alamouti, *A Simple Transmit Diversity Technique for Wireless Communications*, IEEE Journal on Select Areas in Communications, Vol. 16, No. 8, October 1998.

[8] S. Rosset, *Sums of 4 squares and groups of integral quaternions*, In preparation.

[9] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, 1980.