Research project:

Almost universal codes achieving the ergodic capacity of multi-antenna fading channels

Collaboration between Laura Luzzi (ETIS) and Roope Vehkalahti (University of Turku, Finland)

In the last decade, algebraic tools have proven to be very useful to design high-performance codes for fading channels, some of which have been adopted in 3G and 4G communication standards, including WiMAX and terrestrial Digital Video Broadcasting.
In particular, space-time lattice constellations for *number fields* and *division algebras* provide good performance over single and multiple antenna channels [1]. When coding over a single block, the minimum determinant criterion allows to improve the worst-case pairwise error probability in the high signal-to-noise regime, yielding codes that are are optimal in terms of the diversity-multiplexing gain trade-off [2].

It is perhaps surprising that very little attention has been given so far to the question of whether algebraic space-time codes can also approach *ergodic capacity* when we are allowed to encode and decode over a growing number of fading blocks [3].
In our recent work [10–12] we offer a partial answer to this question, by showing that the normalized minimum determinant can be used to measure the gap to capacity of a given family of multi-block lattice codes. Based on this design criterion, we propose a new family of multiblock codes from division algebras which universally achieve a constant gap to capacity for a wide class of fading channel models, both for single and multiple antenna systems.
Our lattice constructions are based on two results from class field theory. First we choose the center K of the division algebra from an ensemble of Hilbert class fields having constant root discriminant, and then we prove the existence of a K-central division algebra yielding a dense lattice.

Closing the gap to capacity

Our codes still have a considerable gap to capacity and further research is needed. We note that this gap depends on several factors. First of all, the normalized minimum determinant affects the value of the gap. Second, our bound for the error probability is based on sphere packing and thus is suboptimal. Thus, the possible improvements to our construction are two-fold. In the first place, one could try to find families of lattices with larger normalized minimum determinant, for instance by replacing the centers in our constructions with families of number fields having smaller discriminants. One can also consider more general examples of lattices, for example ideals of orders, or in the case of number field codes, ideals of the ring of algebraic integers.
In the second place, in our preliminary work we have not considered the issue of *shaping*. Improving the shaping properties of our lattices might lead to a better error probability bound. In particular, an open problem is under which conditions the canonical embedding of a number field results in a lattice whose Voronoi region approaches a sphere.

Applications to physical-layer security

Lattices from number fields with constant root discriminants have been already considered in the context of lattice-based cryptography [4] because of their special structure. We conjecture that our code constructions may also be good for secrecy coding over multiple-antenna fading channels.

Previous joint work

I have been collaborating with Dr Vehkalahti since 2011, and I've visited him in Finland several times (three one-week visits in December 2011, March 2013, June 2014, and a one-month visit in April-May 2015). Our collaboration has led to several joint publications on the topic of space-time coding: a journal paper [5] in *IEEE Transactions on Information Theory*, another recently submitted journal paper [12], and six conference papers [6–11].

References

[1] F. E. Oggier, J.-C. Belfiore, and E. Viterbo, "Cyclic division algebras: A tool for space-time coding", *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 1, pp. 1–95, 2007.

[2] P. Elia, K. R. Kumar, P. V. Kumar, H.-F. Lu, and S. A. Pawar, "Explicit Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff", *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, September 2006.

[3] H.-F. Lu, "Constructions of multi-block space-time coding schemes that achieve the diversity-multiplexing tradeoff", *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3790–3796, Aug. 2008.

[4] C. Peikert, A. Rosen, "Lattices that Admit Logarithmic Worst-Case to Average-Case Connection Factors", *Proceedings of the 39-th annual ACM symposium on Theory of computing*, pp. 478–487, 2007

[5] R. Vehkalahti, H.-f. Lu, L. Luzzi, "Inverse Determinant Sums and Connections Between Fading Channel Information Theory and Algebra", *IEEE Trans. Inform. Theory*, vol 59, pp. 6060–6082, September 2013.

[6] R. Vehkalahti, L. Luzzi, "Connecting DMT of Division Algebra Space-Time Codes and Point Counting in Lie Groups", *IEEE International Symposium on Information Theory*, Cambridge (MA), July 1-6, 2012

[7] L. Luzzi, R. Vehkalahti, "A new design criterion for spherically-shaped division algebra-based space-time codes", *IEEE Information Theory Workshop*, Seville (Spain), September 9-13, 2013

[8] R. Vehkalahti, L. Luzzi, "Measuring the growth of inverse determinants sums of a family of quasi-orthogonal codes", *International Zurich Seminar on Communications* (IZS), February 26-28, 2014

[9] R. Vehkalahti, L. Luzzi, J.-C. Belfiore, "Shifted inverse determinant sums and new bounds for the DMT of space-time lattice codes", *IEEE International Symposium on Information Theory*, Honolulu (HI), June 29 -July 4, 2014

[10] R. Vehkalahti and L. Luzzi, "Number field lattices achieve Gaussian and Rayleigh channel capacity within a constant gap", in *IEEE Int. Symp. Inform. Theory* (ISIT), Hong Kong, China, June 2015

[11] L. Luzzi, R. Vehkalahti, "Division algebra codes achieve MIMO block fading channel capacity within a constant gap", *IEEE Int. Symp. Inf. Theory* (ISIT), Hong Kong, China, June 2015.

[12] L. Luzzi, R. Vehkalahti, "Almost universal codes achieving ergodic MIMO capacity within a constant gap", submitted to *IEEE Trans. Inform. Theory*.