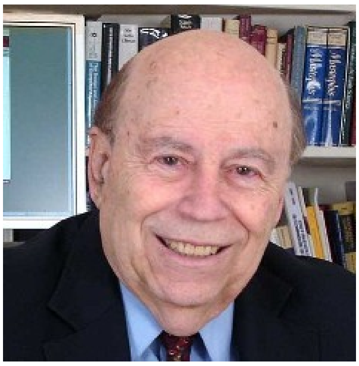
On Michael O. Rabin

Abhisekh Sankaran
Research Scholar, IIT Bombay



The 1976 Turing award citation read [1]:

For their joint paper on "Finite Automata and Their Decision Problems" which introduced the idea of non-deterministic machines, which has proved to be an enormously valuable concept. Their (Scott & Rabin) classic paper has been a continuous source of inspiration for subsequent work in this field.

And he was just 28 when he wrote this paper jointly with Dana Scott! In the times to come, the world was to see continuously deep contributions from the man on a wide range of areas including automata theory, logic, computational complexity, randomized algorithms, parallel and distributed algorithms, cryptography and computer security – nay, some of these areas being founded by him.

Meet our man, the versatile and prolific genius, Michael O. Rabin.

Early life and school days

Michael Rabin was born in Breslau, Germany (known as Wroclaw, Poland, since the end of the Second World War), on September 1, 1931. His father was from Russia and was a Rabbi (a teacher of the Torah, the Jewish sacred text), as were many of his forefathers. Recognizing it was unsafe to stay in Germany at this time, the family moved to Palestine in 1935. Rabin's father wanted him to attend a religious school and become a Rabbi continuing the family tradition, but against his father's wishes, Rabin went to the Reali School, a school that specialized in the sciences. Rabin was initially interested in microbiology, though his interests soon changed to mathematics when at the age of 11, he solved a geometry problem which two ninth-graders condescendingly posed to him. He was so impressed that problems of the real world could be solved through pure thought that he decided to study mathematics.

As he grew up, in the tenth grade, he came in contact with the mathematician Elisha Netanyahu (the uncle of Benjamin Netanyahu, the current Prime Minister of Israel) who was at the time a high school teacher. Elisha conducted, once a week, a so-called "mathematical circle," where he taught a selected group of students number theory, combinatorics, and advanced algebra. He lent Rabin books on advanced mathematics so that at the age of 15, Rabin had already begun reading Hardy and Wright's "An Introduction to the Theory of Numbers", the first volume in German of Landau's "Zahlentheorie", G. H. Hardy's "Pure Mathematics", two volumes of Knopp's "Functions of a Complex Variable" and A. Speiser's "Gruppentheorie" to name a few.

Master's thesis: The first significant work

In 1948, the Arab-Israel war broke out and like everybody else in school, Rabin was drafted into the army. But he continued to study mathematics on his own while in the army. In September 1949, Rabin got in touch with Abraham Fraenkel, an eminent logician and set theorist and a professor of mathematics in Jerusalem, whose book on set theory Rabin had studied. Fraenkel realized Rabin's talents and intervened with the army authorities to discharge Rabin from the army to pursue studies at the university.

Rabin joined the Hebrew University of Jerusalem where he studied mathematics and took keen interest in algebra. In 1952, he wrote a master's thesis under the direction of the algebraist Jacob Levitski who was a student of the famous woman mathematician Emmy Noether. Rabin's thesis was on the algebra of commutative rings and provided a solution to an open problem due to Emmy Noether, by giving a necessary and sufficient condition on a commutative ring for having the property that every ideal is a finite intersection of primary ideals. That became his first paper too - it appeared in the *Comptes Rendus* (the proceedings) of the French Academy of Sciences. He graduated with an M.Sc. degree in algebra in 1953.

Fundamental Works in the United States at Princeton and IBM Research

During his M.Sc. studies, Rabin became interested in computers after reading of the work of Alan Turing in *Metamathematics* by S. C. Kleene. At this time Israel had no computers so to pursue his interest, Rabin had to move to the United States. His initial studies were at the State University of Pennsylvania but the excellent work in his Master's thesis earned him an admission to a Ph.D. programme in logic at Princeton University under Alonzo Church (At the time, only 13 Ph.D. students were admitted every year to the Mathematics Department). Rabin's Ph.D. thesis was on the computational (recursive) unsolvability of group theoretical problems, thus combining his natural interests in algebra and computability.

In 1957, IBM decided to go into research in a big way. They sent people to recruit promising students from top universities and top mathematics departments. And so while writing his thesis, Rabin was offered a summer job with IBM research at Lamb Estate in Westchester County along with other promising mathematicians and scientists. It is here that Rabin met Dana S. Scott. Given free reign to research anything they wanted, the two of them, building upon an earlier work of Walter Pitts and Warren McCulloch, wrote the paper “Finite Automata and Their Decision Problems” in which they proposed the concept of deterministic finite state machines and then generalized this concept to non-deterministic finite state machines. Using this concept, they were able to reprove Kleene's result that finite state machines accept exactly the regular languages and also showed that non-deterministic machines had the same power as their deterministic counterparts. It was however only in 1959 that their paper got published. Little did the authors anticipate that the concept of non-determinism would have a huge impact on computer science in the times to come and indeed fetch them the Turing award too. Rabin frankly admits “We really did not have any deep philosophical reason for considering nondeterminism, even though as we now know nondeterminism is at the center of the P = NP question, a problem of immense practical and theoretical importance. For us, it was just one of the variants” [4].

After completing his thesis, Rabin returned to IBM Research for another summer job and worked with John McCarthy. The latter posed to him the following puzzle about 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 and may leak it to the enemy. How can the spies safely get back home? As a response to this, Rabin proposed the idea of a one-way function – a function easy to compute in one direction but not the other and as a concrete example suggested the “middle square” function John von Neumann had suggested for generating pseudo-random numbers. To define precisely the notion of difficulty of computing, Rabin wrote an article called “Degree of Difficulty of Computing a Function and Hierarchy of Recursive Sets.” which really laid the foundations for the field of computational complexity. Rabin believes that this paper, apart from his paper with Scott, was another important reason for his getting the Turing Award. Quoting him, “The ACM announcement of the Turing Award [...] also suggested that I was the first person to study what is now called complexity of computations.” [4].

Striking a new path yet again: Randomized Algorithms

Rabin returned to Jerusalem from the US and divided his research between working on logic, mainly model theory, and working on the foundations of computer science. He became an Associate Professor and the head of the Institute of Mathematics at 29 and a Full Professor by 33, but completely on the merit of his work in logic and in algebra. Reminescing about those days, he says “There was absolutely no appreciation of the work on the issues of computing. Mathematicians did not recognize the emerging new field” [4].

In 1960, Rabin was invited by E.F. Moore to work at Bell Labs, where he introduced the construct of probabilistic automata - automata employing coin tosses to decide which state transitions to take. He showed examples of regular languages that required a very large number of states, but for which there are probabilistic automata with exponentially lesser number of states which accept the same language with a small error. The paper got published in 1963 in *Information and Control*.

In 1975, Rabin came to MIT as a visiting professor. Gary Miller, a professor at MIT, had a polynomial time test for primality based on the extended Riemann hypothesis, though the latter was an unproven assumption (and is still so). With the idea of using probability and allowing the possibility of error, Rabin took his test and made it into what's now called a randomized algorithm. This test, called the Rabin-Miller test, is the most efficient test for primality even today if a small degree of error is permitted.

Rabin realized the enormous practical uility of randomized algorithms and set for himself the task of finding more applications of randomization. And indeed he succeeded by coming up with randomized algorithms for numerous problems: number theoretic problems like expressing an integer as the sum of four squares, asynchronous fault-tolerant parallel computations and the Byzantine Agreement problem in distributed computing to name a few. These works have had great implications for the areas of secure communication and distributed computing over the Internet.

Rabin's Tree Theorem – one of the deepest results in decidability

Buchi, in a 1960 paper, had generalized finite automata on finite strings to finite automata on infinite strings in a brilliant piece of work and had shown the monadic second-order theory of one successor function to be decidable. In 1966, when Rabin came as visitor to IBM Research at Yorktown Heights, he developed a theory of finite automata on infinite binary trees (called *tree automata*) and proved the decidability of the monadic second order theory of *n*-successors. This breakthrough result has had far reaching implications, for instance the decidability of many other logical theories like modal and temporal logics, amongst a host of other applications. This theorem is widely regarded as one of the deepest decidability results in logic and in Rabin's own words "I consider this to be the most difficult research I have ever done" [4].

Other independent works

In 1979, Rabin invented the *Rabin cryptosystem*, the first asymmetric cryptosystem whose security was proved equivalent to the intractability of integer factorization. In 1981, Rabin reinvented a weak variant of the technique of *oblivious transfer* invented by Wiesner under the name of multiplexing, allowing a sender to transmit a message to a receiver where the receiver has some probability between 0 and 1 of learning the message, with the sender being unaware whether the receiver was able to do so. In 1987, Rabin, together with Richard Karp, created one of the most well-known efficient string search algorithms – the *Rabin-Karp string search algorithm* - that uses hashing to find any one of a set of pattern strings in a text.

Recent research: Applying randomization to cryptography

In recent years Rabin has created, with Y. Aumann and Y. Z. Ding, *Hyper-Encryption*, the first ever encryption scheme provably providing everlasting secrecy against a computationally unbounded adversary. This scheme has been implemented at Harvard and MIT via a novel limited access model. He has invented and implemented, with W. Yang and H. Rao, a micro chip for physical generation of a strong stream of truly random bits. He has invented with S. Micali and J. Kilian, *Zero Knowledge Proofs (ZKP)*, a new primitive for privacy and security protocols and has innovated practical *ZKP*s applicable to auctions and other financial processes. More recently, he has implemented, with Chris Thorpe and Rocco Servedio, an entirely new approach to *ZKP*s, which is "computationally very efficient, does not use heavy-handed and computationally expensive encryption, and achieves everything very efficiently by use of just computationally efficient hash functions" [4]. All of these works are bound to have a tremendous impact in a future in which more and more sensitive information is transmitted on the internet and stored in databases, making secrecy, privacy and protection ever more crucial to society.

Awards and Honours

Apart from the Turing award in 1976, Rabin was awarded the C. Weizmann Prize for Exact Sciences (1960), Rothschild Prize in Mathematics (1974), Israel Prize for Exact Sciences (1995), ACM Kanellaikis Theory and Practice Award (2004), EMET Prize for Computer Science (2004) and recently the Dan David Prize (2010), to name a few. He has honarary doctorates from the University of Bordeaux I (1996), Haifa University (1996), New York University (1998), Ben Gurion University (2000) and Wroclaw University (2007).

Appointments held

They are too many but to mention a few, he was the Albert Einstein Professor of Mathematics at the Hebrew University from 1980 to 1999 serving as its Rector (Academic Head) from 1972 to 1975 and the Thomas J. Watson Sr. Professor of Computer Science at Harvard University from 1983 to the present. He has been a Visiting Professor at various times at Yale University, the Weizmann Institute, the Israel Technion, UC Berkeley, MIT, the Courant Institute of Mathematics, Caltech, ETH Zurich, Columbia University, and Kings College London. He was Saville Fellow at Merton College, Oxford, Steward Fellow at Gonville and Caius College, Cambridge and Fairchild Scholar at California Institute of Technology. From 1982 to 1994 he served on the IBM Science Advisory Committee. In Spring 2009 he was a Visiting Researcher at Google.

Rabin was elected as member or foreign honorary member to academies including: the US National Academy of Sciences, the French Academy of Sciences, the American Academy of Arts and Sciences, the American Philosophical Society, the Israel Academy of Sciences and Humanities, and Foreign Member Royal Society. He has been an editorial board memnber of the Journal of Computer and Systems Sciences, the Journal of Combinatorial Theory and the Journal of Algorithms.

Quotable quotes: From the man himself

“Randomized algorithms, in their pure form, must use a physical source of randomness. So it is cooperation between us as computer scientists and nature as a source of randomness. This is really quite unique and touches on deep questions in physics and philosophy.”

“The study of algorithms will always remain centrally important. Powerful algorithms are enabling tools for every computer innovation and application.”

“Great teaching and great science really flow together and are not mutually contradictory or exclusive of each other.”

Conclusion

It is an incredible feat for a single man to have done such phenomonal amount of work in such a wide variety of areas. Indeed Richard Lipton [5] puts it best when he says “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”. Hats off, O Rabin!

References

[1] http://en.wikipedia.org/wiki/Turing_Award
[2] http://en.wikipedia.org/wiki/Michael_O._Rabin
[3] http://www.bookrags.com/biography/michael-o-rabin-wcs/

[4] Shasha, D., *An interview with Michael Rabin*, Communications of the ACM, Feb 2010, Vol. 53, No. 2, pp. 37 – 42.

[5] http://rjlipton.wordpress.com/2009/03/01/rabin-flips-a-coin/

[6] http://www.seas.harvard.edu/directory/rabin/at_download/facultyCv