Review of the book

*"Mathematical Methods in Computer Science"*

by Jacques Calmet, Willi Geiselmann, Jörn Müller-Quade

Springer, 2008

ISBN: 978-0-540-89993-8

Olivier Blazy, HGI/RUB, Germany

# 1 What the book is about

This book is a compilation of several contributions from the conference "Mathematical Methods in Computer Sciences", held in December 2008 in memory of Thomas Beth. The topics are quite broad but encompass the various interest of Thomas Beth and follows his idea of "Algebra as a language".

After a small preface, about the book organization and a short biography of Thomas Beth, the book follows the conference organization and is divided into 6 parts:

- The first one is entitled *Cryptography I*:
  - It is solely composed of a paper called "On the security of Beth's Identification Schemes against Active and Concurrent Adversaries" by Giovanni Di Crescenzo. This paper takes Beth's Identifications Schemes and proposes minor modifications to allow them to satisfy security under active and concurrent impersonation attacks, under the one-more-dlog assumption.
- The second part is entitled *Designs* and is composed of three different papers:
  - The first one is called "Steiner $t$-Designs for Large $t$, and was written by Michael Huber, in this paper he shows that no block-transitive Steiner 6-design can exist.
  - The second one is on "New Spatial Configurations" by Harald Gropp, this paper builds up on his earlier work in 1994, to present new spatial configurations, in other words new finite incidence structure consisting of a set of points and a set of subsets of this set verifying some properties, mostly that each points can only be linked by at most 2 lines, two lines intersect in at most 2 points.
  - The third one is "Construction of Large Constant Dimension Codes with a prescribed Minimum Distance", it was written by Axel Kohnert and Sascha Kurz. Subspace codes allow some application to network coding and are connected to the theory of design over finite fields. This paper presents new constant dimension codes with more codewords than previously known codes and present a table to compare those results.
- The next part is dedicated to *Quantum Computing*""
  - It begins by an Invited Talk "Embedding Classical into Quantum Computation" by Richard Jozsa, in which he describes a simple formalism for generating classes of quantum circuits that are classically efficiently simulatable and shows that the efficient simulation of Clifford circuit, and other matchgate circuits are only special cases.

  - There is then a paper from Aleksandrs Belovs and Juris Smotrovs entitled "A Criterion for Attaining the Welch Bounds with Applications for Mutually Unbiased Bases". After explaining basic notions on Mutually Unbiased Bases, this paper shows that Welch bounds are a good notion to study them, leading to a necessary and sufficient condition on a set of orthonormal bases to form a complete system of MUBs. In case of homogeneous MUBs, this takes an elegant form.
  - The last paper from this section is entitled "An Efficient Quantum Algorithm for the Hidden Subgroup Problem over Weyl-Heisenberg Groups" was written by Hari Krovi and Martin Rötteler. They based their approach on non-commutative Fourier analysis of coset states to provide speed-ups on hidden subgroup problems. A particularity of their approach resides in the fact that the algorithm operates on two coset states simultaneously.

- The next part of the book is dedicated to *Algorithms*, and includes two papers:
  - The first one is called "Computing Equiangular Lines in Complex Space" by Markus Grassl, and focuses on finding sets of units vectors such that the modulus of the inner product between any two vectors is constant. In this paper they focus on how to build $d^2$ of those vectors in dimension $d$, and how symmetries can be used to simplify the problem.
  - The second one is one the "Complexity of Comparing Monomials and Two Improvements of the Buchberger-Möller Algorithm", where Samuel Lundqvist presents a new projection technique to improve the complexity bound, and evokes that some application in biology may even be more efficient as one may skip the Gröbner basis part of the algorithm.

- The next part is dedicated to *Coding Theory*:
  - It starts with an extended abstract of an invited talk by Teo Mora and Emmanuela Orsini: "Decoding Cyclic Codes: The Cooper Philosophy", where they explain that their talk explains how to use Gröbner basis computation in order to deduce locator polynomials of cyclic codes.
  - Then there is a paper from Jaume Pernas, Jaumes Purjol, and Merce Villanueva called "Kernel Dimension for Some Families of Quaternary Reed-Muller Codes" where they present a structural invariant for binary codes, the kernel dimension, to classify these families of codes.

- The last part is entitled *Cryptography II*:
  - The first paper is dedicated to *Coding-Based Oblivious transfer* by Kazukuni Kobara, Kirill Morozov, and Raphael Overbeck, where they present two flavors of oblivious transfer, the Rabin and the 1-out-of-2. While they cannot directly prove the security of the schemes, they show it might be probably linked to some classical long-standing problem in coding theory.
  - The next paper is on the "Protection of Sensitive Security Parameters in Integrated Circuits" by Dejan E. Lazich and Micaela Wuensche. They introduce a method that uses codewords of error control codes to configure the IC-Eigenkey generator in a way that the generated bits are as statistically independent of each other as possible.
  - The last paper is "On Reconstruction of RC4 Keys from Internal States". Shahram Khazaei and Willi Meier fully exploit the whole distribution of noises expressing theses biases, they then study how far one can go by using only the distribution of noises. The algorithm they propose allows them to estimate its complexity versus success probability.

## 2 What the book is like

The editors tried to pick from MMICS 2008 conference papers in the area interesting Thomas Beth. Those papers cover a very broad domain where algebra is at the core.

This book is mostly a short proceedings of a conference. I find that while most of the papers are really interesting, it is hard to reflect properly on the chosen selection.

One of the invited talk is only represented through an extended abstract, and while the talk seems interesting it is quite a shame to end up with a "paper" shorter than it's bibliography.

There is also another paper presenting an explicit solution to a vector problem. While knowing that such result can be obtained is interesting, I have a hard time believing that someone is going to exploit the 12 values written in plain through 9 pages of appendix.

Except those details, the selection allows an interesting read giving a good overview of the state of the art, and the guideline picked for the selection is really interesting as it allows to look differently at common problems.

# 3 Recommendation

It's never easy to determine who is the best target for a given book. The choice of papers covers a wide range of the field, so I believe everyone can find something new in this book. The chapter division allows to efficiently select which paper is directly in a specific area, but the reader should really look in the rest of the book to see other application to those techniques, and see the link between problems that otherwise may seem independent.

From the reviewer's point of view there is however a minor drawback. If we exclude the preface the book is just a compilation of papers around Thomas Beth work. One might have expected more cohesion between them, with additional presentations (like a direct link to his work, reordering papers to make the whole more consistent), to see a kind of progression throughout the book, whereas here you just have a glimpse on many different areas but without much cohesion between them, at least nothing more than they all gravitate around the problems. On the same idea a conclusion at the end of each unit might have been a good idea to summarize the key elements presented, and also a global selection at the end of the book might have been interested.

Nevertheless, the audience is still really broad. On one hand, specialists (scientific, experts) can find useful information, on the other hand, the book is really accessible to students. The book might help to widen the field of research for many people, as the collection of papers allows to see some underlying link between different problems.

The book can reveal to be really interesting for people working on optimization of mathematical methods.

*The reviewer is a PostDoc at the Ruhr-University, Bochum, Germany.*