IITB-Monash Research Academy

Indian Institute of Technology Bombay | MONASH University

An Indian-Australian research partnership

Project Title: Boolean methods for scalable computation in computer algebra.

Project Number	**IMURA0378**	
Monash Supervisor(s)	Prof. Maria DelaBanda and Prof. Guido Tak	*Full names and titles*
Monash Primary Contact:	Maria.GarciadelaBanda@monash.edu	*Email, phone*
Monash Head of Department:	Judithe Sheard	*Full name, email*
Monash Department:	Caulfield School of IT	*Full name*
Monash ADRT:	Kai Ming Ting	*Full name, email*
IITB Supervisor(s)	Virendra Sule	*Full names and titles*
IITB Primary Contact:	vrs@ee.iitb.ac.in	*Email, phone*
IITBHead of Department:	Abhay Karandikar	*Full names and titles*
IITB Department:	EE	*Email, phone*

Research Academy Themes:

Highlight which of the Academy's Theme(s) this project will address?
(*Feel free to nominate more than one. For more information, see www.iitbmonash.org)*

1. Advanced computational engineering, simulation and manufacture
2. Infrastructure Engineering
3. Clean Energy
4. Water
5. Nanotechnology
6. Biotechnology and Stem Cell Research

The research problem

Define the problem

This proposal is aimed at developing scalable parallel algorithms and their implementation for solving problems of Computer Algebra using Boolean function methods and methods used in solutions of Boolean equations and satisfiability (SAT) problems. Typically some of these problems are, solutions of equations over finite groups, rational solutions of polynomial equations and irreducible factorization of polynomials over finite fields, solutions of quadratic systems of Boolean equations, modular arithmetic for large integer etc. Solutions to these problems have applications to cryptography, verification, Boolean dynamical modelling and simulation in Biology. These applications require computational methods to be scalable for large size problems and work over large number of processing units.Present methods of Computer Algebra are often either not parallel or are difficult for parallel implementation primarily because they are not aimed at scalability.

Project aims

Define the aims of the project

1. Develop Boolean algebraic methods for solving typical problems of Computer Algebra which will be parallel and scalable for large size problems and large number of processors. By large it is meant comparable to sizes in actual applications.
2. Develop parallel implementation of algorithms for test purposes and document their benchmarking.
3. Consider application problems from Cryptology or Biology and develop formulation of computations in the setting of Boolean equations. Determine benchmarks of solutions using algorithms developed.

Expected outcomes

Highlight the expected outcomes of the project

1. Knowhow on parallel algorithms for solving problems of Computer Algebra with application case studies.
2. Implementations of algorithms on a cluster or in a parallel computational framework. Benchmarking of performance of algorithms. Working codes based on open source.
3. By product results on theory of randomness generation, cryptographic primitives and one way functions, efficient solutions for arithmetic etc.
4. Publications arising out of the research.

How will the project address the Goals of the above Themes?

Describe how the project will address the goals of one or more of the 6 Themes listed above.

1. A Ph.D. student shall be guided to develop background of Boolean methods, basic mathematics and parallel computation.
2. Research will be carried out on proposed problems.
3. The student shall carry out implementations of algorithms on a cluster available at IIT Bombay and obtain benchmarks.