

28/04/2017

InterCity - seminar

2

Neuchâtel - Fribourg/Freiburg
Bern

Time	Speaker	Talk
13:45	Joachim Rosenthal (Zürich)	An Overview on Post-Quantum Cryptography with an Emphasis on Code based Systems With the realization that a quantum computer would make many practically used public key cryptographic systems obsolete it became an important research topic to design public key systems which are expected to be secure even if a powerful quantum computer would exist. In the talk we will explain about the major possible candidates for post-quantum cryptography and we will then concentrate on so called code based systems which were first proposed in 1978 by Robert McEliece who demonstrated how the hardness of decoding a general linear code up to half the minimum distance can be used as the basis for a public key crypto system.
15:30	Alessio D'Alì (Fribourg and Genova)	Resolutions of letterplace and co-letterplace ideals Fløystad, Greve and Herzog recently introduced, extending ideas by Ene, Herzog and Mohammadi, a class of squarefree monomial ideals encoding the information about order-preserving maps between two finite posets. When the source poset (respectively, the target) is totally ordered, we say that we are considering a <i>letterplace</i> (respectively, <i>co-letterplace</i>) ideal. The graded Betti numbers of some very diverse monomial ideals (e.g. initial ideals of certain determinantal ideals, strongly stable ideals) can be recovered in this new setting. It is hence interesting to investigate the homological behaviour of general letterplace and co-letterplace ideals: we report on some results in this direction, trying to give some insight about the techniques used (mostly topological for the letterplace case, mostly algebraic for the co-letterplace one). This is joint work with G. Fløystad and A. Nematbakhsh.

The talks will take place in Room ExWi B77, Sidlerstrasse 5, University of Bern.

For further informations please refer to the seminar's webpage

www.combinatorialmethods.ch/intercity/

or contact the organisers:

Emanuele Delucchi (Fribourg) — Jan Draisma (Bern) — Elisa Gorla (Neuchâtel)