University at Buffalo
State University of New York

Department of Computer Science and Engineering

May 29, 2014

Ravi Kannan, Chair
2014 Knuth Prize Committee
Microsoft Research Labs
Bangalore, 560001 India

Dear Ravi:

It is my great pleasure and honor to contribute a supporting letter to nominate Dick Lipton for the Knuth Prize. I know that Dick's publication record is being addressed in other letter(s), but what I can uniquely attest is the incredible breadth and depth and volume of his Unpublication record. The statutory 3-a-year pace for publications means 1 per 4 months, but Unpublications, those we do every 4 *days*. Well not quite: a little over half the posts on the *Gödel's Lost letter and P=NP* blog are entirely about someone else's ideas, or historical or humorous pieces such as ours last week on "STOC 1500." But each of the rest has a new idea, sometimes two, and those are coming from Dick at a rate that I (with my chess research constituting a third professional life) can barely keep up with. To look over the dozen posts since April 5, there are:

- May 27, "Avoiding Monsters and Non-Monsters": to apply the idea of *lineable* from functional analysis to Boolean hardness.
- May 7, "The Easiest Impossible Problem"—Dick re-cast it using Boolean vectors; a mark of non-triviality is that Lance Fortnow corrected us, then a commenter tried to un-correct Lance.
- May 3, "Does Program Size Matter?"—a new try to push a famous construction by Leonid Levin further.
- April 16, "The More Variables, the Better": Dick has generated several ideas on the famous Jacobian Conjecture, with interaction from some prominent mathematicians.
- April 5, "Counting is Sometimes Easy": in search of new applications for counting by finite automata.

One other recent post has a new idea by me, to make it six-of-twelve. Now I must admit that so far only a few of these ideas have grown up to be Real Publications by us (including two recent papers at MFCS conferences and what would be a great one on factoring but it needs fixing) or embraced by others (our posts on a new kind of graph product and on the group isomorphism problem come to mind). It also may not be clear to readers that our ideas really are free for adoption, no need to join with us—we even termed one post a "July 4 Sale of Ideas." But this doesn't dim the fact that we—mostly Dick—keep on generating them, and writing them in a way we hope advertises how our beloved field is vibrant and rich and active.

The old-fashioned pre-blogging sounding rod for ideas that are cast upon the waters is called: *Students*. Here let me mention those of Dick's students who were familiar to me before I knew they'd been his students: Tim Budd, Chee Yap, Hana Galperin, Vijaya Ramachandran, Avi Wigderson, Dimitrios Serpanos, Dan Boneh, Anastasios (Taso) Viglas, Nisheeth Vishnoi, Parikshit Gopalan, Shiva Kintali. I've known Subruk Kalyanasubramanian and Danupon Nanongkai and co-advisee Farbod Shokrieh as his students; Nanongkai co-won the 2013 ACM PODC thesis award. There are

Davis Hall Room 338, Box 602000, Buffalo, NY 14260-2000
Tel: (716) 645-3180 Fax: (716) 645-3464

several field leaders among them—the greatest surprise for me was having referenced Tim Budd for OOP instruction all the way back to my inauguration of intensive C++ teaching in my department in 1996, and only discovering his advisor when Dick sent me a certain post draft. Another offspring was his great expansion of the potential reach of DNA computing after Len Adleman's proof-of-concept, along with co-founding and promoting the DNA Computing and Molecular Programming conference. While some of the particular ideas were argued as "homeopathically" impractical, a mark of Dick's influence is that the conference is still going strong after 20 years.

I've known Dick since STOC 1986 in Berkeley if I recall right. Neither of us is shy about talking with people at conferences, and we shared interest in logical independence related to P vs. NP and also chess. Where I really got to know him was at STACS 1994 in Caen, France, where I had two papers and he had one characteristically titled, "A New Approach to Information Theory." We got talking on two ideas, one joined by others for a STACS 1995 paper, the other joined by Dan Boneh in a draft paper still looking for a proof. In 1997 I proved a graph-separator theorem that is incomparable with Lipton-Tarjan's, and Dick invited me to talk on it at Princeton. Then I got diverted on a new but ultimately-refuted idea for the algebraic version of $\mathsf{P} \neq \mathsf{NP}$, then on chess research, but Boneh invited me to Dick's 60th birthday workshop in 2008 and we "hit it off" again. Dick started the blog while I was on sabbatical in Montreal, and contacted me around May 1 about an idea for attacking Graph Isomorphism via algebraic invariants involving the permanent. My role increased slowly from being one of several editors, often adding a paragraph or two to posts, until it was flumed into partnership by the August 2010 adventure of Vinay Deolalikar's $\mathsf{P} \neq \mathsf{NP}$ proof claim, which I have told in a special first chapter of the second blog collection published by Springer. We found then the full extent of how we mesh on attitudes to the field and community.

Dick and I share a fundamental kind of generosity that comes of implementing gratitude, one I recognize looking over the last paragraph that he's put in practice for far longer. Aspects of it are sometimes labeled "suffering fools gladly," but in this sphere it really involves enabling potential. It seeks comparative advantages. On the personal side I've been struck by how Dick is quantumly easier and more humble with undergraduate students than I am. The blog is a natural outgrowth, a stadium pipe organ not PA blare. We put much care into words; someone this year expressed surprise at how much thought goes into posts. The Knuth Prize cites contributions to foundations, yet strength and harmony come also from sinews, connecting tissue, the Pompidou Centre pipes that we aim to reveal. The Karp-Lipton theorem was a pillar of "Structural Complexity" in the 1980s, and program checking became one in the 1990s; in both self-reducibility is effectively combined with combinatorial ideas. I also have multiple feet in logical, structural, and combinatorial complexity, and I've been incredibly grateful that the blog gives an outlet for these combinations and for creative writing. We have done likewise in a joint textbook on quantum computing being published by MIT Press this summer, which streamlines it from linear algebra alone so as to be most accessible for undergraduates, yet progresses to some advanced topics within 175 pages. Sustained projects that give to the community also reflect the founder of the prize, and I warmly believe Dick would bear it well.

Yours appreciatively,

Kenneth W. Regan
(716) 645-4738, `regan@buffalo.edu`, `http://www.cse.buffalo.edu/~regan/`