Mathematical Computation with SageMath

Paul Zimmermann Alexandre Casamayou
Nathann Cohen Guillaume Connan Thierry Dumont
Laurent Fousse François Maltey Matthias Meulien
Marc Mezzarobba Clément Pernet Nicolas M. Thiéry
Erik Bray John Cremona Marcelo Forets
Alexandru Ghitza Hugh Thomas

Parts of this book are inherited from the book *Calcul formel : mode d'emploi. Exemples en Maple* from Philippe Dumas, Claude Gomez, Bruno Salvy and Paul Zimmermann, distributed under cc-by-sa 2.0 fr, in particular Sections 2.1.5, 2.3.5 and 5.3.

Parts of the Sage examples from Chapter 15 are inherited from the tutorials of MuPAD-Combinat [HT04] and Sage-combinat. The enumeration of complete binary trees in §15.1.2 is partly inspired from a classroom problem designed by Florent Hivert.

Exercise 9 on Gauss problem is inspired from a problem designed by François Pantigny, and Exercise 17 on the Magnus effect is extracted from a classroom problem designed by Jean-Guy Stoliaroff.

Graphs from Figure 4.9 and their interpretation reproduce part of paragraph III.4 from the "Que sais-je ?" book *Les nombres premiers* from Gérald Tenenbaum and Michel Mendès France.

Preface

This book was written for those who want to efficiently use a computer algebra system, and Sage in particular. Symbolic computation systems offer plenty of functionality, and finding the right approach or command to solve a given problem is sometimes difficult. A reference manual provides a detailed analytic description of each function of the system; however, this is not very useful since usually we do not know in advance the name of the function we are looking for! This book provides another approach, by giving a global and synthetic point of view, while insisting on the underlying mathematics, the classes of problems we can solve and the corresponding algorithms.

The first part, more specific to Sage, will help getting to grips with this system. This part is written to be understood by undergraduate students, and partly by high school students. The other parts cover more specialised topics encountered in undergraduate and graduate studies. Unlike in a reference manual, the mathematical concepts are clearly explained before illustrating them with Sage. This book is thus in the first place a book about mathematics.

To illustrate this book, Sage was a natural choice, since it is an open-source system, that anybody can use, modify and redistribute at will. In particular the student who learns Sage in high school will be able to continue to use it at undergraduate or graduate levels, in a company, etc. Sage is still a relatively young system, and despite its already extensive capacities, it does contain some bugs. However, thanks to its very active community of developers, Sage evolves very quickly. Every Sage user can report a bug — maybe together with its solution — on `trac.sagemath.org` or via the `sage-support` list.

In writing this book, we have used version 8.0 of Sage. Nevertheless, the examples should still work with later versions. However, some of the explanations may no longer hold, for example the fact that Sage relies on Maxima for numerical integrals.

When in December 2009 I asked Alexandre Casamayou, Guillaume Connan, Thierry Dumont, Laurent Fousse, François Maltey, Matthias Meulien, Marc Mezzarobba, Clément Pernet and Nicolas Thiéry to write the first version (in French) of this book, all agreed with enthusiasm — including Nathann Cohen who joined us later on. Given the success of the French version, it was clear that an English version would be welcome. In March 2017, I decided to start working on the English version; I want to thank once again those of the "dream team" who helped me translating the text into English, updating the examples to the new version of Sage, and moreover improving the content of the book

(Guillaume Connan, Thierry Dumont, Clément Pernet, Nicolas Thiéry), as well as the new authors of the English version (Erik Bray, John Cremona, Marcelo Forets, Alexandru Ghitza, Hugh Thomas).

Several people had proof-read the French version: Gaëtan Bisson, Françoise Jung, Hugh Thomas, Anne Vaugon, Sébastien Desreux, Pierrick Gaudry, Maxime Huet, Jean Thiéry, Muriel Shan Sei Fan, Timothy Walsh, Daniel Duparc, and especially Kévin Rowanet and Kamel Naroun. The following people helped us to improve the English version by proof-reading one or several chapters, or simply reporting a typo: Fredrik Johansson, Pierre-Jean Spaenlehauer, Jacob Appelbaum, Nick Higham, Helmut Büch, Shashank Singh, Annegret Wagler, Bruno Grenet, Jeroen Demeyer, and last but not least Adil Hasan for his wonderful feedback. On the technical and typographic side, we thank Emmanuel Thomé, Sylvain Chevillard, Gaëtan Bisson, Jérémie Detrey and Denis Roegel.

When writing this book, we have learned a lot about Sage, and we have of course encountered some bugs — some of which have already been fixed. We hope this book will be also useful to others, high school students, undergraduate or graduate students, engineers, researchers or simply mathematical hobbyists. Despite several proof-readings, this book is surely not perfect, and we expect the reader to tell us about any error, typo or make any suggestion, by referring to the page `sagebook.gforge.inria.fr`.

Nancy, France
September 2017

Paul Zimmermann

Contents

I Getting to Grips with Sage **1**

1 First Steps **3**

1.1 The Sage Program . . . 3
1.1.1 A Tool for Mathematics . . . 3
1.2 Sage as a Calculator . . . 7
1.2.1 First Computations . . . 7
1.2.2 Elementary Functions and Usual Constants . . . 10
1.2.3 On-Line Help and Automatic Completion . . . 11
1.2.4 Python Variables . . . 12
1.2.5 Symbolic Variables . . . 13
1.2.6 First Graphics . . . 15

2 Analysis and Algebra **17**

2.1 Symbolic Expressions and Simplification . . . 17
2.1.1 Symbolic Expressions . . . 17
2.1.2 Transforming Expressions . . . 18
2.1.3 Usual Mathematical Functions . . . 20
2.1.4 Assumptions . . . 21
2.1.5 Some Pitfalls . . . 22
2.2 Equations . . . 23
2.2.1 Explicit Solving . . . 23
2.2.2 Equations with no Explicit Solution . . . 26
2.3 Analysis . . . 27
2.3.1 Sums . . . 27
2.3.2 Limits . . . 28
2.3.3 Sequences . . . 28
2.3.4 Power Series Expansions . . . 30
2.3.5 Series . . . 31
2.3.6 Derivatives . . . 33
2.3.7 Partial Derivatives . . . 33
2.3.8 Integrals . . . 33
2.4 Basic Linear Algebra . . . 35
2.4.1 Solving Linear Systems . . . 35
2.4.2 Vector Computations . . . 35
2.4.3 Matrix Computations . . . 36

2.4.4 Reduction of a Square Matrix 37

3 Programming and Data Structures 39
3.1 Syntax 39
3.1.1 General Syntax 39
3.1.2 Function Calls 41
3.1.3 More About Variables 41
3.2 Algorithmics 42
3.2.1 Loops 42
3.2.2 Conditionals 49
3.2.3 Procedures and Functions 50
3.2.4 Example: Fast Exponentiation 53
3.2.5 Input and Output 56
3.3 Lists and Other Data Structures 57
3.3.1 List Creation and Access 57
3.3.2 Global List Operations 59
3.3.3 Main Methods on Lists 63
3.3.4 Examples of List Manipulations 65
3.3.5 Character Strings 66
3.3.6 Shared or Duplicated Data Structures 67
3.3.7 Mutable and Immutable Data Structures 68
3.3.8 Finite Sets 69
3.3.9 Dictionaries 70

4 Graphics 73
4.1 2D Graphics 73
4.1.1 Graphical Representation of a Function 73
4.1.2 Parametric Curve 76
4.1.3 Curve in Polar Coordinates 76
4.1.4 Curve Defined by an Implicit Equation 77
4.1.5 Data Plot 77
4.1.6 Displaying Solutions of Differential Equations 82
4.1.7 Evolute of a Curve 86
4.2 3D Curves 89

5 Computational Domains 93
5.1 Sage is Object-Oriented 93
5.1.1 Objects, Classes and Methods 93
5.1.2 Objects and Polymorphism 95
5.1.3 Introspection 96
5.2 Elements, Parents, Categories 97
5.2.1 Elements and Parents 97
5.2.2 Constructions 98
5.2.3 Further Reading: Categories 99
5.3 Domains with a Normal Form 99
5.3.1 Elementary Domains 99
5.3.2 Compound Domains 104

5.4 Expressions vs Computational Domains . . . 106
5.4.1 Symbolic Expressions as a Computational Domain . . . 107
5.4.2 Examples: Polynomials and Normal Forms . . . 107
5.4.3 Example: Polynomial Factorisation . . . 108
5.4.4 Synthesis . . . 110

II Algebra and Symbolic Computation 111

6 Finite Fields and Number Theory 113
6.1 Finite Fields and Rings . . . 113
6.1.1 The Ring of Integers Modulo n . . . 113
6.1.2 Finite Fields . . . 115
6.1.3 Rational Reconstruction . . . 116
6.1.4 The Chinese Remainder Theorem . . . 117
6.2 Primality . . . 118
6.3 Factorisation and Discrete Logarithms . . . 121
6.4 Applications . . . 122
6.4.1 The Constant δ . . . 122
6.4.2 Computation of a Multiple Integral . . . 123

7 Polynomials 125
7.1 Polynomial Rings . . . 126
7.1.1 Introduction . . . 126
7.1.2 Building Polynomial Rings . . . 127
7.1.3 Polynomials . . . 128
7.2 Euclidean Arithmetic . . . 132
7.2.1 Divisibility . . . 132
7.2.2 Ideals and Quotients . . . 134
7.3 Factorisation and Roots . . . 135
7.3.1 Factorisation . . . 135
7.3.2 Root Finding . . . 137
7.3.3 Resultant . . . 138
7.3.4 Galois Group . . . 140
7.4 Rational Functions . . . 140
7.4.1 Construction and Basic Properties . . . 140
7.4.2 Partial Fraction Decomposition . . . 141
7.4.3 Rational Reconstruction . . . 142
7.5 Formal Power Series . . . 145
7.5.1 Operations on Truncated Power Series . . . 146
7.5.2 Solutions of an Equation: Series Expansions . . . 147
7.5.3 Lazy Power Series . . . 148
7.6 Computer Representation of Polynomials . . . 149

8 Linear Algebra 153
8.1 Elementary Constructs and Manipulations . . . 153
8.1.1 Spaces of Vectors and Matrices . . . 153

8.1.2 Vector and Matrix Construction 155
8.1.3 Basic Manipulations and Arithmetic on Matrices 156
8.1.4 Basic Operations on Matrices 158
8.2 Matrix Computations 158
8.2.1 Gaussian Elimination, Echelon Form 159
8.2.2 Linear System Solving, Image and Nullspace Basis . . . 166
8.2.3 Eigenvalues, Jordan Form and Similarity Transformation 167

9 Polynomial Systems 177
9.1 Polynomials in Several Variables 177
9.1.1 The Rings $A[x_1, \dots, x_n]$ 177
9.1.2 Polynomials 179
9.1.3 Basic Operations 180
9.1.4 Arithmetic 181
9.2 Polynomial Systems and Ideals 182
9.2.1 A First Example 182
9.2.2 What Does Solving Mean? 185
9.2.3 Ideals and Systems 185
9.2.4 Elimination 190
9.2.5 Zero-Dimensional Systems 196
9.3 Gröbner Bases 200
9.3.1 Monomial Orders 201
9.3.2 Division by a Family of Polynomials 202
9.3.3 Gröbner Bases 203
9.3.4 Gröbner Basis Properties 206
9.3.5 Computations 209

10 Differential Equations and Recurrences 213
10.1 Differential Equations 213
10.1.1 Introduction 213
10.1.2 First-Order Ordinary Differential Equations 214
10.1.3 Second-Order Equations 221
10.1.4 The Laplace Transform 223
10.1.5 Systems of Linear Differential Equations 224
10.2 Recurrence Relations 226
10.2.1 Recurrences $u_{n+1} = f(u_n)$ 226
10.2.2 Linear Recurrences with Rational Coefficients 229
10.2.3 Non-Homogeneous Linear Recurrence Relations 229

III Numerical Computation 231

11 Floating-Point Numbers 233
11.1 Introduction 233
11.1.1 Definition 233
11.1.2 Properties and Examples 234
11.1.3 Standardisation 234

11.2 The Floating-Point Numbers 235
11.2.1 Which Kind of Floating-Point Numbers to Choose? . . 236
11.3 Properties of Floating-Point Numbers 237
11.3.1 These Sets are Full of Gaps 237
11.3.2 Rounding 238
11.3.3 Some Properties 238
11.3.4 Complex Floating-Point Numbers 243
11.3.5 Methods 244
11.4 Interval and Ball Arithmetic 244
11.4.1 Implementation in Sage 245
11.4.2 Computing with Real Intervals and Real Balls 248
11.4.3 Some Examples of Applications 249
11.4.4 Complex Intervals and Complex Balls 251
11.4.5 Usage and Limitations 252
11.4.6 Interval Arithmetic is Used by Sage 252
11.5 Conclusion 252

12 Non-Linear Equations 255
12.1 Algebraic Equations 255
12.1.1 The Method `Polynomial.roots()` 255
12.1.2 Representation of Numbers 256
12.1.3 The Fundamental Theorem of Algebra 257
12.1.4 Distribution of the Roots 257
12.1.5 Solvability in Radicals 258
12.1.6 The Method `Expression.roots()` 260
12.2 Numerical Solution 261
12.2.1 Location of Solutions of Algebraic Equations 262
12.2.2 Iterative Approximation Methods 263

13 Numerical Linear Algebra 277
13.1 Inexact Computations 277
13.1.1 Matrix Norms and Condition Number 278
13.2 Dense Matrices 281
13.2.1 Solving Linear Systems 281
13.2.2 Direct Resolution 281
13.2.3 The *LU* Decomposition 282
13.2.4 The Cholesky Decomposition 283
13.2.5 The *QR* Decomposition 284
13.2.6 Singular Value Decomposition 284
13.2.7 Application to Least Squares 285
13.2.8 Eigenvalues, Eigenvectors 288
13.2.9 Polynomial Curve Fitting: the Devil is Back 293
13.2.10 Implementation and Efficiency 296
13.3 Sparse Matrices 297
13.3.1 Where do Sparse Systems Come From? 297
13.3.2 Sparse Matrices in Sage 298
13.3.3 Solving Linear Systems 298

13.3.4 Eigenvalues, Eigenvectors 300
13.3.5 More Thoughts on Solving Large Non-Linear Systems . . 301

14 Numerical Integration 303
14.1 Numerical Integration 303
14.1.1 Available Integration Functions 309
14.1.2 Multiple Integrals 315
14.2 Solving Differential Equations 316
14.2.1 An Example 317
14.2.2 Available Functions 319

IV Combinatorics 323

15 Enumeration and Combinatorics 325
15.1 Initial Examples 326
15.1.1 Poker and Probability 326
15.1.2 Enumeration of Trees Using Generating Functions . . . 328
15.2 Common Enumerated Sets 334
15.2.1 First Example: Subsets of a Set 334
15.2.2 Integer Partitions 336
15.2.3 Some Other Finite Enumerated Sets 338
15.2.4 Set Comprehension and Iterators 341
15.3 Constructions 347
15.4 Generic Algorithms 349
15.4.1 Lexicographic Generation of Lists of Integers 349
15.4.2 Integer Points in Polytopes 351
15.4.3 Species, Decomposable Combinatorial Classes 352
15.4.4 Objects up to Isomorphism 354

16 Graph Theory 361
16.1 Constructing Graphs 361
16.1.1 Starting from Scratch 361
16.1.2 Available Constructors 363
16.1.3 Disjoint Unions 366
16.1.4 Graph Visualisation 367
16.2 Methods of the `Graph` Class 370
16.2.1 Modification of Graph Structure 370
16.2.2 Operators 370
16.2.3 Graph Traversal and Distances 372
16.2.4 Flows, Connectivity, Matching 373
16.2.5 NP-Complete Problems 374
16.2.6 Recognition and Testing of Properties 375
16.3 Graphs in Action 377
16.3.1 Greedy Vertex Colouring of a Graph 377
16.3.2 Generating Graphs Under Constraints 379
16.3.3 Find a Large Independent Set 380

16.3.4 Find an Induced Subgraph in a Random Graph 381
16.4 Some Problems Solved Using Graphs 383
16.4.1 A Quiz from the French Journal “Le Monde 2” 383
16.4.2 Task Assignment 384
16.4.3 Plan a Tournament 385

17 Linear Programming 387
17.1 Definition 387
17.2 Integer Programming 388
17.3 In Practice 388
17.3.1 The `MixedIntegerLinearProgram` Class 388
17.3.2 Variables 389
17.3.3 Infeasible or Unbounded Problems 390
17.4 First Applications in Combinatorics 391
17.4.1 Knapsack 391
17.4.2 Matching 392
17.4.3 Flow 393
17.5 Generating Constraints and Application 395

Annexes 403

A Answers to Exercises 403
A.1 First Steps 403
A.2 Analysis and Algebra 403
A.4 Graphics 412
A.5 Computational Domains 415
A.6 Finite Fields and Number Theory 417
A.7 Polynomials 421
A.8 Linear Algebra 425
A.9 Polynomial Systems 427
A.10 Differential Equations and Recurrences 430
A.11 Floating-Point Numbers 432
A.12 Non-Linear Equations 435
A.13 Numerical Linear Algebra 438
A.14 Numerical Integration 438
A.15 Enumeration and Combinatorics 440
A.16 Graph Theory 446
A.17 Linear Programming 447

B Bibliography 449

C Index 453

Part I

Getting to Grips with Sage