Postdoct position in computer science at LIRMM (Montpellier), France

INFORMATIONS

Location: Montpellier, France at LIRMM (www.lirmm.fr)

Duration: 12 months (possibly with a renewal of 12 months)

Starting date: from February 2012 till October 2012

Salary: 26 000 € (annual net salary including French health care coverage)

Contact: Pascal Giorgi - pascal.giorgi@lirmm.fr

Application: please send a CV and reference letters by email to Pascal Giorgi (pascal.giorgi@lirmm.fr)

CONTEXT

This postdoc position is available within the project HPAC (High Performance Algebraic Computing) funded for four years by the french research agency ANR under grant ANR-11-BS02-013. The overall ambition of the project HPAC is to provide international reference high-performance libraries for exact linear algebra and algebraic systems on multi-processor architecture and to influence parallel programming approaches for algebraic computing. This project gathers researchers working on parallel language and environments, middleware software engineering, exact linear algebra, algebraic systems, cryptology and symbolic-numeric verified computations. The major challenge is the design and implementation of verified mathematical algorithms with provable, adaptive and sustainable performance. LINBOX[1] and FGB[2] are two international reference mathematical libraries. LINBOX offers a large panel of functionalities in exact linear algebra and is used by computer algebra systems such as SAGE for instance. FGB is the reference for Gröbner bases computations usable, for instance, via MAPLE. Both libraries are sequential and rely on exact linear algebra kernels. The central goal of the HPAC project is to extend their efficiency to new trend parallel architectures such as clusters of multi-processor systems and graphics processing units in order to tackle a broader class of problems in lattice cryptography and algebraic cryptanalysis.

In order to guarantee sufficient performances, the first goal of the project HPAC is to design new parallel building blocks for dense linear algebra over finite fields, since they are the core of most exact computations. In particular, this concerns matrix multiplication and normal form such as the echelon form. The purpose of this postdoc position is to work on the design and the implementation of algorithm for such problems which guarantee sustainable performances on a shared memory multi-processor systems. One of the difficulty will be to manipulate elements of a finite fields which possibly do not directly map to the native 64 bit integer representation available in modern processor. For instance, one of our target is finite fields with few hundred of bits size elements. Another purpose of this postdoc is to design new methods which take advantage of a possible block structure in the matrix representation as the one arising in the Gröbner basis computations.

QUALIFICATIONS

The candidate must hold a Ph.D in either computer science or in computational mathematics. He/She must have a strong knowledge of linear algebra algorithms and C/C++ programming. An experience in either high performance computing or computer algebra would be a strong advantage to incorporate our project.

[1] http://www.linalg.org

[2] http://www-polsys.lip6.fr/ jcf/Software/FGb/index.html