Gnilke, Oliver W.; Barreal Fernandez, Amaro; Karrila, Alex; Tran Nguyen Thanh, Ha; Karpuk, David A.; Hollanti, Camilla

Well-rounded lattices for coset coding in MIMO wiretap channels

Published in:
26th International Telecommunication Networks and Applications Conference, ITNAC 2016

DOI:
10.1109/ATNAC.2016.7878824

Published: 14/03/2017

Document Version
Peer reviewed version

Please cite the original version:
Gnilke, O. W., Barreal Fernandez, A., Karrila, A., Tran Nguyen Thanh, H., Karpuk, D. A., & Hollanti, C. (2017). Well-rounded lattices for coset coding in MIMO wiretap channels. In *26th International Telecommunication Networks and Applications Conference, ITNAC 2016* (pp. 289-294). [7878824] IEEE. https://doi.org/10.1109/ATNAC.2016.7878824

Well-Rounded Lattices for Coset Coding in MIMO Wiretap Channels

Oliver W. Gnilke, Amaro Barreal, Alex Karrila, Ha Thanh Nguyen Tran,
David A. Karpuk, Camilla Hollanti, *Member, IEEE*
Department of Mathematics and Systems Analysis
Aalto University School of Science, Finland
Emails: {oliver.gnilke, amaro.barreal, alex.karrila, ha.n.tran, david.karpuk, camilla.hollanti}@aalto.fi

***Abstract*—The concept of well-rounded lattices has recently found important applications in the setting of a fading *single-input single-output* (SISO) wiretap channel. It has been shown that, under this setup, the property of being well-rounded is critical for minimizing the eavesdropper's probability of correct decoding in lower SNR regimes. The superior performance of coset codes constructed from well-rounded lattices has been illustrated in several simulations.**

In the present article, this work is extended to fading *multiple-input multiple-output* (MIMO) wiretap channels, and similar design criteria as in the SISO case are derived. Further, explicit coset codes for Rayleigh fading MIMO wiretap channels are designed. In particular, it is shown through extensive simulations that sublattices of the well-known Alamouti code and Golden code which meet our design criteria perform better than scalar multiples of the code lattice for the same parameters.

I. Introduction

In the setup of a (wireless) wiretap channel, it is assumed that the same signal is received by two different parties via two different, independent channels. The intended recipient, referred to as Bob, is assumed to have a higher quality channel and hence a higher signal-to-noise ratio (SNR) than the eavesdropper, Eve, who has to endure a degraded channel. This imbalance has been shown to be sufficient to achieve information theoretic security, *i.e.*, Eve's received vector has negligible mutual information with the message, while there is a positive information rate from the sender, Alice, to Bob.

Code design in this setup needs to be aimed at achieving several goals simultaneously: while it is critical to maximize Bob's correct decoding probability and information rate, Eve's information needs to be minimized. Coset coding [1] aims at fulfilling these goals by adding random bits to the message to confuse the eavesdropper, while allowing Bob to detect the confusion bits and correctly retrieve the information.

A. Related Work and Contributions

One approach to construct good lattices for coset coding in wiretap channels is to use *Eve's correct decoding probability* (ECDP), studied in [2], [3], where also design criteria were derived from approximations of the ECDP. Recently it has been shown that also in a *multiple-input multiple-output* (MIMO) setting the mutual information between Eve and Alice can be related to Eve's correct decoding probability via the so-called *flatness factor* of the lattice related to the eavesdropper [4]–[6], validating this approach. For related work in terms of flatness factor and its approximations, see further [7], [8].

The previous ECDP-based design criteria are commonly based on relatively coarse approximations, resulting in the so-called *inverse-norm sum* in the *single-input single-output* (SISO) case [2], also studied in [9], or the *inverse determinant sum* [3] in the MIMO setting. See [10] for related work in the reliability setting. In [11] so-called i-th coding gains are defined which were used in [12] to derive a simple geometric criterion for the design of coset codes.

In this paper we derive a similar design criterion based on well-rounded lattices. It stems from a tighter approximation of the ECDP, and we show that it is valid for *space-time* (ST) block codes. Our predictions are verified via extensive simulations and we can show that these lattices outperform the common choice of scalar multiples of the base lattice in the low SNR regime, while performing equally well for high SNR.

We introduce the required basics on lattices and cyclic algebras in Section II, and the concept of ST coding in Section III, wherein we show how to construct codes from cyclic division algebras. As an example and as an ingredient for our simulations, we also introduce the famous Alamouti and Golden codes in detail. The wireless wiretap channel is covered in Section IV, where we further introduce the concept of coset coding and derive a design criterion for MIMO wiretap coset codes. Extensive simulations are then carried out in Section V, where we disclose the performance of sublattices of the Alamouti and Golden codes meeting the derived design criterion when compared to other obvious choices, *i.e.*, scalar multiples of the codebook lattice or other diagonal matrices.

II. Lattices and Cyclic Algebras

In this section, we introduce the basic concept of a lattice and recall also basic properties of cyclic division algebras, two objects which are fundamentally important for the construction of well-performing codes for physical layer communications.

A. Lattices

A *lattice* $\Lambda \subset \mathbb{R}^n$ of *rank* $\mathrm{rk}(\Lambda) = s \leq n$ and dimension $\dim(\Lambda) = n$ is a discrete subgroup of $\mathbb{R}^n$ with the property that there exist s linearly independent vectors $(\mathbf{b}_1, \ldots, \mathbf{b}_s)$ of

$\mathbb{R}^n$ such that

$$\Lambda = \bigoplus_{i=1}^{s} \mathbf{b}_i \mathbb{Z}.$$

The lattice is *full rank* if $s = n$.

A lattice $\Lambda' \subset \mathbb{R}^n$ such that $\Lambda' \subset \Lambda$ is called a *sublattice* of Λ. The group *index* $|\Lambda/\Lambda'|$ of Λ' in Λ is finite provided that $\dim(\Lambda) = \dim(\Lambda')$.

We can conveniently represent a lattice by defining a *generator matrix* $M_\Lambda := [\mathbf{b}_1 \ \cdots \ \mathbf{b}_s] \in \mathrm{Mat}(n \times s, \mathbb{R})$, so that we can equivalently write

$$\Lambda = \{ \lambda = M_\Lambda \mathbf{z} | \ \mathbf{z} \in \mathbb{Z}^s \}.$$

The *volume* of Λ is defined to be $\nu_\Lambda = |\det(M_\Lambda)|$, and is independent of the choice of basis. If Λ is not full rank, then $\nu_\Lambda = \det(M_\Lambda^t M_\Lambda)^{1/2}$. The volume of a sublattice $\Lambda' \subset \Lambda$ can easily been computed to be

$$\nu_{\Lambda'} = \nu_\Lambda \, |\Lambda/\Lambda'| \, ;$$

We define the *Voronoi cell* associated with a lattice point $\lambda \in \Lambda$ as the set

$$\mathcal{V}_\Lambda(\lambda) := \left\{ \mathbf{x} \in \mathbb{R}^n | \, ||\mathbf{x} - \lambda||^2 \leq ||\mathbf{x} - \lambda'||^2, \lambda' \in \Lambda \backslash \{\lambda\} \right\}.$$

Definition 1. *Let $\Lambda \subset \mathbb{R}^n$ be a full rank lattice, and let $\lambda_i = \lambda_i(\Lambda) := \inf\{ r | \dim(\mathrm{span}(\Lambda \cap \mathcal{B}_r)) \geq i \}$ be the succesive minima of Λ, where $\mathcal{B}_r$ is the sphere of radius r around the origin. Then Λ is called* well-rounded *(WR) if $\lambda_1 = \cdots = \lambda_n$.*

B. Cyclic Division Algebras

For a nice general exposition on cyclic division algebras and space-time codes, we refer to [13].

Let L/K be a degree n cyclic Galois field extension, and fix a generator σ of the Galois group $\langle \sigma \rangle = \Gamma(L/K)$. A *cyclic algebra* of degree n is a triple

$$\mathcal{C} = (L/K, \sigma, \gamma) := \bigoplus_{i=0}^{n-1} u^i L,$$

where $u^n = \gamma \in K^\times$ and $lu = u\sigma(l)$ for all $l \in L$. The algebra $\mathcal{C}$ is *division*, if every nonzero element of $\mathcal{C}$ is invertible.

Remark 1. *If $n = 2$, then necessarily $L = K(\sqrt{a})$ for some square-free $a \in \mathbb{Z}$. In this case, the algebra $\mathcal{C} = (L/K, \sigma, \gamma)$ is known as a* quaternion algebra*, and can equivalently be denoted as*

$$\mathcal{C} = (a, \gamma)_K \cong L \oplus jL \cong K \oplus iK \oplus jK \oplus kK,$$

where the basis elements satisfy $i^2 = a$, $j^2 = \gamma$, $ij = -ji = k$. As we will see later, the case $a = \gamma = -1$ and $K = \mathbb{R}$ gives rise to the famous Hamiltonian quaternions *and the well-known* Alamouti code*.*

Given a cyclic division algebra $\mathcal{C} = (L/K, \sigma, \gamma)$ of degree n, the *left-regular representation* is an injective algebra homomorphism $\psi : \mathcal{C} \to \mathrm{Mat}(n, \mathbb{C})$ given by left multiplication $y \mapsto xy$ by a fixed $x \in \mathcal{C}$ for any $y \in \mathcal{C}$. Given an element $y = \sum_{i=0}^{n-1} y_i u^i \in \mathcal{C}$, $y_i \in \mathcal{O}_L$, its representation over the maximal subfield L is given by

$$\psi : y \mapsto \begin{bmatrix} y_0 & \gamma\sigma(y_{n-1}) & \gamma\sigma^2(y_{n-2}) & \cdots & \gamma\sigma^{n-1}(y_1) \\ y_1 & \sigma(y_0) & \gamma\sigma^2(y_{n-1}) & \cdots & \gamma\sigma^{n-1}(y_2) \\ \vdots & \vdots & \vdots & & \vdots \\ y_{n-2} & \sigma(y_{n-3}) & \sigma^2(y_{n-4}) & \cdots & \gamma\sigma^{n-1}(y_{n-1}) \\ y_{n-1} & \sigma(y_{n-2}) & \sigma^2(y_{n-3}) & \cdots & \sigma^{n-1}(y_0) \end{bmatrix}. \quad (1)$$

Choosing y_i above to be in the ring of integers $\mathcal{O}_L$ will guarantee a non-vanishing determinant and hence a good coding gain, provided that the center field K is either the rationals or quadratic imaginary. This is the case for both the Alamouti code ($K = \mathbb{Q}$) and Golden code ($K = \mathbb{Q}(i), i = \sqrt{-1}$).

III. Algebraic Space–Time Codes and MIMO channel model

Algebraic *space–time* (ST) coding is a powerful technique for reliable data exchange in a wireless MIMO setting. It enables spatial and temporal diversity by making use of multiple spatially separated antennas at the transmitter and / or receiver, and by transmitting information redundantly over multiple time instances. The well-known MIMO channel equation is given by

$$Y_{n_r \times T} = H_{n_r \times n_t} X_{n_t \times T} + N_{n_r \times T}. \quad (2)$$

The subscripts n_t, n_r and T denote the number of antennas at the transmitter, receiver, and the number of channel uses, respectively. We only consider the fully symmetric case $n_t = n_r = T = n$ for some n, and henceforth omit all subscripts.

In the above equation, the random complex *channel matrix* H models Rayleigh fading, that is, the norm of its entries, $|h|$, follow a Rayleigh distribution with scale parameter σ_h, *i.e.*, for every entry $h = \Re(h) + i\Im(h)$ the real and imaginary parts follow a Gaussian distribution $\Re(h), \Im(h) \sim \mathcal{N}(0, \sigma_h^2)$. We normalize $\sigma_h = 1$. The matrix N is a noise matrix with zero-mean complex white Gaussian components with variance σ^2. The object of interest in the above equation is the transmitted codeword X, which will be an element of a finite codebook $\mathcal{X}$ of a certain algebraic structure. We assume that the channel is quasi-static, that is, H stays fixed during the transmission of X and then changes independently of its previous state. Perfect channel state information is only assumed at the receivers.

Definition 2. *Let $\{B_i\}_{i=1}^k$ be an independent set of fixed $n \times n$ complex matrices. A* linear space–time block code *of rank k is a set of the form*

$$\mathcal{X} = \left\{ \sum_{i=1}^{k} s_i B_i \middle| \, s_i \in S \right\},$$

where $S \subset \mathbb{Z}$ is a finite signaling alphabet*.*

If the matrices $\{B_i\}_{i=1}^k$ form a basis of a lattice $\Lambda \subset \mathrm{Mat}(n, \mathbb{C})$ *we call $\mathcal{X}$ a* ST lattice code*. Its rank is $k = \mathrm{rk}(\Lambda) \leq 2n^2$, and $\mathcal{X}$ is full-rank in case of equality.*

Henceforth, we will refer to a ST lattice code simply as a ST code. In what follows, we will quickly recall how to construct such ST codes from cyclic division algebras. The interested

reader is referred to [13] for further details. An advantage of using cyclic algebras for ST coding is that a lattice structure is easily ensured by restricting the choice of elements to certain subrings of the algebra. For our examples, the restriction of the coefficients y_i (cf. (1)) to the ring of integers $\mathcal{O}_L$ (or an ideal therein) will suffice. This is typically referred to as the *natural order* of the algebra.

Let k be the absolute extension degree (*i.e.*, the rank of the related lattice) of $\mathcal{C}$ over $\mathbb{Q}$ and $\{B_i\}_{i=1}^k$ a matrix basis of $\psi(\mathcal{C})$ over the integers $\mathbb{Z}$. A ST code constructed from the natural order for a fixed signaling alphabet $S \subset \mathbb{Z}$ is of the form

$$\mathcal{X} = \left\{ \sum_{i=1}^{k} s_i B_i \middle| s_i \in S \right\}.$$

By choosing $\mathcal{C}$ to be division, we can ensure that the difference of any two distinct codewords $X - X'$ will be full-rank, and we refer to such a code as a *full-diversity* code. We define

$$\Delta_{\min}(\mathcal{X}) := \inf_{X \in \mathcal{X}} |\det(X)|^2$$

to be the minimum determinant of the infinite code (normalized to ν_Λ = 1), that is, where $S = \mathbb{Z}$. As briefly mentioned earlier, the restriction of the matrix elements to (an ideal of) $\mathcal{O}_L$ ensures that for any matrix $\psi(y)$, $\det(\psi(y)) \in \mathcal{O}_K$, thus guaranteeing strictly positive minimum determinants $\Delta_{\min}(\mathcal{X})$ for $K = \mathbb{Q}$ or K imaginary quadratic, even as $|S| \to \infty$.

A. The Alamouti Code

The first ST block code was proposed in [14], of which the underlying algebraic structure is that of a quaternion algebra.

Let $n = 2$. The famous *Hamiltonian quaternions* can be described as

$$\mathbb{H} := (-1,-1)_{\mathbb{R}} \cong \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R},$$

where σ stands for complex conjugation, and the basis elements satisfy the relation $i^2 = j^2 = k^2 = ijk = -1$.

In order to ensure a discrete structure on a ST code constructed from $\mathbb{H}$, we consider the restriction of the Hamiltonian quaternions from $\mathbb{C}/\mathbb{R}$ to $\mathbb{Q}(i)/\mathbb{Q}$, that is, consider the cyclic division algebra $\mathcal{C} := (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1)$, and define the *Alamouti code* as a finite subset $\mathcal{X}_{\mathbb{H}}$ of

$$\Lambda_{AC} = \left\{ \tfrac{1}{\sqrt{2}} \begin{bmatrix} x_1 + x_2 i & -(x_3 - x_4 i) \\ x_3 + x_4 i & x_1 - x_2 i \end{bmatrix} \middle| (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \right\}.$$

We remark that $\mathcal{C}$ is a division algebra, so that $\mathcal{X}_{\mathbb{H}}$ is a full-diversity code. The factor $\frac{1}{\sqrt{2}}$ is in order to normalize to $\nu_{\Lambda_{AC}} = 1$. Moreover, by imposing the restriction $x_i \in \mathbb{Z}$ on the entries of the codeword matrices, we have $\Delta_{\min}(\mathcal{X}_{\mathbb{H}}) = \frac{1}{4}$, so that the code indeed has nonvanishing determinants.

B. The Golden Code

The celebrated Golden code was introduced in [15]. For $n = 2$, consider the field extension $L/K = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$, with Galois group $\langle \sigma : \sqrt{5} \mapsto -\sqrt{5} \rangle = \Gamma(L/K)$. Define the *Golden algebra* $\mathcal{G} = (L/K, \sigma, i)$, and let $\theta := \frac{1+\sqrt{5}}{2}$, so that $\mathcal{O}_L = \mathbb{Z}[i, \theta]$.

Defining a ST code from $\mathcal{C}$ without further shaping would result in a non-orthogonal code, *i.e.*, not all codeword matrices would be orthogonal. We force the code to be orthogonal by additionally considering the ideal $(\alpha) = (1 - i + i\theta) \subset \mathcal{O}_L$, and define the Golden code to be a finite subset $\mathcal{X}_{\mathcal{G}}$ of

$$\Lambda_{GC} = \left\{ \tfrac{1}{5^{1/4}} \begin{bmatrix} \alpha(x_1 + x_2\theta) & i\sigma(\alpha)(x_3 + x_4\sigma(\theta)) \\ \alpha(x_3 + x_4\theta) & \sigma(\alpha)(x_1 + x_2\sigma(\theta)) \end{bmatrix} \middle| x_i \in \mathbb{Z}[i] \right\}.$$

The Golden algebra is division, so that the Golden code is fully diverse. The factor $\frac{1}{5^{1/4}}$ is in order to normalize to $\nu_{\Lambda_{GC}} = 1$. Moreover, it is straightforward to compute $\Delta_{\min}(\mathcal{X}_{\mathcal{G}}) = \frac{1}{5}$, so that we have nonvanishing determinants.

IV. Coset Coding for Security

The wiretap channel was introduced by Wyner [16] and coset coding was presented as an approach to achieve secrecy in discrete memoryless channels by Ozarow and Wyner [17]. Nested lattices as a realization of coset coding has been investigated in several papers for use in gaussian wireless wiretap channels, *e.g.*, [3], [4], [18]. When using coset coding, each message M is mapped to several different codewords in $\mathcal{X}$. While this reduces the information rate, it can increase confusion at the eavesdropper.

For a given ST code $\mathcal{X}$ we define a coset coding scheme by fixing a sublattice $\Lambda_E \subset \mathcal{X}$. Two codewords $C, C' \in \mathcal{X}$ then represent the same message iff $C - C' \in \Lambda_E$, *i.e.*, if they lie in the same coset wrt. Λ_E. The set of all possible distinct messages m is then given by $\mathcal{V}_{\Lambda_E}(0) \cap \mathcal{X}$. When sending a certain message M a representative $C = M + R \in \mathcal{X}$ with $R \in \Lambda_E$ from the corresponding coset is chosen and transmitted via the MIMO channel

$$Y = H(M + R) + N, \tag{3}$$

as in (2). R can be either random or a public message.

As signaling alphabets we chose a $2n-PAM$ constellation $S = \{-2n+1, -2n+3, \ldots, 2n-1\}$, the odd integers in a symmetric interval around 0.

Definition 3. *The information rate in* bits per (n) channel uses *(bpcu)* $r_i = \ell_i/n$ *that is achieved by this scheme is given by the number of cosets,* i.e.*, the index* $|\Lambda/\Lambda_E| = 2^{\ell_i}$*. The (average) number of coset representatives* $\frac{|\mathcal{X}|}{|\Lambda/\Lambda_E|} = 2^{\ell_c}$ *defines the rate of confusion* $r_c = \ell_c/n$ *in bpcu.*

We see that the total data rate is $r_d = r_i + r_c = \log_2(|\mathcal{X}|)/n$ bpcu, so that we therefore will need to balance information rate against security.

In [3], the ECDP is used to derive a relatively complex and implicit design criterion. Later it was shown [4]–[7] that the ECDP is in fact related to the mutual information via the flatness factor, as mentioned in the introduction. Ignoring some constant factors it is shown that a good approximation to the ECDP is bounded by an expression of the form

$$\text{ECDP} \lesssim \sum_{X \in \Lambda_E \setminus \{0\}} \det\left(I_n + \sigma_E^{-2n} X X^*\right)^{-n_r - T} \tag{4}$$

where σ_E^2 is the noise variance at Eve, assuming that the fading has normalized Rayleigh parameter $\sigma_h = 1$, while n_r is the number of receive antennas at Eve and T the number of channel uses.

Proposition 1. *For low SNR the expression in equation* (4) *is minimized by a well-rounded lattice.*

A rigorous proof will be presented in an extended version of this paper, but we can quickly outline some intuitive reasoning. We use the definition of *i^{th} normalized coding gain* from [11] which corresponds to the coefficient of the degree i term in a polynomial expansion of the denominator in (4) with respect to σ_E. The first coding gain, which determines the behaviour for low SNR is given by

$$N\delta_1(\Lambda_E) := \inf\{\|X\|_F^2 \mid X \in \Lambda_E\}. \tag{5}$$

Since $\|X\|_F^2 = \|\operatorname{vec}(X)\|_2^2$, where $\operatorname{vec}(X)$ is the vectorized rearrangement of X, we see that a design criterion for the low SNR regime should be given by maximizing the minimum length of vectors in Λ_E. From Minkowski's second theorem we know that for lattices of fixed volume the product of all successive minima is bounded. The minimum is therefore maximized in the case where all succesive minima are equal, leading us to consider WR lattices as choices for Λ_E, similarly to the SISO case [12].

V. Simulations

A. Alamouti

We compare several sublattices of the Alamouti code using the signaling alphabets $S_1 := \{\pm 3, \pm 1\}$ or $S_2 := \{\pm 7, \pm 5, \pm 3, \pm 1\}$ which correspond to a 4-PAM (equivalently, 16-QAM) or an 8-PAM (equivalently, 64-QAM) constellation for the real (equivalently, complex) symbols, respectively. The Alamouti code as a sublattice of $\mathbb{R}^8$ is described by the generator matrix

$$A := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

The codebook is then given by all vectors in $\mathcal{X} = \{A\mathbf{z} : \mathbf{z} \in S^4\}$. For our simulations, we fix $n_r = 2$ and proceed in the following fashion. After choosing a random element $X = Ax \in \mathcal{X}$, we calculate Y as in equation (2) and use a sphere decoder to find the closest vector $Z \in \mathcal{X}$ in the codebook. Since we apply coset coding we have to consider the case that $Z \neq X$, but $X \equiv Z \mod \mathcal{X}_E$, where $\mathcal{X}_E \subset \mathcal{X}$ is a subset, in which case X and Z represent the same message. Instead of defining $\mathcal{X}_E$ directly as a sublattice of the Alamouti code we define a sublattice of the coefficient set $\mathbb{Z}^4$, *i.e.*, let $X = Ax$ and $Z = Az$ then $X \equiv Z \mod \mathcal{X}_E \Leftrightarrow x \equiv z \mod \Lambda_E$. Since A is orthonormal, a well-rounded sublattice $\Lambda_E \subset \mathbb{Z}^4$ will define a well-rounded sublattice $\mathcal{X}_E \subset \mathcal{X}$.

We define three different such sublattices Λ_i by their generator matrices L_i. Each of these lattices provides the same number of cosets and hence the same information rate. The first lattice is a straightforward approach of achieving index 32 in the signaling set, simply by constructing a diagonal matrix. The second matrix has been found by simple computer search and provides the same index, while having a larger minimal length. The lattice Λ_3 is a scaled version of the D_4 lattice. The fourth and fifth lattices have index 256 and are a simple multiple of the base lattice and an optimized WR lattice found by computer search.

$$L_1 := 2 \cdot \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad L_2 := 2 \cdot \begin{bmatrix} -2 & -2 & 0 & 0 \\ 0 & 0 & -2 & -1 \\ -1 & 1 & 1 & -2 \\ 1 & -1 & 1 & -1 \end{bmatrix}$$

$$L_3 := 2 \cdot \begin{bmatrix} 4 & 2 & 2 & 2 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad L_4 := 2 \cdot \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

$$L_5 := 2 \cdot \begin{bmatrix} -2 & -3 & 4 & -1 \\ 0 & -1 & 0 & 3 \\ 0 & -3 & -2 & -3 \\ -4 & -1 & 0 & -1 \end{bmatrix}.$$

The two different signaling sets S_1 and S_2 give us two different codebook sizes. Since the information rate is fixed by the index of the sublattice, an increase in codebook size increases the rate of confusion. The ECDP is lower bounded by the reciprocal of the index, since a correct decoding rate of $\frac{1}{32}$ is equal to randomly guessing the message, hence no mutual information between Alice and Eve. In Figure 1 we can see that the different lattices perform equally well in the high SNR regime, providing the legitimate receiver with comparable reliability. For lower SNRs the different lattices show different performances and it can be seen that the WR lattices approach the lower bound quicker than the non-WR lattices. The higher rate of confusion in the bigger codebooks translates into a 10dB gain.

				16-QAM			64-QAM		
	index	WR	λ_1^2	r	r_i	r_c	r	r_i	r_c
Λ_1	32	no	16						
Λ_2	32	yes	24	4	2.5	1.5	6	2.5	3.5
Λ_3	32	yes	32						
Λ_4	256	yes	64				6	4	2
Λ_5	256	yes	80						

TABLE I
Sublattices of the Alamouti Code

Identical to the observations in [12], [19] we see in Figure 2 that it is advantageous to use WR lattices that are not orthogonal.

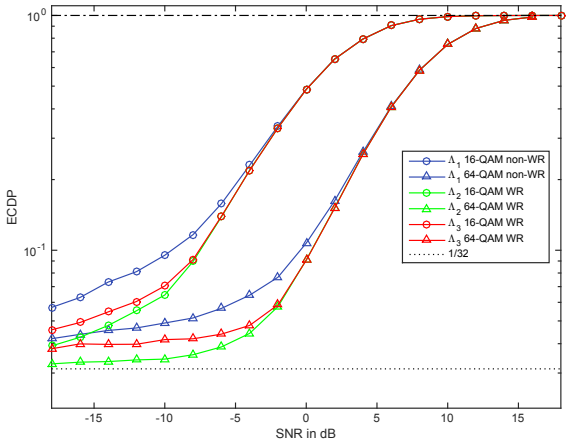

Fig. 1. ECDP for 16-QAM and 64-QAM Alamouti

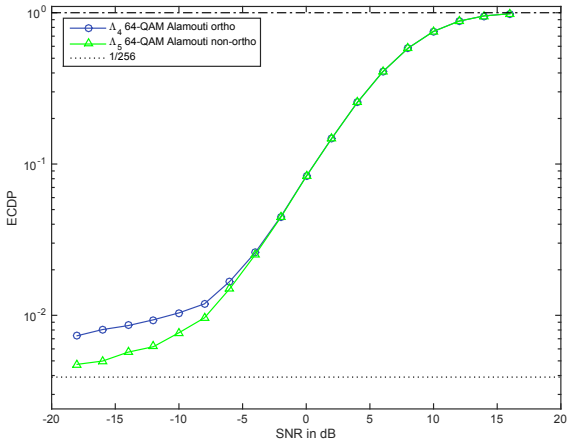

Fig. 2. ECDP for 64-QAM Alamouti

B. Golden Code

The Golden code is an orthonormal sublattice of $\mathbb{R}^8$ with generator matrix

$$G := \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1-\theta & \theta & -1 & 0 & 0 & 0 & 0 \\ \theta-1 & 1 & 1 & \theta & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1-\theta & \theta & -1 \\ 0 & 0 & 0 & 0 & \theta-1 & 1 & 1 & \theta \\ 0 & 0 & 0 & 0 & 1-\bar{\theta} & -1 & -1 & -\bar{\theta} \\ 0 & 0 & 0 & 0 & 1 & 1-\bar{\theta} & \bar{\theta} & -1 \\ 1 & 1-\bar{\theta} & \bar{\theta} & -1 & 0 & 0 & 0 & 0 \\ \bar{\theta}-1 & 1 & 1 & \bar{\theta} & 0 & 0 & 0 & 0 \end{bmatrix}$$

where $\bar{\theta} = \frac{1-\sqrt{5}}{2}$. As in the previous subsection we choose codebooks by defining finite signaling sets. We again use odd integers in a finite range which can be understood as QAM constellations, *e.g.*, $S_1 := \{\pm 1\}$ corresponds to 4-QAM, $S_2 := \{\pm 3, \pm 1\}$ corresponds to 16-QAM, ..., $S_4 := \{\pm 9, \pm 7, \ldots, \pm 1\}$ corresponds to 100-QAM.

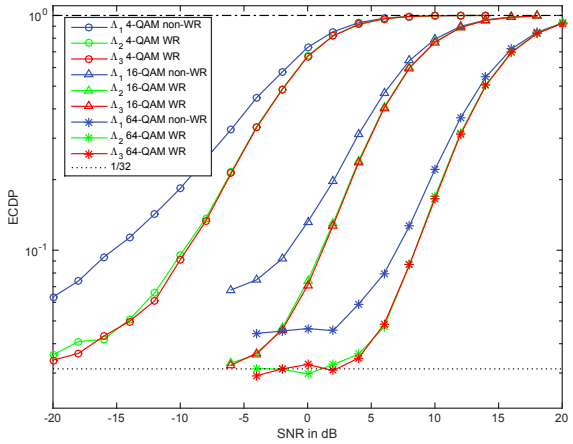

Fig. 3. ECDP for 4-QAM, 16-QAM and 64-QAM Golden Code

We chose sublattices Λ'_i of index 32 with generator matrices

$$L'_1 = 2 \cdot \mathrm{diag}(2,2,2,2,2,1,1,1),$$

$$L'_2 = 2 \cdot \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 \\ 1 & 1 & 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \end{bmatrix},$$

$$L'_3 = 2 \cdot \begin{bmatrix} -1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & -2 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 2 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & -2 & 0 \end{bmatrix}.$$

The first lattice is again a simple diagonal construction, while the other two were found by computer search.

	index	WR	λ_1^2	4-QAM			16-QAM			64-QAM		
				r	r_i	r_c	r	r_i	r_c	r	r_i	r_c
Λ'_1	32	no	4									
Λ'_2	32	yes	12	4	2.5	1.5	8	2.5	5.5	12	2.5	9.5
Λ'_3	32	yes	16									

TABLE II
SUBLATTICES OF THE GOLDEN CODE OF INDEX 32

The simulation results in Figure 3 show even more pronouncedly than in the Alamouti case that the WR lattices outperform the non-WR choices, while maintaining reliability in the high SNR regime. Also the effect of adding more bits of confusion is clearly visible. Again there is a 10dB gap between 1.5 and 5.5 bits of confusion, and a 8dB difference from 5.5 to 9 bits of confusion.

A comparison between the Alamouti and the Golden code in Figure 4 shows that the Golden code achieves higher reliability in the high SNR regime, but catches up with even the best sublattice of the Alamouti code in low SNR. To investigate the effect of the ratio between r_i and r_c we run a simulation with three sublattices that have comparable values r_c but different r_i, when combined with the right signaling set. Their generator

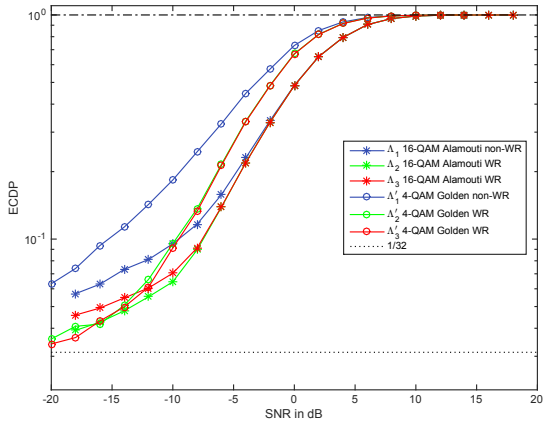

Fig. 4. ECDP for 16-QAM Alamouti and 4-QAM Golden Code

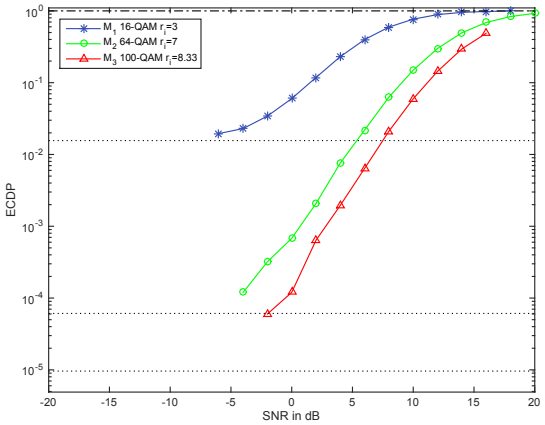

Fig. 5. ECDP for 16-QAM, 64-QAM and 100-QAM Golden Code and $r_c \approx 5$

matrices are given by

$$M_1 = 2 \cdot \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$M_2 = 2 \cdot \begin{bmatrix} -1 & 0 & 0 & 2 & 0 & 0 & -4 & 0 \\ 2 & 1 & 0 & 0 & -4 & 2 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & -3 & 0 & 0 \\ 0 & -1 & 0 & 2 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 4 \\ 3 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & -4 & -2 & 0 & 1 & 0 & 0 \end{bmatrix},$$

$$M_3 = 2 \cdot \begin{bmatrix} -2 & -2 & -2 & 0 & -4 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 & 4 \\ 0 & 1 & -2 & 1 & 0 & 2 & 0 & 1 \\ -1 & 0 & -2 & 0 & 0 & -2 & 5 & 0 \\ -4 & 0 & 1 & -2 & 0 & 0 & 0 & -3 \\ -2 & -1 & 0 & 4 & -1 & 2 & 0 & 0 \\ 1 & -4 & 0 & 1 & 3 & 0 & 1 & 0 \\ 0 & -2 & -3 & 2 & 0 & -3 & 0 & 0 \end{bmatrix}.$$

	index	WR	λ_1^2	Signaling Set	r	r_i	r_c
M_1	64	yes	16	16-QAM	8	3	5
M_2	2^{14}	yes	64	64-QAM	12	7	5
M_3	103996	yes	104	100-QAM	13.29	8.33	4.96

TABLE III
SUBLATTICES OF THE GOLDEN CODE WITH $r_c \approx 5$

In Figure 5 we see that only the first lattice approaches its lower bound in the simulated region. It therefore seems that security is not only determined by r_c, but a reasonable balance between r_i and r_c has to be found.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we have provided a practical design criterion for coset codes in fading MIMO wiretap channels. Simulations using the Alamouti and Golden code show that the proposed criterion indeed decreases the mutual information between the sender and the eavesdropper while maintaining equal reliability for a legitimate receiver in the high SNR regime.

Future work includes further investigations of well-rounded lattices, especially for higher indices. Also we plan on extending this work to other ST codes and perform an analysis of the effect of an outer code on the performance of the system.

REFERENCES

[1] F. Oggier, P. Solé and J. C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis," in *IEEE Transactions on Information Theory*, vol. 62, no. 10, pp. 5690-5708, Oct. 2016.

[2] J. C. Belfiore and F. Oggier, "Lattice Code Design for the Rayleigh Fading Wiretap Channel", in *Proc. IEEE ICC*, 2011.

[3] J. C. Belfiore and F. Oggier, "An Error Probability Approach to MIMO Wiretap Channels," in *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3396–3403, 2013.

[4] C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehle, "Semantically Secure Lattice Codes for the Gaussian Wiretap Channel", *IEEE Trans. Inf. Theory*, vol.60, no.10, pp. 6399–6416, 2014.

[5] H. Mirghasemi and J.-C. Belfiore, "Lattice Code Design Criterion For MIMO Wiretap Channels", *Proc. IEEE ITW*, 2015.

[6] L. Luzzi, C. Ling and R. Vehkalahti, "Almost Universal Codes for Fading Wiretap Channels", *Proc. IEEE ISIT*, 2016.

[7] A. Karrila, A. Barreal, D. Karpuk and C. Hollanti, "Information Bounds and Flatness Factor Approximation for Fading Wiretap MIMO Channels", arXiv:1606.06099, 2016.

[8] A. Barreal, D. Karpuk and C. Hollanti, "Decoding in Compute-and-Forward Relaying: Real Lattices and the Flatness of Lattice Sums", arXiv:1601.05596, 2016.

[9] D. Karpuk, A.-M. Ernvall-Hytönen, C. Hollanti and E. Viterbo, "Probability estimates for fading and wiretap channels from ideal class zeta functions", *AMC*, vol.9, no.4, pp. 391–413, 2015.

[10] R. Vehkalahti, H-f. Lu and L. Luzzi, "Inverse Determinant Sums and Connections Between Fading Channel Information Theory and Algebra", *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 6060–6082, 2013.

[11] R. Vehkalahti and C. Hollanti, "Reducing complexity with less than minimum delay space-time lattice codes," *Proc. IEEE ITW*, 2011.

[12] O. W. Gnilke, H. Thanh Nguyen Tran, A. Karrila and C. Hollanti, "Well-Rounded Lattices for Reliability and Security in Rayleigh Fading SISO Channels", *Proc. IEEE ITW*, to appear, 2016.

[13] F. Oggier, E. Viterbo, and J.-C. Belfiore, "Cyclic Division Algebras: A Tool for Space-Time Coding," *Found. and Trends in Comm. and Inf. Theory*, vol. 4, no. 1, pp. 1–95, 2007.

[14] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications", *IEEE J. Sel. Areas Commun.*, vol. 18, no. 8, pp. 1451-1458, 1998.

[15] J.-C. Belfiore, G. Rekaya and E. Viterbo, "The Golden Code: A 2×2 Full-Rate Space–Time Code with Nonvanishing Determinants", *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432-1436, 2005.

[16] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[17] L. H. Ozarow and A. D. Wyner, "The Wire-Tap Channel II", *Bell System Technical Journal,* vol. 63, pp. 2135–2157, 1984.

[18] X. He and A. Yener, "Providing Secrecy With Structured Codes: Tools and Applications to Two-User Gaussian Channels", arXiv:0907.5388, 2009.

[19] A. Karrila, C. Hollanti, "A comparison of skewed and orthogonal lattices in Gaussian wiretap channels", *Proc. IEEE ITW*, 2015