A Remembrance of Steven Rudich
by Russell Impagliazzo

I and many others were greatly saddened by the death of Steven Rudich, October 29. These are some of my memories of my close friend and collaborator. I am dispensing with any claims of strict factuality. While I won't say anything I know to be false, I will write as if I am much more certain than I actually am and simplify certain complex matters.

It has become customary to deal with death with a celebration of the lives and achievements of the loved one. However, Steven's life was such a mixture of blessings and curses, triumphs and tragedies that I cannot write of the one without describing the other. I hope that mentioning the horrors Steven had to deal with in life make his many achievements even more remarkable, and his failings more forgivable.

Steven's parents were scholars of comparative literature. His father, Prof. Norman Rudich, was a well-known scholar and professor at Wesleyan University, and quite successful despite being legally blind. Steven's mother was Norman's research assistant, reading aloud and discussing the literature his father specialized in. Both were committed communists at a time when Marxism really did have great influence in academia. The two had high intellectual standards and little experience or patience with children.

Today, Steven would have been diagnosed with a learning disability and given special treatment. At the time, he was labelled a failure by both the schools and his parents. There were also a few bright spots for him. Steven's parents had a mathematician friend William Boone who treated Steven as an equal and engaged him about the beauty of mathematics. Steven had free run of the Wesleyan University computer lab, where he learned to hack into the system and play tricks. As a child of French literary scholars, young Steven spent his summers in Paris, which he loved. He gave his first magic shows in the Metro, providing entertainment for the tourists and a distraction for the pickpockets. But, mainly, Steven had an education in fending for himself and his kid sister Suzy with parents who were negligent when they weren't actively hostile.

Somehow, Steven managed to convince his parents to send him to a prestigious boarding high school, Northfield Mount Hermon. For the first time, he found a talented group of friends that accepted him as a social and intellectual equal. (For Steven, this was a huge achievement, and towards the end of his life, he became obsessed with it.) Many of these high school peers would stay close to Steven.

Steven still struggled with standardized tests, and when applying to universities, he was only accepted at Wesleyan, where many of the faculty remembered him as a bright child. As a faculty child, Steven was entitled to reduced tuition, but Norman, who had become paranoid and an alcoholic, refused to put his name on the financial aid application for Steven's second year there. In order to declare himself emancipated, and so apply for financial aid without parental cooperation, Steven took a year's leave of absence and ended up in San Francisco

running a computer lab for middle school students.

Steven always made a point of finding and befriending intellectually talented people throughout his life. So when Steven returned to Wesleyan, and heard of a freshman taking advanced mathematics courses, he sought me out. That was the start of our long-time collaboration and friendship. Together with Julia Kay and Joshua Macy, we spent a large part of almost every day arguing about mathematics, politics, philosophy and everything in between. We never gave in on an argument, but I noticed that, from time to time, we switched sides. One of our on-going arguments was "logic or computer science?" where Steven argued the merits of CS and I of logic. In the end, we both realized that they were two great tastes that taste great together.

Steven supported himself at Wesleyan with programming projects like creating the computer game version of "Class Struggle", a board game which combined all the strategy of chutes and ladders with the eloquence of crude communist propaganda. This was perhaps the only benefit to Steven of being a "red diaper baby" (child of communists), since the project paid surprisingly well for inciting anti-capitalist revolution.

We had two mentors: graduate student David Feldman, who seemed to absorb all areas of mathematics by osmosis through photocopying; and Professor Kevin Compton, who was all of the computer science group and about half of the logic group at Wesleyan. Kevin's classes usually ended with a project. Steven and I challenged each other to invent new mathematical topics for each project. I'm not sure that's what Kevin expected. One of these became Steven's undergraduate thesis. This thesis invented a novel formal framework for learning a function by queries, in a recursion-theoretic setting. While there turned out to be some earlier related work, Steven had invented this framework independently, and proved quite a few simulations and separations among related notions. His motivation discusses identifying structures in graphs such as cliques through queries, so already pointed to topics that he would work on in his later career: NP-completeness, decision trees, relativization and so on. This started a trend of Steven being way ahead of his time, since there was recent related work by Kleinberg and Mullainathan inspired by LLMs. My copy, perhaps the only copy in existence, is inscribed: "I proved a really nifty theorem, but there is so much room left in these margins I fear it would get lost", in typical Steven humor.

Some of the previous work on this subject was by Lenore and Manuel Blum. At Kevin's prompting, Steven sent his thesis to Manuel Blum, which resulted in him going to graduate school at Berkeley to work with Manuel. (Steven still did not test well, and did not get into other programs because of low GREs. While Steven famously rescued me from sleeping right through the GREs, I was unable to rescue him from taking the questions too literally.)

Not coincidentally, I also went to Berkeley, planning to study logic. Steven went first, and helped me find an apartment right next to his, and began research right away. His first project was on inferring a hidden Markov process from its outputs, a question Manuel posed to him. The original motivation was to learn to extract random bits from such a source, but it is a problem of much wider interest. The kind of state exploration required is now relevant

to reinforcement learning, for example. At Berkeley, Steven was in his element, and his apartment became the setting where the gang (Sampath Kannan, Tandy Warnow, Umesh Vazirani, Moni Naor, Noam Nisan, Mark Gross, Ronitt Rubinfeld, Amos Fiat, Valerie King, and many others) would congregate for discussions, food and magic. Continuing the habit established at Wesleyan, I would show up pretty much every night without waiting to be invited. Steven continued his habit of finding and recruiting new talent to TCS, such as the much-missed Roman Smolensky, who, like me, was starting his Ph.D. in logic. Steven was, remarkably, able to identify Roman by my description: "He's got a beard and an accent, and he's really smart."

Also continuing the Wesleyan tradition, Steven would invent new problems for us to work on, such as how to simulate dice by flipping coins or which graphs could have edge relations with simple rules based on the vertex names. Many of these problems seemed frivolous, but turned out to be deeply connected to and improve results in the literature. Not every problem Steven came up with was a winner. A paper we wrote with Mark Gross on the circuit complexity of parity got a review that said "How dare they compare their trivial results to Furst, Saxe and Sipser!". Doing research through the gossip network also led to a lack of clarity about who deserved credit for what, which in turn led to disputes that were both ridiculous and damaging.

Steven's Ph.D. thesis was one of the rare topics suggested by Manuel rather than invented by Steven, but one that Steven interpreted in novel ways. Cryptography uses hard problems, and there seems to be a gap between the types of hard problem that are useful for secure communication using a shared key, private key cryptography, and that the types that are useful for secure communication between strangers, public key cryptography. (I would later phrase this as "Minicrypt" vs. "Cryptomania".) The main result of Steven's thesis was a formal sense in which this gap could be proven to exist, a result I collaborated with him on. The exact statement is a bit delicate, but Steven made a very convincing argument that connected the formal result to the intuitive interpretation. I remember this project as the most challenging one I've ever succeeded at. A high-level approach was clear from the start, but the details were slippery and delicate. When we proved the result, Steven and I went for a special dinner of pomegranate chicken. When we found the bug and fixed it, we had another special dinner at the same restaurant, with the same dish. This happened maybe five times. Towards the end, we were getting very frustrated. Out of the blue, Steven came up with a formula and said that was the key. I asked him why this formula was true, and he couldn't tell me. I asked him why it was going to help us, and again he couldn't tell me. It was only after we worked for another month or so that we figured out why this formula was true and was indeed the key to the whole result. To make matters more suspenseful, we knew that there was another group also working on a similar project. We got in touch with them and offered to merge, but when we compared notes, we realized that they were several chickens behind us. By that time, we had been working on it for over a year, and didn't feel that we could wait for them to catch up, so we published by ourselves.

While this was a productive period for Steven, I don't think it was a happy year for him. He was more isolated during that year, and rarely came into the office. (We mainly worked at his home.) He had some relationships that ended too quickly and some that went on too long. He became more defensive and less free to share ideas. Steven had a colorful and forceful way of communicating, and at the start of graduate school, I was worried that people might take him literally. Then I became worried that many people weren't taking him seriously.

While Steven and I never were in the same department at the same time after that, we visited each other often and talked on the telephone frequently. We had a few weeks of overlap in 1989, when Steven was ending his post-doc at U.of Toronto as I was staring mine. Steven told me about unpublished work inspired by talks with fellow post-doc Josh Benaloh on secret sharing for general access structures. He had some ideas for constructions based on Yao's garbled circuits, but no proof of correctness. A modification of this idea was later presented as "witness encryption", in a 2013 paper that cited Steven's unpublished work. As usual, Steven was well ahead of us. A more disturbing event during Steven's postdoc was that his mother tracked him down in Toronto, and began hounding him for money. He refused all contact with her, and never saw her again.

After his postdoc, Steven started as a faculty member at CMU. His first decade there I think of as the peak period of his life, both professionally and personally. He used his talent for identifying talent to find two extraordinary but independent-minded graduate students, Jim Aspnes and Jiri Sgall. In particular, with Jim and other co-authors, he began considering ways to represent Boolean functions in various algebraic forms, such as thresholds of polynomials. These papers introduced themes and techniques that would become central in circuit complexity, communication complexity, derandomization, and algorithm design (especially in the much later work of Ryan Williams).

But whenever I asked him what he was excited to be working on, he told me he wanted to "use complexity against itself to show that complexity is hard." I was used to interrogating him until cryptic comments like this became formal statements, but on this one, I couldn't get him to budge. Then, late at night, Steven woke me and told me the Natural Proofs theorem, with the proof. He asked me whether I saw any holes or needed any additional cryptographic assumptions. I said, 'No, Steven. You're done. It's complete." and went back to sleep. For some reason I couldn't understand, Steven was reluctant to publish this or even write it down, but he did tell many people about it. His tenure clock was running down, and I was getting worried that he wouldn't get credit for this work in time. Worry turned to panic when I heard that Sasha Razborov also had this result. Fortunately, Sasha remembered an earlier conversation with Steven on the subject, and the two agreed to collaborate.. The result itself is brilliant, and does exactly what Steven said it would do, use complexity against itself. But the collaboration between Sasha and Steven elevated the paper to a true masterpiece. in the rest of the paper, they dissect the known circuit lower bounds for algorithmic content. This paper was acknowledged as a landmark at the time, but its importance has only grown, and like the previous work is now central to circuit complexity, derandomization, average-case complexity,

and converting lower bounds to new algorithms. This paper won the 2007 Gödel Prize, awarded at a conference in San Diego, I think the last time Steven visited me. The prize's name made him as happy as the prize itself.

Steven also blossomed as a teacher at CMU. He started a new course for incoming students, formally called "How to Think like a Computer Scientist" but nicknamed "How to Think like Steven". With Merrick Furst, he started and kept going a massively successful summer program to introduce local high school students to computer science, called "Andrew's Leap". Like every great teacher I know, the key to Steven's success was hard work. He was willing to put in so much time thinking about how to present every idea. He would often ask me for a simple argument for something, and if I gave a three line proof, he wanted a two line proof. Really, his ideal was a zero-line proof, a mathematical statement that made itself intuitively obvious, a brilliant, transparent diamond of truth. He often created these diamonds Superman-style (by crushing metaphorical carbon with his super-brain). He called his teaching style "More is more" because by simplifying complex thoughts into easily understood pieces, he could present a much richer curriculum than most would dare. He created a "fun test", more puzzles and mind-teasers than standard math problems, to use as an entrance exam for Andrew's Leap. (If the student thought the test was fun, they usually got in, which I think was the point.) Many Andrew's Leap alumni are familiar names in theory and other areas of CS now. The hardest parts for Steven were fund-raising and making contact with high school counselors to make sure students in Pittsburgh schools knew about the program. Steven took up magic where he left off as a child and was famous for incorporating magic tricks into his lessons.

The early 90's were also a good period in Steven's personal life. Our friend Nathan Tawil from Wesleyan mentioned a fellow philosophy graduate student, Rachel Rue, and it was love at first description (despite Nathan's loud protests). As he often did upon hearing of someone interesting, Steven immediately arranged to meet Rachel, who was a professor of philosophy at Williams College in Massachusetts. Manuel Blum, with a newly arrived mail-order ordination, performed their wedding ceremony, and the two began a long-distance marriage. However, under Steven's influence, Rachel became intrigued by mathematics and computer science and entered the CMU ACO program as a graduate student (although she already had a Ph.D. from Princeton.) They had two children, Isaac and Avi. They seemed like a perfect couple to me.

In 1999, I took part of my sabbatical at CMU to work with Steven. With his student Ke Yang, we tried to formalize another slippery notion: when are programs provably hard to understand? This evolved into a very large group project with many other great collaborators. Just as in Natural Proofs, the key was to "use complexity against itself", but it was Boaz Barak who figured out how to do that, proving that the most general notion we were studying is in fact impossible to achieve. However, this work also introduced a weaker notion called "indistinguishability obfuscation" which has turned out to (possibly) be achievable and an incredibly powerful tool in cryptography. Again, Steven turned out to be ahead of the times. Unfortunately, this would be my last col-

laboration with Steven. Around that time, disaster struck. Steven had noticed he was having problems with vision, and had a very thorough medical examination. He found out that he had three genetic conditions, that ranged from unpleasant to horrifying. First, he was very sensitive to certain foods, and had to completely eliminate many common foodstuffs from his diet, such as bread. For a gourmet and amateur chef like Steven, this was unpleasant. However, it had a bright side, in that by controlling his diet and eating on a schedule, Steven could avoid the low blood sugar crashes that had been a problem all his life.

Worse was Stargardt disease, a genetic condition that caused yellow flecks to accumulate in the center of his vision, meaning he couldn't look straight. To see anything clearly, he had to magnify it to where he could move his head enough to see it with peripheral vision. Steven had the experience growing up with a blind father to know how to live as a blind person, restructuring his life and even figuring out how to continue performing magic.

The horror was Huntington's disease, a genetic neurological condition that eventually causes involuntary movements, personality shifts, mood swings, memory loss, and in the end, dementia. All aspects of this were loathsome. Steven had always been effortlessly graceful and athletic; the idea of losing control of his motions was terrifying. Losing control of his intellect was far worse. But what he feared most is that colleagues would find out and dismiss him as feebleminded or crazy. Very few people knew about his condition, and I am only reluctantly mentioning it now, because it is hard to explain or justify what came next without bringing it up.

Disentangling the "real" Steven from the disease is impossible. In the end, we are all as nature makes us. But it is also impossible not to notice how much like his parents (who must have had the same condition) Steven became. Like Steven, Norman was perceptive and articulate, a talented and dedicated teacher who made a permanent difference in his students' lives. Like Norman, Steven began to drive away his family and friends. Part of that was his survival regimen. To live an independent life while blind and on strict diets, and subject to spasms, Steven needed to know exactly which foods were where in the kitchen, and to never have any unexpected piece of furniture around to fall over. This type of order is anathema to children and teens, who can't help bring a certain amount of chaos to their surroundings. Steven would get furious with the children when something was misplaced, or they weren't there at the correct times. Steven also became very concerned with finances, at the same time as he, perhaps justifiably, splurged on large-screen televisions and specialized cooking equipment. He alternated between hypochondria and complete denial. He and Rachel got divorced, acrimoniously, and had joint custody of the children, but Steven's relationships with the children got worse and worse over time. (Isaac has sent me something he wrote about this, but I haven't dared to read it yet.)

Norman refused to get genetic testing to help see if any of the children were likely to inherit these conditions. That was the last straw, and Steven cut him off completely. He had also lied about his blindness, saying it was due to an accident, which was near unforgivable. Before that, Norman would sometimes

call Steven and other former friends late at night and rant about FBI surveillance and betrayals.

Then Steven began doing the same thing. He would call friends at all hours, and rant about some conspiracy against him, often an imagined one. Friend after friend had to cut him off. When we tried discussing research, Steven mentioned he was attempting to formalize consciousness, much like Manuel and Lenore. But Steven's thoughts on this were just meaningless streams of consciousness, and my attempts to clarify them into formal statements just left both of us frustrated. He became bitter, and believed that those I knew were his friends secretly looked down on him and were spreading rumors about his mental ability. In the end, he only wanted me to be as furious at these imagined betrayals as he was, and denying the betrayals only made me one of the traitors. I called him less and less often, perhaps once a year, just to ensure he was alive. And then he wasn't.

Steven led a heroic life, guiding many of us fearlessly into the unknown. He touched many lives for the better, even if some were made worse. The beginning and ending are only parts of the journey. I hope you will remember Steven at his best, and let the worst fade. I only bring up the bad parts, because I know some of you experienced them and I felt I should explain why they happened.

Although I only represent myself in this, I think donations to the Huntington's Disease Society of America in Steven's memory would be appropriate.