

Interview with Jeffrey Shallit

Toufik Mansour



Photo by Joe Petrik

Jeffrey Shallit earned a bachelor of arts in mathematics from Princeton University in 1979. He received a Ph.D. at the University of California, Berkeley in 1983, under the supervision of David Goldschmidt (de jure) and Manuel Blum (de facto). Currently, he is a professor of mathematics in the School of Computer Science at the University of Waterloo. Professor Shallit has given lectures and talks at many conferences and workshops. Here we list some of them: Numeration 2019, Erwin Schrödinger Institute, in Austria, 2019; Highlights of Logic, Games, and Automata, in Germany, 2018; LMS Keynote Address in Discrete Mathematics, in England, 2014; Fields Workshop on Challenges in Combinatorics on Words, in 2013; Highlights of AutomathA, in Austria, 2010; Distinguished Lecture Series, University of Victoria, 2002. Professor Shallit's research

interests include combinatorics on words, formal languages and automata theory (especially connections with number theory), algorithmic number theory (primality testing, factoring, etc.), and the ethical use of computers. For his contributions, Professor Shallit, in 2008, was named a Distinguished Scientist by the Association for Computing Machinery. In 2020, Professor Shallit was elected as a Foreign Member of the Finnish Academy of Science and Letters. He has been the editor-in-chief of the Journal of Integer Sequences since 2002.

Mansour: Professor Shallit, first of all, we would like to thank you for accepting this interview. Would you tell us broadly what combinatorics is?

Shallit: Thanks for asking me!

Combinatorics is a pretty diverse area and hard to characterize! Igor Pak has a nice web page¹ where he has catalogued definitions from dozens of sources. Of course, combinatorics is about counting, but it is a lot more than just that.

Mansour: What do you think about the development of the relations between combinatorics and the rest of mathematics?

Shallit: Like many parts of mathematics, combinatorics has become more and more sophisticated, using tools from other areas.

These days, a good combinatorialist often needs to know complex analysis, number theory, ergodic theory, computational complexity, analysis of algorithms, probability theory, logic, and so forth. In the other direction, combinatorial arguments play a huge role in theoretical computer science. Quite a lot of Donald Knuth's magnum opus², *The Art of Computer Programming*, is basically combinatorics.

Mansour: What have been some of the main goals of your research?

Shallit: I do not usually have some overarching goal in mind! I work on what I am currently interested in, and the specific areas have changed over the years. I am not a great problem-solver, so I am never going to prove the Riemann hypothesis, or solve the P=NP

The authors: Released under the CC BY-ND license (International 4.0), Published: May 14, 2021

Toufik Mansour is a professor of mathematics at the University of Haifa, Israel. His email address is tmansour@univ.haifa.ac.il

 $^{^{1}\}mathrm{See}\ \mathtt{https://www.math.ucla.edu/~pak/hidden/papers/Quotes/Combinatorics-quotes.htm}.$

²See, Interview with Don Knuth, http://ecajournal.haifa.ac.il/Volume2021/ECA2021_S3I9.pdf.

question³. Instead, I enjoy finding interesting and unexpected connections between different parts of mathematics, especially with a discrete or computational flavor. Lately, I have been very interested in combinatorics on words, where a lot can be proved or disproved "automatically" using a logical decision procedure.

Mansour: We would like to ask you about your formative years. What were your early experiences with mathematics? Did that happen under the influence of your family or some other people?

Shallit: My parents were very supportive of my interest in mathematics and science. I was also very lucky to have had several excellent mentors. Some that particularly stand out are:

- William Davidon, a professor of physics at Haverford College outside Philadelphia, suggested to my father some mathematics books to read. (Davidon, by the way, was also the covert mastermind of the 1971 break-in at an FBI office that disclosed the COINTELPRO surveillance.)
- my junior-high-school mathematics teacher Robert Stauffer, who conveyed the excitement and breadth of mathematics and told our class over and over, "You can get a Pee-Aitch-Dee in this stuff!"
- Neil Sloane, who encouraged me to contribute to his *Encyclopedia of Integer Sequences*.
- The staff at the IBM Scientific Center in Philadelphia, including Kenneth Iverson, Eugene McDonnell, and Don Orth, who allowed me the opportunity to work during the summer of 1973, where I learned the computer language APL.

Mansour: Were there specific problems that made you first interested in combinatorics? **Shallit**: I can mention a few things. I (re-)discovered the Bell numbers B_n^4 at age 15, and then tried to find out more about them. I tried to read early journal papers about them, but it was a mysterious and almost impenetra-

ble world: nobody I knew could explain to me what the umbral calculus was!

A second problem was mentioned to me by John Hughes in 1980: can one construct an infinite sequence over a ternary alphabet containing no two consecutive identical blocks? At the time I did not know this was a classic problem in combinatorics on words originally due to Axel Thue⁵ in 1906.

I discovered the two beautiful French books of Louis Comtet⁶ on combinatorics when I was an undergraduate, and these certainly increased my interest in the subject. ("Comtet", which sounds like the French word for the verb "to count", is an almost-optimal name for a combinatorialist.)

Mansour: What was the reason you chose the University of California, Berkeley, for your Ph.D. and your advisor Manuel Blum?

Shallit: I wanted to be at a place that had a good number theory program, a good computer science program, and free access to the computer language APL. I narrowed my top choices down to two: Berkeley and Massachusetts Institute of Technology (MIT). But unfortunately, MIT lost part of my application, and I was never even considered by them. So Berkeley it was. It turned out to be a great choice for me.

When I arrived at Berkeley in 1979, I immediately went to see D. H. Lehmer, hoping he would agree to be my thesis supervisor in computational number theory. I had not realized that he was 74 years old and no longer taking students, so after he refused, I had to cast around for a different supervisor. Manuel Blum, in the computer science department, was working on computational problems with number theory aspects, so it was natural that I began to work with his group, which included interesting and creative people like Eric Bach and Shafi Goldwasser.

Mansour: What was the problem you worked on in your thesis?

Shallit: I worked on several problems at Berkeley, but the problem that eventually became my thesis was the analysis of a very sim-

³For example, see S. Aaronson, $P \stackrel{?}{=} NP$, in Open problems in mathematics, Springer, Cham, 2016, 1–122.

⁴See https://oeis.org/A000110.

⁵A. Thue, Über unendliche Zeichenreichen, Norske Vid Selsk. Skr. I. Mat. Nat. Kl. Christiana 7 (1906), 1–22.

⁶L. Comtet, *Analyse combinatoire*, Tomes I, II. (French) Collection SUP: "Le Mathématicien", 4, 5 Presses Universitaires de France, Paris, 1970.

ple algorithm called the Pierce expansion^{7,8}: start with a real number $x = x_0$ between 0 and 1 and repeatedly set $x_{n+1} = 1 \mod x_n$. If x = p/q, a rational number, how many steps are needed to reach 0? And if x is irrational, what is the expected size of x_n ? It turns out that the second question is much easier to answer than the first one: it is about e^{-n} . The first question is still not completely understood, and I offer a cash prize⁹ for improving the best results currently known.

Mansour: What guides you in your research? A general theoretical question or a specific problem?

Shallit: I have always been more interested in specific problems. But sometimes a specific problem might suggest a much bigger underlying theory. One example in my own work is the concept of k-regular sequence¹⁰, which unifies a large number of classical sequences under one framework.

Mansour: When you are working on a problem, do you feel that something is true even before you have the proof?

Shallit: Psychologically, it seems that usually, you have to firmly believe something is true before you can find the proof. If you have significant doubts, somehow you are less motivated. For me, conducting numerical experiments often helps me figure out what the true story is. Mansour: What are the top three open questions in your list?

Shallit: In addition to the problem about Pierce expansions mentioned previously, the ones that appeal to me personally are the following:

• How many binary strings of length 2n can be obtained by taking any binary string x of length n, and "shuffling" it with itself? Here I am not talking about "perfect shuffle" ¹¹, but any left-to-right interleaving of x with itself. Nobody knows an efficient way to compute this, or even good asymptotic bounds. It is sequence A191755 in the On-Line Encyclopedia of Integer Se-

quences ($OEIS^{12}$).

• How many states are necessary and sufficient, in the worst-case, for a deterministic finite automaton to distinguish between two length-n binary strings (that is, accept one but not the other)? Examples where $\Omega(\log n)$ states are needed are known, and the best upper bound currently known is rough $O(n^{1/3})$, due to Zachary Chase¹³. But these bounds are widely separated.

Mansour: What kind of mathematics would you like to see in the next ten-to-twenty years as the continuation of your work?

Shallit: As I mentioned above, I have been working on what parts of combinatorics on words can be proved "automatically" using a decision procedure, with basically no human intervention, and I would be pleased to see other results along these lines. One of your previous interviewees, Doron Zeilberger¹⁴ has been doing this for enumerative combinatorics for years and is a real pioneer in this area.

Mansour: Do you think that there are core or mainstream areas in mathematics? Are some topics more important than others?

Shallit: What's considered "core" or "main-stream" or "important" changes throughout time. The classical invariant theory was actively studied in the late 1800s, but then it almost completely vanished, and now it has been resurrected again. When I was a graduate student, it seemed everyone in theoretical computer science was working on very large scale integration (VLSI) layout problems, but now the interest in theoretical aspects of VLSI has disappeared.

Discrete mathematics, including combinatorics, is becoming more and more viewed as a core area, in part because of its role in computer science and biology.

Mansour: What do you think about the distinction between pure and applied mathematics that some people focus on? Is it meaningful at all in your case? How do you see the

⁷J. Shallit, Metric theory of Pierce expansions, Fibonacci Quart. 24 (1986), 22–40.

⁸P. Erdős and J. Shallit, New bounds on the length of finite Pierce and Engel series, Sém. Théor. Nombres Bordeaux (2) 3:1 (1991), 43—53.

⁹See https://mathoverflow.net/questions/164129/improving-known-bounds-for-pierce-expansions-cash-prize.

¹⁰J.-P. Allouche and J. Shallit, The ring of k-regular sequences, Theoret. Comput. Sci. 98 (1992), 163–197.

¹¹P. Diaconis, R. L. Graham, and W. M. Kantor, The mathematics of perfect shuffles, Adv. in Appl. Math. 4 (1983), 175-196
¹²See https://oeis.org/.

¹³Z. Chase, A new upper bound for separating words, arXiv:2007.12097v2, 2020.

¹⁴ Interview with Doron Zeilberger, http://ecajournal.haifa.ac.il/Volume2021/ECA2021_S3I3.pdf.

relationship between so-called "pure" and "applied" mathematics?

Shallit: Applications have never been that interesting to me. I am more motivated by the intrinsic beauty of a question, its relationship to other areas of mathematics and computer science, and the degree to which answers or methods are surprising. But if there are applications, too, so much the better!

Mansour: What advice would you give to young people thinking about pursuing a research career in mathematics?

Shallit: Read as much as you can, in as many different areas as you can. Browse the *Princeton Companion to Mathematics*¹⁵. Get involved in undergraduate research through programs such as the NSF REU program in the US, and the NSERC USRA in Canada. Read the problem section of the *American Mathematical Monthly* every month, and try to solve the problems. Avoid time-wasters like social media. Find people who know more than you do, and befriend them.

Mansour: Would you tell us about your interests besides mathematics?

Shallit: I have a rather random set of interests, including mineralogy, numismatics, escape literature (that is, books about escapes from prisoner-of-war camps), eclipses, family genealogy, mystery novels, history, linguistics and foreign languages, evolutionary biology, the desert Southwest, natural history, moose, baseball, birds, and guitar music. The history of ideas and the origins of things particularly interest me. Lately, I have been reading a series of books by Ian Mortimer about English history, and I have been enjoying them very much.

Mansour: Before we close this interview, we would like to ask you some more specific questions. In your blog Recursivity¹⁶ you described yourself as an American mathematician, professor of computer science at a major Canadian university, and skeptic. Would you uncover for our readers the term "skeptic"?

Shallit: For me, a "skeptic" is somebody who thinks that "it is undesirable to believe

a proposition when there is no ground whatever for supposing it true" (Bertrand Russell). So a skeptic typically doubts the existence of supernatural beings, Bigfoot and extraterrestrial aliens visiting the Earth, and is not likely to subscribe to preposterous conspiracy theories such as "9-11 Truth" or "the Plandemic". Of course, a skeptic should always be willing to re-examine their beliefs in light of new evidence. But "extraordinary claims require extraordinary evidence".

Mansour: You have contributed to the well-known online mathematical forum *Mathover-flow*. How did you decide to join it? What do you think about this kind of discussion forum? **Shallit**: I cannot remember. Probably some colleague told me about it. Anything that brings people who are interested in mathematics together is a good idea.

Mansour: In one of your major results Polynomial versus exponential growth in repetition-free binary words¹⁷, co-authored by J. Karhumäki, you solved an open problem proposed by Kobayashi¹⁸, and answered the question 'For what value of exponent α does the number of binary words avoiding α -powers switches from polynomial growth to exponential one?' You showed that 'the dividing line' between polynomial and exponential growth is $\frac{7}{3}$. Would you briefly tell us about this problem and why this fraction appears? Are there similar problems and results in your field of research?

Shallit: That was a very fun problem about repetitions in words! To explain it, I need the notion of period and exponent of a word. A period of a word w is a positive integer p such that w[i] = w[i+p] for all meaningful indices i. For example, the word alfalfa has a period 3: each symbol equals the symbol appearing three positions earlier. The exponent of a word is its length divided by its shortest period. So the exponent of alfalfa is 7/3.

If a word contains no block whose exponent is larger than α , we say it is α^+ -free. Thue¹⁹ proved that there are infinitely long words that are 2^+ -free. One can also count the number of

¹⁵T. Gowers et al., editors, The Princeton Companion to Mathematics, Princeton University Press, 2008.

 $^{^{16}\}mathrm{See}\ \mathrm{http://recursed.blogspot.com.}$

¹⁷J. Karhumäki and J. Shallit, *Polynomial versus exponential growth in repetition-free binary words*, J. Combin. Theory Ser. A 105:2 (2005), 335–347.

¹⁸Y. Kobayashi, Repetition-free words, Theoret. Comput. Sci. 44 (1986), 175–197, Problem 6.6.

¹⁹A. Thue, Über unendliche Zeichenreihen, Norske vid. Selsk. Skr. Mat. Nat. Kl. 7 (1906), 1–22 (Reprinted in: T. Nagell (Ed.), Selected Mathematical Papers of Axel Thue, Universitetsforlaget, Oslo, 1977, 139–158).

 2^+ -free binary words of length n, and it turns out that there are only polynomially many²⁰. On the other hand, there are exponentially many 3^+ -free binary words of length n. This suggests that there might be some exponent α where the growth rate of α^+ -free binary words abruptly changes from polynomial to exponential, and it turns out that the switchover point exists and is exactly 7/3.

This is just one in a long line of similar results about the avoidability of patterns in words. There are dozens and dozens of papers on the topic.

Mansour: In your joint paper, Folded continued fractions²¹, co-authored with well-known number theorist Alf van der Poorten, you make some interesting connections between some binary sequences, continued fractions, and paper-folding sequences. Would you tell us about this work?

Shallit: I cannot possibly improve on my coauthor's beautiful article FOLDS?², which appeared in three parts in the *Mathematical Intelligencer* in 1982. So I'll just direct readers to that amazing piece of work, written by Michel Dekking, Michel Mendès France, and Alf²².

Mansour: The continued fraction expansions $[a_0; a_1, a_2, \ldots] = a_0 + 1/(a_1 + 1/(a_2 + \ldots))$ for which the sequence (a_i) is bounded appear in many different fields of mathematics and computer science. You wrote a survey paper²³ on this topic in 1992. Would you tell us about some current research activities on this topic and point out some future research directions? Shallit: Numbers with bounded partial quotients are also called badly approximable, and arise in many different areas of mathematics, including Diophantine approximation, transcendental number theory, and numerical analysis. This class includes all the quadratic irrationals, as well as other numbers such as $\sum_{n\geq 0} k^{-2^n}$ for integers $k\geq 2$. Zaremba's conjecture is probably the most interesting open problem in the area: it says that for every positive integer denominator d, there is an integer numerator n such that the partial quotients in the continued fraction for n/d are bounded by 5. There has been some recent very deep work on this problem, by Bourgain and Kontorovich²⁴ (just to mention two names), but it is still unsolved.

Mansour: In one of your recent interesting joint works, *Critical exponents of infinite balanced words*²⁵, you construct infinite balanced words over an alphabet of different sizes and some interesting numbers appear as critical exponents. Would you tell us about this research and the motivation behind it?

Shallit: Here we are back to words avoiding blocks of a given exponent. The critical exponent of an infinite word w is defined to be the infimum over all α for which w is α^+ -free; it is a measure of the repetitivity of the word. Dejean's conjecture²⁶ (now a theorem, proved by Currie & Rampersad²⁷, and Rao²⁸, independently) specifies the so-called "repetition threshold": the smallest critical exponent one can possibly achieve, considering all words over an alphabet of size k. But it is also interesting to compute this repetition threshold for other classes of words. One interesting class is the so-called balanced words, where every length-n block has approximately the same distribution of letters as every other length-n block. Together with my co-authors Narad Rampersad, Élise Vandomme²⁵, and Aseem Baranwal²⁹, we found the repetition threshold for a number of different alphabet sizes. An interesting feature of our work is that some of the results were proved using a decision procedure where it was just necessary to state the desired result as a first-order logical statement, and sit back and wait for the prover to prove it.

Mansour: Let us briefly discuss your book, co-authored with J.-P. Allouche, *Automatic Sequences: Theory, Applications, Generaliza-*

 $^{^{20}\}mathrm{See}\ \mathrm{https://oeis.org/A007777}$

²¹A. van der Poorten, J. Shallit, Folded continued fractions, J. Number Theory 40:2 (1992), 237–250.

²²M. Dekking, M. M. France, and A. van der Poorten, A. Folds, Math. Intelligencer 4 (1982), 173–181.

 $^{^{23}\}mathrm{J}.$ Shallit, Real numbers with bounded partial quotients, Enseignement Math. 38 (1992), 151–187.

²⁴For example, see J. Bourgain and A. Kontorovich, On Zaremba's conjecture, Ann. of Math. 180:1 (2014), 137–196.

²⁵N. Rampersad, J. Shallit, and É. Vandomme, Critical exponents of infinite balanced words, Theoret. Comput. Sci. 777 (2019), 454–463.

²⁶F. Dejean, Sur un théorème de Thue, J. Combin. Theory, Ser. A 13 (1972), 90–99.

²⁷J. Currie and N. Rampersad, A proof of Dejean's conjecture, Mathematics of Computation 80 (274) (2011), 1063–1070.

²⁸M. Rao, Last cases of Dejean's conjecture, Theoret. Comput. Sci. 412 (2011), 3010–3018.

²⁹A. R. Baranwal and J. Shallit, *Repetitions in infinite palindrome-rich words*, In R. Mercas and D. Reidenbach (eds.) Combinatorics on Words, WORDS 2019, Lecture Notes in Computer Science, Volume 11682, Springer, 2019, 93–105.

³⁰J.-P. Allouche and J. Shallit, Automatic Sequences: Theory, Applications, Generalizations, Cambridge University Press, 2003.

tions³⁰. It is a great source for sequences generated by finite automata, their generalizations, and applications to number theory and theoretical physics. Are you 'optimistic' about other new connections and applications finite automata may appear in? Do you plan to expand it in the new edition? Or maybe you will write another book?

Shallit: Someday we will write a new edition of *Automatic Sequences*, if there is "world enough, and time". In the meantime I am working on a book manuscript where we discuss the interaction between automatic sequences and logic, using a theorem-prover called Walnut created by my former student Hamoon Mousavi³¹.

Mansour: Your paper What this country needs is an 18-cent piece³², published in Math. Intelligencer in 2003, generated a lot of media and bloggers' attention, including Forbes magazine. What was the main point of the paper? Did you expect so much media attention?

Shallit: The motivation originally arose from trying to find interesting problems for an undergraduate course on algorithm design. common exercise in that course is to show that for the existing system of American coin denominations (1¢, 5¢, 10¢, 25¢), the greedy algorithm gives the smallest number of coins for any desired amount of change from one cent to 99 cents. This naturally suggests the question of choosing the denominations optimally, to get the smallest average number of coins needed to make the change. It turns out that if we do not restrict ourselves to using the greedy algorithm, then the best choice of denominations is (1c, 5c, 18c, 25c). So we should replace our dime with an 18-cent piece!

This led to my paper in the *Intelligencer*, which was intended to be tongue-in-cheek, but not everybody had realized this. The best outcome was that my work was featured on National Public Radio's quiz show in the US, *Wait Wait... Don't Tell Me!*, which has to be one of the highlights of my research career.

Mansour: In a 1987 article of the New York Times, they write "Without quite meaning to, Neil J. A. Sloane has become the world's clearinghouse for number sequences." What do you think about OEIS¹² and its future? What are your favorite integer sequences from the database?

Shallit: The OEIS is an incredibly useful resource, and we should all be immensely grateful to Neil Sloane for creating it. I've contributed about 500 sequences to it, which is just a drop in the bucket. I have many favorite sequences, but I will just mention one: $A220950^{33}$, the number of distinct languages recognized by unary nondeterministic finite automata with n states. Only five terms are currently known.

Mansour: Would you tell us about your thought process for the proof of one of your favorite results? How did you become interested in that problem? How long did it take you to figure out a proof? Did you have a "eureka moment"?

Shallit: As a teenager I discovered continued fractions through the marvelous little book of C. D. Olds³⁴. And so I began to expand various real numbers as continued fractions, to see if I could discover any interesting ones. At first, I just used a Texas Instruments calculator, but eventually, I was able to compute them with a digital computer. Mostly, I just rediscovered known results, such as the expansion of the numbers $e^{2/n}$ for odd positive integers n. But then I tried the numbers $\sum_{n\geq 0} k^{-2^n}$. My experiments suggested these numbers have bounded partial quotients, but I could not prove it. As a freshman at Princeton, I found the analysis class so boring—I was never any good at analysis—that I spent most of the class time trying to construct a proof, and eventually succeeded. I would say it took me a year or so, off and on (and I didn't do so well in that course). This paper³⁵ was published in the Journal of Number Theory in 1979, after some very long delays that are another story.

Mansour: Is there a specific problem you have been working on for many years? What progress have you made?

Shallit: Tom Brown (and later Pirillo & Varricchio and Halbeisen & Hungerbühler) asked if an infinite sequence exists over a finite subset

³¹See https://arxiv.org/abs/1603.06017.

³²J. Shallit, What this country needs is an 18-cent piece, Math. Intelligencer 25 (2003), 20–23.

 $^{^{33}\}mathrm{See}$ https://oeis.org/A220950.

³⁴C. D. Olds, *Continued Fractions*, Mathematical Association of America, 1963.

³⁵J. Shallit, Simple continued fractions for some irrational numbers, Journal of Number Theory 11 (1979), 209–217.

of N, the natural numbers, containing no two consecutive blocks of the same size and same sum. This is a fascinating question; a heuristic argument by Pascal Ochem suggests the answer might be "no", but there is still no proof one way or the other. I worked on it for a long time, but could not solve it.

Following the advice that "if you cannot solve the original problem, change it to the one you can solve", I started thinking about the same problem with "two" replaced by "three". In March 2011 I stumbled across the infinite word $03143011\cdots$, the fixed point of the map sending $0 \rightarrow 03$, $1 \rightarrow 43$, $3 \rightarrow 1$, and $4 \rightarrow 01$, which seemed like a good candidate. But I could not prove it had the desired property.

Later on, I had a really brilliant master's student, Luke Schaeffer, who saw how to apply a technique of James Currie to the problem, and together with Julien Cassaigne, we were able to prove that this construction actually works. Our paper³⁶ appeared in the *Journal of the ACM* in 2014. The moral of the story is that it is great to have colleagues and students that are smarter than you are.

But the original problem for two blocks is still—sadly!—unsolved.

Mansour: Professor Jeffrey Shallit, I would like to thank you for this very interesting interview on behalf of the journal Enumerative Combinatorics and Applications.

 $^{^{36}}$ J. Cassaigne, J. D. Currie, L. Schaeffer, and J. Shallit, Avoiding three consecutive blocks of the same size and same sum, J. ACM 61 (2014), Paper 10.