

BY MEENA MAHAJAN, MADHAVAN MUKUND,
AND NITIN SAXENA

Research in Theoretical Computer Science

THEORETICAL COMPUTER SCIENCE has been a vibrant part of computing research in India for the past 30 years. India has always had a strong mathematical tradition. One could also argue that in the 1980s and 1990s, theory offered a unique opportunity to keep up with international research in computing despite limited access to state-of-the-art hardware.

The Annual International Conference Foundations of Software Technology and Theoretical Computer Science (FSTTCS) was launched in 1981. FSTTCS² allowed Indian researchers a natural opportunity to interact with leading academics worldwide.

Another early impetus was funding for international collaboration through agencies such as the Indo-French Centre for Promotion of Advanced Research (CEFIPRA).

Research Highlights

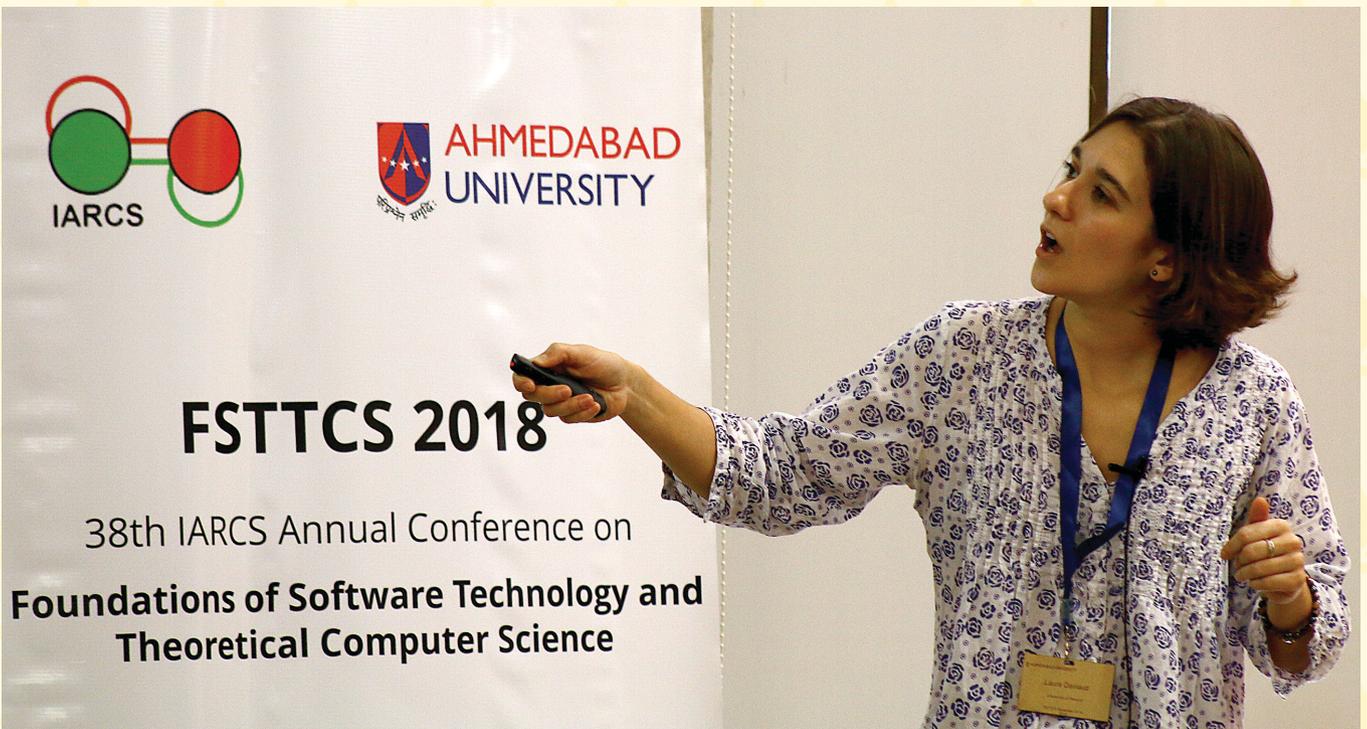
Algorithms. Maximizing the flow that can be routed in a network is one of the most well-studied algorithmic problems, with immense practical applicability. In the 1970s, when computer science research in India was taking root, Sachin Maheshwari and his co-authors V.M. Malhotra and M. Pramodh Kumar devised a max-flow algorithm that matched the best bounds at that time, but was conceptually much simpler and hence ideal for exposition.

Scheduling and facility location problems are often cast as multi-commodity flow problems and are NP-hard. Using ideas from flows and linear programming, efficient approximation problems can be devised in many settings. The Indian Institute of Technology (IIT) Delhi is at the forefront of international research in this area.

Parameterized algorithms and complexity is a relatively recent field that focuses on multivariate analysis of algorithm performance and the development of algorithms for hard problems where combinatorial explosion is confined to specified parameters. This burgeoning field has a very close connection with India—the first international event wholly devoted to this theme took place in Chennai in 1999—and has seen cutting-edge contributions from India, notably from the Institute of Mathematical Sciences, Chennai (IMSc) and Chennai Mathematical Institute (CMI).

Matchings in graphs come in many different flavors—perfect, maximum, stable, popular. Indian researchers have made significant contributions toward obtaining combinatorial characterizations, devising new algorithms, and understanding the parallel complexity of these problems.

Data structures are crucial to the efficiency of many state-of-the-art algorithms. Indian researchers have been part of the community designing data structures for static succinct representations and for maintaining dynamic



PHOTOS COURTESY OF FOUNDATIONS OF SOFTWARE TECHNOLOGY AND THEORETICAL COMPUTER SCIENCE (FSTTCS)

The annual Foundations of Software Technology and Theoretical Computer Science (FSTTCS) Conference, organized by the Indian Association for Research in Computer Science, is a premier forum for presenting original results in initial aspects of CS and software technology. The images here show participants from FSTTCS 2018, held last December at India's Ahmedabad University.

In the 1980s and 1990s, theory offered a unique opportunity to keep up with international research in computing despite limited access to state-of-the-art hardware.

data, as well as in proving non-trivial lower bounds on query complexity and space requirements.

Complexity theory. Primality testing has been studied at least since ancient Greece. However, nontrivial ideas for testing primes appeared only in the last two centuries. Apart from academic interest, primality testing has gained huge practical importance because of the need for arithmetic modulo prime and pseudo-prime numbers in various cryptographic implementations, error-correcting codes, and other fundamental computational problems.

Though randomized polynomial-time algorithms suffice for this purpose, the basic question of derandomization remained open till 2002 when the breakthrough result PRIMES is in P was proved by Agrawal et al.¹ at IIT Kanpur. Agrawal was already a well-established complexity theorist, while Kayal and Saxena were graduate students about to start their Ph.D. thesis work. This paper eventually appeared in the *Annals of Mathematics* and was awarded both the Godel Prize of EATCS-SIGACT and the Fulkerson Prize of AMS.

Algebraic complexity theory deals with the symbolic computation of formal polynomials in models such as circuits. The mathematical analysis of these models involves an interaction between computer science and algebra and enriches both fields. The recent contributions of Indian researchers at CMI, IIT Bombay, IIT Kanpur, IIT Madras, Indian Institute of Science, Bangalore (IISc), IMSc, and Microsoft Research in this technically challenging area have been stunning, with numerous foundational results and proof techniques being developed.

Algebraic methods are also used to show that certain problems are hopelessly hard by proving lower bounds. For example, the notorious problem $P=NP$ involves proving an algorithmic lower bound. There are analogous lower bound problems for algebraic circuits. The theory research community in India has been making steady progress in this area.

Machine learning is a potential area to apply the insights gained from algebraic complexity. An artificial neural network (ANN) is an algebraic

circuit with threshold gates. Thus, better understanding of threshold circuits can lead to better backpropagation algorithms and stronger lower bound results in learning theory. Indian researchers have already started designing circuit reconstruction algorithms.

Isomorphism problems about structures frequently appear in computer science. Some example structures are NP-hard problems, graphs, fields, algebras, and polynomials. Indian theorists have been studying these closely, and have proved some of the best results known.

Communication complexity studies the interaction required to solve a problem when the input is distributed across multiple parties. Indian researchers, notably at Tata Institute of Fundamental Research, Mumbai (TIFR), have made leading contributions to this area.

Logic and automata theory. The close interplay between automata theory and logic was first identified by Buchi. Pnueli introduced temporal logic as a language for specifying properties of reactive systems. Emerson, Clarke, and Sifakis invented model checking: determining algorithmically whether a formal model satisfies a temporal logic specification.

Reactive systems typically consist of many interacting components. Viewing the system as a sequential automaton results in the state explosion problem, severely limiting the effectiveness of model checking. Moreover, temporal logics interpreted over sequences are forced to reason about an exponential number of equivalent interleavings for a set of concurrent actions.

Mazurkiewicz proposed enriching alphabets with an independence relation. Adjacent independent actions commute, creating equivalence classes of words called traces. Traces are labeled partial orders of bounded width and smoothly generalize words in many respects.

Zielonka defined asynchronous automata, a distributed model that precisely captures regular trace languages. This led to a natural question of model checking asynchronous automata with respect to temporal logics defined over traces.

The first temporal logic over

traces, TrPTL, was formulated in CMI. The model checking problem was solved using the gossip automaton that uses a bounded set of time-stamps to dynamically keep track of updates among communicating processes.

Temporal logic is expressively equivalent to the first order theory of sequences. It is not known if TrPTL captures the first order theory of traces. Researchers at CMI, in collaboration with European colleagues, later developed the first expressively complete temporal logics over traces.

Results from trace theory generalize to communicating finite-state machines with bounded channels. Message sequence charts (MSCs) describe interactions between agents communicating through buffers. A robust theory of regular MSC languages was developed at CMI.

The converse of model checking is synthesis: construct an automaton that meets a logical specification. In the sequential setting, this was solved by Buchi and Landweber. In the distributed setting, Pnueli and Rosner proved strong undecidability results that stem from enforcing global specifications across loosely coupled agents. The decidability of distributed synthesis with local specifications is still open. Some of the strongest positive results for subclasses of systems were proved in CMI and IMSc.

Automata theory and logic have expanded to incorporate other features. A number of timed extensions to temporal logic were developed at IMSc and TIFR. In parallel, there was also work on distributed timed automata at CMI and IISc, as well as on timed versions of communicating finite-state machines at CMI and IIT Bombay. There has been work at IMSc on automata and logics over data words, which capture computations over infinite datatypes. There has also been work at CMI and IIT Kanpur in extending model checking from finite-state systems to infinite-state systems such as pushdown automata.

The Academic Ecosystem in India

Indian undergraduate programs in computing date back to the early 1980s—a time that also saw the first generation of graduate students from

India taking up theoretical computer science. In the 1990s, these young researchers helped set up strong theory groups in TIFR, the IITs at Bombay, Delhi, Kanpur, and Madras, IISc, IMSc, and CMI. This network is now expanding to newer IITs at Gandhinagar, Goa, Guwahati, Hyderabad, and Palakkad, as well as IIITs and some traditional universities such as Delhi University.

The FSTTCS Conference gave rise to the Indian Association for Research in Computing Science (IARCS).³ IARCS initiated several activities for the academic community, such as travel grants for Ph.D. students to attend conferences and faculty development programs to improve the quality of teaching. Many of these activities continue today in partnership with ACM India.

Some very robust mechanisms have arisen to sustain international collaborations. The Max-Planck Society of Germany set up the Indo-German Max Planck Center for Computer Science at IIT Delhi. The French National Centre for Scientific Research (CNRS) has established an international Research Lab in Computer Science at CMI in Chennai.

Theoretical computer science attracts some of the brightest graduate students in the country. Since the ACM India Doctoral Dissertation Awards began in 2012, nine of the 13 prizes awarded have been in theoretical computer science.

Finally, there are a large number of outstanding researchers trained in India who are active in theoretical computer science across the world. To name just two: Madhu Sudan and Subhash Khot have both won the Nevanlinna Prize awarded at the International Congress of Mathematicians.

References

1. Agrawal, M., Kaya, N. and Saxena, N. PRIMES is in P. *Annals of Mathematics* 150 (2004), 781–793.
2. Foundations of Software Technology and Theoretical Computer Science; <https://www.fsttcs.org.in/>
3. Indian Association for Research in Computing Science; <https://www.iarcs.org.in/>

Meena Mahajan is a professor at The Institute of Mathematical Sciences, Chennai, India.

Madhavan Mukund is a professor at the Chennai Mathematical Institute, Chennai, India.

Nitin Saxena is a professor at the Indian Institute of Technology Kanpur, Kanpur, India.

© 2019 ACM 0001-0792/19/11



Theoretical computer science attracts some of the brightest graduate students in the country.

