Algebraic lattices and channel coding for digital transmission

Emanuele Viterbo
(joint work with E. Bayer-Fluckiger, J-C. Belfiore, F. Oggier, G. Rekaya)

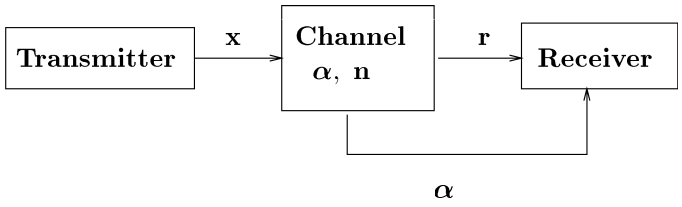
This survey talk presents some applications of algebraic lattices to the problem of code design for digital transmission over fading channels.

1. Algebraic lattices for Rayleigh fading channels

We consider the following communication problem (see the figure below). A transmitter sends a codeword $\mathbf{x}$ through a wireless channel. Since the channel attenuates the signal (this is modeled by the fading $\boldsymbol{\alpha}$) and adds noise ($\mathbf{n}$), we model the modified codeword at the receiver by

$$\mathbf{r} = \boldsymbol{\alpha} * \mathbf{x} + \mathbf{n},$$

where $*$ represents the component-wise vector product. We have that $r_i = \alpha_i x_i + n_i$ for $i = 1, 2, \ldots n$, where the α_i are independent real Rayleigh random variables and n_i are real Gaussian random variables with mean zero and variance σ^2.



The problem that we address is the design of a *codebook* or a *signal constellation* S for this channel, that is, a finite set of points in $\mathbb{R}^n$. In order to derive code design criteria, we estimate the error probability of this transmission system. Assuming the receiver estimates the channel (i.e. $\boldsymbol{\alpha}$), one can estimate the probability that the codeword $\mathbf{y}$ is received while the codeword $\mathbf{x}$ was sent, which is

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2} \prod_{x_i \neq y_i} \frac{8\sigma^2}{(x_i - y_i)^2} = \frac{1}{2} \frac{(8\sigma^2)^l}{d_p^{(l)}(\mathbf{x}, \mathbf{y})^2}$$

where $d_p^{(l)}(\mathbf{x}, \mathbf{y})$ is the *l-product distance* of $\mathbf{x}$ from $\mathbf{y}$, when these two codewords differ in l components, i.e., $d_p^{(l)}(\mathbf{x}, \mathbf{y}) = \prod_{x_i \neq y_i} |x_i - y_i|$. The minimum number of distinct components between any two codewords $L = \min(l)$ is called the *modulation diversity* or *diversity order* of S.

To obtain a good codebook (with a low error probability), we have to:

(1) Maximize the diversity $L = \min(l)$.
(2) For a given L, maximize the minimum product distance

$$d_{p,min} = \min_{\mathbf{x} \neq \mathbf{y}} d_p^{(L)}(\mathbf{x}, \mathbf{y})$$

under the constraint of bounded average energy $\mathcal{E}_S = \frac{1}{|S|}\sum_{x\in S}\|\mathbf{x}\|^2$.

In the design of the signal constellations, two fundamental operations should also be kept in mind: *bit labelling* and *constellation shaping*.

Bit labelling consists in mapping bits to signal points and vice-versa, and is best performed by an efficient algorithm. On the other hand, it is well known that lattice constellations bounded by a sphere have the best shaping gain. Unfortunately, labelling algorithmically a spherically shaped constellation is not easy. Cubic shaped constellations offer a good trade-off: they are only slightly worse in terms of shaping gain but are usually very easy to label.

Moreover, the complexity of the general decoding problem suggests to use constellations with lattice structure for which a more efficient decoder is available.

We conclude that good signal constellations are provided by rotated $\mathbb{Z}^n$–lattices, which have full diversity and maximal minimum product distance.

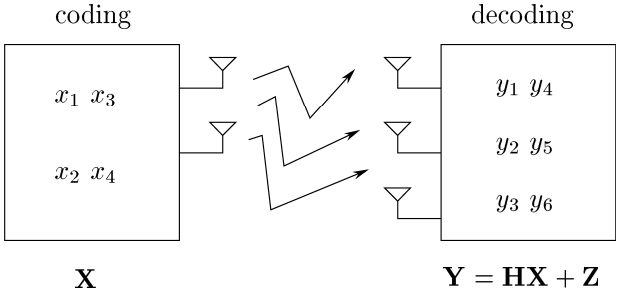
These $\mathbb{Z}^n$-lattices can be constructed via the embedding of a number field. Furthermore, both their diversity and minimum product distance can be related to the properties of the underlying number field. Constructions of such lattice codes and their performance analysis can be found in [1] while a complete survey is given in [2].

2. Algebraic lattices for coherent MIMO channels

We consider the following communication problem (see the figure below). We have a transmitter with M_t transmit antennas and a receiver with M_r receive antennas. If $\mathbf{y}(k) \in \mathbb{C}^{M_r}$ is the received (column) vector at time k, we can write

$$\mathbf{y}(k) = \mathbf{H}(k)\,\mathbf{x}(k) + \mathbf{z}(k)\ ,$$

where the matrix $\mathbf{H}(k) \in \mathbb{C}^{M_r\times M_t}$ represents the channel, the column vector $\mathbf{x}(k) \in \mathbb{C}^{M_t}$ is the channel input and $\mathbf{z}(k) \in \mathbb{C}^{M_r}$ is zero mean i.i.d. Gaussian noise.



The channel is assumed to be block time-invariant, that is, $\mathbf{H}(k)$ is independent of k over a transmission block of m symbols, say $\mathbf{H}(k) = \mathbf{H}$. Looking at a single block of length m, during which the channel is assumed to be time-invariant, we can write

$$\mathbf{Y}_{M_r\times m} = \mathbf{H}_{M_r\times M_t}\mathbf{X}_{M_t\times m} + \mathbf{Z}_{M_r\times m}\ .$$

Information symbols are taken from a complex signal constellation (or alphabet) $\mathcal{A} \subset \mathbb{Z}[i]$ (the Gaussian integers) or $\mathbb{Z}[j]$ (the Eisenstein integers), and are encoded into the codewords $\mathbf{X}$.

The problem that we address is the design of a *codebook* or *space-time block code* $\mathcal{C}$ for this channel, in the case where $M_t = M_r = m$, that is, we have the same number of transmit and receive antennas. If we furthermore assume that the receiver has perfect knowledge of all the channel coefficients (*coherent case*), it has been shown that minimizing the probability of error requires to maximize

$$\min_{\mathbf{X} \neq \hat{\mathbf{X}} \in \mathcal{C}} |\det(\mathbf{X} - \hat{\mathbf{X}})|^2.$$

Cyclic division algebras naturally provide a linear family of invertible matrices, thus codebooks whose minimum determinant is ensured to be different from zero. We further exploit the algebraic structure of the algebra to get

(1) a shaping constraint: vectorized codewords have to be points of a $\mathbb{Z}[i]^n$ (resp. $\mathbb{Z}[j]^n$) lattice with diversity, which is obtained algebraically, as in the previous section.

(2) a non-zero lower bound on the minimum determinant even when increasing the size of $\mathcal{A}$.

The above conditions appear to be a key point in improving the performance of these codes and define the so called *perfect space-time block codes*. In [7] the 2×2 Golden code is presented and in [8] all other perfect space-time codes are given, which appear only for 3×3, 4×4 and 6×6 MIMO systems.

References

[1] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, *New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel*, IEEE Transactions on Information Theory, vol. 50, n. 4, pp. 702–714, April 2004.

[2] F. Oggier, E. Viterbo, *Algebraic number theory and code design for the Rayleigh fading channel*, Foundations and Trends in communication and information theory, vol. 1.

[3] M. O. Damen, A. Tewfik, and J.-C. Belfiore, *A construction of a space-time code based on the theory of numbers*, IEEE Trans. Inform. Theory, vol. 48, no. 3, pp. 753–760, March 2002.

[4] H. El Gamal and M. O. Damen, *Universal space-time coding*, IEEE Trans. Inform. Theory, vol. 49, no. 5, pp. 1097–1119, May 2003.

[5] J.-C. Belfiore and G. Rekaya, *Quaternionic lattices for space-time coding*, in Proceedings of the Information Theory Workshop, Paris, March 31–April 4, 2003.

[6] 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.

[7] J.-C. Belfiore, G. Rekaya, E. Viterbo, *The Golden code: A 2x2 full-rate space-time code with non vanishing determinants*, to apper in IEEE Trans. on Information Theory, 2005.

[8] F. Oggier,J.-C. Belfiore, G. Rekaya, E. Viterbo, *Perfect space-time codes*, submitted to IEEE Trans. on Information Theory, Aug. 2004.