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

Welcome to the Book Reviews Column. We hope to bring you at least two reviews of books every month. In this column three books are reviewed.

1. **Complexity Theory Retrospective II**, edited by: Lane A. Hemaspaandra and Alan L. Selman. Reviewed by: Eric Allender. This book is (mostly) a collection of surveys that whose intention is to introduce the reader to several areas of complexity theory.
2. **Basic Simple Type Theory** by J. Roger Hindley. Reviewed by Brian Postow. This book is an introduction to type theory.
3. **Discrete Mathematics in the Schools**, Edited by Joseph G. Rosenstein, Deborah S. Franzblau, and Fred S. Roberts. Reviewed by Neal Koblitz. This is an unusual book for this column; however, I feel that its contents will be of interest to this community. There is a debate going on about teaching discrete math in the high schools. This book is from a workshop on the topic. The workshop was clearly on the YES side of the debate. Neil Koblitz reviews the book and also interjects his own opinions.

We are **looking for reviewers** for the following books: (1) *Information flow: The logic of distributed systems* by Barwise and Seligman, (2) *Control flow semantics* by Bakker and Vink. I can be contacted at the email address above. (3) *Probabilistic Combinatorics and its applications* edited by Bela Bollobas. In exchange for a review you get a FREE COPY!

Review of: **"Complexity Theory Retrospective II**[2],
Edited by: Lane A. Hemaspaandra and Alan L. Selman
Publisher: Springer Verlag

Reviewed by: Eric Allender, Rutgers University

1 Overview

Complexity theory is a rapidly changing and expanding field. Textbooks in complexity theory are soon out-of-date – often before they are even published. Consequently, it can be difficult to know where to look to get an overview of the field.

Thus the collection of well-written survey articles in this volume edited by Hemaspaandra and Selman is especially welcome. This *Retrospective II* is the companion to an earlier *Complexity Theory Retrospective* published in 1990. That earlier *Retrospective* consisted mostly (but not entirely) of expanded and polished versions of expository presentations from the series of IEEE Conferences on Structure in Complexity Theory (since re-named the IEEE Conference on Computational

[1] © William Gasarch, 1998.
[2] © Eric Allender, 1998

Complexity). This current volume also contains some papers that began life as Structures presentations, but contains a larger proportion of new papers, written expressly for *Complexity Theory Retrospective II.*

Although this volume contains surveys on a very wide variety of topics, it is not intended to be encyclopedic. Certainly there are many important and active areas of complexity theory that are not discussed at all. In the paragraphs that follow, I briefly discuss each contribution in turn. It should be apparent to the reader that many of the most important recent developments in the field are covered by this collection.

2 Summary of Contents

Time, Hardware, and Uniformity. *By David Mix Barrington and Neil Immerman.* Descriptive complexity has enriched the studies of logic and of circuit complexity. In this survey, the authors cover the latest developments in this field, showing how various parameters in the definition of classes of logical formulae correspond to fundamental resources in the definition of uniform complexity classes.

Quantum Computation. *By André Berthiaume.* The title says it all. This is an excellent introduction to the new and rapidly-changing area of quantum computation, starting from the very beginning, and continuing through Shor's factoring algorithm. A discussion of the physical possibility of realizing a quantum computer is also included. The author informs me (personal communication) that a follow-up survey on recent developments is already needed. (Two typos worth mentioning: the summation on the bottom of page 33 should be

$$|\psi\rangle = \sum_{i,j=0}^{1} \alpha_i \beta_j |ij\rangle$$

and "$f(j)$" should be replaced by "$f(i)$" in the expression in line 5 of page 42.)

Sparse Sets versus Complexity Classes. *By Jin-Yi Cai and Mitsunori Ogihara.* The study of complete sets is a central topic in complexity theory. In particular, a question of long-standing interest concerns the issue of whether a complete set can be sparse. Some lovely work in the 1990's led to rapid progress on this front (for various complexity classes and notions of reducibility). This is a survey of this work by some of the people most involved.

Counting Complexity. *By Lance Fortnow.* "Counting" complexity classes are classes defined in terms of the *number* of satisfying assignments of nondeterministic Turing machines. Although counting classes have been around almost since the beginning of complexity theory, our understanding of the properties of these classes has grown dramatically in the past decade. Fortnow surveys these developments, in some cases providing new and simplified proofs.

A Taxonomy of Proof Systems. *By Oded Goldreich.* It is no secret that the study of interactive proof systems is one of the big success stories in the recent history of complexity theory. There has been so much happening that it can be hard to keep it all sorted and in perspective. This survey by Goldreich is a very welcome contribution.

Structural Properties of Complete Problems for Exponential Time. *By Steven Homer.* It is important to understand the class of NP-complete sets. In order to get a hint of what their structure might be like, it has been instructive to consider the complete sets for (deterministic and nondeterministic) exponential time. Homer explains how – in contrast to the polynomial-time setting – current techniques have been sufficient to give a fairly clear picture of the shape of complete sets in the exponential-time world.

The Complexity of Obtaining Solutions for Problems in NP and NL. *By Birgit Jenner and Jacobo Torán.* Most effort in complexity theory has concentrated on the complexity of zero-one valued functions (decision problems). The complexity of other functions (such as the complexity of finding optimal solutions for NP search problems) has received less attention, but there is a significant and growing body of work that does deal explicitly with this topic. Jenner and Torán discuss the issues involved in capturing the relevant notions of complexity, and survey the most important results in this area.

Biological Computing. *By Stuart A. Kurtz, Stephen R. Mahaney, James S. Royer, and Janos Simon.* In contrast to the other papers in this volume, the article on Biological Computing is *not* a survey of recent work in the area. Instead, after presenting a brief introduction to some relevant aspects of biochemistry, the authors present a speculative new approach to using biological machinery to build single-molecule processors, as an alternative to Adleman's model. This makes for provocative and interesting reading.

Computing with Sublogarithmic Space. *By Maciej Liśkiewicz and Rüdiger Reischuk.* Complexity theory has been unable to resolve the basic open questions about the relative power of time, space, nondeterminism, and alternation. There are two notable exceptions, however:

- For constant-depth, polynomial-size circuits (or equivalently, log-time alternating Turing machines making a constant number of alternations), there is an infinite hierarchy. More alternations yield more power.
- When time is unrestricted, but less than logarithmic space is available, there is also a hierarchy. More alternations yield more power.

Liśkiewicz and Reischuk have been very active in discovering the true power of alternation in this second setting (the sublogarithmic space world), and this very well-done survey presents the results, the intuition behind the proofs, and most of the proof techniques.

The Quantitative Structure of Exponential Time. *By Jack H. Lutz.* Resource-bounded measure theory has been around for over a decade, and the number of interesting results in this area has been growing until now more and more people are realizing that they should find out what's going on with measure in complexity theory. This fine survey by Lutz (the main force behind resource-bounded measure) is a good introduction to the area and a useful resource.

Polynomials and Combinatorial Definitions of Languages. *By Kenneth W. Regan.* Algebraic tools were behind a number of the most important advances in complexity theory during the past decade. In particular, it turned out to be extremely useful to consider various ways of representing functions by polynomials in various ways. Regan gathers all of this diverse material together and presents it in a format and organization that will be very useful to students and others wanting to gain a mastery of these techniques.

Average-Case Computational Complexity Theory. *By Jie Wang.* In spite of the good news concerning the growing number of heuristics for solving NP-complete problems that work well in practice, there is evidence that many NP-complete problems really are intractable in any practical sense. The theory of average-case computational complexity is vitally important, as the branch of complexity theory that seeks to address practical considerations of real-world performance (as opposed to worst-case guarantees) in a rigorous way in an effort to prove lower bounds. Surveys have played a big role in the development of this field, and Wang's survey in this volume does an excellent job of motivating the definitions and covering the most important results in the area.

3 Opinion

This is a really fine collection of papers. All of the articles are of uniformly high quality, and all of the topics are important.

I would recommend this volume as supplementary course material for a graduate course or seminar on complexity theory, and I would also recommend it to every active researcher in the field. In most cases, people really wanting to completely understand the proofs of the main theorems presented will have to consult the original sources as well, but these surveys do an excellent job of telling the reader what those important theorems are, and where to go to find the best proofs.

Review of
Basic Simple Type Theory[3]
Series: Cambridge Tracts in Theoretical Computer Science #42
Author: J. Roger Hindley
Publisher: Cambridge University Press, 1997

Reviewer: Brian Postow

4 Overview

Type theory is a field that has implications in several areas of mathematics and computer science. It was first invented in the context of set theory as a method of getting around several paradoxes that were discovered during the beginning of this century. Its relationship to the theory of computation through the lambda calculus was quickly realized, followed soon after by links to logic and proof theory. More recently, the effects of type theory have been felt in many different fields of computer science, from increased understanding of complex type systems used in object-oriented languages to the type deduction used in ML and other modern functional languages. This book is a gentle introduction to the area for those who know a little λ calculus. It attempts to give a flavor of the theory and explain some of the more interesting results, including the type deduction algorithm that was partially developed by the author and is now used in ML.

- Chapters 1 and 2 present the basic underlying definitions and background of type theory. They give a brief introduction to the λ calculus, and add types to λ terms.
- Chapters 3, 7 and 8 present the major algorithms in the text: assigning a type to a λ term, finding a term of a given inhabited type, and counting the number of inhabitants of a given type.
- Chapters 4 and 5 add some functionality and new syntax to the type system that is being developed.
- Chapter 6 is a digression about the relationship between type theory and logic.
- Chapter 9 contains proofs of several details that are glossed over in the rest of the book.

[3] © Brian Postow, 1998

5 Summary of Contents

Chapter 1 very briefly describes the untyped λ calculus. It provides all of the standard definitions (terms, abstractions, α, β and η reductions, etc) a few versions of the Church-Rosser theorem, and three restrictions of the λ calculus that are examined later. Since the purpose of the book is to give a flavor of the systems used, and as the first chapter just provides background, proofs in this chapter are sketchier than in the rest of the book. Several proofs are omitted entirely, replaced instead by references to papers containing the complete proofs.

Chapter 2 adds types to the λ calculus. It describes both the Church approach of typed terms, and the Curry approach of type-assignments and deductions. The majority of the book deals with the Curry model; however, a brief foray into typed-terms is made in chapter 5.

The main purpose of the chapter is to define the system TA_λ which is the type and deduction system that is used in the rest of the book, albeit sometimes with added restrictions. TA_λ is a typed calculus with axioms:

$$x : \tau \mapsto x : \tau$$

for each term-variable x and each type τ. and two deduction rules:

$$(\to E)\ \frac{\Gamma_1 \mapsto P : (\sigma \to \tau) \qquad \Gamma_2 \mapsto Q : \sigma}{\Gamma_1 \cup \Gamma_2 \mapsto (PQ) : \tau}$$

and

$$(\to I)\ \frac{\Gamma \mapsto P : \tau}{\Gamma - x \mapsto (\lambda x.P) : (\sigma \to \tau)}$$

Where Γ is a type context, an association of terms to types. In $(\to E)$, Γ_1 and Γ_2 can't disagree on what type gets mapped to any terms, and in $(\to I)$, Γ must be consistent with $x : \sigma$.

From these two rules and the axioms, we can define a set of terms that are typable in TA_λ . Many untyped terms, such as the Y combinator: $(\lambda x.xx)(\lambda x.xx)$, can not be given a type, so the set of typable terms is non-trivial.

The rest of the chapter describes how the reductions change with the addition of types, and proves various normalization theorems.

Chapter 3 defines the principal type of a term, the most general type that is assignable to a given term. Then, it proves that every typable term has a principal type by providing an algorithm that given an untyped term produces its principal type, or, if the term is untypable, says so. The majority of the chapter is taken up by describing the algorithm and proving its correctness.

In Chapter 2 it was noted that, even though two terms may be β equivalent, it is possible that they have no types in common. Chapter 4 explores the system $TA_{\lambda+\beta\eta}$ which ensures that if two terms are β equivalent, they have the same types by adding the following rule:

$$(Eq_\beta)\ \frac{\Gamma \mapsto M : \tau \qquad M =_\beta N}{\Gamma \mapsto N : \tau}$$

This rule increases the number of typable terms, for example, making:

$$(\lambda uv.v)((\lambda x.xx)(\lambda x.xx))$$

typable, since it β reduces to $\lambda v.v$ which has type $\tau \to \tau$ for any τ. Obviously this is not typable in the previous system of TA_λ , because the second term is the Y combinator which is not typable. The rest of the chapter is devoted to describing other changes that this added rule creates, including the presence of weak normalization, but the loss of strong normalization.

Chapter 5 is a brief foray into typed-terms. The goal of the chapter is not to compare the Curry and Church approaches. Instead typed terms are used only as an alternative notation to describe the type deductions used in the Curry approach. The chapter mainly redefines the terms given in chapter 2, but using typed terms instead of type assignments. It also briefly describes how a typed term will be used to describe a deduction.

Chapter 6 is the obligatory digression into intuitionistic implicational logic. It describes the logic, a little bit of its history, and its proof method. It also discusses and proves the Curry-Howard Theorem, that the provable formulae of intuitionistic implicational logic are exactly the types of closed λ terms, and that there is a one-to-one correspondence between TA_λ type deductions and natural deductions in the intuitionist implicational logic.

In addition, three weaker logics are introduced that have the same relationship with the weaker versions of TA_λ introduced in chapter 1.

Finally a version of Hilbert style logic (classical sentential logic) is described that can be expressed in terms of intuitionistic logic, and equivalent results are proved for it.

Chapter 7 proves the converse of chapter 3, that given a type τ, and a term of that type, M, there is a term for which τ is the principal type. To prove this the book gives an algorithm that given τ and M, finds such a term, and proves the algorithm's correctness. Equivalent theorems are proven for the weaker theories. Chapter 6 is referenced here because the proof goes back and forth between the λ calculus and intuitionistic logic.

Chapter 8 answers the question "Given a type τ how many terms can receive τ in TA_λ?" Obviously if τ is inhabited (ie, there is at least one term that can be assigned type τ) there will be an infinite number of terms because we can always apply the identity function to the term without changing the type. However, the question of how many terms in β-normal form can receive a given type is more interesting. The answer to this question can be infinite, any finite number, or even 0 (even if the type is inhabited, it may have no β-normal terms). Most of the chapter is devoted to describing and proving the correctness of an algorithm that, given a type, outputs the number of β normal terms of that type and enumerates them.

In an attempt to keep the majority of the proofs short and readable the author has chosen to eliminate some details from the actual proofs. However, in order to maintain rigor he includes all of these details in chapter 9. The final chapter contains details about the exact structure of terms, types and deductions, and various other details that were glossed over in other parts of the book. Each section carefully describes which chapter it was meant to be read with.

6 Style

This book is relatively easy to read. The proofs are for the most part short, with references to more complete proofs in the literature. Every section is clearly labeled so you never loose track of where you are or where you are going. In particular, the author labels many subsections with *Note* for important relationships that you might have missed, and (more interestingly) *Warning* for results that you might assume follow from a given theorem but don't.

7 Opinion

This is an excellent introduction to type theory. It doesn't bog the reader down in any of the messy details of the proofs (unless he reads chapter 9) and yet it provides many of the most interesting results in the field. It has some exercises, a few of which have solutions in the back, and a comprehensive bibliography. Overall it is a great book for someone who wants to get his feet wet in type theory, but doesn't want to get in over his head.

Review of
Discrete Mathematics in the Schools [4]
DIMACS Series in Discrete Mathematics and
Theoretical Computer Science, Volume 36, 1997
Editors: Joseph G. Rosenstein, Deborah S. Franzblau, and Fred S. Roberts
Publisher: American Mathematical Society

Reviewer: Neal Koblitz

8 Overview

In response to the recommendations of the National Council of Teachers of Mathematics [9] and the increasing interest on the part of educators and scientists in the teaching of discrete mathematics in the schools, the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) of Rutgers University held a conference on the subject on October 2–4, 1992. The volume under review grew out of that conference. The five-year delay is explained by the editors' decision to solicit expanded articles and additional contributions from people who have played leadership roles in introducing discrete math at precollege levels. The book is well worth the wait. The 34 articles are well written, carefully edited, and full of valuable ideas.

The collection is divided into eight sections as follows:

1. The Value of Discrete Mathematics: Views from the Classroom
2. The Value of Discrete Mathematics: Achieving Broader Goals
3. What Is Discrete Mathematics: Two Perspectives
4. Integrating Discrete Mathematics into Existing Mathematics Curricula, Grades K–8
5. Integrating Discrete Mathematics into Existing Mathematics Curricula, Grades 9–12
6. High School Courses on Discrete Mathematics
7. Discrete Mathematics and Computer Science
8. Resources for Teachers (discussions of books, videos, software, and the Leadership Program in Discrete Mathematics of Rutgers University)

I cannot do justice to all 34 articles in the space available. In the next section I will describe what I found especially interesting in a few of the articles.

9 Partial Summary of Contents

Joseph Rosenstein's "Introduction" includes a succinct explanation of how discrete math can revitalize school mathematics:

> Discrete mathematics is:
>
> **Applicable:** In recent years, topics in discrete mathematics have become valuable tools and provide powerful models in a number of different areas.

> **Accessible:** In order to understand many of these applications, arithmetic is often sufficient, and many others are accessible with only elementary algebra.
>
> **Attractive:** Though easily stated, many problems are challenging, can interest and attract students, and lend themselves to exploration and discovery.
>
> **Appropriate:** Both for students who are accustomed to success and are already contemplating scientific careers, and for students who are accustomed to failure and perhaps need a fresh start in mathematics. (pp. xxvi–xxvii)

In Section 1, Susan Picker describes her experiences with students of the latter sort. In a class of remedial tenth-grade students in Manhattan, she reports remarkable success working with graph coloring to model scheduling conflicts. Not only did her students develop some real "expertise" in this type of problem; more importantly, their whole perception of mathematics and of themselves as students improved dramatically.

In Section 2, Nancy Casey and Michael Fellows use examples from graph theory and knot theory to explain how to introduce exciting mathematical notions in the early grades. They argue that children in K–4 should experience:

- a surprising mathematical truth that contradicts intuition;
- a simply-stated mathematical problem with no known solution;
- logical paradox;
- the notion of a limit;
- mathematical exploration.

They illustrate how elementary activities can give kids a foretaste of such fundamental topics as **mathematical proof**, **algorithmic efficiency**, **unsolved problems**, and **one-way functions**. The authors argue that mathematics should be seen as a kind of "literature" whose value goes far beyond its everyday utility, and they say that children should be exposed to the frontiers of knowledge. In another article [1], Fellows gives examples of how work with young children can even be a stimulus to one's own research in discrete mathematics. (See also [2] and [7] for similar discussions in the context of cryptography.)

Two other articles in Section 2 that I particularly enjoyed were Henry Pollak's piece on mathematical modeling and Fred Roberts' discussion of "The Role of Applications in Teaching Discrete Mathematics." Pollak gives a clear explanation, with examples, of what is really taking place when we use mathematics to try to understand real-world phenomena. Roberts gives nine "rules of thumb" to guide teachers in their classroom use of practical applications, and he illustrates these rules through a number of vivid examples based on the Traveling Salesperson Problem, graph coloring, and Euler paths.

Section 3 contains the longest article in the book — the full text of the chapter on discrete mathematics in the *New Jersey Mathematics Curriculum Framework*, divided into sections for each of the K–2, 3–4, 5–6, 7–8, and 9–12 grade levels. The author is Director of the New Jersey Mathematics Coalition, as well as one of the editors of the book under review.

One of the strengths of the book is the inclusion of reports by in-service teachers. For example, in Section 5, Bret Hoyer (of Cedar Rapids, Iowa) relates "A Discrete Mathematics Experience with General Mathematics Students"; and in Section 6, Charles Biehl (of Wilmington, Delaware) describes his high school "math analysis" course designed for students who are not likely to become math or science majors at college.

10 Opinion

A compelling case can be made for the use of discrete math in certain situations:

1. Classroom visits by scientific researchers. Too often, scientists-in-the-schools programs amount to little more than "show and tell," with the students learning no basic science. If, on the other hand, the scientists introduce discrete math activities to the children, then the kids will develop a deeper appreciation of scientific modes of thinking.
2. Special programs for talented students, run by highly motivated teachers.
3. Programs for slow students who have given up on the standard math subjects. See especially Susan Picker's article "Using Discrete Mathematics to Give Remedial Students a Second Chance" and Charles Biehl's article "A Fresh Start for Secondary Students."

It is not so clear that a new emphasis on discrete math should be mandated for all students throughout the school system. The authors of *Discrete Mathematics in the Schools* are dedicated and talented pedagogues. What works well for them might not turn out so well in the hands of an average teacher.

A common explanation for the disappointing performance of American youngsters in many international comparisons (most recently, in the Third International Math and Science Study) is that the mathematics curriculum in U.S. schools is "a mile wide and an inch deep." That is, every year students glide rapidly through a large number of topics without developing a mastery of any of them.

Most of the authors of the collection under review seem to me to be insufficiently aware of the dangers of handing teachers a new list of concepts and activities to shoe-horn into the curriculum. Given the problems and pressures that confront the average teacher in America, it is not likely that the introduction of discrete math on a massive scale would go as well as the authors imagine.

The main danger I see is that, if handled poorly, a push for discrete math could contribute to a further "dumbing down" of the math curriculum. Responding to pressure from parents and politicians, teachers and textbooks will coddle the children with easy material that is not age-appropriate. If, for instance, an 8th-grade textbook consists mostly of material that should be easy for a 5th grader and contains only a small amount of material that one would think of as challenging at the 8th-grade level, then a teacher who is not careful can easily spend the whole year doing only the part of the book that would make an appropriate 5th-grade textbook.

Students will get high test scores and inflated grades, will never develop self-discipline and good study habits, and will enter college unprepared for university-level mathematics and science courses. This would, of course, be the exact opposite of what the authors of *Discrete Mathematics in the Schools* intend. But as I read the article by Joseph Rosenstein taken from the *New Jersey Mathematics Curriculum Framework* — offering a grab bag of nice topics and activities for students to work on — I was struck by the absence of any concrete indication of what constitutes reasonable measures of satisfactory performance. I could not help noting how easy it would be for teachers and textbook writers to use toned-down versions of the activities that require little sustained mental effort on the part of the youngsters.

I know of only one systematic attempt to address the question of assessment of student achievement in discrete math: the book *Measuring Up* by the Mathematical Sciences Education Board [8]. Like the volume under review, *Measuring Up* has some excellent material; in fact, I use it as a required text in a course I teach for undergraduate math education majors. But unfortunately, most of the assessment standards are, in my judgment, too simple-minded for the intended age level.

When I travel to different parts of the world, I like to develop contacts in the local schools. I often visit math classes to give a workshop in discrete math to children between 9 and 13 years old; I have done this in about a dozen countries of Asia, Africa, and the Americas. Some of the activities I enjoy sharing with the youngsters are discussed either in the book under review or in [8]. But I always use versions that are more sophisticated and challenging than the "assessment prototypes" in [8], because foreign children would find the American versions too easy and simplistic — not challenging enough to be interesting.

Let me give an example. One of the activities in [8] is an arithmetic dice game, played as follows. The children roll 3 dice, find expressions for the integers 1 through 10 in terms of the numbers on the dice and the operations +, −, × and ÷ (using each number exactly once), and see how many of the numbers

7 8 9 10

6 5 4

3 2

1

can be "knocked down" (by analogy with bowling). For more advanced students, the suggestion in [8] is to use 4 dice and put another row of pins numbered 11 through 15 at the top.

Here is the modification that I use when I work with 4th to 7th graders in other parts of the world: Roll 5 dice, allow +, −, ×, ÷ and squaring (and repeated squaring) of any number or expression, and have the kids generate prime numbers, each one larger than the ones before. Once they get numbers above 1000, testing for primality becomes harder. At the end I ask for a show of hands: How many think that the game could go on forever (generating an infinite sequence of primes)? How many don't? This is an unsolved problem of number theory (a generalization of the Fermat prime problem). This prime number dice game has worked well both with average kids (in Belize, Central America, and in Cape Town, South Africa, for example) and with unusually bright kids (in a school in Vietnam). This version of dice arithmetic is more interesting and challenging than the mickey-mouse version in [8].

11 Conclusion

The book *Discrete Mathematics in the Schools* is full of useful material and thought-provoking discussion. Even though it does not answer all questions one might have about the use of discrete math on a massive scale in the schools, it is a valuable first step. All scientists who are interested in improving K–12 math education should be sure to read this book.

References

[1] M. R. Fellows. Computer science and mathematics in the elementary schools, in N. D. Fisher, H. B. Keynes, and P. D. Wagreich, editors, *Mathematicians and Education Reform 1990–1991.* Providence RI: Amer. Math. Society, 1993, 143–163.

[2] M. R. Fellows and N. Koblitz. Kid Krypto, in E. F. Brickell, editor, *Advances in Cryptology – Crypto '92.* New York: Springer-Verlag, 1993, 371–389.

[3] M. R. Fellows and N. Koblitz. *Math Enrichment Topics for Middle School Teachers*, 1995.

[4] S. Garfunkel *et al. For All Practical Purposes: Introduction to Contemporary Mathematics*, 3rd edition, New York: W. H. Freeman and Company, 1994.

[5] Allyn Jackson. The Math Wars: California Battles It Out over Mathematics Education Reform, *Notices of the Amer. Math. Society* **44**, No. 6 & 7, 1997, 695–702 & 817–823.

[6] N. Koblitz. The Case Against Computers in K–13 Math Education (Kindergarten through Calculus), *The Mathematical Intelligencer* **18**, No. 1, 1996, 9–16.

[7] N. Koblitz. Cryptology As a Teaching Tool, *Cryptologia* **21**, 1997, 317–326.

[8] Mathematical Sciences Education Board and National Research Council. *Measuring Up: Prototypes for Mathematics Assessment*, Washington: National Academy Press, 1993.

[9] National Council of Teachers of Mathematics. *Curriculum and Evaluation Standards for School Mathematics*, Reston VA: NCTM, 1989.