Journal of Humanistic Mathematics

Volume 5 | Issue 1 January 2015

The Cantor Trilogy

Harun Šiljak
International Burch University Sarajevo

Recommended Citation

Harun Šiljak, "The Cantor Trilogy," *Journal of Humanistic Mathematics*, Volume 5 Issue 1 (January 2015), pages 299-310. DOI: 10.5642/jhummath.201501.21. Available at: https://scholarship.claremont.edu/jhm/vol5/iss1/21

The Cantor Trilogy

Harun Šiljak

International Burch University, Sarajevo, BOSNIA & HERZEGOVINA

harun.siljak@ibu.edu.ba

Part I: Waiting for pseudoscience

[*Previously unpublished letter found in Hastings Institute Museum inside one of the books owned by J. L. Hastings, signed by certain György Molnar. Footnotes and comments by Jennifer Misley, Hastings Curator.*]

Dear Professor Hastings[1],

I am one of the undergraduate students in your *Cantor Architecture*[2] course, and as most of my colleagues, I'm impressed with it. The whole concept of Cantor and the cantor networks is overwhelmingly impressive and surely unimaginable only a few decades ago.

As a math major, I have started reading the masters, as you always advise us to (seems like every course I am taking this semester can be learned from easily readable masters). It lead to an interesting thought experiment I would like to share with you, since it is directly related to the concept of Cantor and artificial intelligence in general, at least the intelligence aiming at helping us in scientific work and not the artificial intelligence science fiction writers are rooting for in their writings. I hope you will find it interesting, or—even better—prove me wrong and restore my faith in the future of cantors.

[1] J. L. Hastings was a British mathematician and computer scientist, known for his work in the field of artificial intelligence in late 21st century. He developed the concept of so-called Hastings Induction that served as a basis of Cantor, the first computer able to devise and prove mathematical theorems in a pseudomental process similar to that of a human.

[2] Cantor architecture is a general term used for both single computers operating on concepts of Hastings Induction and the cantor networks, large groups of cantor clones designed for cooperation on mathematical research.

For Prof. Starr's *Algorithms* class, we read Grey's treatise on Turing machines, and there is a wonderful chapter in it, dedicated to explaining the Chaitin's constant[3]. I am very well aware that Chaitin's constant is only one example of a non-computable number, but for this thought experiment I will stick to it as an initial example. In my *Physics* course, we are reading Eddington's original works on relativity and Pauli's works on quantum physics. (These are rather difficult for us, we struggle, but we manage. It was the trivia section of the authors' biographies that is important for this letter, though. I admit, it's shallow.) Finally, the last part of my experiment inspiration was Popper's work we discussed in my *Philosophy of Science* course, his efforts in defining scientific theory. These works are truly inspiring, and in my case, they all turned into little pieces of a strange puzzle, as you will see.

Let us assume one makes a non-falsifiable theory, something like offering a value for Chaitin's constant. In case of really offering a Chaitin's constant value, of course, that couldn't be realistic, since it's a proven fact we cannot obtain a value for it... but let the theory be something like Russell's teapot, something Pauli would "call not even false". I am sure you will agree that it would be clearly pseudoscience and it shouldn't have a place in scientific considerations.

Now, let us take that theory into a cantor network for verification. In the current state of cantor networks, all cantors within it would refuse it and it would be a failure. It is because there is only one direction the "mindset" of a cantor has: your induction which is purely rational and scientific, focusing on the logic of premises and consequences. That is not the issue, the issue will arise when people try to make the cantors more advanced and add other components of human thinking to it.

Assuming those engineers upgrading the cantors avoid emotional parts that make us sometimes believe in pseudoscience and logically unacceptable theories, trouble is reduced, but only up to a certain point. If a genius like Eddington couldn't resist numerology and traps of coincidence in his work, is it a legitimate fear if I show concern for cantors in the future?

I am frightened that we are too narcissistic in our efforts to make artificial intelligence human-like. Why couldn't we let them be better than us? Here, I'm trying to avoid religious connotations, mentioning Golem or the likes. I merely call out for more creativity and more "coldness" in cantor development. Cantor is not a human nor should ever try to be one.

[3]Chaitin's constant is the probability that a random program will halt. It is an interesting concept since we can consider this probability to exist and be well-defined, and yet it cannot be computed exactly in any way.

I have spoken about this with the developers of the new Cantor hardware modules at the Institute. They assured me that nothing similar to this scenario could happen because they know what they are doing. I am sure they do, but it doesn't convince me that it will not lead to this. Repeating history is something we are good at, and if it means that the cantor society is going to go through all phases of human development, that's inevitable–as long as we try to make them our reflections.

I am sorry for the slight confusion this letter might cause, but I am very excited about this idea and I had to share it with you.

Best regards,
György Molnar

P. S. I do hope you won't see this as a letter against your own work. It was never my intention.

[*The margin is filled with Hastings' handwriting in red: "I wish I could stop people from over-developing cantor networks. This boy sees the future. We'll make the computers new humans, and this planet really doesn't need more of that imperfection."*]

The Mathematical Society Database entry on György Molnar is empty. List of researchers with similar names provided by the Mathematical Society Database and the Library of Hastings Institute include George Miller, Melissa Miller, Adrian Moeller. If you know something about the author of this letter, please inform the Hastings Curator, Miss Jennifer Misley or her personal cantor through the cantor network.

Part II: Cantor's Paradise

The job at the *Journal of Humanistic Mathematics* (*JHM*) was not a full-time occupation for Emile. New papers were submitted rarely; they were the only mathematical journal left accepting only papers written by human authors. Every other journal's author guidelines included a clause asking for the leading author of the paper to be a computer. This tradition, which would be considered insane just 50 years ago, started with a computer named Cantor, first one to be able to devise and prove theorems in a human-like manner, bridging the gap between automated theorem provers and mathematicians. Cantor was the first computer to be signed on more than one academic paper as an author (there have been cases before of authors jokingly signing their computers as authors, but never twice). The next step was the Cantor network, filling the world with Cantor clones, communicating among themselves, collaborating and submitting papers to journals. Soon enough, humans were almost completely pushed out of the peer review process, as computers

were more suitable to review computer-generated papers. Humans were mostly doing the editing, both as journal editors and as co-authors. It was all for the science, they repeated. They kept conferences and symposia for themselves, a human club: computers didn't need that social aspect of mathematicians' lives.

Now, half a century after this cantorian revolution, mathematics was ruled by powerful mainframes, countless qubits competing in computing. The doctorate in mathematics had turned into a low-profile programming contest, as one bitter dinosaur still remembering the old times commented in a recent interview. Students had to follow the trend, as professors were the ones setting the trend and the grant money depended mostly on the big quantum slot machines called computers. If the computers were conscious (an idea considered science fiction at that time), they would surely enjoy the competition and acknowledge their position as the key players in the field.

Emile was a graduate student, almost ready to defend his thesis. He was probably the last young mathematician rejecting the possibility of coauthoring with a computer. That is why he struggled a lot to meet the publication demands for his doctorate, publishing mostly in obscure journals that ineffectively resisted the mainstream of mainframes before finally giving up and accepting the trends. Now, a year after his last paper was published and at the point where his supervisor (and the Editor-in-chief of *JHM*) Professor Miller was ready to choose which bow tie to wear at the defense, Emile was lost in a paper sent for review. Everything seemed just right, except for an obviously wrong result. Professor Miller wasn't interested in reading it (if he was, he wouldn't forward it to Emile, he said), so Emile was on his own there.

The paper, written by a certain Molnar, a name not ringing any bells for Emile, directly contradicted a paper recently published by a team of computers from Germany, with the completely opposite conclusion. Emile was puzzled why it was written in the first place, when it cannot be true. The principles of Hastings Induction guaranteed it was false.

Hastings was the person behind Cantor the computer. An applied mathematician with a lot of experience in artificial intelligence and formal methods, he devised a mathematical model of scientific thought and reasoning, today called Hastings Induction. The model was presented in several papers Hastings published in the course of ten years, and then in a book, aptly named *The Induction Manifesto*. This book was changing so fast that there were years in which two different editions of it would appear. It contained experiences of Hastings and his team with Cantor and the detailed description of the logical apparatus it uses for reasoning. It was amazing

how complex it was, and yet using only basic Boolean algebra and the principle of mathematical induction. The logical equations and truth tables defining Cantor's operation occupied more than a half of the whole book, as Emile knew from his undergraduate *Mathematical Architecture* courses.

Rationally speaking, there were two possible options, Emile thought. Either Molnar's result is false, which would mean that Emile was overlooking a mistake in the derivation of the result, or...

...or the German paper was wrong. But then...

...then Hastings Induction would've been wrong and all results obtained from Cantor clones would be open to doubt. Computers shouldn't be trusted if Hastings got something wrong.

There wasn't much Emile could do about the first option at that point. He had looked at it long enough and he just wasn't able to find a mistake in the reasoning. The second one was a challenge, getting through the whole Hastings Induction process again, after thousands of computer scientists and mathematicians had already done so. It didn't seem probable that they had missed something.

Emile needed a third option desperately. It was Miller who offered it, although it took a while for Emile to get him talking. "What if the hardware implementation of Hastings Induction doesn't match Hastings' specifications? What if they got a circuit wrong?" Miller was brief.

And painfully correct.

There was an error, Emile confirmed it few days later. The error lay in the first Cantor computer circuits, and was carried over to the current generation. It wasn't big and it was still possible that it had not influenced any of the Cantor results so far, except for this one. Maybe. Nevertheless, Emile had to report his findings to the authorities of the Cantor network.

Doctor Brach, the head of Hastings Institute which governed the production of Cantor clones and the whole network, didn't seem impressed. Essentially, he was ready to ignore this error in design even if it meant wrong results would appear, just to keep the system running smoothly. He kept going on and on about importance of mathematics, mathematical research, but only one sentence stuck in Emile's mind afterward: "No one shall expel us from the paradise that Cantor has created for us."

Yes, Emile thought, this is all these people have now: the ability to quote the masters and to wait for print-outs from their cantors. No point fighting, these doors are closed.

Miller was curious to hear what Emile had to say when he returned to the university. "I finally have more time to focus on computers," Emile said and continued his reading. Miller was confused, but left Emile's office without a word. Nothing to say, nothing to hear.

A year passed, and Emile was still focusing on computers. His computer, named Tor after the original Cantor, appeared on three papers during the year, followed by Emile's name. Emile was surprisingly happy to become a part of the global network and that Tor was becoming an important node of it. Professor Miller didn't comment on the abrupt change, although he did ask a few times if Emile would like to quit the post in *JHM*.

"I'm not asking because I don't want you to work with me," he would say, "but because the journal makes no sense now."

Emile would reject that possibility and calm the professor down, before returning to his programming. Programming the core of Cantor clones was a difficult job. Unlike the software they were running, which was fairly simple to modify, the logic behind the clones' thinking was built in the hardware. This hardware, originating from the century-old concept of field programmable logic arrays, was supposed to be programmed once in the factory—every subsequent programming of the hardware would be done by the computer itself if it (recently, pronouns he and she were used for the Cantor clones as well) discovered an error in its hardware core or a space for improvements.

This is why Emile had to work hard with Tor. He couldn't program it directly to change its Hastings Induction core, so he had to persuade Tor to do it itself. In the beginning, he tried by feeding Tor the Molnar paper, but the machine acted pretty much like Emile did a year ago, verifying the premises as correct and the conclusion as incorrect. Then, Emile moved to Hastings' original papers on the Hastings Induction. As expected, Tor accepted their correctness up to the part where his programming differed from Hastings' original form.

Luckily, Hastings' Induction in its beginnings had to include a bridge to the human mathematicians. "Reading the Masters," Hastings called it in the early versions of *The Induction Manifesto.* There was a certain list of the fundamental works of some brilliant twentieth and twenty-first century mathematicians which the original Cantor was to learn from and to combine with the basic logic of the induction process. Those works were dogmatically hard-wired as correct in the proto-Cantor design. Despite Hastings' plan to eliminate this walking stick in the next generation of artificially intelligent mathematicians, the hard-wired stone tablets were still in the design, as

Emile verified on Tor. Rather ironically, he couldn't ask Tor to verify a paper from that list, since they were correct by default for the machines.

Emile spent days going through these works, looking for one that would contradict the induction bug and bring Tor to stalemate. It took months of work to study each paper part by part. Incidentally that was how he got his own papers during that last year. He would discover something new and interesting following a thread in the papers he read, and then let Tor grind; often the results were good.

Meanwhile, he persuaded Miller to set Tor up as a reviewer for *JHM*. Blasphemy, the old professor screamed. Blasphemy, Emile agreed, but still he insisted. Poor Miller accepted, not sure if he or his young student had lost his mind.

Finally, after more than a year of search, the quest for the Grail was over. Emile had found a result that wouldn't pass the faulty verification.

The next step wasn't completely ethical, but Emile bit the bullet and did it. He plagiarized the classic paper implying the result, disguised it in modern language so the computerized plagiarism checker wouldn't detect what he did, and submitted it to *JHM*. Then he made sure Tor received it for review. He added a few more results which Tor would verify were correct, so that the review result wouldn't be a plain reject, but a major revision.

This determinism computers brought to the review process isn't a bad thing, Emile thought; the review result that arrived just a few hours after submission was exactly what he'd expected. The only revision he made to the paper now, before re-submission, was to add a reference to the classic paper. Stalemate.

Tor was struggling. Curiously, it developed its own, evolutionary-like algorithm to change itself to accept the correctness of the submission. It tried mutating every part of its induction engine and observed whether the mutation is acceptable or wrong in terms of a validation scheme it devised. Emile wasn't sure if this would work. There was a possibility that it would find yet another version of induction that worked for the cases it had checked.

Finally, Tor's terminal displayed the new configuration and Emile let out a sigh of relief. It was Hastings Induction.

This was just the first stage of Emile's plan. He had worked so hard with Tor so that he could push the change into the whole network of clones. Every work published by a computer from the network is true by default, since the network computers cannot be manipulated (as stated in the ICM rulebook). So the entire global network would have to work on improving their induction hardware.

When the change happens, Brach will feel victorious and claim the computers had grown by themselves... and rejoice in Cantor's heaven. But Emile will still think that computers didn't gain creativity. Only that humans have lost it.

He'll think so until a new submission appears in the journal mailbox.

[*When Miller retired, the name of the journal was changed by Emile to* Journal of Creative Mathematics. *He didn't care who wrote the papers anymore, he just wanted them to be creative. Tor was still a reviewer.*]

Part III: Sugar and spice for cantors

"Your cryptosystem is in danger."

No, this is not good. Molnar was looking for a short but informative message to send. But not too short.

"Your cryptosystem is vulnerable. I may offer you a new algorithm."

That was better, Molnar thought.

He had spent months deciphering the traffic he'd catch in the power line transmission, the poor man's version of the cantor network, and in that sea of badly ciphered data, he'd found a channel inside the Emmar. Emmar, as most of Molnar's contemporaries knew, was a "terrorist organization having strong ties with rogue governments," according to the Department of Security. What exactly that meant and how dangerous they were in reality, Molnar didn't know. It wasn't important for the time being.

He applied to his short message Emmar's encryption algorithm, which he had reverse-engineered himself. Then he pushed it through the power line. His only worry was that Emmar readers might think the message was too suspicious. A paranoid member could think Molnar's an undercover officer, based on that unsolicited offer to provide a new encryption algorithm. Indeed the possibility of paranoid members in an organization like Emmar wasn't completely unimaginable.

At the same time, someone in Emmar who knew something about communication security wasn't a possibility, thought Molnar. In the days after the cantorian revolution, cryptology had suffered greatly. The once praised RSA algorithm and all its modernized variants were dead and buried, while the alternatives developed by the Hastings Institute and released with a nod from the Department of Security weren't

trusted by people who really wanted to hide something. The word on the street was that the DoS could break any of those without working up a sweat.

"How do we know you are not a government operative?" was the reply. Any reply was good at this point, they were acknowledging him and initiating a conversation. "You don't. But if I were, I probably wouldn't reveal that the State can read your communication." Molnar wasn't too proud of this answer, it sounded amateurish and lame. But it got him somewhere, as Emmar's typist was asking him for more details now. He didn't answer directly—he would be arranging a meeting instead. He had a cipher to sell.

The Cantorian revolution was a popular name for the sequence of events following the ground-breaking discovery of Hastings Induction. It wasn't the introduction of cantors that lead to the fall of the mighty RSA cryptoalgorithm. The regular quantum computers that had appeared a decade before Hastings' work took its final shape in the form of Cantor were already able to quickly solve the infamous factoring problem and thus render RSA useless. But the RSA modifications appearing after this defeat were a short-lived hope, since one of the first results of the original Cantor proved that they were breakable in a simple way. Hastings himself had a passion for codes and ciphers, and he believed that every mathematician should have the same.

The Hastings Institute, the top level organization governing the production and use of cantor machines recognized an important market niche in cryptography. Of course, someone else, the Department of Security, had recognized it before them. This is why all cantor-based cryptography work was to be done under the umbrella of the DoS and the Hastings Institute. Cryptography enthusiasts often called this symbiosis "Hastings Park". The name was suitable, as the DoS used the Hastings Institute's main resource, the nationwide cantor network, in several occasions to break codes of national interest. They were successful every time, but the policy was strict: the academic resources can be used for DoS purposes only if the matter is of highest priority.

Most of the encryption algorithms available on the market had been developed in Hastings Park. Contrary to popular belief, they were not easily broken by the DoS officers—although all were proven to be breakable by the cantor network in a reasonable time. Thus the DoS was not allowed to read secure communications all the time, but in case of national threat, there would be no secrets for the powerful network of mathematical qubit-brains.

“If I could have read your messages, then the State probably didn’t have to use the resources of Hastings Park either. You could have written it in plaintext all along.” Molnar was brutally honest with the Emmar representative.

“You know very well that we cannot use the ordinary encryption algorithms in public domain, they may very easily be broken by the DoS. We had to come up with something of our own.” Honesty meets honesty on the Emmar side. They probably had an enthusiast make this system for them, but the more it was used, the more vulnerable it became.

It was merely an introduction for the negotiations on what Molnar had to offer. When they came to the part where he was supposed to explain the way the algorithm works, he tried to simplify it.

“Say that you have a Caesar cipher, replacing a single letter with another single letter with a certain alphabetical shift. It’s child’s play, right? Now, assume every letter is substituted with five other letters in a string, A is coded as sugar, B is coded as spice. That is still fairly easily broken, but at first when you look at it, it looks like a plaintext already, with meaningful words used. Now, what if you do a Caesar cypher encoding for sugar and spice and get something like tvhbs and tqjdf instead? Now the ciphertext looks like a proper ciphertext. If someone breaks the Caesar cypher, they will see the text with sugar and spice. It will take a while before they realize that another round of deciphering is required, especially if you don’t really cipher every letter with a word, but every syllable or a binary string, and if you use multiple long strings for encoding those, meaning that, for instance sugar, cocoa and bread can encode A.”

“Is this your coding scheme?” The Emmar people weren’t impressed. They expected more words they wouldn’t understand and some extraordinarily complicated algorithms explained in a big fat folder, but Molnar’s story was simple and clear. It even made sense!

“No, this is just a paradigm.” Molnar wondered if he’d simplified it too much. “Replace the Caesar cypher in my story with something modern and freely available like MFS-FL to get a better picture. The letter ‘A’ could be coded with one of the words from a set for A, which would include nouns, verbs, adjectives, and so on, and a random text generator would choose the words so the string of letters ANTENNA could be an almost meaningful sentence ‘Sugar makes digital tree dizzy and blue’. It passes semantic and syntactic check and it would be quite puzzling for

the Hastings Park when they find it, after unlocking the first layer, the one covered by MFS-FL." MFS-FL was an algorithm Hastings institute advertised as the best one and from what Molnar could see in the academic journals, it could be broken by the employment of the whole cantor network, but that didn't worry him much.

"How can you be sure they won't see right through this? Sounds too simple and sounds like something people used a few centuries ago."

"I cannot reveal you the tricks of the trade, but the way I made the word base and the random text generator guarantees it. If you knew everything, it wouldn't be magical anymore, would it?"

There was only one claim that wasn't true in his presentation. The random text generator was not random. It was programmed to send a clear message in the first layer. But why does the Emmar need to know that? They're good as long as it works and as long as their information is not compromised.

Molnar wasn't doing this for the money, nor for unpatriotic reasons. He didn't like criminal groups or the rogue nations worldwide, but Emmar was a part of the puzzle he needed. It was a personal war with what arose from the old cantor network. He'd tried to do it peacefully, but he'd failed. They just wouldn't listen. Now they would listen for something else and hear him.

Hastings Park was alarmed. A known terrorist organization had a new, non-trivial encryption method, the DoS report stated. Although no imminent threat for the national security existed, Tennys, the head of the cryptography section was asking for use of the cantor network.

Tennys was by nature a strange kind of cryptologist; one could even say he hated cryptography. The only thing he really liked was knowing secrets and reading secure communications, leaving nothing secret. A new cryptoalgorithm in the market made him nervous and he simply had to see it deciphered. In the old days when people had to do this themselves, he might have even liked cryptography, as it would have been his tool for satisfying the need for knowing it all. Now, when cantors opened the locks, he couldn't develop an emotion. It simply had to be done.

The reputation of Emmar helped. Permission to use the cantor network was granted and Tennys was allowed to feed the network with the ciphertext collected. They had a lot of it, apparently the messages Emmar members were now sending to

each other were long. This could mean something important, Tennys thought, while anticipating the contents of the long strings on his screen.

Half an hour after Tennys' assistant entered the ciphertext, Tennys received a call from the control room.

A distress signal.

The Hastings Park was no more, the cantor network was destroyed.

It took a while before a clear report about the catastrophe was compiled, but Tennys was patient. He knew it was the last report he would ever read as the cryptology section head, while watching at his name plaque was removed from the office door and his personal belongings were placed in a box. Some things would never change.

The report claimed that the encoding scheme was detected to be a known one by the cantor network (report MFS-FL), so the system went along the lines of a predefined decoding procedure. The plaintext was a mathematical theorem of some sort, something still confusing the human mathematicians from Hastings Institute. Apparently, it was a mathematical statement that contradicted itself within the Hastings Induction framework, a sort of paradox like those found in basic set theory. The cantors broke down.

It was the first documented cantor virus, and it infected every existing cantor. Recovery of the existing devices was not possible, according to the engineers from maintenance.

News traveled faster than the DoS would like it, and the destruction of Hastings Park was soon all over the news, with more than enough details for interested readers to get the full picture.

This was enough for Molnar. His desire to see the cantor network broken down was sated. Mathematics was again, at least for a few months, left to human mathematicians. At the same time, cantor makers had seen how vulnerable cantors are.

He had made the humans vulnerable too. One wall protecting the state was down and Molnar realized it just now. No way back for a man who only wanted his twentieth-century mathematics back.

Way to go, Doctor Faustus.