Algebra and Number Theory Seminar

Title: Adaptive decoding for evaluation/interpolation codes

Speaker: Clément Pernet (Université de Grenoble)

Date: Thu 3rd June 2010 at 3:00PM

Location: CASL Seminar Room - Belfield Office Park

Abstract: n the context of distributed computations with unsafe resources (global, computing, peer to peer computing, ...), malicious computation nodes can generate byzantine errors. In order to ensure the reliability of the computation, algorithm based fault tolerance (ABFT) allow to detect and correct these errors by introducing the redundancy in the inputs and exploiting algebraic properties of the computation. High performance exact computations (over the ring of integers or polynomials over a field) often use a parallelization based on multi-modular representations (using the Chinese remainder theorem) where each modular computation is an independent task that can be parallelized. Adding a few extra modular computations, means introducing some redundancy: this is the framework for arithmetic codes, which allow to reconstruct a result in the presence of errors on some residues. These codes can be presented in a unified manner over the ring of polynomials, integers or any euclidean ring, and can be viewed as a generalization of the Reed-Solomon codes. We will first introduce a more general error model allowing to derive tighter bounds on the error correction capacities of such codes. Then we will describe two adaptations of the usual unique decoding algorithm (based on the extended euclidean algorithm), making the correction capacity adaptive. Several termination criteria allow to efficiently use these codes without knowledge of their parameters, and use the maximal amount of redundancy available for correction. Furthermore they make it possible to combine

fault tolerance and early termination algorithms.

http://linalg.org/Dublin-developer-meeting-2010.html