Michael Oser Rabin

Automata, Logic and Randomness in Computation

Luca Aceto
ICE-TCS, School of Computer Science, Reykjavik University

Pearls of Computation, 6 November 2015

"One plus one equals zero. We have to get used to this fact of life." (Rabin in a course session dated 30/10/1997)

Thanks to Pino Persiano for sharing some anecdotes with me.

Michael Rabin's accolades

Michael O. Rabin

Selected awards and honours

- Turing Award (1976)
- Harvey Prize (1980)
- Israel Prize for Computer Science (1995)
- Paris Kanellakis Award (2003)
- Emet Prize for Computer Science (2004)
- Tel Aviv University Dan David Prize (2010)
- Dijkstra Prize (2015)

"1970 in computer science is not classical; it's sort of ancient. Classical is 1990." (Rabin in a course session dated 17/11/1998)

Michael Rabin's work: through the prize citations

ACM Turing Award 1976 (joint with Dana Scott)

For their joint paper "Finite Automata and Their Decision Problems," which introduced the idea of nondeterministic machines, which has proved to be an enormously valuable concept.

ACM Paris Kanellakis Award 2003 (joint with Gary Miller, Robert Solovay, and Volker Strassen)

For "their contributions to realizing the practical uses of cryptography and for demonstrating the power of algorithms that make random choices", through work which "led to two probabilistic primality tests, known as the Solovay-Strassen test and the Miller-Rabin test".

ACM/EATCS Dijkstra Prize 2015 (joint with Michael Ben-Or)

For papers that started the field of fault-tolerant randomized distributed algorithms.

Michael Rabin: Early years

- Born in 1931 in Breslau, Germany (today Wroclaw, in Poland). In 1935, he emigrated with his family to Mandate Palestine.
- “Good Will Hunting” moment at age 11.
- At high school, Rabin studied with Elisha Netanyahu (uncle of Benjamin Netanyahu).
- Drafted into the army during the 1948 Arab-Israeli War.
- Abraham Fraenkel intervened with the army command, and Rabin was discharged to study at the university in 1949.
- Received an M.Sc. from Hebrew University of Jerusalem in 1953. His thesis solved an open problem due to Emmy Noether.

Princeton and finite automata

- Ph.D. from Princeton University in 1956 (supervisor: Alonzo Church, thesis on unsolvability of group theoretical problems).
- During his PhD studies he meets Einstein, Gödel and von Neumann amongst others.
- Dana Scott and Rabin were invited to spend the summer of 1957 at IBM Research. Result: Finite Automata and Their Decision Problems, IBM J. Res. Develop. 3:114–125, 1959.

Princeton and finite automata

- Ph.D. from Princeton University in 1956 (supervisor: Alonzo Church, thesis on unsolvability of group theoretical problems).
- During his PhD studies he meets Einstein, Gödel and von Neumann amongst others.
- Dana Scott and Rabin were invited to spend the summer of 1957 at IBM Research. Result:
  Finite Automata and Their Decision Problems, IBM J. Res. Develop. 3:114–125, 1959.
  - Introduces nondeterminism, DFAs and NFAs as we know them.
  - Subset construction.
  - Reproves Kleene's theorem: DFA $=$ Regular Expressions.
  - Studies multi-tape, two-way and linear-bounded automata and their decision problems.

Aside: From models of neural activity to grep/Perl

McCulloch and Pitts (1943) ⇝ Kleene (1956) ⇝ Rabin and Scott (1959) ⇝

WHENEVER I LEARN A NEW SKILL I CONCOCT ELABORATE FANTASY SCENARIOS WHERE IT LETS ME SAVE THE DAY.
OH NO! THE KILLER MUST HAVE FOLLOWED HER ON VACATION!
BUT TO FIND THEM WE'D HAVE TO SEARCH THROUGH 200 MB OF EMAILS LOOKING FOR SOMETHING FORMATTED LIKE AN ADDRESS!
IT'S HOPELESS!
EVERYBODY STAND BACK.
I KNOW REGULAR EXPRESSIONS.
PERL!
TAP TAP

Summer 1958 at IBM Research: The origins of complexity theory

John McCarthy's puzzle: spies, guards, and passwords

Spies must present, upon returning from enemy territory, some kind of secret password to avoid being shot by their own border guards. But the guards cannot be trusted to keep a secret. So, if you give them the password, the enemy may learn the password and safely send over his own spies.

Summer 1958 at IBM Research: The origins of complexity theory

John McCarthy's puzzle: spies, guards, and passwords

Spies must present, upon returning from enemy territory, some kind of secret password to avoid being shot by their own border guards. But the guards cannot be trusted to keep a secret. So, if you give them the password, the enemy may learn the password and safely send over his own spies.

Rabin's solution raised the following questions:

- How does one define the difficulty of computing something?
- How does one prove that something is difficult to compute?

Paper: Degree of Difficulty of Computing a Function and Hierarchy of Recursive Sets, 1960

Summer 1958 at IBM Research: The origins of complexity theory

John McCarthy's puzzle: spies, guards, and passwords

Spies must present, upon returning from enemy territory, some kind of secret password to avoid being shot by their own border guards. But the guards cannot be trusted to keep a secret. So, if you give them the password, the enemy may learn the password and safely send over his own spies.

Rabin's solution raised the following questions:

- How does one define the difficulty of computing something?
- How does one prove that something is difficult to compute?

Paper: Degree of Difficulty of Computing a Function and Hierarchy of Recursive Sets, 1960

> *"You should never re-use a one-time pad. It's like toilet paper; if you re-use it, things get messy."*

Jerusalem and Bell Labs: Enter randomization

Rabin works on logic, mainly model theory, and on the foundations of computer science.

Associate professor and the head of the Institute of Mathematics at 29; full professor by 33.

> *"There was absolutely no appreciation of the work on the issues of computing. Mathematicians did not recognize the emerging new field."*

In 1960, Rabin was invited by Edward F. Moore to work at Bell Labs, where he introduced probabilistic automata (paper in Information and Control, 1963).

Jerusalem and Bell Labs: Enter randomization

Rabin works on logic, mainly model theory, and on the foundations of computer science.

Associate professor and the head of the Institute of Mathematics at 29; full professor by 33.

> *"There was absolutely no appreciation of the work on the issues of computing. Mathematicians did not recognize the emerging new field."*

In 1960, Rabin was invited by Edward F. Moore to work at Bell Labs, where he introduced probabilistic automata (paper in Information and Control, 1963).

> *"I am going to show that in one round the probability of not reaching agreement is less or equal to 2. . . . Yeah, we're establishing new ground in probability theory."*
> *(Rabin during a class held on 17/12/1998)*

Trading certainty for speed: Primality testing

- Gary Miller at MIT had a deterministic, polynomial-time test for primality based on the extended Riemann hypothesis.
- Rabin turned this test into an efficient randomized algorithm (paper in Journal of Number Theory, 1980).

Trading certainty for speed: Primality testing

- Gary Miller at MIT had a deterministic, polynomial-time test for primality based on the extended Riemann hypothesis.
- Rabin turned this test into an efficient randomized algorithm (paper in Journal of Number Theory, 1980).

Mathematicians did not like to trade certainty for speed

A hostile referee wrote that “if he had attached a pen to his dog’s tail he would have proved Riemann’s hypothesis with positive probability”!

In his submission, Rabin wrote: “These numbers are of the order of 10^{123}!” The same reviewer interpreted the exclamation mark as “factorial” and refuted the “claim”.

Trading certainty for speed: Primality testing

- Gary Miller at MIT had a deterministic, polynomial-time test for primality based on the extended Riemann hypothesis.
- Rabin turned this test into an efficient randomized algorithm (paper in Journal of Number Theory, 1980).

Mathematicians did not like to trade certainty for speed

A hostile referee wrote that "if he had attached a pen to his dog's tail he would have proved Riemann's hypothesis with positive probability"!

In his submission, Rabin wrote: "These numbers are of the order of 10^{123}!" The same reviewer interpreted the exclamation mark as "factorial" and refuted the "claim".

"The probability of an error is smaller than the probability that none of us is awake and we are all dreaming this." (Rabin in a class held on 16/10/1997)

Randomized algorithms at work

> *"This is revolutionary, and it's going to become very important." (Joseph Traub on hearing Rabin's talk at CMU on randomized primality testing.)*

Rabin applies randomization

- to number theoretical algorithms,
- distributed computing (using a random shared bit for solving Byzantine Agreement),
- cryptography, piracy prevention and zero-knowledge, and
- preventing collusion in second-price (Vickrey) auctions (joint CACM paper from 2014 with Silvio Micali).

Randomized algorithms at work

> *"This is revolutionary, and it's going to become very important." (Joseph Traub on hearing Rabin's talk at CMU on randomized primality testing.)*

Rabin applies randomization

- to number theoretical algorithms,
- distributed computing (using a random shared bit for solving Byzantine Agreement),
- cryptography, piracy prevention and zero-knowledge, and
- preventing collusion in second-price (Vickrey) auctions (joint CACM paper from 2014 with Silvio Micali).

"I must admit that after many years of work in this area, the efficacy of randomness for so many algorithmic problems is absolutely mysterious to me. It is efficient, it works; but why and how is absolutely mysterious."

Other highlights in Rabin's work

- The Rabin-Karp algorithm for string searching. A practical application of the algorithm is detecting plagiarism.
- Oblivious transfer protocols (1981): "a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred."
- Rabin fingerprint: "a method for implementing fingerprints using polynomials over a finite field."

Other highlights in Rabin's work

- The Rabin-Karp algorithm for string searching. A practical application of the algorithm is detecting plagiarism.
- Oblivious transfer protocols (1981): "a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred."
- Rabin fingerprint: "a method for implementing fingerprints using polynomials over a finite field."

"You should be in a situation where you can just be woken in the middle of the night and be asked about finite fields and be able to recite everything out of your head. That's real knowledge." (Rabin in a class held on 22/10/1998).

Back in time: Decidability of logical theories

A fundamental algorithmic problem

Consider your favourite logic $\mathcal{L}$. Is there an algorithm to determine whether formulae in $\mathcal{L}$ are valid over some class of structures?

Back in time: Decidability of logical theories

A fundamental algorithmic problem

Consider your favourite logic $\mathcal{L}$. Is there an algorithm to determine whether formulae in $\mathcal{L}$ are valid over some class of structures?

- No for the first-order theory of $\mathbb{N}$ with $+$ and $\times$. (Church and Turing 1936)

$$\forall x \exists r \exists s \exists t \ (t \neq 0 \wedge tx = r^3 + s^3) \text{ is true}$$

- Yes for the first-order theory of $\mathbb{R}$ with $+$ and $\times$. (Tarski)
- Yes for the first-order theory of $\mathbb{N}$ with $+$. (Presburger in his master's thesis)

$$\exists z \ (x + z = y)$$

Back in time: Decidability of logical theories

A fundamental algorithmic problem

Consider your favourite logic $\mathcal{L}$. Is there an algorithm to determine whether formulae in $\mathcal{L}$ are valid over some class of structures?

- No for the first-order theory of $\mathbb{N}$ with $+$ and $\times$. (Church and Turing 1936)

$$\forall x \exists r \exists s \exists t \ (t \neq 0 \wedge tx = r^3 + s^3) \text{ is true}$$

- Yes for the first-order theory of $\mathbb{R}$ with $+$ and $\times$. (Tarski)
- Yes for the first-order theory of $\mathbb{N}$ with $+$. (Presburger in his master's thesis)

$$\exists z \ (x + z = y)$$

Monadic second-order logic allows quantifiers that range over sets of elements.

$$\exists X. \ [0 \in X \wedge (\forall n. \ n \in X \rightarrow (n + 2 \in X \wedge n + 1 \notin X))]$$

Automata and logic: A match made in heaven

Exhibit 1: Richard Büchi and Calvin Elgot used finite automata to show the decidability of Presburger Arithmetic. (Huge complexity, though! Lower bound: $2^{2^{cn}}$ for some $c > 0$ by Fischer and Rabin.)

Automata and logic: A match made in heaven

Exhibit 1: Richard Büchi and Calvin Elgot used finite automata to show the decidability of Presburger Arithmetic. (Huge complexity, though! Lower bound: $2^{2^{cn}}$ for some $c > 0$ by Fischer and Rabin.)

Exhibit 2: Richard Büchi showed the decidability of monadic second-order theory of one successor function using finite automata on infinite strings (Büchi Automata) $\rightsquigarrow$ automata-theoretic approaches to model checking for LTL, synthesis of controllers. . . .

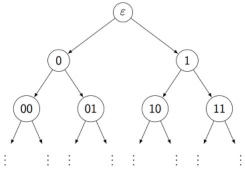
Automata and logic: A match made in heaven

Exhibit 1: Richard Büchi and Calvin Elgot used finite automata to show the decidability of Presburger Arithmetic. (Huge complexity, though! Lower bound: $2^{2^{cn}}$ for some $c > 0$ by Fischer and Rabin.)

Exhibit 2: Richard Büchi showed the decidability of monadic second-order theory of one successor function using finite automata on infinite strings (Büchi Automata) $\rightsquigarrow$ automata-theoretic approaches to model checking for LTL, synthesis of controllers. . . .

Exhibit 3: Rabin showed the decidability of monadic second-order theory of two successor functions using finite automata on infinite trees (Tree Automata) $\rightsquigarrow$ automata-theoretic approaches to model checking for branching-time logics, synthesis of controllers. . . .

What does Rabin's Tree Theorem mean for computer scientists?



Rabin's Tree Theorem (1969)

The monadic second order theory of the infinite binary tree is decidable.
(Rabin says: "I consider this to be the most difficult research I have ever done.")

Wolfgang Thomas calls it a "fundamental decidability result that appears in hundreds of applications in theoretical computer science".

"One of those moments in math which leave us mere mortals with our mouths open in astonishment." (Rabin in a class held in Fall 1997, on what he was about to do)

Rabin on research and teaching

"There is this misconception that there is a conflict and maybe even a contradiction between great teaching and being able to do great science. I think this is completely incorrect, and that wonderful teaching . . . flows from a deep understanding of the subject matter."

- Select the "right topics".
- Really understand the essence, the main motifs, of each particular topic to present, and to show it to the class in a way that the class gets these essential ideas.

Rabin on research and teaching

“There is this misconception that there is a conflict and maybe even a contradiction between great teaching and being able to do great science. I think this is completely incorrect, and that wonderful teaching . . . flows from a deep understanding of the subject matter.”

- Select the “right topics”.
- Really understand the essence, the main motifs, of each particular topic to present, and to show it to the class in a way that the class gets these essential ideas.

“. . . b_1 . . . b_{12}. That’s not a vitamin; it’s the name I give to this coefficient, so don’t eat it.” (Rabin in a class held on 23/09/1997)

Conclusion

Richard Lipton in "Rabin Flips a Coin"

Michael Rabin is one of the greatest theoreticians in the world. . . . What is so impressive about Rabin's work is the unique combination of depth and breadth; the unique combination of solving hard open problems and the creation of entire new fields. I can think of few who have done anything close to this.

Advice from Rabin to the students in the audience

As the Lehman Brothers say, "Trust me." What I'm trying to say is that your future is not in financial engineering but in computer science. (Rabin in CS 226r, fall 2008)

Conclusion

Richard Lipton in "Rabin Flips a Coin"

Michael Rabin is one of the greatest theoreticians in the world. . . . What is so impressive about Rabin's work is the unique combination of depth and breadth; the unique combination of solving hard open problems and the creation of entire new fields. I can think of few who have done anything close to this.

Advice from Rabin to the students in the audience

As the Lehman Brothers say, "Trust me." What I'm trying to say is that your future is not in financial engineering but in computer science. (Rabin in CS 226r, fall 2008)

"Zero plus zero is still zero, even in this advanced class."
(Rabin in Spring 2002)