CDMTCS
Research
Report
Series

The 5th Anniversary Workshop on Discrete Mathematics and Theoretical Computer Science

C. S. Calude and M. J. Dinneen
(Editors)
University of Auckland, New Zealand

CDMTCS-134
May 2000

Centre for Discrete Mathematics and
Theoretical Computer Science

Introduction

These are the abstracts of talks to be given at the One-Day Workshop *Discrete Mathematics and Theoretical Computer Science Day* to be held at the University Auckland on 26 May 2000 to mark the 5th anniversary of the Center for Discrete Mathematics and Theoretical Computer Science.

The Conference Committee for the workshop consisted of the following people: Douglas S. Bridges, Canterbury, Cristian S. Calude, Auckland, Michael J. Dinneen, Auckland, John Hosking, Auckland, Gaven Martin, Auckland, Alan Williamson, Auckland.

Cristian S. Calude
Michael J. Dinneen
Auckland
May 2000

Messages from Members of the International Advisory Board

I congratulate the CDMTCS on its 5th anniversary. Already, the CDMTCS has established itself as a world class research center, definitely *the* research center in discrete mathematics and theoretical computer science in the Southern hemisphere. I hope that our cooperation will continue, and that the new edition of the international conference, “Unconventional Models of Computation”, to be held in Brussels in December will be another grand success.

John L. Casti
Santa Fe Institute, USA
Technical University of Vienna, Austria

To the Members of the CDMTCS!

Greetings from New York and congratulations on your fifth anniversary! You may be far away in New Zealand, but your work is visible around the world. Keep up the good work!

With all my best wishes,

Gregory Chaitin
CDMTCS IAB
IBM Research Division
May 2000

I congratulate the Center for having provided for five years a focal point for research in computer science and discrete mathematics. The Center provides a new home for world class research, a place where those in the Southern hemisphere know they can meet and work with the scientific leaders of the world without an obligatory 10,000 mile visit to Europe or the United States. I only wish I could join you on this joyful occasion. Unfortunately, it is exactly at the end of term here. My best wishes for ever increasing success in the future!

Anil Nerode
Former Director, Mathematical; Sciences Institute, 1987-96
Director, Center for the Foundations of Intelligent Systems
Goldwin Smith Professor of Mathematics and Computer Science
Cornell University Ithaca, New York, USA

I would like to congratulate CDMTCS very warmly, and wish you much success also in the future. In spite of its youth, CDMTCS has already established itself as one of the international centers of Theoretical Computer Science. That your many meetings and conferences have attracted some really big names cannot be explained only by the paradise-like outer conditions in New Zealand. The scientific community has realized that the scientific level of these meetings is high. Personally, I am very happy that I have been involved (for a very small part) in some of your activities, including publication series. I regret that I cannot be present now, because of reasons of health. But I sincerely hope that our cooperation will continue, both at the personal and at the institute level, between CDMTCS and TUCS. Many Happy Returns!

Arto Salomaa
Turku Centre for Computer Science
Turku University, Finland

Messages from the Dean of Science and Head of Computer Science Department

Dear Cris,

CDMTCS CONFERENCE

I wish to congratulate the Centre for Discrete Mathematics and Theoretical Computer Science on its excellent success over the past 5 years. Its contributions to basic research at the interface of mathematics and computing have been outstanding. CDMTCS strength lies in its capacity to draw together leading researchers from several different Departments and other New Zealand universities as well as involving researchers from several international universities. The success of the centre in attracting research students and producing high quality international publications is outstanding.

Please convey to all those associated with the CDMTCS both my warmest congratulations on achievements so far, and my best wishes for future success. Also, my congratulations to you personally, for your outstanding leadership of this Centre.

I hope that the conference will be great success. I look forward to hearing about the outcomes of the conference.

Yours sincerely,

Ralph Cooney
Professor
Dean of Science

It is my pleasure to welcome you to the Fifth Anniversary Workshop of the Centre for Discrete Mathematics and Theoretical Computer Science. This is a time to celebrate five positive and productive years of work by all involved in the Centre, and to recognise the achievements made.

I would like to take a few minutes to reflect on the meaning of centre and show how the CDMTCS truly reflects those various meanings. One meaning of centre is as a midpoint. In that respect the CDMTCS can be seen to be a midpoint between the Departments of Mathematics and Computer Science, a place where our common research interest join together.

Another meaning of centre is the notion of a place where people are attracted to. Clearly the CDMTCS has been highly successful in that regard. The Centre has attracted some 40 of the country's most highly respected Mathematicians and Computer Scientists as internal and external members. It has an international advisory board that reads like a who's who in the area. Importantly it has attracted over 70 visitors, including some of the distinguished guests here today, together with an average of 15 research students a year.

Centre also implies a notion of excellence. I have already commented on the calibre of the members and advisory board. The excellence of this group is further demonstrated by the close to 50 research grants gained by members of the group, and, in particular, the impressive number of Marsden, PGSF, and NSF grants awarded to its members. It is also demonstrated by the calibre of the presenters attracted to this meeting today.

A further meaning of centre is that of a place where people look to for guidance and knowledge. With 14 books in the Springer series, over 700 refereed publications by members and over 130 research reports, the CDMTCS is clearly acting in that capacity. It has also organised 2 major conferences and a summer school workshop (on the Black Sea coast!), together with workshops such as the one you are attending today.

So, by any measure the CDMTCS is fulfilling its claim to be a Centre of academic excellence and achievement. I offer my congratulations to members of the Centre on your achievements and wish you all well for a successful workshop.

Assoc. Professor John Hosking
HOD Department of Computer Science

Abstracts

Abstract Data Types Viewed as Abstract Machines

Michael Atkinson
University of Otago
Otago
E-mail: mda@scitec.auckland.ac.nz

Abstract data types may be regarded as abstract machines and then a program for an ADT is any sequence of operations allowed by its specification. The effect of such programs on container ADTs is captured by the relationship between each input sequence and the set of possible output sequences that can result from it. A survey of combinatorial results will be given.

How to Eliminate Crossings in Graphs by Adding Handles

Dan Archdeacon
Vermont University, USA
E-mail: dan.archdeacon@uvm.edu
Paul Bonnington
Auckland University
Auckland
E-mail: p.bonnington@auckland.ac.nz
Jozef Siran
Slovak Technical University, Slovakia
E-mail: siran@lux.svf.stuba.sk

Determining the minimum number of edge crossings in a drawing of a graph on a surface has important applications to electronic circuit design. Let $c_k = cr_k(G)$ denote the minimum number of edge crossings when a graph G is drawn on an orientable surface of genus k. The (orientable) *crossing sequence* $c_0, c_1, c_2, \ldots$ encodes the trade-off between adding handles and decreasing crossings.

We focus on sequences of the type $c_0 > c_1 > c_2 = 0$; equivalently, we study the planar and toroidal crossing number of doubly-toroidal graphs. For every $\epsilon > 0$ we construct graphs whose orientable crossing sequence satisfies $c_1/c_0 > 5/6 - \epsilon$. In other words, we construct graphs where the addition of one handle can save roughly 1/6th of the crossings, but the addition of a second handle can save 5 times more crossings.

More Constructive Ideas on Apartness Spaces

Douglas S. Bridges
Canterbury University
Christchurch
E-mail: d.bridges@math.canterbury.ac.nz

Following on the material covered by Luminiţa Dediu, this talk deals first with product apartness spaces. It then introduces recent investigations, by Bridges, Dediu and Schuster, on the axiomatic constructive theory of apartness between subsets.

A Special Group with Applications

John C. Butcher
University of Auckland
Auckland
E-mail: `butcher@scitec.auckland.ac.nz`

Let G be the set of mappings on the set of all rooted trees (arborescences) to the real numbers, together with a binary operation that will be defined. With this operation, G is group which we note is not Abelian. We will introduce some of the normal subgroups and quotient groups and other structures associated with G, and point out some of the applications, especially to numerical analysis.

Liars, Demons and Dragons

Cristian S. Calude
Auckland University
Auckland
E-mail: `cristian@attglobal.net`
Elena Calude
Massey University at Albany
Auckland
E-mail: `e.calude@massey.ac.nz`
Peter Kay
Massey University at Albany
Auckland
E-mail: `p.kay@massey.ac.nz`

We will show that some well-known chaotic maps appear as estimations of truth values of the Liar's Paradox; their fixed-points are automatic chaotic reals which relate again to the Liar's Paradox. The automaticity of fixed-points reveals a rather unexpected relation between Liar's Paradox and Maxwell demon.

Graph Symmetries, 2-groups, Sierpinski's Gasket and the Gray Code

Marston Conder
University of Auckland
Auckland
E-mail: `conder@math.auckland.ac.nz`

A construction is described for an infinite family of finite vertex-transitive non-Cayley graphs X_n of degree 4 with the property that the order of the vertex-stabilizer in the smallest vertex-transitive group of automorphisms of X_n is a strictly increasing function of n. The construction uses Sierpinski's gasket to produce generating permutations for the vertex-stabilizer (which is an arbitrarily large 2-group). Unexpectedly, the same modification of Sierpinski's gasket gives rise to an explicit definition for any given word of the binary reflected Gray code.

Apartness Spaces—A Framework for Constructive Topology

Luminiţa Simona Dediu
University of Canterbury
Christchurch
E-mail: `LDE15@student.canterbury.ac.nz`

In this paper, which is intended to be the first in a series, we lay down the foundations of one possible road to constructive topology: apartness spaces, analogues of the nearness spaces studied by some classical topologists. We introduce an axiomatic development of the theory of apartness and nearness of a point and a set, then study the relation between the topology induced by an apartness structure and the apartness induced by a topology on a set that carries a nontrivial inequality relation. We also investigate different continuity properties of mappings between apartness spaces.

Recent Work on Graph Minors

Michael J. Dinneen
Auckland University
Auckland
E-mail: `mjd@cs.auckland.ac.nz`

We look at the practical aspects of graph minors from the computational point of view. I'll talk about some of the current C++ implementations that have recently been completed and tested.

Reals, Randomness and Reducibilities

Rod Downey
Victoria University
Wellington
E-mail: `Rod.Downey@MCS.VUW.AC.NZ`

I will discuss some recent results on presentations of computably enumerable reals and randomness.

Random Fields as Image Models: Discrete vs. Continuous Paradigms

Georgy Gimelfarb
Auckland University
Auckland
E-mail: `g.gimelfarb@auckland.ac.nz`

In probabilistic image modeling, discrete images are frequently considered as more or less precise approximations of the continuous images so that traditional parametric random field models of these latter images are adapted to the discrete counterparts. Actually, more efficient way for image modeling is to develop and use inherently discrete models that have no immediate parallels in the continuous case. To illustrate both the continuous and discrete paradigms, texture modeling by Gibbs random fields is discussed.

Extracting Algebraic Information from Finite Automata

Bakh Khoussainov
Auckland University
Auckland
E-mail: bmk@cs.auckland.ac.nz

In this talk we introduce the concept of defining algebraic structures by finite automata. We give a formal definition to this concept, present several examples and results. We motivate and propose a program to systematically study algebraic structures by using automata from algebraic, complexity, and model-theoretic points of view.

Multigrid Convergence and Image Analysis

Reinhard Klette
Auckland University
Auckland
E-mail: r.klette@auckland.ac.nz

Archimedes estimated π based on regular n-gons. For n to infinity we have a convergence to the true value. Schwarz and others have shown in the 19th century that triangulations of surfaces do not necessarily converge to the surface area even in case of a straight cylinder. Techniques in image analysis for measuring the length of a curve or the surface area of a 3D set should converge to the true value if the grid resolution increases (multigrid convergence of calculated features). The talk reviews a few results in this area.

Regularity Preserving Metrics

Margaret Ng
University of Auckland
Auckland
E-mail: cng034@cs.auckland.ac.nz

We study various distances which preserve regularity, that is, distances on strings δ such that for every positive ε the set $E(L, \delta, \varepsilon) = \{x \mid \delta(x, y) \leq \varepsilon, \text{ for some } y \in L\}$ is regular provided L is regular. A Java program which acceptes a DFA M, a regularity preserving metric and a positive real ϵ, and produces the minimal DFA accepting the language $E(L(M), \delta, \varepsilon)$ will be presented. A graphical representation of the resulting DFA is also produced. The program can run on the web or in a Java environment.

Program Development, Refinement and Z

Steve Reeves
Waikato University
Hamilton
E-mail: stever@cs.waikato.ac.nz

This talk covers some recent work done within the Z-lambda project (a joint project between Essex and Waikato: see http://cswww.essex.ac.uk/FSS/projects/pdsrz.html) on a framework for program development within the schema calculus of Z. We'll provide some examples which show the major mathematical design decisions we made, which centre around regarding operation schemas as sets of programs (i.e. intensional objects). This leads us to a notion of refinement which differs (in useful ways) from the 'traditional' refinement calculus based on weakest precondition semantics.

Computing Approximations of a Chaitin's Ω Number

Chi-Kou Shu
University of Auckland
Auckland
E-mail: cshu004@cs.auckland.ac.nz

The talk will report on recent progress on the computation of a finite approximation of a Chaitins Ω Number, the halting probability of a specific universal self-delimiting Turing machine. The main difficulty is the randomness of Ω, which implies its uncomputability. Relying of the fact that Ω is computably enumerable, an algorithm has been designed and implemented in Java to simulate the execution of programs which eventually stop on the universal Turing machine, so allowing the computation of an approximation of Ω. Various combinatorial and programming techniques have been employed to make the huge computation feasible.

History of Algebraic Computation

Garry J. Tee
University of Auckland
Auckland
E-mail: tee@aitken.scitec.auckland.ac.nz

In 1840 the mathematician J. J. Sylvester published a paper on algebra, in which he expressed his hope that his distinguished friend (Charles Babbage) would soon complete a machine for performing intricate algebraic operations.
In 1843, Babbage's disciple Augusta Ada published a brilliant study of what a computer could and could not be programmed to do. She emphasized that a computer would not be limited to arithmetic, but could perform algebraic operations.
In 1943, COLOSSUS 1 became the first computer to operate, cracking cyphers. It was designed to perform logical and algebraic operations, but it was soon programmed to perform decimal arithmetic.
In 1945, Alan Turing explained that the Automatic Calculating Engine which he had designed could perform general arithmetic and algebraic operations, such as "the enumeration of groups of order 720".
In 1946, Douglas Hartree emphasized that digital computers performed general symbolic operations, and could compute the 230 space groups.
By 1960, some algebraists were using computers for studying groups.
In March 2000, Eamonn O'Brien and his colleagues completed the enumeration (by computer) of the 49,910,529,484 finite groups of order at most 2000.

How Combinatorial Graph Theory Can Improve Software Security

Clark Thomborson
University of Auckland
Auckland
E-mail: cthombor@ec.auckland.ac.nz

Most software products, including “shareware” and “freeware”, are distributed under a license agreement which forbids their end-user from selling copies. We have recently invented a method for detecting that illegal copying has occurred. Essentially, our technique is to embed a “software fingerprint” in the data structures that are built when a licensed copy is run. Because each licensed copy has its own fingerprint, we can discover whose license is being violated if we discover multiple copies in use. We embed our fingerprints in the dynamic data structures of the program, so that a software pirate will be unable to remove it without engaging in a long and expensive process of reverse engineering. In graph-theoretic terms, our fingerprints may be chosen from any family of graphs that are of low out-degree and are easily enumerable. Ideally the graphs will have some easily-testable property that we would use for tamperproofing (so that a fingerprinted program is rendered inoperable by a simple and unobtrusive runtime test, if the fingerprint is partially or wholly removed). One suitable family of graphs is the planted plane cubic trees. There must be many others: we invite your comments and collaboration.