Calude – a person with many talents

Hermann Maurer

Professor at Graz University of Technology and Chair of Informatics Section of Academia Europaea

Presentation for Cris Calude
Auckland, February 21, 2012
Academia Europaea is a European, non-governmental association whose members are top-notch scientists and scholars, mainly from Europe, who want to promote learning, education and research.

AE provides independent advice to various bodies, coordinates national activities, and tries to improve public understanding of issues in science, humanity and bio-medicine.
Foundation Meeting Cambridge Sept. 1988

First Plenary Meeting 1989 with 627 members

For more see History of AE on www.ae-info.org/ae/Acad_Main
Today: Over 2200 members, including 47 European Nobel Laureates, 4 European Turing awardees, etc... and many other top researcher like Cris Calude

Headquarter on top floor of the Royal Institution, founded 1799 (picture 1837)

Second office: Knowledge Hub Wroclaw, Poland, opposite City Hall (Opened 2011, here with President Professor Lars Walleo)

Support office for server www.ae-info.org in Graz, Austria
Although I am exactly two months early:

Happy birthday, Cris!

My wish to you, Cris:
All the best for your further personal and professional life

My wish for me, Cris:
That we will meet more often in the future than we manged to do in the last few years

We will hear lots about scientific achievements in areas Cris has worked in in the next days … I want to show that Cris has also been involved in many other things using two examples:

(1) J.UCS
(2) You are wrong with probability only $10^{-50}$
J.UCS – Journal of Universal Computer Science
www.jucs.org

--- A peer-reviewed journal that appears at least 12 times yearly in electronic issues
--- It appears in printed form after a year is over

What is so special about J.UCS?

--- started in 1994 (!)
--- publishing and reading are free of charge, only printed versions have to be purchased at cost
--- 5 year impact factor 0.8
--- 700,000 downloads of full papers (after seeing title and abstract)
--- new functionalities
Last volumes have over 3.000 pages
Why I am telling you about J.UCS? Because it started with ideas of Cris, when I kept bugging him with the advantages of a new SW system „Hyperwave“ my group in Graz had developed.

To understand, briefly look at early attempts trying to offer activities via the internet.
Major activities to use internet beyond email started all in the same year!

First Gopher Server (Minnesota: Mark McCahill): **1991**
First WWW Server (CERN: B. Lee, R. Cailliau): **1991**
First Hyperwave Server (Graz: Kappe, Maurer): **1991**

Of the above, WWW was the most rudimentary one, originally only intended for one area (physics) and no interactivity, only dissemination.

Gopher had much better structure, more functionality.

Hyperwave was by far the most powerful… but also required most effort to install and learn how to use it.

In 1993, Gopher was most widespread all over the world (80,000 servers), WWW and Hyperwave had below 100 each.
Breakthrough of WWW due to the first graphic browser **Mosaic** in 1993, and because it was very easy to use.

Berners Lee leaves Europe for MIT and takes WWW with him. Some would say: He betrayed his friends at CERN (Robert Cailliau) and Europe.

Foundation of W3C: October 1994

WWW boom starts in 1994. Berners Lee enjoys being called the inventor of WWW (although it was a team of 4, he was just the alphabetically first one). He never acknowledges the main leader Robert Cailliau. With team of lawyers he minimizes role of Europe.

Gopher disappears. Hyperwave survives in Intranets and some applications. How come Hyperwave has survived?
Hyperwave as multi-window system, capable of handling 3D images and tracing moving objects.
Some Features of Hyperwave

--- Avoids broken links
--- Introduces structure in addition to links
--- Stores information about information
--- Introduces powerful access right system
--- Breaks the „dictatorship of the webmaster“
--- Introduces automatic version control
--- Supports multi-linguality
--- Provides flexible search
--- Allows annotations to everything
--- Provides basis for workflow and compliance
…
Some Features of Hyperwave

**Avoids broken links:**

Automatic link management possible using
--- bidirectional links
--- link info kept separate from document

Thus, if document pointed to is moved, all links pointing to it are adjusted; if document is removed, all links pointing to it are removed (made invisible)
Some Features of Hyperwave

Introduces structure in addition to links

Why? Because large WWW servers using links only create "huge spaghetti bowl" that is VERY difficult to maintain!

(Quote from: Robert Cailliau, co-developer of the original WWW, CERN)

Note: All parts on yellow background (like the one above) are actually taken from slides some 15 years old!)
Some Features of Hyperwave

In designing Hyperwave, some basic lessons learnt from programming and data bases were incorporated, but ignored by the non-computer science group at CERN.

Design Rules

- In programming
  - avoid GOTOS’s
  - use structures (procedures, block, …)
- In data management
  - avoid POINTER
  - use structures (records, classes, …)
- In HTML/Web
  - avoid LINKS
  - use structures (folders, cluster, …)
Some Features of Hyperwave
Introduces structure in addition to links

Advantages: Intuitive, easier to understand, many link maintenance difficulties just disappear. Feeling of directories!
Main Features of Hyperwave

Introduces powerful access right system
Breaks the „dictatorship of the webmaster“

Hierarchical user rights administration

Different views for different people
Main Features of Hyperwave

„Black“ and „red“ have entirely different views of same data universe due to different access rights for folders, documents and links (!)
Some Features of Hyperwave

Provides flexible search
Allows annotations to everything

Search as you would expect now, including search on metadata and links

Annotations to any object possible, and annotations to them, etc., etc. Today we would say: „A blog can be attached to any object“
Some of the things I told Cris tickled him. Finally he said, „If the system is as good as you claim, why don‘t we build an electronic journal on top of it? I have some ideas for it :“

Cris: „A contribution once published cannot be changed, but anyone can comment it. You said this is built into Hyperwave, and the original author is notified automatically?“ I: „Yes“

Cris: „We can build a new refereeing system involving all members of editorial board to speed up publication?“ I: „Yes“

Cris: „Using the bidirectional link structure, could Hyperwave not automatically support Links into the Future?“ I: „Yes“

So we started implementation of J.UCS end of 1993, went online 1994. And ever since, J.UCS has been running on a Hyperwave server: www.jucs.org
Unique features of J.UCS
## Content of Issue 14

**DOI:** 10.3217/jucs-017-14

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCWD: New Applications and Challenges</td>
<td>M.R.S. Borges, J.A. Pino, W. Shen</td>
<td>1384</td>
</tr>
<tr>
<td>Achieving Transparent and Real-time Collaboration in Co-AutoCAD Application</td>
<td>L. Gao, T. Lu</td>
<td>1387</td>
</tr>
<tr>
<td>Enabling Crowd Participation in Governmental Decision-making</td>
<td>A.C.B. Garcia, A.S. Vivaqueta, T.C. Tavares</td>
<td>1931</td>
</tr>
<tr>
<td>An Adaptive Genetic Algorithm and Application in a Luggage Design Center</td>
<td>C.-F. Tsai, W. Li, A. James</td>
<td>2029</td>
</tr>
<tr>
<td>Web Services Discovery in a Pay-As-You-Go Fashion</td>
<td>Y. Pan, Y. Tang, S. Li</td>
<td>2029</td>
</tr>
</tbody>
</table>
Government, Cryptography, and the Right to Privacy

Jenny Shearer (HyperMedia Unit, University of Auckland, New Zealand)

Peter Gutmann (Computer Science Department, University of Auckland, New Zealand)

Abstract: The notion of a right to privacy of citizens in their communications is discussed in the context of an international movement by governments towards regulation of cryptography, and consideration of key forfeiture systems in national cryptography use. The authors argue that the right to privacy in communications networks is an issue of major importance, assuring freedom of the individual in national and global communications. Regulation and control of cryptography use on the Internet by national governments may lead to an imbalance in the citizen/government power relationship, with sequelae including unprecedented surveillance of citizens, disruption of international commerce due to lack of powerful cryptography (and lack of standardisation), human rights abuses by less democratic or non-democratic governments, and limiting of the political potential of an Internet global political system.

Categories: E.3, K.4.2, K.5.2
Publication date: 1996-03-28

written by
Jenny Shearer ( )
Peter Gutmann ( pgut01@cs.auckland.ac.nz )

Links into the Future
This feature identifies the most relevant papers for the current paper from the J.UCS database. More information can be found here.

This article was cited in the following J.UCS papers:
1. Jenny Shearer,
   One Net One World Global Citizenship and the Internet
   in: Vol. 2 Issue 12 Page: 842 - 857
2. Hermann Maurer, Jenny Shearer,
   Is Democracy Possible in the Internet?
   in: Vol. 8 Issue 3 Page: 396 - 407

Experts associated with the topics of the paper
This feature identifies experts (members of the J.UCS editorial board and authors of articles published in J.UCS) for the topics of the current paper. More information can be found here. Click the name to access FacetedDBLP.

This paper belongs to the topics listed below. Related papers and assigned editors for the topics of the paper can be found by following any of the links:

E.3: DATA ENCRYPTION  K.4.2: Social Issues  K.5.2: Governmental Issues

Active research areas in J.UCS related to the topics of the paper and the top 10 ranked experts are shown below:

E.3: DATA ENCRYPTION:
   Yang-Sun Lee, Seokhie Hong, Jongsung Kim, Changhoon Lee, Mufutau Akinwande, Jeong+Ok Kwon, Ik+Rae Jeong, Oscar Perez, Yves Berviller, Camel Tanougast

K.4.2: Social Issues:
   Lucila+Maria Santarosa, Andreas+U. Schmidt, Ian+H. Witten, Zbigniew Hulicki, Anne Baumgärt, Benedikt Meuthrat, Claudia Müller, Wolf-Tilo Balke, Narayanan Kulathuramaiyer

K.5.2: Governmental Issues:
   Narayanan Kulathuramaiyer, Wolf-Tilo Balke, Gio Wiederhold

Get: External J.UCS Features
Government, Cryptography, and the Right to Privacy

Jenny Shearer (HyperMedia Unit, University of Auckland, New Zealand)

Peter Gutmann (Computer Science Department, University of Auckland, New Zealand)

Abstract: The notion of a right to privacy of citizens in their communications is discussed in the context of an international movement by governments towards regulation of cryptography, and consideration of key forfeiture systems in national cryptography use. The authors argue that the right to privacy in communications networks is an issue of major importance, assuring freedom of the individual in national and global communications. Regulation and control of cryptography use on the Internet by national governments may lead to an imbalance in the citizen/government power relationship, with sequelae including unprecedented surveillance of citizens, disruption of international commerce due to lack of powerful cryptography (and lack of standardisation), human rights abuses by less democratic or non-democratic governments, and limiting of the political potential of an Internet global political system.

Categories: E.3, K.4.2, K.5.2
Government, Cryptography, and the Right to Privacy
The notion of a right to privacy of citizens in their communications is discussed in the context of an international movement by governments towards regulation of cryptography, and consideration of key forfeiture systems in national cryptography...
In: Vol. 2 / Issue 3 page 113 - 146

Is Democracy Possible in the Internet?
Concepts of democracy have been developed and refined since Aristotle's time. However it is not until the new millennium that a unique set of circumstances, social, technical, and economic, have enabled a realistic plan of an e-democratic world to...
In: Vol. 8 / Issue 3 page 396 - 407

Levels of Anonymity
In this paper we make a first attempt at systematically investigating levels of anonymity required in networked computer systems: we feel it is often overlooked that beyond such obvious cases as identified by means of a password or anonymous use ...
In: Vol. 1 / Issue 1 page 35 - 47

Will Internet Ever Be Secure?
The users of the Internet in general have not developed a perception of where what security is crucial and beneficial for their applications. At present the average user is provided very few information independent of what is transported over the...
In: Vol. 7 / Issue 5 page 447 - 456

New Advances in Reconfigurable Computing and its Applications
In: Vol. 13 / Issue 3 page 345 - 348
The Future of PCs and Implications on Society

Hermann Maurer (Graz University of Technology, Austria)

Ron Oliver (Edith Cowan University, Australia)

Abstract: In this paper we argue that in about ten years time PCs as we now know them, will no longer exist. Their functionality will be totally integrated into mobile telephony devices, or putting it differently, in ten years time mobile phones will incorporate all functions one would expect from a powerful PC. These new devices, let us call them eAssistants, will be with us all the time and will change our lives enormously. In this paper we take a first look at both the technological and applied aspects of this prediction.

Keywords: display technology, future computers, societal implications, wearable PC

Categories: H.4, J.0, K.4, K.8
Refereeing system

The abstract of each paper is sent to all members of the Editorial Board (preferably in the area of the paper, to avoid overload)

Editorial Board: ~ 350 members, qualifications well defined
(Basically: Tenured associate professor or above, And solid publication record in good journals)
Editors-in-Chief

- Muhammad Tanvir Afzal
- Wolf-Tilo Balke
- Michael Granitzer
- Christian Gütl (Managing Editor)
- Matthias Jarke
- Narayanan Kulathuramaiyer
- Hermann Maurer
- Peter Serdyukov

Alphabetical List of Editors

A

- Abraham A.
- Afzal M.
- Aguilar-Ruiz J.
- Aiello L. C.
- Akritas A.
- Albert J.
- Alcalá R.
- Alimi A.
- Allen M.
- Al-Rabadi A.
- Antoniou I.
- Antunes P.
- Arroyo S.
- Arslanov M. M.
- Augusto J. C.
- Azuma J.

B

- Baier C.
- Balke W.-T.
- Banach R.
- Barker P.
- Baumgartner P.
- Benest I.
- Bergel A.
- Bergstra J.
- Bernardini F.
- Bischof H.
- Bode A.
- Boman D.
- Börger E.
- Borghoff U. M.
- Bratko I.
- Brattka V.
- Brauer W.
- Brenner E.
- Bridges D. S.
- Broy M.
- Brusilovsky P.
- Buchberger B.
- Burgos D.
- Burkard R.
- Butcher J.

C

- Cabrerozo F. J.
- Caelli W.
- Calude C.
- Camponogara E.
- Cantoni L.
- Carballo J.-A.
- Carlson P.
- Carmichael P.
- Carvalho L.
- Case J.
- Christodoulakis S.
- Chua A.
- Clayton P.
- Cools R.
- Corchuelo R.
- Cortesi A.
- Cotta C.
- Cremers A.
- Curran K.
Various geographical „mash-ups“ are available in JUCS:

More specifically:

--- see where editors in some area are located (important for both administrators and submitters of papers)
--- see where papers come from (in particular year and scientific area, for both administrators and submitters)
--- see where referees for a particular paper come from (for editor in chief only, to avoid cronyism)
Please help us to update the profile of the selected person.
With the refereeing system of J.UCS a problem remains: What if author asks three friends to review paper favorably?

We need a function $f$ that, given two persons $A$ and $B$, gives $f(A, B) = g$ with $0 \leq g \leq 1$ as a “guessed” probability that $A$ and $B$ are friends.

Interesting problem! Algorithm uses: co-location, past co-location, co-authorship, joint committee work, social networks, etc. etc. to arrive at educated guess. If $g > 0.75$ we choose different referee.

Also interesting but still more difficult: estimate if $A$ and $B$ are enemies! (E.g. co-located but never on same committee, sentiment analysis of reviews of $A$ of papers of $B$ gives negative score, etc.)
Although there is more to J.UCS than this, I guess it is enough for today. Let me give some final facts.

J.UCS is going strong...papers are downloaded 3,000 times on average!

J.UCS is now run by a consortium of 9 organisations. I stepped down as Managing Editor-in-Chief January 2012 in favour of Christian Guetl, from my institute in Graz.

J.UCS has now over 300 members of the editorial board, but could need another 200. If interested, tenured associate professor or above and with good publication record, please do join!

A completely new submission system will be opened before mid-year.
I said at the beginning:

We will hear lots about scientific achievements in areas Cris has worked in in the next days … I want to show that Cris has also been involved in many other things using two examples:

(1) J.UCS
(2) You are wrong with probability only 10⁻⁵₀

So, what does the mysterious point (2) mean?
Paul Gillard (Memorial University, New Foundland) and I wanted to write a program that would allow students to practice differentiation of functions.

Basic idea is clear. We would generate functions of a complexity depending on what they had learnt so far.

Given such an $f(x)$ students would compute derivative $g(x)$ and computer would also compute derivative $h(x)$.

It remained to check if $g(x) \equiv h(x)$, i.e., the identity of $g(x)$ and $h(x)$.

However, this has been known to be undecidable since 1968!
The undecidability of this problem (to find out if two functions $g$ and $h$ are identical) has held back this and many other efforts for decades!

Paul and I decided to examine if $g(x) = h(x)$ at 100 random points. And if so, we would grade student answers as correct... risking a (very) small percentage of error:

Of course it can be that $g(x) = h(x)$ at 100 hundred random values for $x$, but still for some $y$ $g(y) \neq h(y)$.

Paul and I thought it highly unlikely, but could not put a probability to it. It was Cris who showed: Under mild assumptions, the likelihood that $g$ and $h$ are not identical if they agree on 100 random values, is less than $10^{-50}$.
Since then, I sleep well. I know that for all practical purposes we have solved an unsolvable problem.

Thanks, Cris for helping us with this result. Thanks for believing we can do something nice with J.UCS, and for helping to find the first 150 editors. And, most of all, thanks for your friendship.

Again, best wishes to Cris, and thanks to all who made my visit here possible!

hmaurer@iicm.edu   www.iicm.edu/maurer