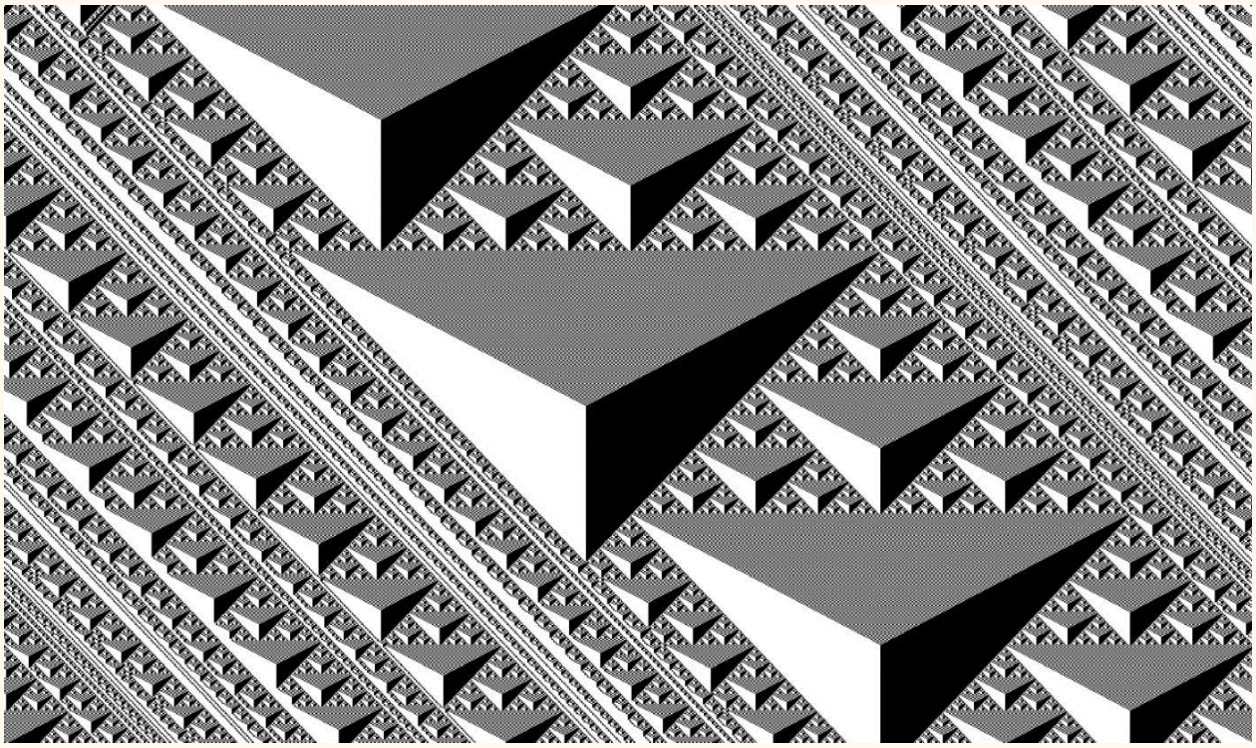
First Asian Symposium on Cellular Automata Technology (ASCAT 2022)

03-05 March, 2022



Hosted By

Indian Institute of Engineering Science and Technology, Shibpur

Sponsored By

SPARC (Scheme for Promotion of Academic and Research Collaboration)
Ministry of Human Resource Development, Government of India

प्रो. पार्थसारथि चक्रवर्त्ती
निदेशक
Prof. Parthasarathi Chakrabarti
Director

भारतीय अभियान्त्रिकी विज्ञान एवं प्रौद्योगिकी संस्थान, शिबपुर
(एमएचआरडी, भारत सरकार के अधीन एक राष्ट्रीय महत्वपूर्ण संस्थान)
INDIAN INSTITUTE OF ENGINEERING SCIENCE AND TECHNOLOGY, SHIBPUR
(An Institute of National Importance under MHRD, Govt. of India)

Message from Chief Patron

Warm and happy greetings to all!

It gives me immense pleasure to pen a message for this event which highlights a brilliant accomplishment of India as a country in the vibrant research domain of cellular automata - an unconventional model of computation and one of the most emergent areas in natural computing. I am happy and proud to announce that our Institute, the second oldest in the Country, is the center of this attainment as two of its Departments – the Department of Information Technology and the Department of Computer Science and Technology are organizing the "First Asian Symposium on Cellular Automata Technology (ASCAT 2022)".

I thank the eminent scientists who agreed to deliver invited talks and applaud individual authors for their invaluable contributions. I also congratulate Dr. Sukanta Das, Department of Information Technology, Prof. Biplab Sikdar, Department of Computer Science and Technology and their team for their efforts in organizing in this Conference.

I wish the Conference all the success and encourage it to have a spirit to surpass its own accomplishment in the years to come.

Chakrabarti
01.03.2022

Prof. Parthasarathi Chakrabarti
Director, Indian Institute of Engineering Science and Technology, Shibpur

पो : बोटानिक गार्डन, हावड़ा- 711 103, पश्चिमबंग, भारत
P.O. : Botanic Garden, Howrah- 711 103, West Bengal, India
Telephone : 091-033-2668 2674, Fax ; 091-033-2668 7575, e-mail : director@iiests.ac.in • pchakrabartiece@iitbhu.ac.in

Foreword

The European countries (UK, France, Germany, Italy, Finland, etc.), Japan in Asia, and Brazil in South America, USA and Canada in North America established a strong base of theory and applications of Cellular Automata Research (CAR) since 1970s. In early 1980s, the CAR seed was planted at Indian Institute of Technology (IIT) Kharagpur, India. A group of research scholars came forward to ensure development of a full-grown tree out of this seed. Along with development of theory, the group concentrated on different applications of CA Technology - one of the major focuses was testable VLSI design. The seed grown out of this tree was later planted at Bengal Engineering College (currently named as IIEST – Indian Institute of Engineering Science and Technology). The group of research scholars at IIEST carried forward the research, developing theory and wide varieties of applications. In addition to these two institutes (IIT Kharagpur and IIEST), faculties and research scholars of other institutions in India (ISI Kolkata, IIT – Delhi, Kanpur, Madras, NIT - Trichy, Kashmir University) contributed in the field of CAR.

In this background it is a pleasure for me to write this '*Foreword*' for the first Asian Symposium on Cellular Automata Technology (ASCAT), 2022. In the last few years, faculty and research scholars of IIEST and IIT Kharagpur have been planning to organize a CA symposium in India.

Looking back at Cellular Automata research of last five decades in different regions of the world, we come across publications of a large number of research papers and books on Cellular Automata. This is a natural process in academia due to the universal appeal of CA as a modelling tool, demonstrated by wide varieties of its evolution patterns. In 'Nature' we observe evolving patterns out of interaction of local physical entities around us. Further, the growth of human civilization in the last few centuries can be viewed as temporal evolution of relevant patterns in all the fields of human society – be it legal system, administrative/political structure, civil society in a country, or international relations among different countries in the world. Researchers of diverse disciplines are naturally attracted to develop models based on Cellular Automata Technology (CAT). However, development of an appropriate model for any physical phenomenon is an upheaval task due to higher complexity of evolving patterns of CA, specifically with neighborhood (larger than three) and change of seed in CA cells prior to evolution. In view of such complexity, we hardly find any fruitful industrial/commercial application of CAT. Unless the researchers in the field of Cellular Automata can overcome this bottleneck and develop fruitful applications, it will not be able to serve the human society of the twenty-first century, even though CAR has enormous potential to build new class of models to address the problems human society faces in current digital world.

In this context, I look forward to industrial/commercial applications of CAT from the current and future generation of researchers. In all probability, Data Science and Machine Learning (ML) framework to learn/analyze the evolving patterns of physical domain data (currently available in modern digital society) could be a good pointer for development of appropriate model for a specific application domain.

I conclude with an appeal to the global CA community to spread the discipline of CAR to different countries of the globe so that the new generation of researchers are encouraged to come forward with innovative and 'out of box' thinking of CAT, that would attract researchers of other disciplines to develop industrial/commercial applications of their interest.

P Pal Chaudhuri

Kolkata

Date: March 3, 2022

Prologue

The First Asian Symposium on Cellular Automata Technology, 2022 (ASCAT 2022) contains six invited talks and fourteen contributed talks that were selected for presentation during March 3-5, 2022. The symposium is officially hosted by the Indian Institute of Engineering Science and Technology, Shibpur (IIEST, Shibpur), India through video conferencing mode and sponsored by SPARC (*Scheme for Promotion of Academic and Research Collaboration*), an initiative of the Ministry of Human Resource Development, Government of India, under the project titled "Exploring Cellular Automata Model for Hardware Security" with Sukanta Das as Indian PI, Jarkko Kari as Foreign PI, Biplab K Sikdar as Indian Co-PI, Hannu Tenhunen and Pasi Liljeberg as Foreign Co-PIs.

Cellular automata as an emergent area of natural computing have been explored by a divergent group of researchers. There are a number of international conferences and workshops that consider cellular automata as the primary theme and deal with various aspects of cellular automata, their theoretical, modeling and application development. Since late 1980s, cellular automata have been used to devise solutions for technological problems, particularly in the domain of VLSI (Very Large Scale Integration) Design and Test, Pattern Recognition and Classification, Security and Image Processing. The aim of this symposium is to focus on the technology development issue. In our view, ASCAT is the first event of this kind. Since technology cannot get matured without a solid theoretical base, this symposium targets theoreticians and engineers to exchange their views and ideas.

ASCAT 2022 is proud to have Stephen Wolfram, Mihir K Chakraborty, Jarkko Kari, Kenichi Morita, Craig S Lent and Debdeep Mukhopadhyay as invited speakers, who kindly agree to deliver talks on related topics. We are indebted to them. We have received 32 submissions in this event, each of which is reviewed by 2-3 experts. Apart from the members of the Program Committee, four additional reviewers have reviewed the papers. We are thankful to all the reviewers for their effort. An online Program Committee meeting was held on December 16, 2021 to consider the reviews, and based on a detailed discussion, 14 papers have been accepted for presentation in the symposium. We thank all the authors for their contributions and hard work that make the event possible.

We are very much grateful to Professor Parimal Pal Chaudhruri who is a pioneer in cellular automata technology research and has promoted cellular automata research in India. Presently

India has a footprint in cellular automata research for which we are indebted to Professor Pal Chaudhuri.

During this ongoing pandemic, the Indian researchers have come forward to form '*Cellular Automata India'* research group. The group has hosted two webinar series on various topics of cellular automata and a special lecture series in the memory of John Horton Conway. Eminent scientists around the Globe have delivered invited talks and shared their research in this platform. It has taken the leading role to launch the symposium as a meeting place for the international intelligentsia.

No international event like ASCAT can succeed without a great Program Committee. We are grateful to all members of the Program Committee who have kindly accepted our invitation and extended their support in organizing this event. Special thanks to the members of the Organizing Committee and to the members of the departments of Information Technology, and Computer Science and Technology, IIEST, Shibpur for extending their support towards the event. We are thankful to Easychair, the popular conference management system, for allowing us to manage the submissions. Our sincere thanks to the officials of Springer who agreed to publish the proceedings of this event as part of their Springer AISC Series. We are also thankful to *JCA* (Journal of Cellular Automata) and *Complex Systems* which have agreed to publish Special Issues with the extended versions of the selected papers. Finally, we extend our gratitude to the Indian Institute of Engineering Science and Technology, Shibpur for giving us permission to host this symposium as an event of this institute.

Biplab K Sikdar — Sukanta Das

Jarkko Kari — Genaro J Martinez

General Co-chairs — Program Co-chairs

Date: March 3, 2022

Committee

Chief Patron:

Parthasarathi Chakrabarti	Director, Indian Institute of Engineering Science and Technology, Shibpur, India

Patron:

Dipanwita Roy Chowdhury	Indian Institute of Technology, Kharagpur, India

General co-chairs:

Biplab K Sikdar	Indian Institute of Engineering Science and Technology, Shibpur
Jarkko Kari	University of Turku, Finland

Programme co-chairs:

Sukanta Das	Indian Institute of Engineering Science and Technology, Shibpur
Genaro Juarez Martinez	National Polytechnic Institute, Mexico City, Mexico

Program committee:

Dipanwita Roy Chowdhury	Indian Institute of Technology, Kharagpur, India
Biplab K Sikdar	Indian Institute of Engineering Science and Technology, Shibpur
Kenichi Morita	Hiroshima University, Japan
Jarkko Kari	University of Turku, Finland
Mihir K Chakraborty	School of Cognitive Science, Jadavpur University, Kolkata, India
B R Shankar	National Institute of Technology Karnataka, Surathkal, India
N P Gopalan	National Institute of Technology Tiruchirappalli, India
R Ramanujam	The Institute of Mathematical Sciences, India
Fasel Qadir	University of Kashmir, India

Anna Lawniczak	Guelph University, Canada
Stefano Nichele	Oslo Metropolitan University, Norway
Niloy Ganguly	Indian Institute of Technology, Kharagpur, India
Pradipta Maji	Indian Statistical Institute, Kolkata, India
Genaro Juarez Martinez	National Polytechnic Institute, Mexico City, Mexico
Sukanta Das	Indian Institute of Engineering Science and Technology, Shibpur

Organizing committee:

Biplab K. Sikdar	Indian Institute of Engineering Science and Technology, Shibpur
Abhik Mukherjee	Indian Institute of Engineering Science and Technology, Shibpur
Amit Roy Chowdhury	Indian Institute of Engineering Science and Technology, Shibpur
Chandan Giri	Indian Institute of Engineering Science and Technology, Shibpur
Surajit Roy	Indian Institute of Engineering Science and Technology, Shibpur
Ashish Layek	Indian Institute of Engineering Science and Technology, Shibpur
Kamalika Bhattacharjee	National Institute of Technology, Tiruchirappalli, India
Souvik Roy	Indian Institute of Engineering Science and Technology, Shibpur
Sumit Adak	Indian Institute of Engineering Science and Technology, Shibpur
Sukanta Das	Indian Institute of Engineering Science and Technology, Shibpur

Registration Chairs:

Supreeti Kamilya	Birla Institute of Technology, Mesra, Ranchi, India
Sukanya Mukherjee	Institute of Engineering and Management, Kolkata, India

Table of Contents

Program Schedule

Meeting link is same for all sessions throughout the event

https://us02web.zoom.us/j/83683720520?pwd=K2gvMzNtaHZXZlZGTXIrYjd6Tzdhdz09

Platform: Zoom **Meeting ID: 836 8372 0520** **Passcode: 103497**

Day 1: 03 March 2022	
09:00 - 09:30	**Inauguration**
Session I **Chairs:** Kolin Paul, Indian Institute of Technology, Delhi & Kamalika Bhattacharjee, National Institute of Technology, Tiruchirappalli	
09:30 - 10:30	*Invited Talk* **The Ruliological View of Cellular Automata** Stephen Wolfram Founder & CEO of Wolfram Research
10:30 - 11:00	**Tea Break**
11:00 - 11:30	*Contributed Talk* **Grade Estimation of Mineral Resources: An Application of Cellular Automata** Soumyadeep Paty and Supreeti Kamilya
11:30 - 12:00	*Contributed Talk* **Shape Generation using Cellular Automata with Clustering** Lynette Van Zijl and Caleb Zeeman
12:00 - 12:30	*Contributed Talk* **Evolution Patterns of Some One-Dimensional Non-uniform Cellular Automata** Sreeya Ghosh and Sumita Basu
12:30 - 14:30	**Lunch Break**
Session II **Chairs:** Pabitra Pal Chaudhuri, Indian Statistical Institute, Kolkata & Supreeti Kamilya, Birla Institute of Technology, Mesra	

14:30 - 15:30	*Invited Talk* **Church-Turing Thesis and Gödel** Mihir K. Chakraborty School of Cognitive Science, Jadavpur University, Kolkata, India
15:30 - 16:00	*Contributed Talk* **Relationship of Two Discrete Dynamical Models: One-dimensional Cellular Automata and Integral Value Transformations** Sreeya Ghosh, Sudhakar Sahoo, Sk. Sarif Hassan, Jayanta Kumar Das and Pabitra Pal Choudhury
16:00 - 16:30	*Contributed Talk* **Emulating Mersenne Twister with Cellular Automata** Kamalika Bhattacharjee, Nitin More, Shobhit Kumar Singh and Nikhil Verma

Day 2: 04 March 2022	
Session I **Chairs:** Samir Roy, National Institute of Technical Teachers' Training and Research, Kolkata & Sukanya Mukherjee, Institute of Engineering of Management, Salt Lake	
09:30 - 10:30	*Invited Talk* **Computing in a Simple Reversible and Conservative Cellular Automaton** Kenichi Morita Hiroshima University, Japan
10:30 - 11:00	**Tea Break**
11:00 - 11:30	*Contributed Talk* **Defining Reachability Tree under Adiabatic and Reflexive Boundary Condition Cellular Automata** Nazma Naskar and B K Sivaraj
11:30 - 12:00	*Contributed Talk* **First Degree Cellular Automata as Pseudo-random Number Generators** Kamalika Bhattacharjee
12:00 - 12:30	*Contributed Talk* **A new notion of universality in respect of logic gates generation capability of ECAs** Raju Hazari
12:30 - 14:30	**Lunch Break**

Session II **Chairs:** Nazim Fatès, Inria-Loria, France & Mamata Dalui, National Institute of Technology, Durgapur	
14:30 - 15:30	*Invited Talk* **Algorithms for Group Cellular Automata** Jarkko Kari Department of Mathematics and Statistics, University of Turku, Finland
15:30 - 16:00	*Contributed Talk* **Cellular-automata based simulation of dynamic recrystallization and statistical analysis of resulting grain growth** Subramanian R S, Sai Shree Ramadev and Prince Gideon Kubendran Amos
16:00 - 16:30	*Contributed Talk* **Asynchronous Cellular Automata as Randomness Enhancer** Souvik Roy and Sumit Adak

Day 3: 05 March 2022	
Session I **Chairs:** Abhik Mukherjee, Indian Institute of Engineering Science and Technology, Shibpur & Sumit Adak, Defense Research and Development Organization (DRDO)	
09:30 - 10:30	*Invited Talk* **Quantum-dot Cellular Automata: Computing from the Ground Up** Craig S Lent Department of Electrical Engineering, University of Notre Dame, United States
10:30 - 11:00	**Tea Break**
11:00 - 11:30	*Contributed Talk* **Impact of Genetic Algorithm on Low power QCA Logic Circuit with Regular Clocking** Amit K Pramanik, Jayanta Pal, and Bibhash Sen
11:30 - 12:00	*Contributed Talk* **Cellular automata based model for finding minimum spanning tree in wireless sensor networks** Parijat Sen and Debopriya Barman

12:00 - 12:30	Contributed Talk **A Novel Hash Function based on Hybrid Cellular Automata and Sponge Functions** Anita John, Alan Reji, Ajay P Manoj, Atul Premachandran, Basil Zachariah and Jimmy Jose
12:30 - 14:30	**Lunch Break**
Session II **Chair(s):** Nazma Naskar, Kalinga Institute of Industrial Technology University	
14:30 - 15:30	*Invited Talk* **Revisiting Logic Obfuscation Using Cellular Automata** Debdeep Mukhopadhyay Indian Institute of Technology, Kharagpur, West Bengal, India
15:30 - 16:00	*Contributed Talk* **Synthesis of Single Length Cycle Two Attractor CA using NSRT Diagram.** Suvadip Hazra and Mamata Dalui
16:00 - 16:30	**Valedictory**

Inauguration Program: (9:00 am to 9:30 am IST, 03-March-2022)

- Welcome Address by
    - Dr. Sukanta Das, Program co-chair, ASCAT, 2022
    - Prof. Sudip Kumar Roy, Dean of Academic, IIEST, Shibpur
    - Prof. Hafizur Rahaman, Dean of Research & Consultancy, IIEST, Shibpur
    - Prof. Arindam Biswas, Institute Coordinator of SPARC Projects
- Inauguration by Prof. Parthasarathi Chakrabarty, Director, IIEST, Shibpur

Valedictory Program: (16:00 pm to 16:30 pm IST, 05-March-2022)

Vote of thanks by

- Prof. Jarkko Kari, General co-chair, ASCAT, 2022
- Prof. Biplab K Sikdar, General co-chair, ASCAT, 2022
- Dr. Genaro J. Martinez, Program co-chair, ASCAT, 2022
- Dr. Sukanta Das, Program co-chair, ASCAT, 2022

Abstracts of the Invited Talks

The Ruliological View of Cellular Automata

Stephen Wolfram

Founder & CEO of Wolfram Research

s.wolfram@wolfram.com

A great and fundamental mystery of science could be discovered nearly 50 years ago when the complexity of nature was figured out using some sorts of computations. Starting from randomness, experimental works are done based on observations of several patterns and the different patterns are classified depending on the observations. It is simplified further by replacing random initial states with the simplest possible seed and the pattern is observed. The magical moment comes when it is seen that a simple rule and simple seed is making something that seems extremely complex.

"Ruliology" is a new and slightly unusual-sounding word that indicates the pure basic science of what simple rules do. It is about setting up abstract rules, and then seeing what they do: exactly how a cellular automaton works. A magnificent discovery of science, based on the paradigm of computation is described in the magnum opus "A New Kind of Science". The computational universe and its applications are explored in the book. For three centuries before 1990s, theoretical science had been dominated by the idea of using mathematical equations to describe the world. However, there was a new idea during 90s. The idea was not of solving equations, but instead of setting up computational rules that could be explicitly run to represent and reproduce things in the world. Without the computational paradigm, systems that showed significant complexity had seemed quite inaccessible to science. But now there is an underlying way to model them, and to successfully reproduce the complexity of their behavior.

Ruliology tends to start with specific cases of specific rules and then it generalizes, looking at broader ranges of cases for a particular rule, or whole classes of rules. However, it quickly comes face to face with computational irreducibility. Some particular case of some particular rule may require an irreducible amount of computational effort and if one insists on knowing what amounts to a general truly infinite-time result, it may be formally undecidable. Ruliology in some ways starts as an experimental science, and in some ways is abstract and theoretical from the beginning. It is experimental because it is often concerned with just running simple programs and seeing what they do. But it is abstract and theoretical in the sense that what is being run is not some actual thing

in the natural world, with all its details and approximations, but something completely precise, defined and computational.

If one looks at the literature of complexity, one finds all sorts of models for all sorts of systems. And the models are very complicated. But the question is: are there simpler models lurking underneath? Models are simple enough that one can readily understand at least their basic rules and structure as well as it is plausible that they could be useful for other systems as well. To find such things is in a sense an exercise in what one can call "metamodeling": trying to make a model of a model, doing reductionist science not on observations of the world, but on the structure of models. The activity of metamodeling is not a common one in science. However, metamodeling has seemed very natural like language design: one starts off from a whole collection of computations, and descriptions of how to do them. And then he/she can try to drill down to identify a small set of primitives that let him/her conveniently build up those computations.

Cellular automata are in a sense minimal models in which there's a definite (discrete) structure for space and time and a finite number of states associated with each discrete cell. And it has been remarkable how many different kinds of systems can successfully be modeled by cellular automata. Through the computational paradigm, there is a clear notion of where complexity fundamentally comes from. And by leveraging the basic science of the computational universe, and the metamodeling and ruliology, there is a tremendous opportunity that now exists to dramatically advance everything that has been done under the banner of complexity.

Church-Turing Thesis and Gödel

Mihir K. Chakraborty

School of Cognitive Science, Jadavpur University, Kolkata,India

mihirc4@gmail.com

The purpose of this talk is to investigate the question, "whether the Church-Turing thesis (CTT) is a thesis or a theorem". Has this question been resolved satisfactorily? In this context we shall look into the opinions of Gödel and Turing himself among others as reflected in the current research in this domain.

By the term 'thesis' is meant a proposition laid down to be debated upon, not an established fact. But it is more than a hypothesis, it has already been tested several times and no evidence toward refuting it has been obtained so far. On the other hand, a theorem is a proposition proved rigorously by firm argumentation. While in literature we find the terminology 'Church-Turing thesis', we do not encounter a term like 'Gödel's completeness thesis', rather the latter is called a 'Theorem'. So, the discussion of the current talk is basically on the question: should CTT be called a theorem instead of a thesis.

There are many versions of the Church-Turing thesis of which I take the following: a function on the integers is effectively calculable if and only if it is Turing Computable. 'Effectively calculable' is an informal concept which means that an intelligent and efficient idealized human being can calculate the function. Because of the words 'intelligent', 'efficient' and 'idealized' the above notion turns out to be vague, however.

The concept emerged in the 1920s. If one accepts CTT, the notion of effective calculativity may be considered to have a definitive meaning, through Turing's work in 1936. While Church and Kleene believed in CTT, Gödel did not accept it. Gödel was looking for a proper demonstration. He was not convinced by Church's (informal) argument. though he believed that CTT was true. We shall deal with Gödels opinion in this matter in some detail.

Some researchers wish to place CTT in a position in between thesis and theorem. Soare is more inclined towards calling it a thesis. Sieg proposes a proof and hence according to him it is a theorem. Gurevich presents another approach to proving the thesis. Feferman thinks that the

statement of CTT may not be a matter within Zermelo-Fraenkel Set theory (ZFC) but that does not make it less mathematical so as to rule out a proof of it. The debate, I think, still persists perhaps in a deeper domain.

From ‘effectively calculable’ the term ‘effectively computable’ was coined but some scholars think that computability is a more general term than merely computability of number theoretic functions. Even though CTT turns out to be a theorem it makes Turing computable and effective computable functions to be co-extensive. Descartes’ dictum ‘Let us calculate’ has perhaps that deeper meaning of computability.

In this talk we shall delve into these issues from the philosophical and historical perspectives.

Algorithms for Group Cellular Automata

Jarkko Kari

Department of Mathematics and Statistics, University of Turku, Finland

jkari@utu.fi

We consider subshifts and cellular automata in the setup where the state set is a finite group. The group does not need to be commutative. A subshift that is also a subgroup is called a group shift, and we call a cellular automaton on a group shift a group cellular automaton if it is also a group homomorphism. Group cellular automata generalize the much studied concept of additive cellular automata into non-commutative groups. The set of space-time diagrams of a group cellular automaton is a group shift, so we can apply classical results by Bruce Kitchens and Klaus Schmidt on group shifts to analyze group cellular automata. In particular, we can effectively construct the limit set and the trace subshifts of any group cellular automaton. We can then algorithmically decide many properties concerning the cellular automaton that are in general undecidable. The talk is based on a joint work with Pierre Béaur.

Computing in a Simple Reversible and Conservative Cellular Automaton

Kenichi Morita

Hiroshima University, Higashi-Hiroshima 739-8527 Japan

km@hiroshima-u.ac.jp

We show how to construct reversible computers in a simple reversible and conservative two-dimensional cellular space. We introduce the framework of an *elementary square partitioned cellular automaton* (ESPCA), and use a particular ESPCA with the hexadecimal ID number "01caef", which is denoted by ESPCA P_0 for short in this paper. A cell of ESPCA P_0consists of four parts each of which has two states 0 and 1. The class of ESPCAs is the simplest subclass of square partitioned cellular automata, and each of their local functions is described by only six local transition rules. ESPCA $P_0$is not only reversible, but also conservative in the sense that the total number of state 1's is conserved throughout its evolution process. We show that a space-moving pattern called a *glider* exists in P_0. Colliding a glider with another pattern called

a *blinker*, several interesting phenomena appear. We give a method of constructing reversible Turing machines (RTMs) using such phenomena. We first implement a *reversible logic element with memory* (RLEM), rather than a reversible logic gate, using only three of these phenomena. Then, we compose reversible Turing machines out of RLEMs. In this systematic and modularized way, we can construct any RTM out of only two small patterns in a simple reversible and conservative cellular space.

Quantum-dot Cellular Automata: Computing from the Ground Up

Craig S Lent

Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana, United States

lent@nd.edu

This talk will discuss the foundational aspects of QCA (Quantum-dot cellular automata) - using the physics of cellular interactions to enable binary computation. I will describe various implementations, natural architectures, and the challenges in both.

Revisiting Logic Obfuscation Using Cellular Automata

Akashdeep Saha, Hrivu Banerjee, Rajat Subhra Chakraborty, Debdeep Mukhopadhyay

Indian Institute of Technology, Kharagpur, West Bengal, India

debdeep@cse.iitkgp.ac.in

Logic obfuscation has evolved as a promising countermeasure against IP piracy. The Finite State Machine (FSM) is often obfuscated in a sequential circuit using suitable strategies. One such strategy proposed to obfuscate each state transition of the FSM using a class of non-group additive cellular automata (CA) called *D1*CA* and $D1^*CA_{dual}$. This CA-based obfuscation strategy conceals the FSM states, providing high testability hence eliminating the requirement of any scan-based Design-for-Testability techniques. However, utilizing the information leaked by the implemented FSM observable externally, an end-to-end attack strategy (named ORACALL) was proposed. It could extract the secret key for each transition of the CA-based obfuscated FSM along with the CA state encodings of the FSM states. In this work, we investigate the root cause of the success of ORACALL on a CA-based obfuscation strategy. Utilizing those findings, we propose a couple of mitigation techniques by appending non-linearity to the existing CA structure along with a slight modification of the *D1*CA* rule vector. Experimental validation proves that these simple yet effective countermeasures could thwart ORACALL while preserving the elegance of the underlying structure of the CA-based obfuscation technique with minimal overhead.

Abstracts of the Contributed Talks

Grade Estimation of Mineral Resources: An Application of Cellular Automata

Soumyadeep Paty [1] and Supreeti Kamilya [2]

[1] Department of Mining Engineering,
Kazi Nazrul University, Asansol, West Bengal, India
soumyadeep.paty@gmail.com
[2] Department of Computer Science and Engineering,
BIT Mesra, Ranchi, Jharkhand, India
kamilyasupreeti779@gmail.com

Mineral industry contributes a major part of economical growth to a nation. Therefore, it is important to understand the concentration measurement of minerals in different locations of earth's crust. The concentration refers to as the grade values of minerals. A block model is a simplified geometrical representation of a mineral deposit. There are several methods to find out the grade values of each block, such as, inverse distance method, copula, krigging etc. Krigging is a popular method to find out the grade values. However, number of mathematical calculations increase with the increasing number of sample points and thus the computational complexity becomes high. Here, we use a mathematical tool, cellular automata (CAs) where each cell is represented as a block. Using cellular automata, we here find out the grade values with much less computations. 2 dimensional CAs are used in this study where the local rule is the ordinary krigging estimator function using spherical variogram model. Also, in this study we deal with multiple horizontal slices of 3 dimensional mineral deposits. It can be seen that the CA based estimation is same as ordinary krigging based estimation, however, in a much simpler way.

Shape Generation using Cellular Automata with Clustering

Caleb Zeeman and Lynette van Zijl

Dept. of Computer Science, Stellenbosch University, South Africa

21018030@sun.ac.za, lvzijl@sun.ac.za

When using cellular automata with clustering in the Lumer-Faieta ant sorting algorithm, the method used to drop the cells in a cluster affects the geometric shape that the cluster will form. We investigate various algorithms for dropping strategies that can be used to generate pre-defined geometric shapes.

Evolution Patterns of Some One-Dimensional Non-uniform Cellular Automata

Sreeya Ghosh and Sumita Basu

Dept. of Applied Mathematics, Calcutta University, Kolkata-700009, India
Indian Statistical Institute, Kolkata-700108, India
Email: sreeya135@gmail.com

Retired Professor, Bethune College, Kolkata 700006, India,
Guest Faculty, Dept. of Mathematics,The Heritage College, Kolkata-700107,
Email: sumi basu05@yahoo.co.in

This paper investigates patterns generated by some one-dimensional spatially non-uniform cellular automata. The non-uniform cellular automaton is taken to be composed of finite celled blocks where each block has a different local transition function and within any block all the cells follow same local transition function. The evolution patterns generated by identity, complementary, constant and shift functions and a combination of them as local transition functions are studied in this paper.

Relationship of Two Discrete Dynamical Models: One-dimensional Cellular Automata and Integral Value Transformations

Sreeya Ghosh [a,b], Sudhakar Sahoo [c] , Sk. Sarif Hassan [d] , Jayanta Kumar Das [b,e] , and

Pabitra Pal Choudhury [b]

[a] Dept. of Applied Mathematics, University of Calcutta, Kolkata-700009, India

[b] Applied Statistics Unit, Indian Statistical Institute, Kolkata-108 , India

[c]Institute of Mathematics and Applications, Bhubaneshwar-751029, India

[d]Dept.of Mathematics, Pingla Thana Mahavidyalaya, Paschim Medinipur-721140, India

[e]School of Medicine, Johns Hopkins University, MD-21287, USA

Emails: sreeya135@gmail.com ∗ , sudhakar.sahoo@gmail.com, sarimif@gmail.com, dasjayantakumar89@gmail.com, pabitrapalchoudhury@gmail.com

Cellular Automaton(CA) and an Integral Value Transformation(IVT) are two well established mathematical models which evolve in discrete time steps. Theoretically, studies on CA suggest that CA is capable of producing a great variety of evolution patterns. However computation of non-linear CA or higher dimensional CA maybe complex, whereas IVTs can be manipulated easily.

The main purpose of this paper is to study the link between a transition function of a one-dimensional CA and that of IVTs. Mathematically, we have also established the algebraic structures of a set of transition functions of a one-dimensional CA as well as that of a set of IVTs using binary operations.

Emulating Mersenne Twister with Cellular Automata

Kamalika Bhattacharjee, Nitin More, Shobhit Kumar Singh, and Nikhil Verma

Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, Tamilnadu, 620015, India
{kamalika.it, Nitinmore6990, sks.shobhit12, nikhilverma793}@gmail.com

Mersenne Twister (MT19937) is by far the most widely used general-purpose pseudo-random number generator (PRNG) but it has been 30 years since it was introduced. This paper aims to use the advancement in technology and knowledge of a cellular automaton (CA) and its properties to create a PRNG that can use resources more effectively while giving an equivalent or a better result than MT19937. The research involves creation of suitable generator by finalizing an appropriate length of the CA that fits perfectly with space-time trade-off, finding the seed, running the PRNG on various testbeds like Dieharder, TestU01 and progressively improving it. In the end, it is shown that our PRNG is at least at par with MT19937 and also a good challenger to today's more advanced pseudo-random number generators like SFMT and TinyMT.

Defining Reachability Tree under Adiabatic and Reflexive Boundary Conditions

Nazma Naskar[1] and B K Sivaraj[2]

[1] Assistant Professor, School of Computer Science,
KIIT Deemed to be University, Bhubaneswar, Odisha-751024, India.
nazma.naskarfcs@kiit.ac.in

[2] National Institute of Technology Tiruchirapalli (NIT-T),
Tiruchirapalli, Tamil Nadu-620015, India.
sbksivaraj@gmail.com

In this paper the elementary cellular automata is explored under adiabatic boundary condition and reflexive boundary condition, using the reachability tree. To construct the reachability tree under the mentioned conditions, structures of those boundary conditions are analysed. The valid RMTs of root level and leaf level are identified. It was found that only at root level and leaf level, the structures and arrangements differ slightly with the reachability tree of null boundary condition.

First Degree Cellular Automata as Pseudo-random Number Generators

Kamalika Bhattacharjee

Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, Tamilnadu, 620015, India
kamalika.it@gmail.com

This paper depicts simple Cellular Automata (CAs) as potential pseudo-random number generators (PRNGs). It introduces a technique to represent CAs as first degree equation identified by some tuples. Some 3-neighborhood 10-state CAs, identified by 6 tuples, are selected following greedy criteria. Concept of window is used to extract a number from each configuration. We observe that, our scheme of choosing the CAs has potentiality to beat all other existing PRNGs.

A new notion of universality in respect of logic gates generation capability of ECAs

Raju Hazari

Department of Computer Science and Engineering
National Institute of Technology Calicut, Kerala, India - 673601
hazariraju0201@gmail.com

This paper studies the gate generation capability of elementary cellular automaton (ECA). We first show that the basic logic gates, such as AND, OR, NOT, NAND, NOR, XOR, XNOR etc. can be realized by evolving ECAs. Since any logic circuit can be implemented by utilizing basic logic gates, the CA can implement all logic circuits. Therefore, we get a new notion of universality of CAs. We find out that there are some ECAs rules which have the universality property. Finally, we compare the gate generation capability of these CAs.

Cellular-automata based simulation of dynamic recrystallization and statistical analysis of resulting grain growth

Subramanian R S , Ramadev Sai Shree , and P G Kubendran Amos

Theoretical Metallurgy Group,
Department of Metallurgical and Materials Engineering,
National Institute of Technology Tiruchirappalli,
Tamil Nadu, India
prince@nitt.edu

By employing cellular automata technique, in this work, a polycrystalline system corroborating experimentally observed microstructure is developed. Moreover, through appropriate transition functions, microstructural changes accompanying dynamic recrystallization, a manufacturing technique associated with the production of wide-range of components, is simulated. The grain growth that characterises this change is analysed to explicate the trend in the temporal evolution of mean grain size and its kinetics. As opposed to a progressive increase in mean grain size, which generally typifies a conventional grain growth, in dynamic recrystallization, it is observed that the mean grain size increases and decreases sequentially, thereby rendering a oscillating pattern. A perceptive investigation of the fluctuating trend unravels individual growth events, characterised by monotonic increase in mean grain size, whose kinetics follow the third-order power law.

Asynchronous Cellular Automata as Randomness Enhancer

Souvik Roy and Sumit Adak

Department of Information Technology
Indian Institute of Engineering Science and Technology, Shibpur
Howrah, West Bengal, India-711103
svkr89@gmail.com, maths.sumit@gmail.com

This work explores randomness enhancing capability of asynchronous cellular automata. This paper first reports theoretical results to identify elementary cellular automata under fully asynchronous updating scheme with large cycle of length 2^n or 2^n-1. To predict the pseudo-random number generation capability, we classify these large cycle asynchronous cellular automata into fully and partially exposed systems. Finally, it is observed that asynchronous cellular automata are able to improve randomness quality of a 'poor' random number generator.

Impact of Genetic Algorithm on Low power QCA Logic Circuit with Regular Clocking

Amit Kumar Pramanik [1,3] , Jayanta Pal [2] , and Bibhash Sen [3]

[1]Department of CSE, Dumka Engineering College, Jharkhand, India
amit.pramanik21@gmail.com
[2] Department of Information Technology, Tripura University, Suryamaninagar, India
jayantapal@tripurauniv.ac.in
[3] Department of CSE, National Institute of Technology, Durgapur, India
bibhash.sen@cse.nitdgp.ac.in

Quantum-dot Cellular Automata (QCA) is the alternative approach to synthesize the logic circuit with high density and low power dissipation to overcome the limitation of current VLSI technology. The underlying regular clocking scheme plays a significant role in the systematic cell layout, scalability, and reliability of the QCA circuit. This work analyzes the impact of genetic algorithm (GA) on regular QCA circuits for less power dissipation. The elitism-based methodology is utilized to effectively realize multi-output boolean functions, embedding regular

clocking schemes. A detailed analysis of power dissipation with different regular clocking schemes is reported. QCADesigner is used for logic synthesis, whereas QCAPro and QCADesignerE have been utilized for energy dissipation analysis.

Cellular automata based model for finding minimum spanning tree in wireless sensor networks

Parijat Sen and Debopriya Barman

Department of Information Technology
Indian Institute of Engineering Science and Technology, Shibpur
Howrah, West Bengal, India 711103
psen8044@gmail.com , debopriyabarman@gmail.com

This work presents a cellular automata (CA) based model for finding minimum spanning tree in wireless sensor networks (WSN) with distinct edge weights. A regular grid topology network is created by the sensor nodes where every sensor node can have maximum four neighbor nodes in the tree. To perform the computation every sensor node communicates with its immediate neighbour nodes which are within its communication range . Nodes use simple CA based localized algorithms which can optimize the performance. By limiting the maximum num- ber of neighbour nodes it also minimizes the redundancy in the network which can increase the lifetime of the network.

A Novel Hash Function based on Hybrid Cellular Automata and Sponge Functions

Anita John [1] , Alan Reji [2] , Ajay P Manoj [2] , Atul Premachandran [2] , Basil Zachariah [2] , and Jimmy Jose [1]

[1] Department of Computer Science and Engineering,
National Institute of Technology Calicut, Kozhikode, India
{anita_p170007cs, jimmy}@nitc.ac.in

[2] Department of Computer Science and Engineering,
Rajagiri School of Engineering and Technology, Kochi, India

Hash functions serve as the fingerprint of a message. They also serve as an authentication mechanism in many applications. Nowadays, hash functions are widely used in blockchain technology and bitcoins. Today, most of the work concentrates on the design of lightweight hash functions which needs minimal hardware and software resources. This paper proposes a lightweight hash function which makes use of Cellular Automata (CA) and sponge functions. This hash function accepts arbitrary length message and produces fixed size hash digest. An additional property of this function is that the size of the hash digest may be adjusted based on the application because of the inherent property of varying length output of sponge function. The proposed hash function can be efficiently used in resource constraint environments in a secure and efficient manner. In addition, the function is resistant to all known generic attacks against hash functions and is also preimage resistant, second preimage resistant and collision resistant.

Synthesis of Single Length Cycle Two Attractor CA using NSRT Diagram

Suvadip Hazra and Mamata Dalui

NIT Durgapur, West Bengal, India 713209
sh.16cs1102@phd.nitdgp.ac.in
mamata.dalui@cse.nitdgp.ac.in

Cellular Automata (CA) is a discrete model that is increasingly being employed in scientific study and simulations. It has several applications in the domains such as VLSI design, error-correcting codes, test pattern generation, and cryptography, etc. The majority of these applications make use of three-neighbourhood 1-dimensional CA. In this work, a comprehensive study on 3-neighborhood CA with 2-states per cell has been reported. The Next State RMT Transition Diagram (NSRTD), a graph-based tool, is presented to analyse CA's state transition behaviour with fixed points. A methodology has been proposed for synthesising Single Length Cycle Two Attractor CA (TACA).