The Book Review Column[1]

by William Gasarch
Department of Computer Science
University of Maryland at College Park
College Park, MD, 20742
email: gasarch@cs.umd.edu

In this column we review the following books.

1. **Random Curves: Journeys of a Mathematician** by Neal Koblitz. Review by William Gasarch. Neal Koblitz is a mathematician who has lead an interesting life. How interesting? Read his autobiography and find out!

2. Review of **Games of No Chance (1998, Edited by Richard Nowakowski)**, **More Games of No Chance (2002, Edited by Richard Nowakowski)**, and **Games of No Chance III (2009, Edited by Michael Albert and Richard Nowakowski**. Review by William Gasarch. The mathematics behind games that do not involve any luck is deep. On the other hand you also want to learn how to WIN these games. These volumes contain several types of articles- mathematical, practical, natural games, unnatural games.

3. **Mathematical Treks: From Surreal Numbers to Magic Circles** by Ivars Peterson. Review by William Gasarch. A math book for the layperson. I would certainly give it to my great niece (she's 12).

4. **Decisions and Elections: Explaining the Unexpected**. by Donald G. Saari. Review by David Pritchard. Voting gives rise to many paradoxes. There are times where you should not vote for who you really want. Can you explain this? Donald Saari can!

5. **The Mathematics of Voting and Elections: A Hands-On Approach** by Jonathan K. Hodge and Richard E. Klima. Review by Mark C. Wilson. This is a textbook designed for a course on voting for non-majors.

6. **Branching Programs and Binary Decision Diagrams: Theory and Applications** by Ingo Wegener. Review by Samuel Johnson. Branching programs are a model of computation that we can actually prove things about! Binary Decision Diagrams are actually used in the real world. Read about both in this book.

7. **Quantum Computer Science: An Introduction** by N. David Mermin. Review by Eleanor Rieffel. As the title says, its an introduction to Quantum Computer Science.

8. **Cryptographic Applications of Analytic Number Theory: Lower Bounds and Pseudorandomness** by Igor Shparlinski. Review by Jeffrey Shallit. This book uses deep techniques of number theory and algebra to analyze problems arising in cryptography and algorithmic number theory.

9. **When Least is Best. How Mathematicians Discovered Many Clever Ways to Make Things as Small (or as Large) as Possible** by Paul J. Nahin. Review by Yannis Haralambous. How did people find max and min before calculus? How do people even now find max and min of discrete objects? Read the book to find out both the math and the history of such things.

10. **The Space and Motion of Communicating Agents** by Robin Milner. Review by Nick Papanikolaou. This book is about Robin Milner's way to model many computing agents using bigraphs.

BOOKS I NEED REVIEWED FOR SIGACT NEWS COLUMN

Handbooks and Edited Collections

1. *Algorithmic Algebraic Combinatorial and Grobner Bases* Edited by Klin, Jones, Jurisic, Muzychuk, Ponomarnko.

2. *Game of Life Cellular Automata* Edited by Adamatzky (This really is the title even though it doesn't look right.)

Cryptography and Coding Theory

1. *The Mathematics of Coding Theory* by Garrett.

2. *Understanding and Applying Cryptography and Data Security* by Elbirt.

3. *Secure Key Establishment* by Choo.

Combinatorics and Probability

1. *Erdos on Graphs: His Legacy of Unsolved Problems* Chung and Graham.

2. *Digital Dice: Computational solutions to Practical Probability Problems.* by Nahin.

3. *Elementary Probability for Applications* by Durrett

Semantics and Programming Languages

1. *Drawing Programs: The theory and Practice of Schematic Functional Programming* by Addis and Addis.

2. *Semantic techniques in Quantum Computation.* Edited by Gay and Mackie.

3. *From semantics to computer science: Essays in honour of Gilles Kahn* Edited by Bertot, Huet, Levy, Plotkin.

4. *Transitions and Trees: An Introduction to Structural Operational Semantics* by Hans Huttel.

Misc

1. *New Mathematical Diversions (revised edition)* By Martin Gardner.

2. *Polynomia and Related Realms* by Dan Kalman.

3. *Biscuits of Number Theory* Edited by Author Benjamin and Ezra Brown.

4. *Making Transcendence Transparent: An intuitive approach to classical transcendental number theory* by Burger and Tubbs.

5. *Mathematica: A problem centered approach* by Hazrat.

6. *Grammatical Inference: Learning Automata and Grammars* by Colin de la Higuera.

7. *Origins and Foundations of Computing* by Frederich L. Bauer in cooperation with Heinz Nixdorf MuseumsForum (that is not a typo, its really one word).

8. *Integer Partitions* by Andrews and Eriksson.

Review[2] of
Random Curves: Journeys of a Mathematician
by Neal Koblitz
Published by Springer 2008
390 pages, Hardcover, $40.00 on amazon new, $25.00 used
Review by
William Gasarch gasarch@cs.umd.edu

1 Introduction

Neal Koblitz is a mathematician who works on Number Theory and Cryptography. To quote Wikipedia *The use of Elliptic Curves in Cryptography was suggested independently by Neal Koblitz and Victor S. Miller.* However, this is not a math book. The first two words of the title are math-words, but the rest of the title gives away the content:

Random Curves: Journeys of a Mathematician.

This is Neal Koblitz's autobiography. Why did Neal Koblitz write an autobiography? Why did Springer publish it? Why did I read it (that one is easy— I got a free copy)? Should you read it? This review will give you enough information to decide for yourself.

Neal Koblitz has lead an interesting life and he is an excellent writer. The book has very little mathematics in it (that may be a corollary to saying that he has lead an interesting life). He has traveled a lot and has many opinions, mostly on academia, politics, and academic politics (not just in Math and CS— his wife Ann is a Women and Gender Studies Professor.) I found myself agreeing with some of it, disagreeing with some of it, and wanting to ask him follow up questions on some of it. Some of those follow up questions, with responses from him, are in the last section of this review.

His politics are mostly *left wing*. I do not like the term since *left wing* and *right wing* change over time. At one time Evolution was disliked by the left[3] since they (incorrectly) thought that Biological Evolution implied Social Evolution. Now it is disliked by the right since they (incorrectly) think that a belief in Biological Evolution indicates a lack of religious faith. There are other examples as well. Unfortunately, we are stuck with the term so I will use it.

2 Summary of Chapters

Chapters 1,2,3, 4 and 5 are entitled *Early years*, *Harvard*, *SDS*, *The Army*, and *The Spring of 1972*. These are mostly about his days as an undergraduate (Harvard), in the Army, and graduate school (Princeton). He was involved in many student protests against the Vietnam war, though as the quote below shows, he had a broader viewpoint. He disagrees with many on the left on both tactics and strategy and he discusses the disagreements intelligently. Here is an enlightening excerpt:

It should be stressed that the difference between the liberal and the radical wings of the anti-war movement were not just a matter of tactics. Most liberal activists believed in a single issue coalition

[2] ©2010, William Gasarch

[3] During the Scopes Trial, in 1925, the anti-evolution side was argued by the liberal William Jennings Bryan.

to end the War, and they thought that they could best forge such a coalition by talking almost exclusively of the U.S. deaths in Vietnam and the damage to the U.S. from the War. In contrast, our UAG (University Action Group) chapter consistently spoke about the Vietnamese victims, lauded the Vietnamese for their struggle first against French colonialism and then against the U.S., and combined anti-war activities with protests against other forms of social injustice, especially domestic racism.

Some on the left thought it was good to join the army (or agree to be drafted) and try to talk to soldiers directly about the war. He was one of them and did indeed join, though he never actually went to Vietnam. He was assigned Helicopter Repair (which he says he was terrible at) and, after passing out anti-war material, served time in a military jail.

Chapter 6 is entitled *Academics*. It is part of the idiosyncratic nature of the book that after 87 pages in which he never mentions any actual math he has a paragraph that only a number theorist could understand (full of *p-adics* and *Jacobi sums*). Of more interest are his comments on his wife Ann's academic career. He claims that after she did an excellent undergraduate thesis nobody encouraged her to go to graduate school. Why? Because she was a woman, and because she was from the lower classes. I cannot imagine someone being discouraged from going to grad school nowadays for either of these reasons. Perhaps I lack imagination. This chapter is a real eye opener to how things were way back in 1973. Later in the book (Chapter 13) there is more on Ann not getting jobs for these two reasons, as well as because of her field (History of Science and History of Women) and because she was a leftist feminist. Again, I cannot imagine these being reasons nowadays.

Chapters 7,9,10,11,12 are entitled *The Soviet Union*, *Vietnam part I*, *Vietnam part II*, *Nicaragua and Cuba*, and *El Salvador and Peru*. (I'll come back to chapter 8 later.) These chapters are about his travels to the countries in the titles. He has sympathy with the people of these countries and their leftist politics. He is not naive about the Soviet Union; however, he seems naive about some of the other places. These chapters offer interesting though biased views of these countries.

Chapter 8 is entitled *Racism and Apartheid*. Recall that South Africa had a government whose very laws were oppressive to blacks. By law, whites and blacks were separated and blacks had much worse facilities. This was called apartheid. Many organizations, including schools, had investments in South Africa. There was a big movement called divestiture— stop investing in South Africa. This chapter tells about Harvard's policy and how Neal Koblitz (and others) tried to fight it.

Chapter 13 is entitled *Two Cultures*. It is about the differences between the Sciences and the Humanities. Since he is married to a Social Scientiest, he has seen both cultures. This chapter is interesting and covers a lot of ground. The most interesting part was his discussion of how he helped Serge Lang in his campaign to make sure that Huntington (a social scientist) was not admitted to the National Academy of Sciences. See my questions to Neal Koblitz below for more on that.

Chapter 14 is entitled *Cryptography*. He notes that many papers in Cryptography have errors in them or are not practical. And he notes that, unlike an incorrect paper in (say) recursive algebraic topology[4] a paper in crypto may actually be read and used. Hence errors are much more important. He also points out that the computer science culture of rushing things out to conferences is one of the causes of the errors. I doubt anyone in Cryptography would disagree with any of the above.

[4]This is not really a field. It is my stand in for any rather abstract field of Mathematics.

He then suggests that Crypto papers should stop using the word *proof* and use the word *argument*. He also suggests that the entire field of *Provable Security* is bogus. I find his arguments compelling for the field in its *current state*. However, theoretical computer science changes and the models move towards practicality over time. Some fields do not get there. Why single out this field?

Chapter 15 is entitled *Education*. I expected him to blast the American Education System. While there is some of that, he also talks about education in other countries and his own (largely successful) attempts to introduce math in a fun way to some middle schools. (Much of this has been in conjunction with Mike Fellows.)

Chapter 16 is entitled *Arizona*. Ann got a job in Arizona[5] and the first part of this chapter is about buying land there. This part is serene and noncontroversial. Later in the chapter he discusses a controversy that Ann got involved with on the question of whether the Hohokam Indians (who lived in Arizona) were a warlike tribe or not. The conventional theory was that the Hohokam were not warlike. There was massive evidence for this. Then some archaeologists who had the preconceived notion that War is inherent in any society claimed to find evidence that the Hohokam were warlike. Here is an example of their evidence:

On at least three occasions they write about the insights that were derived from late night male bonding sessions around the campfire.

Ann wrote an article that was *not* on archaeology but rather on *meta-archaeology* (a word that probably does not exist). Her main point was that the archaeologists' macho hang-ups led them to become enthusiastic about a theory that was based on flimsy evidence.

3 Opinion

What I have discussed above is less than a tenth of what is in this book. There is a lot more and much of it is interesting. The book is very readable and has interesting things to say about academia, politics, and academic politics. You may well disagree with what he says; however, if you are open minded then you will learn much from this book.

Neal Koblitz does not just have opinions. He acts on them. He has protested, been arrested, joined the army, and has made waves wherever he was. I find this quite admirable. I am surprised he has gotten any math done.

4 A List of Questions for Neal Koblitz

There are several points in the book that made me or members of my book club (who read the book) want to ask Neal a question. I emailed Neal the questions. He was happy to get them and emailed me responses. Below are the questions and his responses.

1. Page 26.

   ... since 1965 when I read the article by Kahin and Lewis in the Bulletin of the Atomic Scientists, I firmly believed that the Vietnamese communist guerrillas were fighting for the interests of the people, and that the U.S. was totally wrong.

[5]His job is at The University of Washington. Ann and Neal have often had jobs in different locations.

Given the brutality of the North Vietnamese communists when they conquered the south do you really believe they were fighting for the interest of the people?

Neal Koblitz's Reply:

I don't agree with the premise of this question about the "brutality" of the Vietnamese victors. U.S. officials had predicted a "bloodbath" if the NLF and North Vietnam won, but none occurred. Later, when a flood of "boat people" left Vietnam in the late 1970's, the U.S. again claimed that the Vietnamese victors in the war were a bunch of brutes. But for the most part the "boat people" were economic, not political refugees.

Of course, there were some reprisals against the South Vietnamese who'd collaborated with the American occupiers. But they were milder than most people expected. I recall reading that after the American Revolution, Tories (Americans who had supported the British) were tarred and feathered and sent off to Canada. One could ask: "Given the brutality of the victorious forces in the American Revolution, do you really believe that George Washington and his men were fighting for the interests of the American people?" To which I would answer "yes". I also answer "yes" to the analogous question about the Vietnamese.

2. Page 72. Admiral Thomas H. Moorer, Chairman of the Joint Chiefs of Staff was going to give a talk at Princeton to show that the anti-war movement was dead. The University Action Group (UAG) of which you are a member disrupted this talk which (a) shows that the anti-war movement is not dead (yeah!) and (b) makes him unable to give his speech (boo!). The yeah and boo are mine. Curtailing free speech that you happen to not like is a dangerous precedent. You point out that you did not violate any university rules. I do not care. The ideal of free speech is nonpartisan.

   Neal Koblitz's Reply:

   Conservative students claimed that we had prevented Admiral Moorer from speaking, but in reality we had not. I remember my own personal contribution to the heckling. At one point the Admiral was talking about the "winding down" of the war and the decrease in the number of American casualties. I angrily yelled out "What about the Vietnamese?" I heard what he was saying, and he probably heard me. No one's free speech was being prevented. The reason why he stopped speaking after 15 minutes was presumably because his film crew could not get footage that would show the success of his visit to Princeton, and hence his talk would not have any propaganda value for the Pentagon. So the purpose of our protest was achieved.

3. Page 89. Your wife's undergraduate thesis was about Darwin being a racist. (a) Was he a racist compared to his contemporaries? (b) Why does this matter? (c) Did it influence his work? Just proving that he is a racist seems like a factoid unless it is connected to other issues.

   Neal Koblitz's Reply: Ann's undergraduate thesis was not "about Darwin being a racist", but rather about the complicated relationship between the social Darwinists and the eugenicists in America in the late 19th and early 20th centuries. The part about Darwin's racism was a small part of the dissertation, although it was apparently the part that most upset a few of her professors, such as C. C. Gillispie, who virtually worshiped Darwin. (a) Yes, he was a racist compared to other major contemporary evolutionary biologists, such as Alfred

Russel Wallace in Britain and Kropotkin in Russia. (b) This matters because many people used Darwinism ("survival of the fittest") as a rationale and justification for racial inequality and discrimination, and in evaluating Darwin's legacy it is important to know whether or not he shared some of the blame for this misuse of his theories. (c) It didn't influence his work on plants and non-human animals, but it influenced his and other people's attempts to apply his theories to explain inequalities among human populations.

4. Page 93 (and elsewhere). You claim that at one time being on the Left would hurt someone in (say) a history department. I have heard that now these departments are dominated by the Left. Is there still a problem with political bias now?

   Neal Koblitz's Reply:

   I commented that some faculty members in the 1960's intensely disliked student leftists and let that influence the opinions expressed in letters of recommendation, and that the main reason for the intensity of their antipathy to leftist students was that we were disrupting the university – in other words, we were not just theoretical leftists and did not confine our protests to non-university issues. I don't think there's anything analogous to that now.

   In our time conservative pundits frequently complain about "leftist" domination of academia. But what the conservatives really mean by "leftist" is liberal (or even middle-of-the-road – remember, these are the same people who call Obama a socialist). Liberal is not the same as "leftist". In fact, many liberal academics dislike leftist radicals as much as they dislike conservatives.

   In any case, my own impression (and Ann's) is that the main forms of bias in history departments are not related to the liberal/conservative or leftist/rightist divides, but rather to other things. For example, there are biases against people from lower-middle class background, there are still biases against women (sometimes, sadly, by "queen bee" senior women faculty), and of course there are biases against people who oppose the currently-fashionable theories. (Just try to get a job at Duke if you're an opponent of post-modernism.) The biases vary tremendously from one college to another, so the good news is that if one place is biased against you, there are still about 2999 more colleges in the U.S. that you can try.

5. Page 98. You comment that Shafarevich should not be kicked out of the NAS for his anti-Semitic views. I agree- the only criteria should be the quality of the science. You also say that it would be hypocritical since the American Racist William Shockley remained in the NAS until his death in 1989. Do you think William Shockley should have been kicked out? Should personal views have *any* bearing on membership in the NAS?

   Neal Koblitz's Reply:

   The point is to be consistent. It is reasonable for an organization – even an organization of scientists – to have some non-scientific criteria for membership. But if you kick out one guy for being a racist against one group (in this case Jews), you should kick out the other guy for also being a racist (against blacks). In practice, the NAS does not normally have a policy of non-scientific criteria for membership. I also thought that on a professional and interpersonal level Shafarevich had a very good reputation, even among Jews. His anti-semitism was theoretical, not operational.

6. Page 102.

   Many leftists in the West were much more inclined to look for models of revolutionary idealism in the Third World (China, Cuba, and later Nicaragua) than in the Soviet Union.

   China and Cuba have awful human rights records and suppress basic freedoms such as freedom of speech and religion. How can these be good models? (The usual answer I hear is that the United States is worse. This does not answer the question.)

   Neal Koblitz's Reply: In the U.S., unlike in many other parts of the world, "human rights" has a rather narrow definition, usually just freedom of speech (meaning mainly freedom from government reprisals for criticizing the government) and religious freedom. Even in the U.S. some people favor a broader definition; for example, in his famous Four Freedoms speech, Pres. Roosevelt included "freedom from want" as a basic human right.

   A country like Cuba should be compared to other poor countries, in which case it comes out very well by many criteria of human rights, such as "freedom from want", women's reproductive rights, and the right to medical care (in the latter case, if you believe Michael Moore, it compares well to the U.S., too).

   Regarding freedom of speech, the custom in the U.S. is again to adopt a narrow definition. When we use the term, we usually don't think of free speech in the private sector. Because most Americans in the private sector don't have much job security (with some exceptions, such as tenured professors and workers with strong unions), it's easy to fire someone for his/her opinions. To put it another way: An American who tells everyone "Obama is an idiot" would be less likely to suffer any reprisals from his government than a Cuban who tells everyone "Raul Castro is an idiot". On the other hand, an American who proclaims that "my boss is an idiot" would be more likely to be fired than a Cuban who proclaims the same thing.

   There's also the issue of SLAPP lawsuits, which intimidate people who criticize a commercial product. It's true that Oprah won in court on this issue. But people with less money for lawyers than Oprah has can be effectively silenced. Again, in Cuba you can freely say "this product sucks" and be sure that no one will sue you.

7. Page 130. I also recall the *divest out of South Africa* movements. How come there has been no *divest out of XXX* movements or other such things for today's regimes that are far worse than South Africa was? (You can fill in XXX with Sudan, Uganda, Saudi Arabia, and many others.)

   Reply from Neal Koblitz:

   A good question – in fact, it was the very first question in the "question-answer" publication that my friend Luther Ragin and I wrote in 1979 (called "The ABCs of Divestiture"). So I'll just quote from that brochure that was published 31 years ago by the Harvard anti-apartheid movement (please forgive the lack of brevity):

   QUESTION: Why South Africa? Aren't there other equally repressive regimes?

   ANSWER: South Africa is a special case for several basic reasons. (1) It is the only country in the world in which racial supremacy is the central element in the ideology of the entrenched

ruling party and the basis for the entire legal, political, economic and social system. Never since the Third Reich has a tyrannical system been so thoroughly grounded in racial oppression. (2) U.S. companies provide vital support to the South African economy, especially in its most strategic sectors (they provide 43% of its petroleum, control 23% of the auto market and 70% of computer sales, and South Africa's multi-billion-dollar SASOL coal-gasification project is under the direction of the Los Angeles-based Fluor Corporation). (3) Because a large proportion of the U.S. population is black, and because the nation as a whole remembers its history of slavery and the recent civil rights movement, Americans should react with special concern to racial oppression. The type of human rights violations that pervade all areas of South African life speaks with particular intensity to Americans. (4) Especially since the Nazi Holocaust international revulsion against crimes of racial persecution (as expressed in the Nuremberg Principles and the Genocide Convention) has been particularly strong. In the case of South Africa this revulsion has led to a broad and intensifying international campaign against the apartheid government.

"Of course, there are many other oppressive regimes around the world. We believe in encouraging efforts to struggle against all human rights violations. But the impracticality of simultaneously cleansing the world of all evil should not provide an excuse for doing nothing in a particularly shocking case."

8. Page 130. Do you think that the divestiture movement helped bring about actual divestiture? Did it help bring down apartheid?

   Reply from Neal Koblitz:

   I think that the divestiture movement was effective in discouraging new investment in South Africa, but did not cause a significant number of companies to pull out if they were already there. However, this movement did play a role in galvanizing U.S. opposition to apartheid and increasing pressure to end it. At the end of the chapter on South Africa I give some examples of the effects of the movement.

9. Page 232.

   When looking for roofers we saw ads in the Phoenix Yellow Pages that included the words "no language barrier" as a code for "we don't have Spanish speaking workers." Since companies with Spanish-speaking workers always have English-speaking supervisors, there was no practical reason why a customer should care.

   I have had it happen that the supervisor is there at the beginning but then takes off, and I have had questions that I could not get across. This is a minor point but this is one case where I know from personal experience that you are incorrect.

   Reply from Neal Koblitz:

   I apologize for the inaccuracy – I should have included a phrase such as "in our experience". In our experience, we're always given a cellphone number of the boss or supervisor when he leaves. We've had several major projects on which the workers were Spanish speaking, such as our roof in Phoenix, our patio also in Phoenix, and pre-commercial thinning on some forest property we own (see the answer to question 12 below). We both speak Spanish and have

exchanged pleasantries with the workers, but we have never had any reason to talk to any of the workers about any substantive issue connected to the project; rather, we always spoke to their boss (in English) about such matters.

10. Page 237. This story is from Nicaragua in 1987.

    The only woman not politically on the left was Emilisa Callejas from Honduras. She was the sister of a candidate for the presidency of Honduras (who was later elected). At one point she objected to a draft statement from the group condemning "the actions which the U.S. government is conducting to finance and maintain the war in Central America." Emilisa said that in order to be evenhanded, the group should also condemn Soviet interventionism. Everyone reacted angrily to that, and she withdrew her amendment, after which the statement passed unanimously.

    Actually condemning both sounds good to me, not for evenhandedness but for accuracy. What do you think?

    Reply from Neal Koblitz:

    The Soviet Union gave (not very generous) foreign aid to the leftist government of Nicaragua, as did several West European countries. Other than that, the Soviet Union had no significant involvement in Central America. In contrast, the U.S. put billions of dollars into financing the Contra war against Nicaragua and the brutal counter-insurgency in El Salvador. So it would have been inaccurate to "evenhandedly" condemn both the U.S. and U.S.S.R.

11. Page 287. You have just told the story of how you helped Serge Lang make sure Huntington did not get into the National Academy of Sciences (NAS) since the math that he used in his papers was bogus. You then comment:

    It was not only because of his misuse of mathematics that Lang and I were glad to see Huntington voted down by the NAS. During the Kennedy and Johnson administrations he had been one of the architects of American policy in Vietnam and had played a key role in establishing the "strategic hamlet" program. In a 1967 article in Foreign Affairs Huntington had expressed satisfaction that the influx of refugees to the cities (caused by the bombing of the countryside) would hasten what he called South Vietnam's "urbanization" and "modernization" at the same time as it undercut potential support for the guerrillas.

    If a left wing social scientist used bogus math in their articles would you also fight against the case? Would Serge Lang? Should political views and actions have *any* bearing on membership in the NAS?

    Reply from Neal Koblitz:

    Yes, I'm also against leftists who misuse mathematics. For example, one of my main opponents in the debate about provable security – which from my point of view is a case of the misuse of mathematics – is Oded Goldreich. He's actually someone whom I greatly admire, not only for his contributions to theoretical cryptography, but also for his leftist politics. On his website he identifies himself as non-religious, socialist, and strongly opposed to Israeli policy on the

Palestinian question. This takes some courage, living as he does "in the "belly of the beast". So his clumsy attempt to block publication in J. Cryptology of my first provable security paper with Menezes was particularly unpleasant to me because it was done by a fellow leftist.

To put it another way: If the person using bogus math is a leftist rather than a rightist, then I would still fight against it, but I wouldn't enjoy the fight as much. Huntington was easy to demonize (since he really was a demon), so the fight brought me (and Lang) more satisfaction.

12. Did you ever build your dream house on Copper Mountain in Arizona?

Reply from Neal Koblitz:

No, Ann and I had to give up on the dream house because of outrageous cost overruns. In late 2007 we switched to our Plan B, which was to buy some land in Washington State. That turned out very well, and we now regard Plan B as much more sensible than our earlier Plan A (the house on Copper Mountain). We own two forest properties (totaling 283 acres) two hours north of Seattle, near the Canadian border. We've had to learn a lot about forest ecology, and it's been great fun. If you or any of your readers feel like visiting the Seattle area and getting a highly non-touristy view of the Pacific Northwest, we'd be glad to take you hiking in our beautiful forests.

Joint Review of[6]
Games of No Chance (1998, Edited by Richard Nowakowski)
and
More Games of No Chance (2002, Edited by Richard Nowakowski)
and
Games of No Chance III (2009, Edited by Michael Albert and Richard Nowakowski
Published by Cambridge Press)

Review by
William Gasarch gasarch@cs.umd.edu

1 Introduction

These three books are actually Workshop proceedings and hence are collections of articles. All of the articles are about Games that do not involve luck; however, there is still a great deal of variety within this field. Rather than review them book-by-book, I will review them topic-by-topic.

We divide the books into three broad topics: (a) Combinatorial Games, (b) non-combinatorial games that people do not usually play, and (c) real games.

2 Combinatorial Game Theory

Here is an easy example of a combinatorial game:

[6] ©2010, William Gasarch

There are n sticks on the table. During a player's turn he removes 1,2,3 or 4 sticks. The player who cannot move loses.

The question to ask is: for which values of n does player I have a winning strategy? We leave this to the reader.

Here is another easy example of a combinatorial game.

There are two piles of sticks on the table. One has n_1 sticks, one has n_2 sticks. During a players turn he removes 1,2,3 or 4 sticks from pile 1 or remove 1,3, or 4 sticks from pile 2. The player who cannot move loses.

The most general form of combinatorial game is as follows: The board is a directed acyclic graph. Originally a token is placed on a vertex. During a players turn he moves the token from its vertex to a neighbor along a directed edge. The player who cannot move loses.

Given a graph one can solve this problem using Sprague-Grundy Numbers. Often the game can be split into two subgames that can be solved separately and then combined. This is the case for the two-pile game above. This is the real win of the method. However, sometimes the graph may be rather large and is hard to decompose, so one looks for shortcuts for particular games.

All three books have articles on combinatorial game theory or variants on such games. We describe some of these articles.

1. *Take Away Games* by Michael Zieve. From *Games of Chance*. Let $f : N \to N$ be a function. There is a pile of sticks on the table. On the first move the player may remove any number of sticks so long as there is at least one left. In all future moves, let n be the number of sticks removed in the previous turn. The current player may remove 1 or 2 or $\cdots$ or $f(n)$ sticks. For which functions f, and which initial number-of-sticks, does which player win? The article explores this for linear f.

2. *Richman Games* by Andrew Lazarus, Daniel Loeb, James Propp, and Daniel Ullman. From *Games of Chance*. The game is played by Alice and Bob; however, there is no notion of first or second player. Let G be a graph. Some of the vertices are labeled ALICE and some are labeled BOB. A token is placed at one of the vertices. Alice and Bob begin with one dollar each. During a turn they place a sealed bid (any real number between 0 and what they have). After the bids are revealed the player who bid more gets to decide where to move the token (along an edge out of the current vertex, to a neighbor); however *the other player gets the money bid!*. (There are special rules for ties.) The first player to get to a node that bears his or her name wins. This article tells how to find the optimal strategy for any acyclic directed graph.

3. *Scenic Trails from Sea-level Nim to Alpine Chess* by Aviezri Fraenkel. From *Games of Chance*. This is a 30-page article that develops the theory of combinatorial games from the ground up. It starts with simple examples and ends with quite complex ones. (Franekal has other surveys in these volumes as well.)

4. *What is a Game* and *Impartial Games* by Richard Guy The first article defines combinatorial games rigorously and gives many examples. The second looks a subset of such games where, at each move, both players have the same options. (Guy has other surveys in these volumes as well.)

5. *The Gamesman Toolkit* by David Wolfe. This article describes a computer package that is useful to analyze combinatorial games.

6. *A Simple FSM-based proof of the Additive Periodicity of the Sprague-Grundy Function of Wythoff's Game* by Howard Landman. From *More Games of Chance*. Wythoff's game is as follows: Initially there are two piles of sticks which, a in the first pile and b in the second pile. We denote the game position (a, b). During a turn a player can remove any number of sticks from one pile, or the same number of sticks from both piles. The Sprague-Grundy Function for this game was known to be periodic. This article gives a simplified proof of this theorem.

7. *Advances in Losing* by Thane Plambeck. From *Games of No Chance 3*. The usual Sprague-Grundy theory works very well for the games where the first player who can't move *loses*. What if the first player who can't move *wins*. While there are some scattered results for particular games, there is no general theory. This article is an attempt to make one.

8. *The Game of End Wythoff* by Aviezri Fraenkel and Elnatan Reisner. From *Games of No Chance 3*. End-Wythoff is as follows: Initially there are several piles labeled $P_1, \ldots, P_L$ of sticks. We assume that there are a_i sticks in pile P_i. During a move a player can remove any number of sticks from any one pile or the same number of sticks to the two piles at the ends. (When a pile is empty it is removed.) This article describes winning positions and strategies for this game.

3 Non-Combinatorial Games that People Do Not Play

The book also introduces several games that are not combinatorial games. The chapters introduce the games and tell what is known about them which usually is not much.

1. *The Angel Games* by John Conway. From Games of No Chance. The Angel and the Devil play their game on an infinite chessboard. The Devil removes a square during his turn. The Angel moves (say) 1000 squares during his turn. Can the Devil strand the Angel. When this chapter was written this was not known. Now it is: see `http://en.wikipedia.org/wiki/Angel_problem`

2. *Monotone Subsequence Games* by M.H. Albert, R.E.L. Aldred, M.D. Atkinson, C.C. Handley, D.A. Holton, D.J. McCaughan, and B.E. Sagan. The following is well known: for all sequences of $n > (a-1)(d-1)$ distinct elements from a linear order there must be either a monotone ascending subsequence of length a or a monotone decreasing subsequence of length d. This inspires the following game. Let L be an infinite linear order. Let a, d be naturals. Alice and Bob play as follows: Each picks an element of L and they get written down: $a_1, b_1, a_2, b_2, \ldots$. The first one to play an element that completes either an ascending subsequence of length a or a descending subsequence of length d wins. The subsequence can use any of the numbers played. The theorem implies that the game cannot go any more than $(a-1)(d-1)$ moves, even with poor play. What if both players are awesome players (play perfectly). Then who wins? This question is explored.

4 Real Games

Most people do not play NIM. They play Chess, Backgammon, Go, and other Real Games. There are several articles on real games in these books. While these articles seem quite good, they are not theoretical.

1. *Chess:* There are two articles on Chess Endgames in *Games of No Chance*, two articles on Chess Endgames in *More Games of No Chance*, and none in *Games of Chance III*. One article of particular interest was *On Numbers and Endgames: Combinatorial Game Theory in Chess Endgames* which tries to use the techniques of Combinatorial Game Theory in chess.

2. *Go:* There are four articles on Go in *Games of No Chance*, three articles on Go in *Games of No Chance*, and four article on Go in *Games of Chance 3*.

3. *Checkers:* There are two articles on checkers in *Games of No Chance* but none in any of the other books.

4. *Miscellaneous:* There is one article on each of the following: Nine Men Morris (Games of No Chance), Dukego (More Games of No Chance), Hex (More Games of No Chance), Hypercube tic-tac-toe (More games of no chance).

5 Opinion

The articles are, overall, well-written. This is not some hastily put together collection of articles that often comes after a workshop. The articles range over a wide variety of types of games. The good news is that some of them will interest YOU. The bad news is that some of them won't. You can guess my tastes by seeing which articles I described in more detail.

There is an endless supply of ideas for projects in these articles. The projects could be on a variety of levels: high school, College, even graduate students.

The usual question: Should you buy a copy yourself or have your school buy a copy. This is such a 1990's question. If you Google the names of these books you will find where to download most of the articles. The site seems to be official. I applaud Cambridge Press, the editors, and the authors, for doing this.

Review[7] of
Mathematical Treks:
From Surreal Numbers to Magic Circles
by Ivars Peterson
Published by the MAA, 2002
170 pages, Softcover, $30.00

Review by
William Gasarch gasarch@cs.umd.edu

(Disclaimer: The first paragraph of this review is similar to the first paragraph of a joint review I did for several *Math for the layperson* books.)

[7]

This book is in the category *Mathematics for the layperson.* Hence the question to ask is not *Will I learn something I don't already know.* I suspect that 9/10 of my readers already know at least 103/104 of the material in this books. The question is *Would this book be a good gift for my mathematically-inclined great niece?.* This boils down to *are they well written?* and *is the choice of topics appropriate?.* Even if you know the material there may still be some pleasure in reading it to see how it would be presented to someone who does not. And there is indeed (at least for me) some new material of interest in all of them.

Mathematical Treks is a collection of 33 very short expository articles on various branches of mathematics. Some are on old (to me) topics (e.g., the game of Sprouts, Waring's theorem) and some are on new (to me) topics (e.g., the mathematics of playing Dreidel, the shape of home plate in baseball). The articles are well written but too short. Just as I am getting interested they seem to stop. In the modern web-age this may be okay— your great niece can get interested an then look up more on the web.

Here are a few things I learned:

1. The shape of the home plate in baseball is impossible. According to the rules of baseball there is a 12-12-17 right triangle.

2. In football it is thought that time-of-possession is a key to winning. This seems to be false.

3. If in poker you allow some cards to be wild then the probabilities of getting various hands changes (this is obvious). However, since some hands can be interpreted two ways it is impossible to assign a ranking of hands. (There are ways around this.)

4. Personal computers have gotten so powerful that some of the recent searches for the largest primes have been done by them, not by big Clay (or other) computers.

5. The following problem is well known: Given n points in the plane you want to connect them up (possibly using new points as well, called Steiner points) so that the sum of all the distances between pairs of points is minimized. There is a discrete version of this problem that seems much harder.

For just getting a taste of a subject this is a fine book. For more depth there are better books, such as *Professor Stewart's Cabinet of Mathematical Curiosities* by *Group Theory in the Bedroom and Other Mathematical Diversions* by Brian Hayes. or anything by Martin Gardner.

Review of

Decisions and Elections: Explaining the Unexpected [8]

Author: Donald G. Saari

Publisher: Cambridge University Press, 2001

ISBN 0-521-80816-2, $32.99

Reviewer: David Pritchard (daveagp@gmail.com)

[8]

1 Overview

In *Decisions and Elections: Explaining the Unexpected*, Donald Saari gives a highly accessible introductory tour of decision theory: the study of mechanisms that amalgamate several separate preferences into a single preference (for example elections, in which voters' preferences over candidates are combined). The book has an excellent style that combines a deep understanding of mathematics, good pedagogy, and lighthearted prose; Saari provides compelling arguments, high-level insights, and interesting applications.

The book combines the nice flavors of paradoxes and puzzles, important real-world applications, and a good sense of humor. There are a number of examples drawn from engineering and group dynamics which make interesting food for thought. One example is about a non-voting chair of a meeting: even if she has no vote and thus seems powerless, she can tremendously determine the outcome of an election (page 91). Another example (page 54) is that in an engineering company, when solving a huge problem like the design of an aircraft, divide-and-conquer/decentralization is not always a good idea, as it can introduce new problems due to having to combine the answers to the various parts.

The book is aimed at undergraduates and professionals according to its introduction, and it seems it would serve this purpose well. I think many other people (e.g. researchers from related fields) would appreciate the book as an interesting, relatively quick read. The pedagogical style mostly eschews formality except where it is needed. Saari introduces new terms only after providing enough background to warrant them; I wish all mathematics authors had this skill! An example of the level of discourse is that Saari takes the time to explain a proof by contradiction ("If the Moon were Purple," page 47). Thus, for example, I think that the book would make nice secondary reading material for a game theory class aimed at people from other disciplines. I would urgently recommend any future teachers/researchers in decision theory to read this book.

2 Summary of Contents

The central formal result in the book is Arrow's theorem (1951): any group ranking mechanism with at least 3 candidates is either a dictatorship, fails to respect unanimous pairwise rankings, or allows some pairwise rankings to interact with others, i.e. fails to have "Independence of Irrelevant Alternatives." Saari gives a full proof, but defers it to the appendix due to its technical nature. Literature references also occur only in the appendix, giving the book high readability but also giving the interested reader pointers to more details. Proofs are usually sketched, and sometimes omitted. The flip-side of this approach is that sometimes the reader is not precisely sure what Saari means; although usually, ambiguities either can be clarified with a little effort of the reader, or are made clear later in the book.

Saari spends a considerable amount of time looking at the ramifications of Arrow's theorem, and discussing variants. Over the course of the book, one accumulates the view that Arrow's theorem should be thought of as saying that Independence of Irrelevant Alternatives (IIA) is too strong to expect from a reasonable voting system. Here are two nice results in this vein: first, even with a weaker version of IIA where we consider triples instead of pairs, Arrow's theorem still holds (Section 5.4); second, if we replace IIA by a more detailed variant "Intensity of Binary Independence," then Arrow's theorem fails to hold (Section 6.5). The book acts in part as an introduction to some of Saari's research from the last two decades, e.g. both of the aforementioned results come from

publications of Saari and coauthors.

Sen's theorem (1970) is discussed at length. In a decision mechanism, a given voter is "decisive" over two given alternatives if the mechanism's ranking of those two always agrees with that voter. Then Sen's theorem says that for any ranking mechanism with at least two decisive voters (over any two pairs of alternatives), that mechanism will sometimes disagree with a pairwise ranking agreed on unanimously by all voters. Saari phrases this differently: if unanimous pairwise rankings are to be respected, then the mechanism sometimes produces cyclic preferences (i.e., not a ranking). Saari gives a number of examples which illustrate applications — sharing an apartment, book censorship, and a stock-buying club — which at same time illustrate the most important ideas in the full proof of Sen's theorem.

An explicit mantra in the book has to do with what goes wrong in the standard impossibility results of Arrow, Sen, and others. Saari notes that in many cases, a potential explanation is that we are disregarding valuable information: e.g. in Arrow's theorem, we essentially throw away the voters' full preference lists and focus only on pairwise rankings. We read on page 97 that "suspect outcomes can occur should the decision procedure ignore portions of the available information." Saari notes more concretely that even irrational voters with cyclic preferences can submit pairwise rankings, but if we want to think rationally about a good voting procedure, we should certainly demand that the voters be rational!

Saari pinpoints a certain sub-structure, a "Condorcet tuple," as the source of many problems. E.g. in a Condorcet triple, we have three players, one of whom prefers outcome A to outcome B to outcome C, another who prefers B to C to A, and a third who prefers C to A to B; then any global ordering upsets a majority of the voters in at least one pairwise comparison. Small modifications to this sort of example are fodder for the book, and Saari describes a certain result saying that indeed all impossibility results of a certain type come from modifications of Condorcet tuples, although I did not find his description of this result clear enough to properly parse.

If one were to read Saari's book with the goal of choosing a voting system to put in to practice, the reader would be very persuaded to use the Borda Count: each voter ranks all n candidates and gives n points to their top-ranked one, $n-1$ to their second-ranked one, and so forth; then we order the candidates by total points. This avoids some problems of the usual plurality vote (where each voter contributes just one point to their favorite candidate) and has several other nice properties, for example the Borda Count is the only ranking mechanism which is never backwards in all pairwise comparisons, i.e. it ranks at least one pair of candidates in accordance with the majority of voters (Section 5.4.3). On page 193 Saari mentions a few other natural conditions that together get "close to creating an axiomatic representation of the Borda Count" although he later (in Section 8.3.2) tempers this by pointing out that axiomatic representations alone do not warrant a given protocol is best. For the election-designer, Saari's book has no explicit advice (unfortunately) on what to do if more than one candidate should be elected, although there is certainly lots of implicit advice in the book. I should also note that, according to Wikipedia, the Borda Count is generally not used in practice, but replaced by other mechanisms with better properties; it would have been nice if Saari attempted to describe what sort of sophisticated voting methods are used in practice and what distinguishes them from the Borda Count.

3 Style and My Opinion

The book is sprinkled with a lot of specific small abstract examples, and also relevant real-world examples steeped in modern culture. The initial abstract examples in the first couple of chapters illustrate that even for a fixed set of preferences, different choices of reasonable-looking voting procedures can yield drastically different results; and often, the results of a vote seem clearly not to agree with the intent of the voters. Some of the real-world examples include Ross Perot's Reform Party, the election of Jesse "The Body" Ventura, and scoring in professional figure skating (where IIA fails to hold). It is quite helpful to see these connections between theory and real life. The ubiquitous Prisoner's Dilemma is given an atypical presentation — usually notions from strategic games are used but since this is the only strategic game in the book it would not make sense. I liked the Prisoner's Dilemma example of two lanes merging on the highway, which I had not seen before. (Here two drivers may either be polite or a jerk, where each driver gets home faster as a jerk regardless of the other drivers, but two polite drivers get home faster than two jerks.)

I have a few general criticisms of the book. The lack of formality is a promising approach but sometimes important terms are used before they are introduced or informally defined. E.g. I was several times confused whether a "decision procedure" or "choice procedure" is supposed to give a ranking of candidates, or just a (possibly cyclic) list of pairwise rankings. Smoothing problems like this would save readers time. Likewise, there are a number of grammatical and numerical bugs which slow the reader down. At a higher level, I found the numerous small examples in the first couple chapters to lack structure, in the sense that I didn't quite see how each one differed from the other, and so they appeared repetitive. Likewise, the discussion and corollaries surrounding the discussion of Arrow's theorem in Chapter 2 seemed repetitive. Section 7.2 mentioned some nice theorems involving "strong" rankings; but since this term was never even precisely defined informally, that section only read like a mathematical parable, taking the details on faith.

The book sometimes has too many "scare quotes" in a small section. Let me take one funny quote from page 185 as an example:

> All this "coordinate component" and "fractional voter" tech talk makes Theorem 10 seem impractical and restricted only to those weird "number-crunchers" whose sense of a "hot Saturday night" is checking new web features while designing a C++ program. Fortunately, this is not the case. What saves us from this nerdy fate is [a property of the Borda Count.]

To conclude I will mention the top reasons that I liked the book. It shed light on fundamental results that I never fully understood before (Arrow's theorem, Sen's theorem, Black's single-peaked condition). I learned of new interesting fundamental theorems (e.g. the extensions of Arrow's theorem to quasi-transitive or restricted preferences in Chapter 6, where a dictator is respectively replaced with an oligarchy or partial dictator). Its mantras gave new high-level perspectives which would be useful for guiding research or in practice. Finally, I enjoyed the folksy writing style; if you appreciate real-life (or plausible-fake) stories in mathematical discussion, then you probably would enjoy this book.

Review of[9]
The Mathematics of Voting and Elections: A Hands-On Approach
by Jonathan K. Hodge and Richard E. Klima
American Mathematical Society (Mathematical World series, volume 22)
226 + xiv pages, softcover

Review by
Mark C. Wilson, mcw@cs.auckland.ac.nz
University of Auckland

1 Introduction

The mathematics of collective decision-making ("social choice theory") has been studied for centuries, and until recently almost exclusively by political scientists and economists. The main areas of study concern protocols for aggregating the preferences of individual agents (of which voting is the most common type) and for fair division of resources.

In the last decade these topics, and areas of economics and political science such as mechanism design and game theory more generally, have become interesting to computer scientists. Algorithmic game theory in particular has attracted much research energy from theoretical computer scientists.

The field of Computational Social Choice has developed considerably over the last decade. For example,

- considering search engines as voters and web pages as candidates has proved fruitful;
- conferences on multiagent systems in artificial intelligence, and on electronic commerce, typically have many papers on voting rules;
- the computational complexity of various operations such as determining the winner or manipulating the result of the election has been the subject of much research;
- quantitative versions of famous social choice results such as Arrow's Theorem and the Gibbard-Satterthwaite Theorem have been proved;
- new international workshop series have started, such as COMSOC and ADT.

I see a clear need for teaching materials aimed at introducing this area of research to beginners and outsiders. No single book exists for this purpose. It is probably best to begin with a book on social choice and supplement with research articles. Most books on (classical) social choice theory are research monographs, some rather old, and not well suited to classroom use. The book under review begins to fill this gap.

2 Summary

The book is organized into 10 chapters. The core of the book consists of Chapters 1–5 and the remaining chapters depend very little on these or on each other. Chapter 1 discusses elections with 2 candidates, desirable features of voting rule, and some possible rules. Then majority rule is treated in detail, including its characterization by May's theorem. Chapter 2 introduces elections with 3 or more candidates, and concentrates on the plurality and Borda rules. Chapter 3 deals with the Condorcet criterion and paradox, focusing on sequential pairwise rule and the Instant Runoff (also called Single Transferable Vote) rule. Chapter 4 considers the Independence of Irrelevant Alternatives criterion, and states and discusses in detail various versions of Arrow's famous impossibility theorem. Chapter 5 gives proofs of Arrow's theorem and looks at Approval Voting. Chapter 6–8 deal with weighted voting rules. Chapter 6 covers the basic definitions and properties, while Chapter 7 is concerned with voting power, and the Banzhaf and Shapley-Shubik indices. Chapter 8 covers the United States Electoral College in detail. Chapter 9 focuses on paradoxes around referendum. Chapter 10 is concerned with apportionment ("proportional" allocation of seats in a legislative body), its history and paradoxes.

The authors have tried to keep the spirit of a class taught via the "Moore" (Socratic) method. They have taught such a class for undergraduates with a wide range of backgrounds. A notable feature is the use of questions rather than worked examples or exercises. Some of these questions come with answers, and many are open-ended and require substantial work by the reader.

3 Opinion

The book succeeds admirably in presenting material to its intended audience, which is, roughly speaking, North American undergraduates in the final two years of a degree who have a general interest in the topic. Explanations are careful and detailed, and the questions are very well chosen, often containing a wealth of interesting detail on voting systems used in practice. The material is developed logically and with regard to what the reader can absorb. The mathematical requirements are minimal and much of the book would be appropriate for interested high school students. It would also be very appropriate for more advanced students using it for self-study. The text is very clear and free from errors (there is an errata page at http://www.ams.org/bookpages/mawrld-22/errata1.pdf). The table of contents, index and typesetting are all good. Although some of the cultural references aimed at the target audience may be confusing to a wider audience, even these are interesting. This book should be considered by anyone teaching social choice, as a main textbook or supplemental reading.

Of course, no book can serve all audiences. For computer science students and (potential) researchers interested in proceeding further, clearly some extra reading will be required. We can only hope that a book as well written as this one can fill the gap soon. One possible minor difficulty would be that the book under review occasionally uses idiosyncratic (or at least nonstandard) terminology. Such common terms as social welfare function and profile do not appear (instead, we have societal preference order and preference schedule).

The book's topics are chosen with good taste, but of course some important ones are omitted. Standard topics not mentioned, or only mentioned in passing, which could have been included without excessive technical requirements on the reader include: single-peaked preferences, the median voter theorem, and Condorcet's jury theorem. The most obvious omission (to this reviewer)

is any discussion of manipulation, bribery, control, and strategic behavior in general (apart from a brief mention of agenda control in sequential pairwise voting). This is a substantial part of research in the computational social choice community.

List of recommended further reading after finishing the book under review:

- A Primer in Social Choice Theory by Wulf Gaertner (revised edition), Springer, 2009.
- Handbook of Social Choice and Welfare, volume 1, Elsevier, 2002.
- Mathematics and Voting by Donald G. Saari, American Mathematical Society *Notices*, April 2008.

  Available from http://www.ams.org/notices/200804/tx080400448p.pdf.
- A Short Introduction to Computational Social Choice by Yann Chevaleyre, Ulle Endriss, Jérôme Lang and Nicolas Maudet, Proceedings of SOFSEM 2007.

  Available from http://staff.science.uva.nl/ ulle/pubs/files/ChevaleyreEtAlSOFSEM2007.pdf.

Review of[10] of
Branching Programs and Binary Decision Diagrams: Theory and Applications
by Ingo Wegener
Society for Industrial and Applied Mathematics, 2000
408 pages, HARDCOVER, $119 (US)

Review by Samuel Johnson (samjohnson@ucdavis.edu)

(The author of the book, Ingo Wegener, passed away recently. There is an obituary here: `http://ls2-www.cs.uni-dortmund.de/~wegener/obituary.html`)

1 Introduction

From the title of this monograph, one may easily infer its subject matter. Briefly, a *Branching Program (BP)* (or a *Binary Decision Diagram (BDD)*) that represents a Boolean function[11] B_n is specified by a Boolean variable set $X_n = \{x_1, \ldots, x_n\}$ and a directed acyclic graph $G = (V, A)$. The inner nodes of G get labels from X_n and the sinks get labels from $\{0, 1\}$. Each inner node has out-degree two with one edge labeled 0 and the other labeled 1. (The sinks have out-degree zero.) Each node $v \in V$ represents a Boolean function function f_v as follows: for an input string $a \in \{0,1\}^n$, $f_v(a)$ equals the value of the sink reached by following the path in G that begins at node v and traverses along the edges labeled by the value of a_i leaving the node(s) labeled by x_i. That is, each input $a \in \{0,1\}^n$ activates the a_i-edge leaving every x_i-node so that, for any $v \in V$, $f_v(a)$ equals the label of the sink reached by following the activated path starting at node v.

The investigations into BPs and BDDs had for many years proceeded independently by theoreticians and practitioners, respectively. Theoreticians studied BPs as restricted computational

[10] ©2010, Samuel Johnson

[11] The notation $B_{n,m}$ represents the class of Boolean functions $f : \{0,1\}^n \to \{0,1\}^m$, and we use the shorthand B_n to stand for $B_{n,1}$.

models in the hope of proving lower bounds on explicitly defined Boolean functions. On the other hand, (computer science) practitioners were largely motivated by the development of efficient data structures for Boolean functions, particularly ones that balance the need for efficient algorithms for various operations and the space required to store the structure in memory.

2 Summary

This book is made up of 15 chapters which seem to fit into three thematic segments. This first segment (chapters 1-7) reviews the "standard", deterministic BDD representation for Boolean functions B_n and goes on to examine a number of restrictions and variants of the basic representation. The second segment (chapters 8-11) addresses a small assortment of topics which do not necessarily fit with themes followed in the first segment such as randomized and nondeterministic decision diagrams, and multivalued and edge-valued decision diagrams. The final segment (chapters 12-15) moves on to a survey of applications of binary decision diagrams. The remainder of this section will summarize the book's content at a finer granularity.

The first two chapters introduce the reader to BDDs and BPs (as defined in the introductory section of this review) and discuss the relationship between BDD complexity, circuit complexity, and (Boolean) formula complexity. The book's topic is clearly motivated from both theoretical and practical perspectives. Key BDD operations – *evaluation*, *synthesis*, *SAT*, and *equivalence test* to name just a few – are defined. Algorithms for these operations will be discussed throughout the book as a basis for comparing the various BDD representations. Finally, some upper and lower bound techniques are discussed for BDDs.

Chapters 3 through 5 study *Ordered Binary Decision Diagrams (OBDDs)*. A *π-Ordered Binary Decision Diagram (π-OBDD)* is a BDD variant with the restriction that a permutation π of the indices $\{1, \ldots, n\}$ of the variable set $X_n = \{x_1, \ldots, x_n\}$ is specified so that a sequence of tests along any path of G must obey π. An OBDD is simply a π-OBDD for some ordering π. Upper and lower bounding techniques for OBDDs are presented, and it is shown that OBDDs can be exponentially larger than general BDDs. The connection between communication complexity and OBDDs is introduced as a means to establishing lower bounds on OBDD size. Finally, the problem of finding an optimal variable ordering π is thoroughly addressed where the quality of a particular ordering is determined by the size of the resulting π-OBDD – the smaller the better.

Chapter 6 presents a DD representation that is more general than OBDDs. A *Free BDD (FBDD)*, also called a *read-once BP* is a DD for which each variable $x_i \in X_n$ labels at most one node. In contrast to OBDDs, in FBDDs each path can have a distinct variable ordering. Thus, FBDDs can represent in polynomial size some functions that require exponential size when represented by an OBDD. This chapter also addresses upper and lower bounding techniques and algorithms for various operations, building upon similar discussions from previous chapters.

Chapter 7 extends the read-once BP representation from chapter 6 to BP representations that include multiple tests. In particular, chapter 7 focuses on the following two models: a *read-k-times BP (k-BP)* where each path contains at most k nodes labeled x_i, for each $i \in \{1, \ldots, n\}$; and a *$(1, +k)$-BP* where for each path p there is a set of variables $P(k) \subseteq X_n$ of cardinality k such that p contains at most one node for each variable $x_i \in X_n \setminus P(k)$. Once more, algorithms for various operations along with upper and lower bound techniques are presented.

Chapter 8 briefly investigates some additional representations including *Zero-Suppressed Binary Decision Diagrams (ZBBDs*, *Ordered Functional Decision Diagrams (OFDDs)*, and *Ordered*

Kronecker Functional Decision Diagrams (OKFDDs). Of note in this chapter is the discussion on BDD evaluation based on the Shannon and Reed-Muller decomposition rules.

Chapter 9 turns to multivalued and integer-valued BDD variants. Put simply, these representations consider functions with variables from a finite set of integers to a finite set of integers. Also investigated in this chapter are *Edge-Valued Binary Decision Diagrams (EVBDDs)* in which the 1-edges are accompanied by an integer weight. The functions represented by EVBDDs are of the form $f_v = (1 - x_i)f_0 + x_i(f_1 + w)$ where f_0 and f_1 are the functions represented by the 0- and 1-successors of node v, and node v is labeled with x_i.

Chapters 10 and 11 turn to nondeterministic and randomized DDs. Here, nondeterminism plays a similar role as it does in nondeterministic Turing machines. Structurally, a nondeterministic DD contains (the usual) variable-labeled nodes and (the new) nondeterministic nodes, where each nondeterministic node is labeled by some function $g \in \Omega$. Ω can be the sets $\{OR\}$, $\{AND\}$, $\{EXOR\}$, or $\{AND, OR\}$, each set representing a particular variant of nondeterminism. In a *Randomized BDD*, the DD contains (the usual) variable-labeled nodes and (the new) random nodes, where the outgoing edge of a random node is chosen uniformly (that is, each with probability 1/2). As usual, algorithms for a variety of operations, along with upper and lower bounding techniques are discussed extensively.

Chapter 12 provides a consolidated summary of the results from sections 1-11. This summary is supplemented with several figures and tables and is enormously helpful.

The last three chapters (13-15) address applications that rely heavily upon BDDs. These applications include combinatorial and sequential circuit verification, symbolic model checking, two-level logic minimization, multilevel logic synthesis, functional simulation, test generation, timing analysis, technology mapping, synchronizing sequences, and Boolean unification. In these sections, it is not the intent of the author to present the latest and greatest techniques for this variety of applications; rather, he presents the basic conceptual insights at the foundation of the latest and greatest.

3 Opinion

This book seems intended for graduate students and researchers in theoretical computer science (computational complexity theory in particular). It requires a prior familiarity with complexity theory, algorithms, and maybe a little algebra. It is by no means an introductory text, though the first two chapters are rather accessible. This book aims to be comprehensive, and toward this end it is quite a success.

Wegener's mastery of explaining difficult topics in a clear and concise manner is obvious. The structure and flow within and between chapters is excellent. Material presented in later chapters builds upon that presented earlier on, and the chosen selection and arrangement of topics makes this flow seem intuitive. However, due to the sheer denseness of the material in this monograph, the reader will expect to refer back to previous sections to refresh their memory on a particular definition, theorem, or proof technique. Toward this end, I found the index to be a little disappointing as there were several times that I needed to refer back to something and had to scan page-by-page through a couple of chapters since I found little guidance in the index.

To conclude: Wegener has provided us with a well-written, thorough monograph on a topic for which very few (if any!) other texts exist. If indeed this is the only thorough treatment of BDDs, we should be profoundly grateful that *this* is the one we have.

Review[12] of
Quantum Computer Science: An Introduction
Author of Book:N. David Mermin's
Publisher: Cambridge Press, 2007
Hardcover, 236 pages
List Price:$43.00
Price on Amazon: $18.00 New, %17.00 Used

Author of Review: Eleanor Rieffel, FX Palo Alto Laboratory, rieffel@fxpal.com

1 Introduction

Over the years I have enjoyed Mermin's colorful, idiosyncratic, and insightful papers. His interest in the foundations of quantum mechanics has led him to discover alternative explanations for various quantum mechanical puzzles and protocols. These explanations are often superior to previous explanations in both simplicity and insight, and even when they are not outright better, they provide a valuable alternative point of view. His book is filled with such explanations, and with strong, sometimes controversial, opinions on the *right way* of seeing something, which make his book both valuable and entertaining.

Quantum computation is currently theory. Ardent efforts [2] are underway to build quantum computers, but it is too early to say which efforts will be successful. Mermin does not discuss implementation efforts. He is primarily interested in the artistry of the field: "there is a beauty to the theory of quantum computation that gives it a powerful appeal as a lovely branch of mathematics, and as a strange generalization of the paradigm of classical computer science." Quantum computation is more than that, however; it is the result of thoughtful inquiry into the computational implications of the physical theory that best describes our world. For this reason, I wish that he had included more physics in the book, particularly in motivating the basic concepts. For example, I would have liked to see the definition of a qubit, and the behavior of a qubit under measurement, grounded in the physics of photon polarization.

Quantum computing explores the implications of replacing the fundamental notions of information and computation with quantum mechanical ones. The supremely successful abstraction of computer science means that we can design algorithms without considering how the operations are carried out physically, obscuring the fact that our notion of computation is grounded in classical physics. The book starts with "It is tempting to say that a quantum computer is one whose operation is governed by the laws of quantum mechanics. But since the laws of quantum mechanics govern the behavior of all physical systems, this temptation must be resisted." For decades quantum mechanics has improved modern computers, but computers continue to encode information as bits and perform the same logical operations. Quantum computing changes that.

Shor's discovery of fast quantum algorithms for the cryptographically important problems of factoring and the discrete logarithm propelled the field from a curious side water into mainstream research. The two algorithms together mean that all standard public key encryption systems are insecure. This stunning, practical result was followed by Grover's discovery of a search algorithm that, while less spectacular in its speed up, was the first quantum algorithm of practical significance that was provably better than any classical algorithm, known or unknown. After Grover's

algorithm, there was a hiatus of five years in which no significantly new quantum algorithms were discovered, only variations on existing algorithms. From 2002 on, a variety of novel algorithms have been discovered [7]. Mermin's book, unfortunately, does not cover any results, as opposed to novel explanations, discovered after 1999. Readers will have to look elsewhere for more recent developments in quantum computation.

Mermin, who is famous for fanciful titles such as *Is the moon there when nobody looks? Reality and the quantum theory*, chose the pedestrian title *Quantum Computer Science* to emphasize the tight connection between classical (traditional, non-quantum) computer science and quantum computing. One of the joys of the books is watching him explain well known quantum protocols as elaborations on the simplest of classical manipulations. These original arguments make a strong case that classical computer science informs quantum computing. I am sorry he missed discussing the other side of the argument, the ever increasing evidence that quantum computing informs classical computer science. Drucker and de Wolf survey [1] a wealth of purely classical computational results, in such diverse fields as polynomial approximations, matrix theory, and computational complexity, that resulted from taking a quantum computational view. I know of two additional examples, not in their survey: Kuperberg's proof of Johansson's theorem, and Gentry's fully homomorphic encryption scheme.

2 A summary of the contents

Chapters 3, 4 and 5 give clear accounts of Shor's algorithm, Grover's algorithm, and quantum error correction respectively, adding to the many excellent expositions of these subjects. This review concentrates on Chapters 2 and 6 which contain the best expositions I've seen of some topics. After discussing these two chapters, I return to Chapter 1 to discuss its strengths and weaknesses. While Mermin uses completely nonstandard terminology, *Qbit* and *Cbit*, instead of *qubit* and *bit*, I will use the standard terminology except when quoting Mermin.

2.1 The contents of Chapter 2

Chapter 2 begins with a discussion of quantum parallelism, a commonly misunderstood concept. It is the favored explanation of journalists for the speed up enabled by quantum computation. This explanation, that quantum computers compute all values of a function at once, has lost favor among quantum computer scientists. One reason is lower bound results that prove that, for many problems, quantum computation cannot provide any significant benefit over classical computation. Mermin's exposition of the "apparent miracle" of quantum parallelism is enjoyable and accurate: "A major part of the miracle is only apparent. One cannot say that the result of the calculation is 2^n evaluations of f, though some practitioners of quantum computation are rather careless about making such a claim. ... Before drawing extravagant practical, or even only metaphysical, conclusions from quantum parallelism, it is essential to remember that when you have a collection of Qbits in a definite but unknown state, *there is no way to find out what that state is.*"

Mermin's exposition of Deutsch's algorithm emphasizes that the algorithm yields "less information than we get in answering the question with a classical computer," and that "by renouncing the possibility of acquiring that part of the information which is irrelevant to the question we wish to answer, we can get the answer with only a single application of the black box." It is a lovely section, containing multiple views on the algorithm, some original to Mermin. I wish he had defined *black*

box for readers new to the concept, but in all other respects it is the best exposition of Deutsch's problem I have seen.

Mermin's insight shines brightly when he discusses the Bernstein-Vazirani algorithm. The standard argument is phrased in terms of quantum parallelism and quantum interference: compute a function on all inputs in superposition and use a trick to make the bad answers cancel, leaving only the good answer. Explaining the power of quantum computation in terms of quantum parallelism has gone out of favor as other, more insightful, explanations have been found. Mermin's explanation of the Bernstein-Vazirani algorithm, originally published in his paper *Copenhagen Computation: How I Learned to Stop Worrying and Love Bohr*, contributed to this enlightenment. He was the first to see that, without changing the algorithm at all, just viewing it in a different light, the algorithm becomes clear, almost obvious, and definitely not a trick. The key insight is to view the algorithm in a different basis. Part of the magic of quantum computation, as Mermin likes to say, is that the role of control and target qubits in a controlled operation can reverse in a different basis. By changing viewpoint, the algorithm goes from one in which a calculation is needed to see that it gives the desired result, to one in which the outcome is evident.

The Bernstein-Vazirani algorithm, and Mermin's argument in particular, deserves to be better known because of the insight it has given into quantum computation. The algorithm is not discussed, for example, in Nielsen-Chuang [8]. Mermin could have written an even stronger section on this problem had he chose to include Meyer's recognition [6] that there is no entanglement in the Bernstein-Vazirani algorithm. This observation leads directly into the fascinating, and still evolving, question of the role of entanglement in quantum computation's superior computing capabilities. Entanglement remains the most popular explanation among quantum computer scientist for the power of quantum computing, in spite of increasingly serious questions as to how satisfactory an answer it can provide. Jozsa and Linden [3] show that entanglement is required in order for a quantum algorithm to achieve an exponential speed up over classical algorithms. In that same paper, however, they end their abstract with "we argue that it is nevertheless misleading to view entanglement as a key resource for quantum-computational power." I had hoped that, with Mermin's strong interest in foundations and why things work, he would discuss the role of entanglement, but he does not.

2.2 The contents of Chapter 6

Mermin's colorful and clear account of quantum key distribution could have benefited from a mention that it must be combined with an authentication protocol to defeat man-in-the-middle attacks. In other respects it is a pleasure to read, with scattered shrewd observations such as the following comment on the usefulness of key distribution mechanisms, whether quantum or classical: "What is bizarre is that human ingenuity combined with human perversity has succeeded in inventing a context in which the need to hide information from a third party actually provides a purpose for such an otherwise useless exchange of random strings of bits."

It is unfortunate and surprising that Mermin continues to perpetuate the impression that quantum cryptography is synonymous with quantum key distribution. Quantum cryptography is a broad field with protocols for tasks such as secret sharing, fingerprinting, and authentication. Mermin makes a rare mistake in claiming that "Nobody has figured out how to exploit quantum mechanics to provide a secure means for directly exchanging meaningful messages," when Gottesman's unclonable encryption does just that. He does discuss the status of quantum bit commitment, concluding

that "the structure of quantum mechanics might be uniquely determined by requiring it to enable the secure exchange of random strings of bits ..., but not to enable bit commitment."

Mermin is at his best when he develops both quantum dense coding and quantum teleportation as elaborations of a simple classical operation. This way of looking at these protocols appeared in two earlier papers of Mermin. It is good to see them collected here. His discussions of the GHZ puzzle and the Hardy paradox, both of which deserve to be better known, are also strong.

2.3 The contents of Chapter 1

I now return to discuss the first chapter which, while containing a number of gems, also has some failings. Sections 1.2 through 1.4 walk the reader through the most basic notions of classical computer science, bits and operations on bits, represented in an unusual way that reflects how the basic notions of quantum computing, qubits and operations on qubits, will be represented. These sections are the most problematic of the book. They require the reader to take on faith Mermin's claim that "Playing unfamiliar and somewhat silly games with Cbits will enable you to become acquainted with much of the quantum mechanical formalism in a familiar setting." I worry that some readers will find his short introduction insufficiently motivating to make it through these fifteen pages of classical computer science in an odd notation. In addition, to benefit from these sections, readers must take the initiative to play with this new notation on their own. These early sections call out for exercises, but none are provided.

In these sections, Mermin introduces the quantum computationally important phase change and Hadamard operators. I question whether introducing them in a classical context, in which they cannot be given meaning, will make the reader more comfortable with them. On the other hand, it is here that Mermin introduces the Pauli operators through the classical Swap operation. As Mermin says, "It is pleasing to find them here, buried in the interior of the operator that simply swaps two classical bits." It certainly is!

Sections 1.8 through 1.10 discuss measurement. Mermin emphasizes that the state of an n qubit system is "not associated with any ascertainable property of those qubits," and that "To the extent that it suggests that some preexisting property is being revealed, "measurement" is a dangerously misleading term, but it is hallowed by three quarters of a century of use by quantum physicists." Mermin does not define general quantum measurements, only the measurement of a single qubit, and only one type of single qubit measurement from among the infinite number of possibilities. Mermin has emphasized, in papers such as *On the Absence of a Measurement Problem in Quantum Computer Science* that because quantum computation requires only one type, the simplest type, of measurement, the theory of quantum computation avoids one of the trickiest conceptual issues of quantum mechanics.

Quantum computing is intricately connected, however, to the tricky concepts of tensor product decompositions and entanglement, concepts that are key to the difference between classical and quantum mechanics. Readers would have benefited from a more extended introduction to tensor products and their central role in quantum computation. Similarly, Mermin only briefly defines what it means for a state to be entangled, without giving examples, or explaining its dependence on which tensor product decomposition is under consideration.

Mermin devotes an entire section to the use of measurement for state preparation, a use he correctly says plays a crucial role that is not often emphasized. In his discussion of the common use of the word "collapse" to describe the effect of measurement on a quantum state, he cautions

that the state is "nothing more than an abstract symbol, used ... to calculate probabilities of measurement outcomes." I would have loved to see him go further, making explicit the ties with classical probability theory, and elucidating the differences between classical probability theory and quantum mechanics. This viewpoint has appeared in a number of places including [4], but is waiting for an popular, elementary explanation of the sort Mermin does so well.

2.4 The index, and the lack of references

Not all topics mentioned in the index are actually covered. For example, *Schmidt decomposition*, *mixed state*, and *density operator* appear, but none of these concepts are described; they are only mentioned in passing. Most surprising is that Bell's Theorem, while appearing in the index, is never described even though Mermin has written eloquently on the subject [5].

The omission I found most dismaying is that the book has no reference section. A few references are given in footnotes, but in most cases the reader is left with little indication of how to get more information on a given topic. As one example, Mermin comments that Grover's algorithm requires knowledge of the number of solutions in order to know how many iterations to apply. He then mentions that "a clever application" provides a means to estimate this number, but no reference is given. Authors of introductory books intend to intrigue readers enough that they will want to pursue the subject further. Mermin succeeds. It is unfortunate that he does not make it easier for readers to do so.

3 Concluding thoughts

This book provides an enjoyable and insightful read that will enhance both the novice and expert reader's knowledge of quantum computation. I would not recommend it as a sole source of information on quantum computation; it leaves out too many important topics such as fault tolerance, all algorithmic results more recent than 1999, the known limits on quantum computation, and any study of quantum subsystems and the insight they give into entanglement. Its lack of exercises and a reference section also limit its use as a single source. But anyone with an interest in quantum computation will enjoy reading Mermin's highly personal account of the subject.

References

[1] Andrew Drucker and Ronald de Wolf. Quantum proofs for classical theorems. arXiv:0910.3376, 2009.

[2] Richard Hughes and et al. Quantum cryptography roadmap, version 1.1. http://qist.lanl.gov, July 2004.

[3] Richard Jozsa and Noah Linden. On the role of entanglement in quantum computational speed-up. *Proceedings of the Royal Society of London Ser. A*, 459:2011–2032, 2003.

[4] Alexei Kitaev, Alexander Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation.* American Mathematical Society, Providence, RI, 2002.

[5] N. David Mermin. Hidden variables and the two theorems of John Bell. *Reviews of Modern Physics*, 65:803–815, 1993.

[6] David A. Meyer. Sophisticated quantum search without entanglement. *Physical Review Letters*, 85:2014–2017, 2000.

[7] Michele Mosca. Quantum algorithms. arXiv:0808.0369, 2008.

[8] Michael Nielsen and Isaac L. Chuang. *Quantum Computing and Quantum Information*. Cambridge University Press, Cambridge, 2001.

Book Review[13]

Cryptographic Applications of Analytic Number Theory:
Lower Bounds and Pseudorandomness
Author of Book:Igor Shparlinski

Birkäuser, 2003

Author of Review: Jeffrey Shallit[14]

1 Introduction

Igor Shparlinski is a very prolific mathematician and computer scientist at Macquarie University in Australia. In this 411-page book he uses deep techniques of number theory and algebra to analyze problems arising in cryptography and algorithmic number theory. The book is written at a very high level, suitable for graduate students and researchers in computer science and mathematics. The book has a unique perspective, and is not really comparable to other books in the area.

2 Description

The book, largely devoted to the author's own work, consists of seven sections. In the first, the author develops some of the essential mathematical techniques: linear recurrences, linear complexity (essentially the length of the shortest linear recurrence for a given sequence), exponential sums, discrepancy, lattices, and complexity theory.

The second section is devoted to the discrete logarithm problem. Here we are given a prime p, a generator g of $(\mathbf{Z}/(p))^*$, an element $x \in (\mathbf{Z}/(p))^*$ and we want to find the index $e = \mathrm{ind}(x)$ such that $x \equiv g^e \pmod{p}$. It is well-known that $\mathrm{ind}(x) \equiv -1 + \sum_{1 \le k \le p-2} (g^{-k} - 1)^{-1} x^k \pmod{p}$; this representation of the discrete logarithm has large degree and is dense. The author proves that these properties still hold for representations of $\mathrm{ind}(x)$ over sufficiently large intervals and for approximations of $\mathrm{ind}(x)$. He goes on to prove various theorems about the computation and inapproximability of the discrete logarithm by linear recurrences and Boolean circuits. For example, Theorem 10.2 proves that any Boolean circuit that determines whether x is a quadratic residue mod p, given the base-2 representation of x, needs depth at least $\log \log p$. He also discusses approximation by real polynomials; for this result, the Weil bound on exponential sums is needed.

[14]School of Computer Science, University of Waterloo, Waterloo, ON N2L 3G1, Canada, shallit@graceland.uwaterloo.ca, http://www.cs.uwaterloo.ca/~shallit

The third section discusses the Diffie-Hellman key exchange protocol. Here g is a generator for $\mathbf{F}_q$, the finite field with q elements, we are given g^x and g^y, and we want to efficiently determine g^{xy}. The author again proves various inapproximability results, and also some results on the bit security of this protocol.

The fourth section is devoted to a number of constructions from cryptography. The so-called "cycling attack" on RSA is addressed, as well as the ElGamal signature scheme, the bit security of RSA encryption, the NTRU cryptosystem, and other topics.

The fifth section is devoted to the analysis of various generators of pseudorandom numbers. The power generator method uses the recurrence $u_n \equiv u_{n-1}^e \pmod{m}$, $n \geq 1$. The author proves that if the period is sufficiently long, then the elements of the sequence are uniformly distributed (mod m), and a positive fraction of the rightmost bits is also uniformly distributed. The author also address the $1/M$ generator, which generates random bits from the base-g expansion of $1/M$, and other types of pseudorandom generators, such as polynomials and subset sum.

The sixth section is entitled "Other applications". The author proves a lower bound on the size of Boolean circuits computing whether an integer is squarefree (a notorious hard problem from number theory). For example, if d denotes the depth of such a circuit and S denotes the size, and the circuit works for integers of $\leq r$ bits, the author proves $d \log\log S \geq (\log r)/2 + O(\log\log r)$. He goes on to discuss a trade-off between the depth of Boolean and arithmetic circuits for non-linear functions, modulo p.

The seventh and last section gives 55 open problems in the theory. For example, he asks if Theorem 10.2 (discussed above) has an analogue for branching and randomized Boolean circuits.

An extensive bibliography of 571 items completes the book.

3 Evaluation

This book contains many deep results, and the mathematically-sophisticated reader can find much that is novel. From a complexity theory point of view, most of the results are not impressively strong; as the author forthrightly admits in the introduction, "our complexity bounds are much lower than what is really expected". Nevertheless, it is quite impressive how much work is required to derive these weak results.

The exposition could be improved in several ways. There are are a number of misspellings (e.g., "well-known" misspelled on p. 67; "Cusick" misspelled twice on p. 377) and run-on sentences. The author has chosen to use numbers for his citations instead of the name-date format that is generally preferred; this means the reader has to leaf back and forth between the text and the bibliography to ascertain the provenance of each result, as in the following example (p. 105):

> "A partial case of Lemma 2.2 from [15] gives a lower bound ... (which has actually been used in [509]). However, as it has been noticed in [299], using a certain result of [448], one can get a better value for the constant."

There is no index to notation, which sometimes makes it difficult to determine where a piece of notation has been introduced.

Despite these minor flaws, this is an impressive work that will be of significant interest to researchers in cryptography and algorithmic number theory.

Review[15] **of**
When Least is Best. How Mathematicians Discovered Many Clever Ways to Make Things as Small (or as Large) as Possible
by Paul J. Nahin
Princeton University Press, 2004
xxvi+372 pages, softcover

Review by
Yannis Haralambous, yannis.haralambous@telecom-bretagne.eu
Dép. Informatique, Télécom Bretagne, CS 83818, 29238 Brest Cedex 3, France

1 Introduction

There are two good things in History of Mathematics: History (because we like to hear about older times, it makes us feel better, cleverer, healthier, happier) and Mathematics (because it is the common language we have with people from the past, and because it's fun). But History of Mathematics can also be quite dry, for example in scholarly publications dealing with some unknown mathematician using obscure notations... Not in this book. The author describes a *long* series of problems together with their solutions (or solutions-wannabe). The common theme is optimization: minimize/maximize physical or abstract quantities, length, time, area, volume, cost, etc. Unlike history books, topics are zigzagging on the timeline (and that is good practice to keep the reader motivated). But between the lines you can feel a steady progress in concepts and methods. It is a long way from Polybius to dynamic programming, and one enjoys every step of it.

2 Summary

Preface

The preface is characteristic of the whole book: in only six pages, the author manages to talk about limits of sine functions, Stephen Hawking, the Pythagorean theorem, integrals, Torricelli's paradoxical funnel (= a surface of infinite area delimiting a finite volume), Hobbes' philosophical powers, irrational numbers and $\sqrt{2}^{\sqrt{2}}$. It is both a caveat (there will be math in the book!) and a test: if you like reading it, then you will adore the book—if not, think twice before you start.

What I liked the most is how the author took the classical example of *non-intuitionistic proof*[16] and made a *criterion of mathematical maturity* out of it: mature is the student who replies with "Wow, what a *neat* proof". I'm now systematically applying this test to my students!

Chapter 1

Reading this introductory chapter you give up our reflexes and you see how people in earlier times have solved problems the best way they could, that is: without calculus-related techniques and

[15]

[16] How do we show that there exist irrationals p, q such that p^q is rational? It is easy to show that $\sqrt{2}$ is irrational. Take $\sqrt{2}^{\sqrt{2}}$: either it is rational and we are done, or it is irrational and in that case we take $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ which is equal to 2, and once again we are done. Intuitionists don't accept this proof because the rationality (or irrationality) of $\sqrt{2}^{\sqrt{2}}$ is not really established, and thus "we talk about things we do not know".

mainly without the derivative. A nice example: find the maximum of $3\cos(4\pi x - 1.3) + 5\cos(2\pi x + 0,5)$; the typical first reaction "8" (since both cosine factors are positive, one would take the maximum of the sum to be the sum of the maxima) is far from being correct; the typical second reaction: "take the derivative", also leads nowhere. Using the computer to compute it by successive approximations is still the best.

Seeking ways to avoid the derivative, the author presents the AM-GM inequality (= arithmetic mean of n numbers is always greater than geometric mean, and equality occurs only if the numbers are equal), which he uses to solve some nice problems, like the one of the optimal food can: among all cylinders of volume V which one has minimum surface? This is typically a problem used to illustrate the use of the derivative in geometry, and it is quite surprising to see it solved without derivatives in just a few lines. In the final example of this chapter, he considers a geometric problem about minimizing the time a man needs to swim or walk in a given situation. After having plotted several cases on the computer, he finds the best geometric solution by a clever interpretation of the results.

Chapter 2

Having gone through Chapter 1 we are able to appreciate efforts by people in previous centuries for solving extrema problems. Chapter 2 starts with ancient times. It seems that Greeks cared a lot about the relation between circumference and area of some surface (for example a city). Even historians like Polybius and philosophers like Proclus felt the need to remind their fellow citizens that a town with longer perimeter is not necessary "bigger" (in the sense of having more area). The author mentions some counterintuitive facts in this area, starting with Proclus' example of triangles of sides 5, 5, 6 and 5, 5, 8 having the same (!) area, and ending with von Koch's fractal-like "snowflakes" of infinite perimeter and finite area. Talking of perimeters and areas, the author very naturally arrives to the *isoperimetric problem* (what is the surface of maximal area with a given perimeter? answer: a circle) which is a kind of leitmotiv in this book. After discussing how the Greeks proceeded, the author gives an almost correct proof by Steiner (1842) and discusses Dirichlet's and his own objections to it (the most important being that Steiner takes it as granted that there actually *is* a solution, while there are cases in geometry where, contrarily to our intuition, there is none).

Chapter 3

Exit Antiquity, enter the Middle Ages, starting with *Regiomontanus* (= Knigsberg) *problem* (1471): a painting is hanging on the wall, how far should we stand to watch in order to have a maximal viewing angle? If a (resp. b) is the difference of height between the viewers' eyes and the bottom (resp. top) of the painting, the answer is $\sqrt{ab}$. The proof (without calculus) uses tangent function and AM-GM inequality. A variant of this problem: where on Saturn should we stand to get the best view of its rings? After some simple trigonometry the author solves the problem in Matlab: the value is latitude 33.5°.

The triangle folding problem: take an orthogonal triangle and fold it so that the orthogonal angle falls upon the hypotenuse. Where should be the folding axis so that the folded part has minimal area? Same method: first trigonometry, then computer. Another problem solved in the same way: how do you move a couch around a hallway corner from one room to another: the *pipe-and-corner problem*. And finally, a problem of everyday medieval life: how high can mud be

ejected by a rolling wagon wheel? This one is solved using methods shown in the next chapter, with a beautiful sentence creating all the suspense you need to stay awake another hour and read the next chapter: "As late as the start of the seventeenth century, there were no mathematicians on earth who could have done this analysis. At the end of the century there were many. What happened during that century [...] is the central topic we take up next."

Chapter 4

Surprisingly, this chapter is not about an era in the history of mathematics, but about two individuals: messieurs Descartes and Fermat. As one could expect from the title ("The forgotten war of Descartes and Fermat"), the author gives an amusing account about a harsh personal conflict in a scientific context. The story begins with the Dutch physicist Snell experimentally discovering the law of refraction (= when light crosses the border between two media, the ratio of sines of incidence angles is constant). Descartes, using a corpuscular view of light, tries to explain that constant by claiming it is the ratio of speeds of light in the two media, a statement which implies that *light travels faster in denser media* which, of course, is absurd. At the same time, he also claims that light travels at infinite speed, but then how can it travel "faster" in dense media? These arguments are clearly phony, and so thought Fermat as well. To solve the problem, Fermat developed new methods and *almost* invented the derivative, years before Newton and Leibniz were even born. The reason why Fermat is not known today as the inventor of the derivative, is—according to the author—that irritated Descartes rejected it as revenge for Fermat's criticisms. So much for the guy who said "cogito ergo sum"...

Fermat explained the refraction law by using the *principle of least time*: incidence angles are such that the light uses a path of minimum time. We know today that the path is actually not minimal, but *stationary*, so it can also be maximal. The author gives an example of such a situation.

Chapter 5

In this chapter we enter the era of differential and integral calculus. The first example showing how useful first and second derivatives can be, is quite exotic (and certainly not of the kind you find in textbooks): imagine you are stranded on a desert island (without logarithm tables or computers) and—probably due to an emotional shock—your only concern is to find out which one among numbers π^e and e^π is bigger. The solution is: take $h(x) = \frac{\ln(x)}{x}$, derive it twice, prove that $x = e$ is an maximum, and that gives $e^\pi > \pi^e$. Next, the author treats some geometric problems typically solved by calculus: find the cylindrical wine barrel of maximum volume for a given diagonal, find the maximum UPS package (with maximum allowable length and length+girth), release a projectile so that the distance it will attain is maximal for a given initial speed. The latter example is applied to two different concrete cases: find the angle and initial speed of the perfect basketball shot, lob a projectile onto a target located above the gun.

The next section is about the French mathematician l'Hospital. Here we find out that his famous book *Analyse des infiniment petits* was actually written by Johann Bernoulli (brother of the famous Jakob Bernoulli). Nahin presents a problem taken from this book, it is about a system of cables, a pulley and a weight, in equilibrium.

Finally, the last part of this very dense chapter is about rainbows: the author gives a complete description of the rainbow's mechanism, where it can be seen, where the secondary one will occur in especially bright days, and why the tertiary exists in theory but has never been seen. The

calculations are based on Snell's law. The chapter ends with a poetic touch, since we find out that there is indeed, and has always been, "undetected since before the presence of man on this planet", an *infrared* rainbow, as stated in a 1971 *Science* paper.

Chapter 6

The sixth chapter, by far the largest one, is called "Beyond Calculus". Its first part (which could very well be a chapter by its own) is dedicated to the *Brachistochrone* (= shortest time) problem: take two arbitrary points A and B in physical space (B located lower than A), connect them by a wire, let a bead glide on the wire, under the influence of gravity and without friction. What should be the form of the wire so that the bead travels from A to B in *minimum time*? In 1638, Galileo erroneously assumed that the Brachistochrone curve would be a quarter of a circle (actually the error is no more than 1.52%). It was Bernoulli, in 1696, who proved that this curve is a *cycloid* (= the trajectory of a point on a circle which is rolling on a plane without friction). This curve is already interesting enough, but it became one of the most fascinating mathematical objects ever, when Huygens discovered that the Brachistochrone is also a *tautochrone* (= same time): if $\mathcal{C}$ is the Brachistochrone between A and B, then for any $X \in \mathcal{C}$ the time needed to travel from X to B is *the same* (!) as from A to B. The author shows this remarkable result by using the Euler-Lagrange equation.[17] As shown in the *Amer. J. of Physics* paper, using cycloids you can travel from L.A. to New York in 28 minutes (!) with no other means of propulsion than terrestrial gravity: all you have to do is to build a tunnel going up to 1,000 miles under the surface (you have to dress lightly, though, since temperature there is about 2,300° C).

The remaining of the chapter deals with several interesting problems: what will be the form of a wire hanging from two points in space? Once again Galileo picked the wrong answer: he claimed it would be a parabola, but in fact it is a *catenary*, as shown by Bernoulli and Leibniz. In a symmetric way, the (inverted) catenary is also the best choice for building arches. Next, the author applies the Euler-Lagrange formula to the isoperimetric problem (which has been discussed already in Chapter 2) and to the Plateau problem (= given a closed curve in space, show that there exists a surface of minimal area, bounded by it). Long before soap operas, Plateau used to work with soap films to experimentally produce such minimal surfaces. This work has led to 20th century research on soap bubbles, culminating with the proof of the *double-bubble conjecture* (= the minimal surface to enclose two given and separated volumes is a double bubble, where the two bubbles meet at an angle of 120 degrees), given by Frank Morgan *et al.* in 2001.

Chapter 7

The last chapter deals mostly with computers. The author starts by discussing optimal locations, like finding the point which minimizes the sum of distances to three vertices of a triangle. Then, he discusses shortest paths between polygons, shortest paths in graphs, and the traveling salesman problem. After that, he provides a lengthy discussion of *linear programming*: he describes the *simplex method* for finding the extrema of a linear function of n variables together with a system of linear inequalities on them. After some examples, he discusses the complexity of the simplex algo-

[17] The Euler-Lagrange equation is as follows: suppose we want to find $y(x)$ such that $\int_{x_1}^{x_2} F\{x, y(x), y'(x)\}dx$ is minimal for a given function F of x, y and y', and for given values x_1 and x_2. Then y is a solution of the equation $\frac{\partial F}{\partial y} - \frac{d}{dx}\left(\frac{\partial F}{\partial y'}\right) = 0$.

rithm (exponential in theory, but linear in most cases) and of the *ellipsoid algorithm* by Karmarkar, which is $O(n^{3.5})$.

Finally, he concludes with an interesting description of *dynamic programming* as being "working backwards". The examples given are: first the values of $(x_1, \ldots, x_n)$ such that $\sum x_i = a$ and $\prod x_i$ is minimal; and second an algorithm for calculating the minimal distance in a directed acyclic graph by starting from the last vertex and going backwards. Last example: how to organize a machine building factory with constraints on production, costs, storage and deadlines. The program is modeled in the form of a dag and the previous method is applied to it. This leads to a comparison between linear and dynamic programming methods and to an intriguing final note: "[authors of a medical report] concluded that 'Optimal pain control should be the minimum acceptable standard.' No one would disagree in spirit with the noble nature of this goal, but I'm afraid it is a priori an impossible goal. After reading this book, you should know why."

3 Opinion

Anyone having knowledge of mathematics on the undergraduate level would benefit from this book: besides the pleasure of reading it, one gets insight in several important concepts and techniques, through the study of the history of mathematical events that led to them.

In a typical textbook, mathematics are presented in a linear, teleological, order. Some textbooks have a short historical section, but it is mostly separated from the mathematics per se, to avoid confusion or doubt: the trend is to consider the present (mathematical) discourse as the "best of all possible worlds", and as the only one indispensable. What impression would an average student retain, if instead of a simple "modern" definition of real numbers, we would tell him all the torments and joys, uncertainties and revelations, dead-ends and discoveries of Dedekind, Cantor and Frege? Applying the least energy principle, we stick with the simplest approach, and this goes for every brick of the building of mathematical knowledge.

This book uses a different pedagogical approach: the reader is shown all the complex paths that mathematics have taken in a vast network of mutual influences, historical events, philosophical or theological contexts, and interactions with other (similarly evolving) sciences. No man is an island, and that holds also for theories, experiments, conjectures, applications.

Some readers will find this approach providentially enriching, they will enjoy every page of the book and will regret that they haven't learned all of mathematics in that very way. Others may find it confusing, or feel disoriented in front of constantly changing problems, times and places, without a clear goal or explicit landmarks. Some will appreciate the amount of interesting, clear and easy-to-read information collected in this book. Other will deplore the fact that it is neither a real textbook on extrema methods, nor a real history of mathematics book.

To those who are open-minded and find pleasure in reading mathematics, or in reading *about* mathematics, I warmly recommend this book.

Review[18] of
The Space and Motion of Communicating Agents
Author: Robin Milner
Publisher: Cambridge University Press, 2009
ISBN 978-0-521-73833-0

Reviewer: Nick Papanikolaou (N.Papanikolaou@warwick.ac.uk)

The reviewer recently learned of Robin Milner's passing away on 20th March 2010. Milner leaves behind a great legacy in theoretical computer science, and was one of the founding fathers of process algebra and the study of concurrency. This review is a summary of his last published book, which describes in detail a mathematical model of reactive systems, namely the formalism of bigraphs.

4 Overview

Milner develops in this book an approach to modeling ubiquitous systems; he begins by observing that modern computing, or rather *informatics*, is more about communication than it is about calculation. He emphasizes that, as computing devices increasingly pervade our lives, we will need means of understanding how they interoperate. Even though we may understand thoroughly the functionality of any one device or component, we need to be able to reason about the ways in which that device or component interacts with others, and importantly how an entire network of devices can meet high-level goals and requirements including, among several others, security and privacy constraints.

An analogy is made in the book between properties of ubiquitous systems and the tonal qualities possessed by an orchestra; like a complex system of agents acting and interacting to achieve some goal, the instruments in an orchestra combine in various subtle ways to produce the overall sound. There are qualities of the overall sound which may be translated, or reduced, to qualities of individual instruments, or subgroups of instruments. A ubiquitous system comprises thousands of components, sensors, agents, all of which operate in unison, so the analogy to an orchestra works but there is a difference of scale.

While methods for understanding complex systems exist in the natural sciences, it is still a challenge to develop sufficiently general informatic modeling techniques. Such techniques will be essential in order to design and analyze the information systems of tomorrow, and to this end Milner proposes the *bigraph model*. The purpose of the model is to express clearly, on one hand, the *structure* of ubiquitous systems. This is very significant as there are likely to be several common structures, or system architectures, that will emerge in practical applications; it will be useful to have means of identifying these common structures and extracting key properties. Furthermore, ubiquitous systems are *self-organizing*, in that they change their own structure; this poses various design and implementation challenges for humans, who will need ways of visualizing and reasoning about such changes.

The two key aspects that needed to be accounted for in order describe these systems are *locality* and *connectivity*, or as Milner prefers, **placing** and **linking**. A formalism suited to the description

of ubiquitous systems, he argues, must account for these concepts. The dynamics of a system correspond to *changes in structure and in the links between structures.*

The bigraph model generalizes existing process algebraic models such as CCS and the π-calculus, but requires very rigorous mathematics: the bigraph model described in the book is expressed using a good deal of category theory [6, 7].

5 Summary of Contents

The book is divided into three parts dealing, respectively, with the structure, dynamics, and further extensions of bigraphs.

A bigraph is defined as a mathematical object comprising two structures over a set of vertices V and a set of edges E, in particular:

- a **place graph**, namely a forest f, or set of rooted trees, whose vertices are elements of V; these trees embody the nesting of vertices in the bigraph.
- a **link graph**, namely a hypergraph h with vertices V and edges E, which simply links together the vertices.

What is essential in the concept of a bigraph is the separation of structure and links. By structure we refer in particular to the nesting of vertices: any vertex in a bigraph can contain any number of other vertices. Links occur between arbitrary vertices, and so there are links that occur on many different levels.

Part I – Space

The mathematical notion of a bigraph is developed thoroughly in the first of the book, which contains a plethora of formal definitions, notations, and operations on bigraphs. For instance, composition of bigraphs is defined, and a formal semantics of bigraphs as s-categories is given.

An s-category is a form of *precategory*, a structure similar to a category with the difference that composition of arrows may not always be defined. The place graph and link graph of a bigraph are both essentially s-categories. It is also possible to ignore the details of a particular bigraph and study its structure in the abstract, in which case the resulting object is a symmetric partial monoidal (spm) category.

We will not dwell on these aspects here, but it should be noted that the categorical formulation of bigraphs is useful in order to define a graphical calculus that expresses practical operations. Thinking back to applications of the formalism, consider a ubiquitous system with many components: if this system belongs to enterprise A, and it needs to be interfaced with another system in enterprise B, how can one link the two correctly, unambiguously, and prove that no link has been ignored or incorrectly matched? Interfacing corresponds to composition of bigraphs; composition of maps or arrows is at the core of all category theory, which provides a solid setting in which to study these questions. In essence, the first part of the book develops rigorously the algebra and axioms of bigraphs.

It is worth noting that, in the sixth and final chapter of Part I, the author develops a formal translation of the operators in the process algebra CCS to bigraphs, and similarly for a class of Petri nets, which are widely used in systems modeling. These translations involve mapping to special

forms of bigraphs, which are of course defined as needed (e.g. an *ion* is a bigraph consisting of a single vertex with n ports; *ports* are where links to other vertices can be made).

A remark about the graphical notation for bigraphs is in order here. The symbols used in bigraphs are simply a matter of convention; in most examples, the book uses nested ellipses for vertices, and curves for links. However, there are examples which are more intuitive in which vertices can have different shapes to represent aspects of a concrete system, such as rooms, terminals etc. What is important is to be able to represent aspects of real systems, and the author has made sure that bigraphs are flexible enough to cater for many different applications. However, getting the graphics right can be a tricky affair, as evident even on the front cover of the book (which depicts an example bigraph, and has a couple of edges out of kilter).

Part II – Motion

In the second part of the book, the text develops the dynamics of bigraphs, namely how we can define reactive systems as changing bigraphical structure. Here bigraphs are studied in the abstract, treated as pure mathematical objects without reference to concrete examples as those are simply instances of the general results.

What is key here is how one can define a bigraphical reactive system. A bigraphical reactive system (or simply BRS) is an s-category (such as the place and link graphs of which is a bigraph is made) equipped with *reaction rules*. Reactions express transformations of bigraphs that are meant to correspond to changes and reconfigurations that occur in real systems. In other words, BRSs express *behavior*.

Given an s-category we can define a transition system, similar in nature to the familiar transition systems of CCS or CSP processes. For transition systems corresponding to given BRSs we can define bisimilarity and congruence. These relations allow one to compare given BRSs, again, much in the spirit of classical process algebra.

In order to describe practical systems, it is necessary to impose conditions on the structure of a BRS, otherwise the definition is too broad; for this reason Milner defines in Chapter 8 a set of 'niceness' conditions. Ultimately this leads to a mathematical definition of so-called *prime engaged transitions*, which are the kinds of transitions that are acceptable in practice.

From a practical point of view, understanding the properties of BRSs and corresponding transition systems is important: for any particular domain of application for bigraphs, one needs to formulate a set of reaction rules that express how structures of interest change. These reaction rules need to obey the conditions above mentioned in order to be mathematically sound.

Chapters 9 and 10 develop the theoretical link between BRSs and corresponding transition systems further, with applications to Petri nets and CCS.

Part III – Development

The final part of the book devotes space to a discussion of issues and possible extensions. The discussion is technical and detailed, and tries to account for certain potential shortcomings and/or issues with bigraphs:

- **tracking:** how to store a history of changes made to a bigraph through successive applications of reaction rules,
- **growth:** how to cope with the expansion of a bigraph as its link and place graphs grow,

- **binding:** how to restrict the scope of a link within a certain space, akin to binding of names in process algebra,
- **stochastics:** how to incorporate relative probabilities or rates in reactions, as particularly relevant in the modeling of e.g. biological systems. The book mentions some existing work on *stochastic bigraphs* [5].

In the final chapter of the book, the author gives a brief historical account of the ideas that led to the development of bigraphs, and links this model to CCS, the π-calculus, graph and term rewriting methods for systems modeling and analysis. He also cites implementations of algorithms for matching, simulating and inferring from bigraphs, esp. work on bigraphical programming languages at ITU Copenhagen (see `http://www.itu.dk/research/bpl`). Also mentioned are the stochastic bigraphical models of membrane budding discussed in [5].

Milner concludes the main body of the book[19] thus:

> "It can be seen from this work that the bigraph model is being developed through a combination of mathematical intuition and experiment. The experiment involves real interactive systems — both natural, as in biology, and artificial as in ubiquitous computing and business systems. The model tests the hypothesis that the simple ideas of *placing* and *linking*, both physical and metaphorical, unite the mathematical foundation of interactive systems with their applications."

6 Opinion

This work is the result of a pioneering effort to formulate, in a mathematically rigorous way, a model of reactive behavior, as it arises in many applications ranging from computational biology to ubiquitous computing.

The mathematical expression of the model in terms of categories enables several things, namely: 1)a solid, unambiguous definition of how and when bigraphs may be composed together (there are similar benefits for the definitions of other operations on these structures),

2) a graphical notation which is relatively intuitive and has a formal semantics,

3) a unification of existing theories of reactive behavior, especially process algebras such as CCS and Petri net models.

These benefits must be weighed against the potential criticism that the categorical formulation is abstract and mathematically intensive.

The author himself admits that the definition of bigraphical reactive systems is very broad and that the 'niceness' conditions that are imposed subsequently may be rather taxing. He counters this argument, of course, by pointing out that the generality is needed so as to permit existing models – such as CCS – to be translated to bigraphs.

There is a case to be made for a more usable definition of the transition system corresponding to a BRS, for the labels on transitions are usually identity arrows and do not contain useful information regarding the changes taking place in a particular system. For simulations and analysis of concrete bigraphs, it is likely that further development of this aspect will be desirable. For instance, Michael Goldsmith (University of Warwick) is leading an ONR-funded project that aims

[19] There are a couple of appendices with technical details and solutions to exercises.

to address such issues and ultimately develop practical tool support for bigraphs, especially for use in formal verification [4].

This book should be read by anyone interested in foundations of computer science. Those who are already familiar with CCS and/or π-calculus will be interested in the development of Milner's thinking about modeling techniques and their applications to various information systems. The generality afforded by the bigraph formalism will interest many, and surely this work will spawn many practical applications and foster the development of simulation and reasoning tools for bigraphs. We are particularly interested in Blackwell's formalism of *spygraphs* [1], which are an extension of bigraphs intended for reasoning about cryptographic protocols. Other relevant work we are aware of is the work of Garner and Hirschowitz [3] and the PORGY project, which is focused on visualization (see `https://gforge.inria.fr/projects/porgy/`).

,

References

[1] Clive Blackwell. Reasoning about cryptographic protection with spygraphs, 2008. Presentation at BCTCS 2008.

[2] Mario Bravetti and Gianluigi Zavattaro, editors. *CONCUR 2009 - Concurrency Theory, 20th International Conference, CONCUR 2009, Bologna, Italy, September 1-4, 2009. Proceedings*, volume 5710 of *Lecture Notes in Computer Science*. Springer, 2009.

[3] Richard H. G. Garner, Tom Hirschowitz, and Aurélien Pardon. Variable binding, symmetric monoidal closed theories, and bigraphs. In Bravetti and Zavattaro pages 321–337.

[4] Michael Goldsmith. Beyond Mobility: What Next After CSP/π. In P. H. Welch, H.W. Roebbers, J.F. Broenink, F.R.M. Barnes, C.G. Ritson, A.T. Sampson, G.S. Stiles, and B. Vinter, editors, *The thirty-second Communicating Process Architectures Conference, CPA 2009, Eindhoven, 1-4 November 2009*, volume 67 of *Concurrent Systems Engineering Series*, pages 1–6. IOS Press, 2009.

[5] Jean Krivine, Robin Milner, and A. Troina. Stochastic bigraphs. In *Proc. 24th International Conference on Mathematical Foundations of Programming Systems*, Electronic Notes in Theoretical Computer Science, 2008. To appear.

[6] F. William Lawvere and Stephen H. Schanuel. *Conceptual Mathematics: A first introduction to categories*. Cambridge University Press, 2nd edition, 2009.

[7] Saunders Mac Lane. *Categories for the Working Mathematician*. Springer Verlag, New York, 1971.

[8] Robin Milner. Axioms for bigraphical structure. *Mathematical Structures in Computer Science*, 15:1005—1032, 2005.

[9] Robin Milner. Pure bigraphs: structure and dynamics. *Information and Computation*, 204:60—122, 2006.

[10] Robin Milner. *The Space and Motion of Communicating Agents*. Cambridge University Press, 2009.