

OGGIER Frederique
Assistant Professor

Division of Mathematical Sciences
School of Physical & Mathematical Sciences
B.Sc. of Mathematics, Geneva University
M.Sc. of Mathematics & Computer Science, Geneva University
PhD in Mathematics, Ecole Polytechnique Federale de Lausanne

Major Research Interest: Coding theory and its connections to wireless communication and cryptography

Email: frederique@systems.caltech.edu
Tel: (65) 6513 2026



Algebraic coding theory has been successful at providing good codes for discrete channels. In the meantime, research in communication has evolved, and new channel models have appeared in the context of wireless communication, requiring thus the construction of new families of codes. Some of my work has consisted on designing codes for application to wireless communication, namely lattice codes for single antenna channels and space-time codes for multiple antenna channels.

Algebraic lattice codes:

In the context of single antenna channels, it has been shown that lattices built over number fields provide good modulation schemes, mainly thanks to the fact that the code design criteria are related to invariants of the underlying number field, such as signature and discriminant. Some of my early work has been to find explicit constructions of such codes.

Algebraic Space-Time Coding:

Space-time codes have been introduced for coding over multiple antenna channels. Following the work of Sundar Rajan and Sethuraman, division algebras have been proposed as a tool for building good space-time codes. I have worked on designing efficient space-time codes based on cyclic algebras. I have extended some of these techniques to provide unitary space-time codes for coding over channels where channel side information is not available, and more recently to obtain distributed space-time codes, available for coding over wireless relay networks.

Wireless channels have addressed new problems not only in the area of coding, but also in the area of security, where the question is to obtain secure wireless communication. I am considering this issue mainly from an information theoretical point of view.

Information theoretical security:

On the one hand, I am working on bringing security into wireless communication. From this point of view, I am interested in the notion of secrecy capacity and the design of wiretap codes. On the other hand, I am also studying the reverse application, that is bringing coding techniques into the cryptographic world, for example, using codes for continuous noisy channels to design cryptographic primitives such as bit commitment.

Selected publications:

- F. Oggier, B. Hassibi, **The Secrecy Capacity of the MIMO Wiretap Channel**, preprint 2007.
- F. Oggier, B. Hassibi. **An Algebraic Coding Scheme for Wireless Relay Networks with Multiple-Antenna Nodes**, to appear in *IEEE Transactions on Signal Processing*, 2008.
- F. Oggier, J.-C. Belfiore, E. Viterbo. **Cyclic division algebras: a tool for space-time coding**, *Foundations and Trends in Communications and Information Theory*, December 2007.
- F. Oggier. **Cyclic Algebras for Noncoherent Differential Space-Time Coding**, *IEEE Transactions on Information Theory*, vol. 53, no 9, September 2007.
- F. E. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo. **Perfect Space Time Block Codes**, *IEEE Transactions on Information Theory*, vol. 52, no 9, September 2006.
- F. E. Oggier, N. J. A. Sloane, S. N. Diggavi and A. R. Calderbank. **Nonintersecting Subspaces Based on Finite Alphabets**, *IEEE Transactions on Information Theory*, vol. 51, no 12, pp. 4320-4325, December 2005.
- F. Oggier, E. Viterbo. **Algebraic number theory and code design for Rayleigh fading channels**, *Foundations and Trends in Communications and Information Theory*, December 2004.