Eric P. Tressler

Tressler@gmail.com

2800 Quebec St. NW, Apt. 744
Washington, DC 20008
(858) 699-5288 (Cell)

Education

- **University of California, San Diego**, La Jolla, CA. Fall 2004 – Spring 2010
  Ph.D. Mathematics, Spring 2010 (Advisor: Ron Graham)
- **Virginia Tech**, Blacksburg, VA. Fall 2000 – Spring 2004
  M.S. Mathematics, Spring 2004 (Advisor: Mark Shimozono)
  B.S. Computer Science, Graduated Summa Cum Laude, Spring 2004
  B.S. Mathematics, Graduated Summa Cum Laude, Spring 2003

Other Qualifications and Affiliations

- Member of the American Mathematical Society (AMS)

Research Interests

My primary research interests are graph theory, combinatorics, discrete geometry, and the development of algorithms in these fields. Within these overlapping areas, I have worked on both extremal problems, which are of mostly theoretical interest, and on the practical problems of analyzing real-world data sets. Some of these data sets have been very large (gigabytes or terabytes), and have required distributed compututation.

For real-world data, I am interested in finding good solutions to optimization problems such as route planning and graph partitioning. For these, I have used a range of evolutionary algorithms to approximate solutions to intractable problems. I have analyzed these algorithms and performed statistical analysis of simulation results using applications such as R and Sage.

Work Experience

- **Computer Scientist** February 2015 – Present
  Internal Revenue Service *Washington, DC*
  Full-time
  Supervisor: Chris Hess (`christopher.e.hess@irs.gov`, (202) 803-9209)

  As a researcher at the IRS, I am engaged in large-scale analysis of taxpayer data. This primarily consists of processing, visualizing, and analyzing networks of related individual and corporate entities using high-level programming languages such as Java. Specific work I have done at the IRS includes

  - writing and tuning algorithms to visualize very large graphs, on the order of 10-100M nodes;
  - implementing and using modern community detection algorithms;

– creating tools to help revenue agents and compliance officers handle large networks of taxpayer data;
– researching uses for personalized PageRank and related algorithms for the detection of fraud, tax evasion, and identity theft.

The IRS employs many researchers with extensive domain knowledge in economics, taxation, and global finance. A significant portion of my time is spent assisting domain experts who have encountered a technical barrier. For example, when a new tax evasion scheme is identified, it is natural to ask whether other instances of the scheme can be identified. This question leads naturally to the problems of motif detection and subgraph isomorphism; I help to formalize these problems and identify possible solutions, and then often go on to implement these solutions and provide data to the rest of the team.

▷ **Research Scientist** October 2010 – January 2014
HRL Laboratories, LLC *Malibu, CA*
Full-time (40 hours per week)
Supervisor: Roy Matic (`rmmatic@hrl.com`, (310) 317-5931)

At HRL Laboratories, I worked primarily on cryptography, cybersecurity, graph theory, and optimization. My responsibilities included

– working in teams to write research proposals to government agencies such as DARPA, DHS, and IARPA, as well as to HRL's owners, Boeing and General Motors;
– leading and participating in research efforts to satisfy the requirements of these contracts;
– minimally supervised research (both individual and cooperative) culminating in patents, internal white papers, and conference and journal publications;
– writing reports summarizing my findings to HRL management;
– presenting my findings periodically to HRL management and to the organization funding the research.

In particular, I led a team researching fully homomorphic encryption, leading to a secure pattern-matching protocol called 5PM, which allows for database searches that reveal neither the search terms to the server nor extraneous information to the client. This has broad implications, such as allowing for parties to perform medical or criminal searches without revealing unintended information to the outside world (which could, for instance, violate HIPAA).

Much of my work was for the defense industry (DARPA, DHS, and IARPA), which involved cybersecurity problems such as intrusion detection and damage mitigation. This included designing and simulating model networks, analyzing real-world networks, and evaluating different means of detecting and thwarting attackers. A goal of recent governmental cybersecurity efforts is to accomplish these goals in real time, so my work included data mining and analysis with (simulated) live data streams.

I worked on a similar project whose mission was to detect specific vulnerabilities in networks, and to find methods to reconfigure them to avoid catastrophes such as the cascading failure of the Northeast U.S. power grid in 2003. In doing this, I developed general robustness criteria with applications to distributed software and hardware agents, and wired and wireless networks.

While working for HRL, I was granted a Secret security clearance by the Department of Defense at the end of 2011.

▷ **Postdoctoral Researcher** June 2010 – October 2010
HRL Laboratories, LLC *Malibu, CA*
Full-time (40 hours per week)
Supervisor: Roy Matic (rmmatic@hrl.com, (310) 317-5931)

Prior to being hired as a full member of the research staff at HRL, I was a postdoctoral researcher, working on encryption and cybersecurity. This was the beginning of the work leading to the 5PM protocol mentioned above.

▷ **Instructor** March 2008 – June 2008
University of California, San Diego *La Jolla, CA*
I was the instructor for a precalculus course, in which I designed and delivered lectures, trying to use engaging examples to illustrate concepts. I also managed a teaching assistant and a grader, and determined the students' final grades.

▷ **Teaching Assistant** September 2004 – June 2009
University of California, San Diego *La Jolla, CA*
I have been a teaching assistant for differential, integral, and vector calculus, as well as advanced calculus, linear algebra, numerical integration, complex analysis, and statistics. As a teaching assistant, I explained concepts to students and helped lead them through exercises, in addition to grading their exams.

▷ **Teaching Assistant and Tutor** September 2003 – June 2004
Virginia Tech's Math Emporium *Blacksburg, VA*
I worked as a mentor to students who were learning basic math courses, such as linear algebra.

▷ **Intern** May 2002 – August 2002
U.S. Naval Research Laboratory *Washington, D.C.*

My job at the Naval Research Lab was to help design a protocol for communication among distributed software agents in a network; I primarily codified this protocol using SOAP, which is based on XML.

Selected Technical Skills

▷ C/C++ (including the Boost libraries and the GNU Multiple Precision Arithmetic Library (GMP)), Java, JavaScript, Python, PHP

▷ Mathematica, MATLAB, R, Sage

▷ HTML5, CSS, LaTeX

▷ Proficient in algorithmic analysis and optimization, machine learning, and evolutionary algorithms

Publications

▷ **5PM: Secure Pattern Matching**, (with J. Baron, K. El Defrawy, K. Minkovich, and R. Ostrovsky), proceedings of the 8th conference on Security and Cryptography for Networks (SCN) (2012), and the SCN 2012 special issue of *Journal of Computer Security*.

In this paper we consider the problem of secure pattern matching that allows single-character wildcards and substring matching in the malicious (stand-alone) setting. Our protocol, called 5PM, is executed between two parties: Server, holding a text of length n, and Client, holding a pattern of length m to be matched against the text, where our notion of matching is general and includes non-binary alphabets, non-binary Hamming distance and non-binary substring matching.

Employing a generic homomorphic encryption scheme, this allows the Client to perform a secure search of the Server's database, without revealing the search terms or the results of the search to the Server. Moreover, nothing is revealed to the Client about the database contents, except for the relevant results of the search.

▷ **Hypercube orientations with only two in-degrees**, (with J. Buhler, S. Butler and R. Graham), *Journal of Combinatorial Theory, Series A* **118** (2011), 1695-1702.

We consider the problem of orienting the edges of the n-dimensional hypercube so only two different in-degrees a and b occur. We show that this can be done, for two specified in-degrees, if and only if an obvious necessary condition holds. Namely, there exist non-negative integers s and t so that $s + t = 2^n$ and $as + bt = n2^{n1}$. This is connected to a question arising from constructing a strategy for a "hat puzzle."

▷ **Open problems in Euclidean Ramsey theory**, (with R. Graham), in *Ramsey Theory: Yesterday, Today and Tomorrow*, A. Soifer (ed.), Birkhauser, Boston (2010), 115-120.

This book chapter is a survey of open problems in Euclidean Ramsey theory, with emphasis on recent activity in the field.

▷ **Intersecting domino tilings**, (with S. Butler and P. Horn), *The Fibonacci Quarterly* **48** (2010), 114-120.

We examine a variant of the classical Erdős-Ko-Rado problem concerning maximal intersecting families of sets. In our construction, we consider tilings of $2 \times n$ and $3 \times 2n$ strips by dominos, and say that any two tilings intersect if they have a domino in common. We completely characterize the maximal intersecting families of these tilings.

▷ **Monochromatic triangles in $\mathbb{E}^2$**, *Geombinatorics* **XIX (3)** (2009).

We examine the current state of a long-standing conjecture about partitions of the Euclidean plane, and present a few new results.

▷ **The first nontrivial Hales-Jewett number is four**, (with N. Hindman), *Ars Combinatoria* **113** (2014), 385-390.

We give a proof by hand of the first nontrivial Hales-Jewett number, previously unknown. We also provide an algorithm that can prove this result quickly, as well as produce lower bounds for other Hales-Jewett numbers.

Patents

▷ **System and method for insider threat detection**, United States Patent 9,043,905 (26 May 2015)

▷ **Secure pattern matching**, United States Patent 9,009,089 (14 April 2015)