

---

# References

*Release 10.4*

**The Sage Development Team**

**Jul 20, 2024**



# CONTENTS

**Bibliography**

**3**



The references for Sage, sorted alphabetically by citation key.

REFERENCES:

*ABCDEFGHIJKLMNOPQRSTUVWXYZ*

**A**  
**B**  
**C**  
**D**  
**E**  
**F**  
**G**  
**H**  
**I**  
**J**  
**K**  
**L**  
**M**  
**N**  
**O**  
**P**  
**R**  
**S**  
**T**  
**U**  
**V**  
**W**  
**X**  
**Y**  
**Z**

- [Index](#)
- [Module Index](#)
- [Search Page](#)



## BIBLIOGRAPHY

- [AAGMRZ2019] M. Aagaard, R. AlTawy, G. Gong, K. Mandal, R. Rohit, N. Zidaric “WAGE: An Authenticated Cipher Submission to the NIST LWC Competition” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/wage-spec.pdf>
- [Ab1995] Julian R. Abel, On the Existence of Balanced Incomplete Block Designs and Transversal Designs, PhD Thesis, University of New South Wales, 1995
- [Ab2022] Willie Aboumrad, *Quantum computation with anyons: an F-matrix and braid calculator* (2022). <https://arxiv.org/abs/2212.00831>
- [Alekseyev2006] M. Alekseyev: (Forum post on counting irreducible multivariate polynomials), 2006. <https://dxdy.ru/post7034.html>
- [AB2007] M. Aschenbrenner, C. Hillar, *Finite generation of symmetric ideals*. Trans. Amer. Math. Soc. 359 (2007), no. 11, 5171–5192.
- [AB2008] M. Aschenbrenner, C. Hillar, *An Algorithm for Finding Symmetric Groebner Bases in Infinite Dimensional Rings*. arXiv 0801.4439.
- [ABBDHR2019] R. Avanzi, S. Banik, A. Bogdanov, O. Dunkelman, S. Huang, F. Regazzoni “Qameleonev. 1.0” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/qameleonev-spec.pdf>
- [ABBR2011] A. Abad, R. Barrio, F. Blesa, M. Rodriguez. “TIDES tutorial: Integrating ODEs by using the Taylor Series Method.” <http://www.unizar.es/acz/05Publicaciones/Monografias/MonografiasPublicadas/Monografia36/IndMonogr36.htm>
- [ABBR2012] A. Abad, R. Barrio, F. Blesa, M. Rodriguez. Algorithm 924. *ACM Transactions on Mathematical Software*, **39** no. 1 (2012), 1–28.
- [ABCFHLLMRT2019] A. Abdomicai, T. P. Berger, C. Clavier, J. Francq, P. Huynh, V. Lallemand, K. Le Gouguec, M. Minier, L. Reynaud, G. Thomas. “Lilliput-AE: a New Lightweight Tweakable Block-Cipher for Authenticated Encryption with Associated Data” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/LILLIPUT-AE-spec.pdf>
- [ABCMT2019] V. Arul, A. J. Best, E. Costa, R. Magner, and N. Triantafyllou, *Computing zeta functions of cyclic covers in large characteristic*, The Open Book Series, vol. 2, no. 1, pp. 37–53, Jan. 2019.
- [ABZ2007] R. Aharoni and E. Berger and R. Ziv. *Independent systems of representatives in weighted graphs*. Combinatorica vol 27, num 3, p253–267, 2007. doi:10.1007/s00493-007-2086-y.
- [AC1994] R.J.R. Abel and Y.W. Cheng, Some new MOLS of order  $2np$  for  $p$  a prime power, The Australasian Journal of Combinatorics, vol 10 (1994)

- [ACFLSS04] F. N. Abu-Khzam, R. L. Collins, M. R. Fellows, M. A. Langston, W. H. Suters, and C. T. Symons: Kernelization Algorithm for the Vertex Cover Problem: Theory and Experiments. *SIAM ALENEX/ANALCO* 2004: 62-69.
- [Ack2016] Lennart Ackermans, Oplosbaarheid van Kegelsneden. <http://www.math.leidenuniv.nl/nl/theses/Bachelor/>.
- [ACHRS2008] L. Addario-Berry, M. Chudnovsky, F. Havet, B. Reed, P. Seymour, *Bisimplicial vertices in even-hole-free graphs*. Journal of Combinatorial Theory, Series B, vol 98, n.6, pp 1119-1164, 2008. doi:10.1016/j.jctb.2007.12.006.
- [ABS2004] N. Alon, I. Benjamini and Alan Stacey, *Percolation on finite graphs and isoperimetric inequalities*, The Annals of Probability 32 (2004), no. 3A, 1727-1745.
- [ASV2020] Federico Ardila, Mariel Supina, and Andrés R. Vindas-Meléndez, *The Equivariant Ehrhart Theory of the Permutohedron*, Proc. Amer. Math. Soc. Volume 148, Number 12, 2020, pp. 5091–5107.
- [ADKF1970] V. Arlazarov, E. Dinic, M. Kronrod, and I. Faradzev. ‘On Economical Construction of the Transitive Closure of a Directed Graph.’ Dokl. Akad. Nauk. SSSR No. 194 (in Russian), English Translation in Soviet Math Dokl. No. 11, 1970.
- [ADKLPY2014] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, and T. Yalcin, *Block ciphers - focus on the linear layer (feat. PRIDE)*; in CRYPTO, (2014), pp. 57-76.
- [ABBS2013] J.-C Aval, A. Boussicault, M. Bouvel, M. Silimbani, *Combinatorics of non-ambiguous trees*, arXiv 1305.3716
- [AD2010] Arett, Danielle and Doree, Suzanne, *Coloring and counting on the Hanoi graphs*. Mathematics Magazine, Volume 83, Number 3, June 2010, pages 200-9. doi:10.4169/002557010X494841.
- [AE1993] A. Apostolico, A. Ehrenfeucht, Efficient detection of quasiperiodicities in strings, Theoret. Comput. Sci. 119 (1993) 247–265.
- [AG1988] George E. Andrews, F. G. Garvan, *Dyson’s crank of a partition*. Bull. Amer. Math. Soc. (N.S.) Volume 18, Number 2 (1988), 167-171. <http://projecteuclid.org/euclid.bams/1183554533>
- [AGHJLPR2017] Benjamin Assarf, Ewgenij Gawrilow, Katrin Herr, Michael Joswig, Benjamin Lorenz, Andreas Paffenholz, and Thomas Rehn, Computing convex hulls and counting integer points with polymake, Math. Program. Comput. 9 (2017), no. 1, 1–38, doi:10.1007/s12532-016-0104-z
- [AguSot05] Marcelo Aguiar and Frank Sottile, *Structure of the Malvenuto-Reutenauer Hopf algebra of permutations*, Advances in Mathematics, Volume 191, Issue 2, 1 March 2005, pp. 225–275, arXiv math/0203282v2.
- [AH2002] R. J. Aumann and S. Hart, Elsevier, eds. *Computing equilibria for two-person games*. <http://www.maths.lse.ac.uk/personal/stengel/TEXTE/nashsurvey.pdf> (2002)
- [AHK1994] Sheldon B. Akers, Doy Horel and Balakrishnan Krishnamurthy, *The star graph: An attractive alternative to the previous n-cube*. In Interconnection Networks for High-Performance Parallel Computers, pp. 145-152, 1994. IEEE. doi:10.5555/201173.201191
- [AHK2015] Karim Adiprasito, June Huh, and Eric Katz. *Hodge theory for combinatorial geometries*. arXiv 1511.02888.
- [AHKOS2014] Aubin Arroyo, Isabel Hubard, Klavdija Kutnar, Eugenia O’Reilly, and Primož Šparl. *Classification of Symmetric Tabčajn Graphs*. Graphs and Combinatorics 31:1137-1153, 2015. doi:10.1007/s00373-014-1447-8
- [AHMP2008] J.-P. Aumasson, L. Henzen, W. Meier, and R. C-W Phan, *Sha-3 proposal blake*; in Submission to NIST, (2008).
- [AHU1974] A. Aho, J. Hopcroft, and J. Ullman. ‘Chapter 6: Matrix Multiplication and Related Operations.’ The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974.

- [AIKMMNT2001] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, *Camellia: A 128-bit block cipher suitable for multiple platforms - Design and analysis*; in SAC, (2000), pp. 39–56.
- [Aj1996] M. Ajtai. Generating hard instances of lattice problems (extended abstract). STOC, pp. 99–108, ACM, 1996.
- [AK1994] S. Ariki and K. Koike. *A Hecke algebra of  $(\mathbb{Z}/r\mathbb{Z}) \wr \mathfrak{S}_n$  and construction of its irreducible representations*. Adv. Math. **106** (1994), 216–243, [MathSciNet MR1279219](#)
- [AKMMMP2002] Sang Yook An, Seog Young Kim, David C. Marshall, Susan H. Marshall, William G. McCallum, Alexander R. Perlis, *Jacobians of Genus One Curves*, Journal of Number Theory 90 (2002), pp.304–315, <http://www.math.arizona.edu/~wmc/Research/JacobianFinal.pdf>
- [AKMRVW] A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, C. Vincent, and M. West, *A robust implementation for solving the S-unit equation and several applications*. [arXiv 1903.00977](#)
- [AJL2011] S. Ariki, N. Jacon, and C. Lecouvey. *The modular branching rule for affine Hecke algebras of type A*. Adv. Math. 228:481–526, 2011.
- [Aki1980] J. Akiyama. and G. Exoo and F. Harary. Covering and packing in graphs. III: Cyclic and acyclic invariants. Mathematical Institute of the Slovak Academy of Sciences. Mathematica Slovaca vol 30, n 4, pages 405–417, 1980
- [Al1947] A. A. Albert, *A Structure Theory for Jordan Algebras*. Annals of Mathematics, Second Series, Vol. 48, No. 3 (Jul., 1947), pp. 546–567.
- [AL1978] A. O. L. Atkin and Wen-Ch'ing Winnie Li, Twists of newforms and pseudo-eigenvalues of  $W$ -operators. Inventiones Math. 48 (1978), 221–243.
- [AL2015] M. Aguiar and A. Lauve, *The characteristic polynomial of the Adams operators on graded connected Hopf algebras*. Algebra Number Theory, v.9, 2015, n.3, 2015.
- [Ald1990] D. Aldous, *The random walk construction of uniform spanning trees*, SIAM J Discrete Math 3 (1990), 450–465. [doi:10.1137/0403039](#).
- [ALPRRV2019] E. Andreeva, V. Lallemand, A. Purnal, R. Reyhanitabar, A. Roy, D. Vizar “ForkAE v.1” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/forkae-spec.pdf>
- [AM1969] **M. F. Atiyah and I. G. Macdonald, “Introduction to commutative algebra”, Addison-Wesley, 1969.**
- [AM1990] R. Abraham and J. E. Marsden, “Foundations of Mechanics”, Addison-Wesley, 1980.
- [AM1974] J. F. Adams and H. R. Margolis, “Sub-Hopf-algebras of the Steenrod algebra,” Proc. Cambridge Philos. Soc. 76 (1974), 45–52.
- [AM2000] S. Ariki and A. Mathas. *The number of simple modules of the Hecke algebras of type  $G(r, 1, n)$* . Math. Z. 233 (2000), no. 3, 601–623. [MathSciNet MR1750939](#)
- [AM2020] A. L. Agore and G. Militaru. *A new invariant for finite dimensional Leibniz/Lie algebras*. Preprint, [arXiv 2006.00711](#) (2020).
- [AMOZ2006] Asahiro, Y. and Miyano, E. and Ono, H. and Zenmyo, K., *Graph orientation algorithms to minimize the maximum outdegree*. Proceedings of the 12th Computing: The Australasian Theory Symposium, Volume 51, page 20. Australian Computer Society, Inc. 2006.
- [Ang1997] B. Anglès. 1997. *On some characteristic polynomials attached to finite Drinfeld modules*. manuscripta mathematica 93, 1 (01 Aug 1997), 369–379. <https://doi.org/10.1007/BF02677478>
- [AP1986] S. Arnborg, A. Proskurowski, *Characterization and Recognition of Partial 3-Trees*, SIAM Journal of Alg. and Discrete Methods, Vol. 7, pp. 305–314, 1986. [doi:10.1137/0607033](#).

- [Ap1997] T. Apostol, *Modular functions and Dirichlet series in number theory*, Springer, 1997 (2nd ed), section 3.7–3.9.
- [APR2001] George E. Andrews, Peter Paule, Axel Riese, *MacMahon's partition analysis: the Omega package*, European J. Combin. 22 (2001), no. 7, 887–904.
- [Ar2006] D. Armstrong. *Generalized noncrossing partitions and combinatorics of Coxeter groups*. Mem. Amer. Math. Soc., 2006.
- [AR2012] D. Armstrong and B. Rhoades. “The Shi arrangement and the Ish arrangement”. Transactions of the American Mathematical Society 364 (2012), 1509–1528. [arXiv 1009.1655](#)
- [Ariki1996] S. Ariki. *On the decomposition numbers of the Hecke algebra of  $G(m, 1, n)$* . J. Math. Kyoto Univ. 36 (1996), no. 4, 789–808. [MathSciNet MR1443748](#)
- [Ariki2001] S. Ariki. *On the classification of simple modules for cyclotomic Hecke algebras of type  $G(m, 1, n)$  and Kleshchev multipartitions*. Osaka J. Math. 38 (2001), 827–837. [MathSciNet MR1864465](#)
- [Arn2002] P. Arnoux, Sturmian sequences, in *Substitutions in Dynamics*, N. Pytheas Fogg (Ed.), Arithmetics, and Combinatorics (Lecture Notes in Mathematics, Vol. 1794), 2002.
- [Ass1978] J. Assion: *Einige endliche Faktorgruppen der Zopfgruppen*, Math. Z., 163 (1978), 291–302.
- [ARVT2005] Michael Artin, Fernando Rodriguez-Villegas, John Tate, On the Jacobians of plane cubics, *Advances in Mathematics* 198 (2005) 1, pp. 366–382 doi:10.1016/j.aim.2005.06.004 <http://www.math.utexas.edu/users/villegas/publications/jacobian-cubics.pdf>
- [AS-Bessel] F. W. J. Olver: 9. Bessel Functions of Integer Order, in Abramowitz and Stegun: *Handbook of Mathematical Functions*. [https://personal.math.ubc.ca/~cbm/aands/page\\_355.htm](https://personal.math.ubc.ca/~cbm/aands/page_355.htm)
- [AS-Spherical] H. A. Antosiewicz: 10. Bessel Functions of Fractional Order, in Abramowitz and Stegun: *Handbook of Mathematical Functions*. [https://personal.math.ubc.ca/~cbm/aands/page\\_435.htm](https://personal.math.ubc.ca/~cbm/aands/page_435.htm)
- [AS-Struve] M. Abramowitz: 12. Struve Functions and Related Functions, in Abramowitz and Stegun: *Handbook of Mathematical Functions*. [https://personal.math.ubc.ca/~cbm/aands/page\\_495.htm](https://personal.math.ubc.ca/~cbm/aands/page_495.htm)
- [AS1964] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, National Bureau of Standards Applied Mathematics Series, 55. 1964. See also <https://personal.math.ubc.ca/~cbm/aands/>.
- [As2008] Sami Assaf. *A combinatorial realization of Schur-Weyl duality via crystal graphs and dual equivalence graphs*. FPSAC 2008, 141–152, Discrete Math. Theor. Comput. Sci. Proc., AJ, Assoc. Discrete Math. Theor. Comput. Sci., (2008). [arXiv 0804.1587v1](#)
- [AO2018] Sami Assaf and Ezgi Kantarci Oguz. *A local characterization of crystals for the quantum queer superalgebra*. Preprint (2018). [arXiv 1803.06317](#)
- [AS2003] Jean-Paul Allouche, Jeffrey Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, 2003.
- [As2008b] Sami Assaf. *Dual equivalence graphs and a combinatorial proof of LLT and Macdonald positivity*. (2008). [arXiv 1005.3759v5](#).
- [AS2011] R.B.J.T Allenby and A. Slomson, “How to count”, CRC Press (2011)
- [ASD1971] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, “Modular forms on noncongruence subgroups”, Proc. Symp. Pure Math., Combinatorics (T. S. Motzkin, ed.), vol. 19, AMS, Providence 1971
- [At1990] M. D. Atkinson. *On computing the number of linear extensions of a tree*. Order 7 (1990) 20–25.
- [At1992] M. D. Atkinson. *Solomon's descent algebra revisited*. Bull. London Math. Soc. 24 (1992) 545–551. <http://www.cs.otago.ac.nz/staffpriv/mike/Papers/Descent/DescAlgRevisited.pdf>

- [Atk1992] A. Oliver L. Atkin. ‘Probabilistic primality testing’ (Chapter 30, Section 4) In Ph. Flajolet and P. Zimmermann, editors, *Algorithms Seminar*, 1991-1992. INRIA Research Report 1779, 1992, <http://www.inria.fr/rrrt/rr-1779.html>. Summary by F. Morain. <http://citeseer.ist.psu.edu/atkin92probabilistic.html>
- [Ath1996] C. A. Athanasiadis, *Characteristic polynomials of subspace arrangements and finite fields*. *Advances in Mathematics*, 122(2):193-233, 1996.
- [Ath2000] C. A. Athanasiadis, *Deformations of Coxeter hyperplane arrangements and their characteristic polynomials*. *Adv. Stud. Pure Math.*, 27, 2000.
- [Av2000] D. Avis, *A revised implementation of the reverse search vertex enumeration algorithm*. *Polytopes-combinatorics and computation*. Birkhauser Basel, 2000.
- [Ava2007] J.-C. Aval. *Keys and alternating sign matrices*. *Sem. Lothar. Combin.* 59 (2007/10), Art. B59f, 13 pp.
- [Ava2017] R. Avanzi, *The QARMA block cipher family*; in ToSC, (2017.1), pp. 4-44.
- [AW2006] Adams, M.D. and Wise, D.S., *Fast additions on masked integers*, *ACM SIGPLAN Notices*, 2006, vol. 41, n.5, pages 39–45. doi:10.1145/1149982.1149987. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.86.1801&rep=rep1&type=pdf>
- [AY1983] I. A. Aizenberg and A. P. Yuzhakov. *Integral representations and residues in multidimensional complex analysis*. *Translations of Mathematical Monographs*, **58**. American Mathematical Society, Providence, RI. (1983). x+283 pp. ISBN: 0-8218-4511-X.
- [AZZ2005] V. Anne, L.Q. Zamboni, I. Zorca, *Palindromes and Pseudo- Palindromes in Episturmian and Pseudo-Palindromic Infinite Words*, in : S. Brlek, C. Reutenauer (Eds.), *Words 2005*, Publications du LaCIM, Vol. 36 (2005) 91–100.
- [Bab86] L. Babai. *On Lovász’ lattice reduction and the nearest lattice point problem*, *Combinatorica*, 6(1), 1986, 1-13. doi:10.1007/BF02579403.
- [Baer2020] Christian Bär. *The Faddeev-LeVerrier algorithm and the Pfaffian*. *arXiv 2008.04247*, 2020.
- [BaKi2001] Bakalov and Kirillov, *Lectures on tensor categories and modular functors*, AMS (2001).
- [BRP2018] Basson D., Breuer F., Pink R., *Drinfeld modular forms of arbitrary rank. Part I: arXiv 1805.12335*, Part II: *arXiv 1805.12337*, Part III: *arXiv 1805.12339*, 2018.
- [Ba1994] Kaushik Basu. *The Traveler’s Dilemma: Paradoxes of Rationality in Game Theory*. *The American Economic Review* (1994): 391-395.
- [BaSt1990] Margaret M. Bayer and Bernd Sturmfels. *Lawrence polytopes*. *Canadian J. Math.* 42 (1990), 62–79.
- [BAK1998] E. Biham, R. J. Anderson, and L. R. Knudsen, *Serpent: A new block cipher proposal*; in *FSE*, (1998), pp. 222-238.
- [Bar1970] Barnette, “Diagrams and Schlegel diagrams”, in *Combinatorial Structures and Their Applications*, *Proc. Calgary Internat. Conference 1969*, New York, 1970, Gordon and Breach.
- [Bar2006] G. Bard. ‘Accelerating Cryptanalysis with the Method of Four Russians’. *Cryptography E-Print Archive* (<http://eprint.iacr.org/2006/251.pdf>), 2006.
- [Bat1991] V. V. Batyrev, *On the classification of smooth projective toric varieties*, *Tohoku Math. J.* **43** (1991), 569-585
- [Bat1994] Victor V. Batyrev, “Dual polyhedra and mirror symmetry for Calabi-Yau hypersurfaces in toric varieties”, *J. Algebraic Geom.* 3 (1994), no. 3, 493-535. [arXiv alg-geom/9310003v1](https://arxiv.org/abs/alg-geom/9310003v1)
- [Baz2011] Ivan Bazhov, *On orbits of the automorphism group on a complete toric variety*. *Beitr Algebra Geom* (2013) 54: 471, [arXiv 1110.4275](https://arxiv.org/abs/1110.4275), doi:10.1007/s13366-011-0084-0.
- [BB1997] Mladen Bestvina and Noel Brady. *Morse theory and finiteness properties of groups*. *Invent. Math.* **129** (1997). No. 3, 445-470. [www.math.ou.edu/~nbrady/papers/morse.ps](http://www.math.ou.edu/~nbrady/papers/morse.ps).

- [BB2005] A. Björner, F. Brenti. *Combinatorics of Coxeter groups*. New York: Springer, 2005.
- [BB2005a] V. Batagelj and U. Brandes. *Efficient generation of large random networks*. Phys. Rev. E, 71, 036113, 2005. doi:10.1103/PhysRevE.71.036113.
- [BB2009] Tomas J. Boothby and Robert W. Bradshaw. *Bitslicing and the Method of Four Russians Over Larger Finite Fields*. arXiv 0901.1413, 2009.
- [BB2013] Gavin Brown, Jaroslaw Buczynski: *Maps of toric varieties in Cox coordinates*, arXiv 1004.4924
- [BBBCDGLLLMPPSW2019] D. Bellizia, F. Berti, O. Bronchain, G. Cassiers, S. Duval, C. Guo, G. Leander, G. Leurent, I. Levi, C. Momin, O. Pereira, T. Peters, F. Standeart, F. Wiemer. “Spook: Sponge-Based Leakage-Resilient Authenticated Encryption with a Masked Tweakable Block Cipher” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Spook-spec.pdf>
- [BCDM2019] T. Beyne, Y. L. Chen, C. Dobraunig, B. Mennink. *Elephant v1* (2019) <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/elephant-spec.pdf>
- [BCL2022] Paolo Bellingeri, Hugo Chemin, and Victoria Lebed. *Cactus groups, twin groups, and right-angled Artin groups*. Preprint, arXiv 2209.08813 (2022).
- [BeBo2009] Olivier Bernardi and Nicolas Bonichon, *Intervals in Catalan lattices and realizers of triangulations*, JCTA 116 (2009)
- [BBGL2008] A. Blondin Massé, S. Brlek, A. Garon, and S. Labbé, Combinatorial properties of  $f$ -palindromes in the Thue-Morse sequence. Pure Math. Appl., 19(2-3):39–52, 2008.
- [BBHP2004] Anne Berry, Jean R. S. Blair, Pinar Heggernes, Barry W. Peyton. *Maximum Cardinality Search for Computing Minimal Triangulations of Graphs*. Algorithmica 39(4):287-298, 2004. doi:10.1007/s00453-004-1084-3
- [BBISHAR2015] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, *Midori: A block cipher for low energy*; in ASIACRYPT, (2015), pp. 411-436.
- [BBKMW2013] B. Bilgin, A. Bogdanov, M. Knezevic, F. Mendel, and Q. Wang, *Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware*; in CHES, (2013), pp. 142-158.
- [BBLSW1999] Babson, Björner, Linusson, Shareshian, and Welker, *Complexes of not  $i$ -connected graphs*, Topology 38 (1999), 271-299
- [BBMF2008] N. Bonichon, M. Bousquet-Mélou, E. Fusy. *Baxter permutations and plane bipolar orientations*. Séminaire Lotharingien de combinatoire 61A, article B61Ah, 2008.
- [BCDGNPY2019] Z. Bao, A. Chakraborti, N. Datta, J. Guo, M. Nandi, T. Peyrin, K. Yasuda. “PHOTON-Beetle Authenticated Encryption and Hash Family” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/PHOTON-Beetle-spec.pdf>
- [BH1965] L. D. Baumert, M. Hall Jr. *A new construction for Hadamard matrices*. Bulletin of the American Mathematical Society 71(1):169-170, 1965.
- [Bodin2007] A. Bodin: Number of irreducible polynomials in several variables over finite fields, The American Mathematical Monthly 115(7), pp. 653-660, 2008. <https://arxiv.org/abs/0706.0157>
- [BH2012] A. Brouwer and W. Haemers, Spectra of graphs, Springer, 2012, <http://homepages.cwi.nl/~aeb/math/ipm/ipm.pdf>
- [BMFPR2011] M. Bousquet-Mélou, É. Fusy, L.-F. Préville-Ratelle, *The number of intervals in the  $m$ -Tamari lattices*. Electronic Journal of Combinatorics 18(2), 2011. doi:10.37236/2027
- [BPPSST2017] Banik, Pandey, Peyrin, Sasaki, Sim, and Todo, GIFT : A Small Present Towards Reaching the Limit of Lightweight Encryption. *Cryptographic Hardware and Embedded Systems - CHES 2017*, 2017.

- [BPW2006] J. Buchmann, A. Pychkine, R.-P. Weinmann *Block Ciphers Sensitive to Groebner Basis Attacks* in Topics in Cryptology – CT RSA’06; LNCS 3860; pp. 313–331; Springer Verlag 2006; pre-print available at <http://eprint.iacr.org/2005/200>
- [BBS1982] L. Blum, M. Blum, and M. Shub. Comparison of Two Pseudo-Random Number Generators. *Advances in Cryptology: Proceedings of Crypto ’82*, pp.61–78, 1982.
- [BBS1986] L. Blum, M. Blum, and M. Shub. A Simple Unpredictable Pseudo-Random Number Generator. *SIAM Journal on Computing*, 15(2):364–383, 1986.
- [BIANCO] L. Bianco, P. Dell’Olmo, S. Giordani An Optimal Algorithm to Find the Jump Number of Partially Ordered Sets Computational Optimization and Applications, 1997, Volume 8, Issue 2, pp 197–210, doi:10.1023/A:1008625405476
- [BC1977] R. E. Bixby, W. H. Cunningham, Matroids, Graphs, and 3-Connectivity. In Graph theory and related topics (Proc. Conf., Univ. Waterloo, Waterloo, ON, 1977), 91-103
- [BC2003] A. Biryukov and C. D. Canniere *Block Ciphers and Systems of Quadratic Equations*; in Proceedings of Fast Software Encryption 2003; LNCS 2887; pp. 274-289, Springer-Verlag 2003.
- [BC2012] Mohamed Barakat and Michael Cuntz. “Coxeter and crystallographic arrangements are inductively free.” *Adv. in Math.* **229** Issue 1 (2012). pp. 691-709. doi:10.1016/j.aim.2011.09.011, arXiv 1011.4228.
- [BC2018] Patrick Brosnan and Timothy Y. Chow. *Unit interval orders and the dot action on the cohomology of regular semisimple Hessenberg varieties*. *Advances in Mathematics* 329 (2018): 955-1001. doi:10.1016/j.aim.2018.02.020, arXiv 1511.00773v1.
- [BCCCNSY2010] Charles Bouillaguet, Hsieh-Chung Chen, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, Adi Shamir, and Bo-Yin Yang. *Fast exhaustive search for polynomial systems in GF(2)*. In Stefan Mangard and François-Xavier Standaert, editors, CHES, volume 6225 of Lecture Notes in Computer Science, pages 203–218. Springer, 2010. pre-print available at <http://eprint.iacr.org/2010/313.pdf>
- [BCCM2015] M. Borassi, D. Coudert, P. Crescenzi, and A. Marino. On Computing the Hyperbolicity of Real-World Graphs. *Proceedings of the 23rd European Symposium on Algorithms (ESA 2015)*, doi:10.1007/978-3-662-48350-3\_19.
- [BCdLOG2000] Volker Braun, Philip Candelas, Xendia de la Ossa, Antonella Grassi, *Toric Calabi-Yau Fourfolds, Duality Between  $N=1$  Theories and Divisors that Contribute to the Superpotential*, arXiv hep-th/0001208
- [BCGKKKLNPRRTY2012] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalcin, *PRINCE - A low-latency block cipher for pervasive computing applications*; in ASIACRYPT, (2012), pp. 208-225.
- [BCH2002] G. Brinkmann, G. Caporossi and P. Hansen, *A Constructive Enumeration of Fusenes and Benzenoids*, *Journal of Algorithms*, 45:155-166, 2002. doi:10.1016/S0196-6774(02)00215-8.
- [BCHOPSY2017] G. Benkart, L. Colmenarejo, P. E. Harris, R. Orellana, G. Panova, A. Schilling, M. Yip. *A minimaj-preserving crystal on ordered multiset partitions*. *Advances in Applied Math.* 95 (2018) 96-115, doi:10.1016/j.aam.2017.11.006. arXiv 1707.08709v2.
- [BCJ2007] Gregory V. Bard, and Nicolas T. Courtois, and Chris Jefferson. *Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers*. *Cryptology ePrint Archive: Report 2007/024*. available at <http://eprint.iacr.org/2007/024>
- [BCM15] Michele Borassi, Pierluigi Crescenzi, and Andrea Marino, Fast and Simple Computation of Top-k Closeness Centralities. arXiv 1507.01490.
- [BCMS1988] I. Z. Bouwer, W. W. Chernoff, B. Monson, and Z. Star. *The Foster Census*, Charles Babbage Research Centre, 1988.
- [BCN1989] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-Regular Graphs*, Springer, 1989.

- [BdJ2008] Besser, Amnon, and Rob de Jeu. “Li<sup>p</sup>-Service? An Algorithm for Computing p-Adic Polylogarithms.” *Mathematics of Computation* (2008): 1105-1134.
- [BDLS2020] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith: Faster computation of isogenies of large prime degree. ANTS XIV, Open Book Series Vol. 4, No. 1, 2020. [arXiv 2003.10118](#)
- [BD1989] R. J. Bradford and J. H. Davenport, *Effective tests for cyclotomic polynomials*, Symbolic and Algebraic Computation (1989), pp. 244–251, [doi:10.1007/3-540-51084-2\\_22](#)
- [BD2004] M. Becker and A. Desoky. *A study of the DVD content scrambling system (CSS) algorithm*; in Proceedings of ISSPIT, (2004), pp. 353-356.
- [BD2007] Michael Brickenstein, Alexander Dreyer; *PolyBoRi: A Groebner basis framework for Boolean polynomials*; pre-print available at [http://www.itwm.fraunhofer.de/fileadmin/ITWM-Media/Zentral/Pdf/Berichte\\_ITWM/2007/bericht122.pdf](http://www.itwm.fraunhofer.de/fileadmin/ITWM-Media/Zentral/Pdf/Berichte_ITWM/2007/bericht122.pdf)
- [BDHPR2019] Marthe Bonamy, Oscar Defrain, Marc Heinrich, Michał Pilipczuk, and Jean-Florent Raymond. *Enumerating minimal dominating sets in  $K_t$ -free graphs and variants*. [arXiv 1810.00789](#)
- [BDKR2013] D. Best, D.Ž. Đoković, H. Kharaghani and H. Ramp. *Turyn-Type Sequences: Classification, Enumeration, and Construction*, *Journal of Combinatorial Designs* 21(1) (2013): 24-35. [doi:10.1002/jcd.21318](#)
- [BDLV2006] S. Brlek, S. Dulucq, A. Ladouceur, L. Vuillon, *Combinatorial properties of smooth infinite words*, *Theoret. Comput. Sci.* 352 (2006) 306–317.
- [BDP2013] Thomas Brüstle, Grégoire Dupont, Matthieu Pérotin *On Maximal Green Sequences* [arXiv 1205.2050](#)
- [BDPR2011] Marcus Bishop, J. Matthew Douglass, Götz Pfeiffer, Gerhard Röhrle, *Computations for Coxeter arrangements and Solomon’s descent algebra: Groups of rank three and four*; *Journal of symbolic computation*, volume 50, 03-2013, pp. 139-158.
- [BDMW2010] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe, *An APN permutation in dimension six*; in *Finite Fields: Theory and Applications - FQ9*, volume 518 of *Contemporary Mathematics*, pages 33–42. AMS, 2010.
- [BdVO2012] Christopher Bowman, Maud De Visscher, Rosa Orellana. *The partition algebra and the Kronecker coefficients*. [arXiv 1210.5579v6](#).
- [BE1992] A. Brouwer and C. Van Eijl, *On the p-Rank of the Adjacency Matrices of Strongly Regular Graphs*, *Journal of Algebraic Combinatorics* (1992), vol.1, n.4, pp329-346, [doi:10.1023/A%3A1022438616684](#).
- [Bec1992] Bernhard Beckermann. “A reliable method for computing M-*Padé* approximants on arbitrary staircases”. *J. Comput. Appl. Math.*, 40(1):19-42, 1992. [doi:10.1016/0377-0427\(92\)90039-Z](#).
- [BeCoMe] Frits Beukers, Henri Cohen, Anton Mellit, *Finite hypergeometric functions*, [arXiv 1505.02900](#)
- [BEdG2009] Dietrich Burde, Bettina Eick, and Willem de Graaf. *Computing faithful representations for nilpotent Lie algebras*. *J. Algebra*, **322** no. 3 (2009) pp. 602-612. [doi:10.1016/j.jalgebra.2009.04.041](#), [arxiv:0807.2345](#).
- [Bee] Robert A. Beezer, *A First Course in Linear Algebra*, <http://linear.ups.edu/>. Accessed 15 July 2010.
- [Bei1970] Lowell Beineke, *Characterizations of derived graphs*, *Journal of Combinatorial Theory*, Vol. 9(2), pages 129-135, 1970. [doi:10.1016/S0021-9800\(70\)80019-9](#).
- [Bel2011] Belarusian State University, *Information technologies. Data protection. Cryptographic algorithms for encryption and integrity control*; in STB 34.101.31-2011, (2011).
- [Bel1927] E.T. Bell, *Partition Polynomials*, *Annals of Mathematics*, Second Series, Vol. 29, No. 1/4 (1927 - 1928), pp. 38-46
- [Ben1998] I. Benjamini, *Expanders are not hyperbolic*, *Israel Journal of Mathematics* 108 (1998), 33-36.

- [BS1997] I. Benjamini and O. Schramm, *Every graph with a positive Cheeger constant contains a tree with a positive Cheeger constant*, Geometric and Functional Analysis 7 (1997), no. 3, 403-419.
- [Ben2019] Benedetto, Robert L. Dynamics in one non-archimedean variable. Graduate Studies in Mathematics, Volume 198. 2019.
- [Benasque2009] Fernando Rodriguez Villegas, *The L-function of the quintic*, <http://users.ictp.it/~villegas/hgm/benasque-2009-report.pdf>
- [Ber1987] M. Berger, *Geometry I*, Springer (Berlin) (1987); doi:10.1007/978-3-540-93815-6
- [Ber1987a] M. Berger, *Geometry II*, Springer (Berlin) (1987); doi:10.1007/978-3-540-93816-3
- [Ber1991] C. Berger, “Une version effective du théorème de Hurewicz”, <https://tel.archives-ouvertes.fr/tel-00339314/en/>.
- [Ber2007] Jean Berstel. Sturmian and episturmian words (a survey of some recent results). In S. Bozapalidis and G. Rahonis, editors, CAI 2007, volume 4728 of Lecture Notes in Computer Science, pages 23-47. Springer-Verlag, 2007.
- [Ber2008] W. Bertram : *Differential Geometry, Lie Groups and Symmetric Spaces over General Base Fields and Rings*, Memoirs of the American Mathematical Society, vol. 192 (2008); doi:10.1090/memo/0900; arXiv math/0502168
- [BerZab05] Nantel Bergeron, Mike Zabrocki, *The Hopf algebras of symmetric functions and quasisymmetric functions in non-commutative variables are free and cofree*, J. of Algebra and its Applications (8)(2009), No 4, pp. 581–600, doi:10.1142/S0219498809003485, arXiv math/0509265v3.
- [BeukersHeckman] F. Beukers and G. Heckman, *Monodromy for the hypergeometric function  ${}_nF_{n-1}$* , Invent. Math. 95 (1989)
- [BF1999] Thomas Britz, Sergey Fomin, *Finite posets and Ferrers shapes*, Advances in Mathematics 158, pp. 86-127 (2001), arXiv math/9912126 (the arXiv version has fewer errors).
- [BF2001] Boucheron, S. and Fernandez de la Vega, W., *On the Independence Number of Random Interval Graphs*, Combinatorics, Probability and Computing v10, issue 05, Pages 385–396, Cambridge Univ Press, 2001. doi:10.1017/S0963548301004813.
- [BF2005] R.L. Burden and J.D. Faires. *Numerical Analysis*. 8th edition, Thomson Brooks/Cole, 2005.
- [BFS2004] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy, On the complexity of Groebner basis computation of semi-regular overdetermined algebraic equations. Proc. International Conference on Polynomial System Solving (ICPSS), pp. 71-75, 2004.
- [BFSS2006] A. Bostan, P. Flajolet, B. Salvy and E. Schost, *Fast Computation of special resultants*, Journal of Symbolic Computation 41 (2006), 1-29
- [BFZ2005] A. Berenstein, S. Fomin, and A. Zelevinsky, *Cluster algebras. III. Upper bounds and double Bruhat cells*, Duke Math. J. 126 (2005), no. 1, 1–52.
- [BG1972] A. Berman and P. Gaiha. A generalization of irreducible monotonicity. Linear Algebra and its Applications, 5:29-38, 1972.
- [BG1980] R. L. Bishop and S. L. Goldberg, *Tensor analysis on Manifolds*, Dover (New York) (1980)
- [BG1985] M. Blum and S. Goldwasser. An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pp. 289–299, Springer, 1985.
- [BG1988] M. Berger & B. Gostiaux : *Differential Geometry: Manifolds, Curves and Surfaces*, Springer (New York) (1988); doi:10.1007/978-1-4612-1033-7
- [BG2013] J. A. Baldwin and J. E. Grigsby, *Categorified invariants and the braid group*, arXiv 1212.2222

- [BGM2012] G. Brinkmann, J. Goedgebeur and B.D. McKay, *Generation of Fullerenes*, Journal of Chemical Information and Modeling, 52(11):2910-2918, 2012. doi:10.1021/ci3003107.
- [BI1984] Eiichi Bannai, Tatsuro Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin/Cummings, 1984
- [Bil2011] N. Billerey. *Critères d'irréductibilité pour les représentations des courbes elliptiques*. Int. J. Number Theory, 7 (2011); doi:10.1142/S1793042111004538
- [BH1994] S. Billey, M. Haiman. *Schubert polynomials for the classical groups*. J. Amer. Math. Soc., 1994.
- [BH2017] Georgia Benkart and Tom Halverson. *Partition algebras  $P_k(n)$  with  $2k > n$  and the fundamental theorems of invariant theory for the symmetric group  $S_n$* . Preprint (2017). arXiv 1707.1410
- [BHKP2008] Anand Bhalgat, Ramesh Hariharan, Telikepalli Kavitha and Debmalya Panigraha. *Fast edge splitting and Edmonds' arborescence construction for unweighted graphs*. ACM-SIAM Symposium on Discrete Algorithms (SODA), pp 455-464, 2008. doi:10.5555/1347082.1347132
- [BHS2008] Robert Bradshaw, David Harvey and William Stein. strassen\_window\_multiply\_c. strassen.pyx, Sage 3.0, 2008. <http://www.sagemath.org>
- [BHS2023] Jose Bastidas, Christophe Hohlweg, and Franco Saliola. *The primitive Eulerian polynomial*. Preprint, (2023) arXiv 2306.15556.
- [BrHu2019] Petter Brändén, June Huh. *Lorentzian polynomials*. Ann. Math. (2) 192, No. 3, 821-891 (2020). arXiv 1902.03719, doi:10.4007/annals.2020.192.3.4.
- [BHN2004] S. Brlek, S. Hamel, M. Nivat, C. Reutenauer, On the Palindromic Complexity of Infinite Words, in J. Berstel, J. Karhumäki, D. Perrin, Eds, Combinatorics on Words with Applications, International Journal of Foundation of Computer Science, Vol. 15, No. 2 (2004) 293–306.
- [BHZ2005] N. Bergeron, C. Hohlweg, and M. Zabrocki, *Posets related to the Connectivity Set of Coxeter Groups*. arXiv math/0509271v3
- [Big1993] Norman Linstead Biggs. *Algebraic Graph Theory*, 2nd ed. Cambridge University Press, 1993. doi:10.1017/CBO9780511608704
- [Big1999] Stephen J. Bigelow. The Burau representation is not faithful for  $n = 5$ . Geom. Topol., 3:397–404, 1999.
- [Big2003] Stephen J. Bigelow, *The Lawrence-Krammer representation*, Geometric Topology, 2001 Georgia International Topology Conference, AMS/IP Studies in Advanced Mathematics 35 (2003). arXiv math/0204057v1
- [BIP] Rene Birkner, Nathan Owen Ilten, and Lars Petersen: Computations with equivariant toric vector bundles, The Journal of Software for Algebra and Geometry: Macaulay2. <http://msp.org/jsag/2010/2-1/p03.xhtml> <http://www.math.uiuc.edu/Macaulay2/doc/Macaulay2-1.8.2/share/doc/Macaulay2/ToricVectorBundles/html/>
- [Bir1975] J. Birman. *Braids, Links, and Mapping Class Groups*, Princeton University Press, 1975
- [Bj1980] Anders Björner, *Shellable and Cohen-Macaulay partially ordered sets*, Trans. Amer. Math. Soc. 260 (1980), 159-183, doi:10.1090/S0002-9947-1980-0570784-2
- [BjWe2005] A. Björner and V. Welker, *Segre and Rees products of posets, with ring-theoretic applications*, J. Pure Appl. Algebra 198 (2005), 43-55
- [BJKLMPSSS2016] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, *The SKINNY family of block ciphers and its low-latency variant MANTIS*; in CRYPTO, (2016), pp. 123-153.
- [BK1973] Coen Bron and Joep Kerbosch. *Algorithm 457: Finding All Cliques of an Undirected Graph*. Commun. ACM. v 16. n 9. 1973, pages 575-577. ACM Press. [Online] Available: <http://www.ram.org/computing/rambin/rambin.html>

- [BK1977] James R. Bunch and Linda Kaufman. Some Stable Methods for Calculating Inertia and Solving Symmetric Linear Systems. *Mathematics of Computation*, 31(137):163-179, 1977.
- [BK1992] U. Brehm and W. Kuhnel, *15-vertex triangulations of an 8-manifold*, *Math. Annalen* 294 (1992), no. 1, 167-193.
- [BK2001] W. Bruns and R. Koch, *Computing the integral closure of an affine semigroup*. *Uni. Iagellonicae Acta Math.* 39, (2001), 59-70
- [BK2008] J. Brundan and A. Kleshchev. *Blocks of cyclotomic Hecke algebras and Khovanov-Lauda algebras*. *Invent. Math.* 178 (2009), no. 3, 451–484. [MathSciNet MR2551762](#)
- [BK2009] J. Brundan and A. Kleshchev. *Graded decomposition numbers for cyclotomic Hecke algebras*. *Adv. Math.* 222 (2009), 1883–1942. [MathSciNet MR2562768](#)
- [BK2017] Pascal Baseilhac and Stefan Kolb. *Braid group action and root vectors for the  $q$ -Onsager algebra*. Preprint, (2017) [arXiv 1706.08747](#).
- [BK2005] P. Baseilhac and K. Koizumi. *A new (in)finite dimensional algebra for quantum integrable models*. *Nuclear Phys. B* 720 (2005), pp. 325-347.
- [BKK2000] Georgia Benkart, Seok-Jin Kang, Masaki Kashiwara. *Crystal bases for the quantum superalgebra  $U_q(\mathfrak{gl}(m, n))$* , *J. Amer. Math. Soc.* 13 (2000), no. 2, 295-331.
- [BKLPPRSV2007] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, C. Viskell-soe. *PRESENT: An Ultra-Lightweight Block Cipher*; in *Proceedings of CHES 2007*; LNCS 7427; pp. 450-466; Springer Verlag 2007; available at [doi:10.1007/978-1-4419-5906-5\\_605](#)
- [BKW2011] J. Brundan, A. Kleshchev, and W. Wang, *Graded Specht modules*, *J. Reine Angew. Math.*, 655 (2011), 61-87. [MathSciNet MR2806105](#)
- [BL1994] Bernhard Beckermann, George Labahn. “A Uniform Approach for the Fast Computation of Matrix-Type Padé Approximants”. *SIAM J. Matrix Anal. Appl.* 15 (1994) 804-823. [doi:10.1137/S0895479892230031](#)
- [BHMPW20a] Tom Braden, June Huh, Jacob P. Matherne, Nicholas Proudfoot, and Botong Wang, *A semi-small decomposition of the Chow ring of a matroid*, [arXiv 2002.03341](#) (2020).
- [BHMPW20b] Tom Braden, June Huh, Jacob P. Matherne, Nicholas Proudfoot, and Botong Wang, *Singular Hodge theory for combinatorial geometries*, [arXiv 2010.06088](#) (2020).
- [BMP2007] S. Brlek, G. Melançon, G. Paquin, Properties of the extremal infinite smooth words, *Discrete Math. Theor. Comput. Sci.* 9 (2007) 33–49.
- [BMPS2018] Jonah Blasiak, Jennifer Morse, Anna Pun, and Daniel Summers. *Catalan functions and  $k$ -schur positivity* [arXiv 1804.03701](#)
- [BL1977] Buckles, B.P. and Lybanon, M., *Algorithm 515: generation of a vector from the lexicographical index*, *ACM Transactions on Mathematical Software (TOMS)*, 1977 vol. 3, n. 2, pages 180–182.
- [BL1984] A. Brouwer, J. van Lint, *Strongly regular graphs and partial geometries*, *Enumeration and design*, (Waterloo, Ont., 1982) (1984): 85-122. <http://oai.cwi.nl/oai/asset/1817/1817A.pdf>
- [BL2000] Anders Björner and Frank H. Lutz, “Simplicial manifolds, bistellar flips and a 16-vertex triangulation of the Poincaré homology 3-sphere”, *Experiment. Math.* 9 (2000), no. 2, 275-289.
- [BL2003] S. Brlek, A. Ladouceur, A note on differentiable palindromes, *Theoret. Comput. Sci.* 302 (2003) 167–178.
- [BLL1998] F. Bergeron, G. Labelle, and P. Leroux. “Combinatorial species and tree-like structures”. *Encyclopedia of Mathematics and its Applications*, vol. 67, Cambridge Univ. Press. 1998.
- [BLL2008] François Bergeron, Gilbert Labelle, and Pierre Leroux. “Introduction to the Theory of Species of Structures”, March 14, 2008.

- [BraLea2008] C. Bracken and Gregor Leander: *New families of functions with differential uniformity of 4*, Proceedings of the Conference BFCA, Copenhagen, 2008.
- [BLRS2009] J. Berstel, A. Lauve, C. Reutenauer, F. Saliola, Combinatorics on words: Christoffel words and repetitions in words, CRM Monograph Series, 27. American Mathematical Society, Providence, RI, 2009. xii+147 pp. ISBN: 978-0-8218-4480-9
- [BLS1999] A. Brandstadt, VB Le and JP Spinrad. *Graph classes: a survey*. SIAM Monographs on Discrete Mathematics and Applications, 1999.
- [BLV1999] Bernhard Beckermann, George Labahn, and Gilles Villard. “Shifted normal forms of polynomial matrices”. In ISSAC’99, pages 189-196. ACM, 1999. doi:10.1145/309831.309929.
- [BLV2006] Bernhard Beckermann, George Labahn, and Gilles Villard. “Normal forms for general polynomial matrices”. J. Symbolic Comput., 41(6):708-737, 2006. doi:10.1016/j.jsc.2006.02.001.
- [BM1940] Becker, M. F., and Saunders MacLane. The minimum number of generators for inseparable algebraic extensions. Bulletin of the American Mathematical Society 46, no. 2 (1940): 182-186.
- [BM1977] R. S. Boyer, J. S. Moore, A fast string searching algorithm, Communications of the ACM 20 (1977) 762–772.
- [BM1983] Buer, B., and Mohring, R. H. A fast algorithm for decomposition of graphs and posets, Math. Oper. Res., Vol 8 (1983): 170-184.
- [BM1993] M. Broué and G. Malle, *Zyklotomische Heckealgebren*, Asterisque, **212** (1993), 119-89.
- [BM1997] K. Bremke and G. Malle, *Reduced words and a length function for  $G(e, 1, n)$* . Indag. Mathem., N.S., **8** (1997), no. 4, 453-469.
- [BM2008] John Adrian Bondy and U.S.R. Murty, “Graph theory”, Volume 244 of Graduate Texts in Mathematics, 2nd edition, Springer, 2008.
- [BM2003] Bazzi and Mitter, {it Some constructions of codes from group actions}, (preprint March 2003, available on Mitter’s MIT website).
- [Boa1982] J. M. Boardman, “The eightfold way to BP-operations”, in *Current trends in algebraic topology*, pp. 187–226, Canadian Mathematical Society Proceedings, 2, Part 1. Providence 1982. ISBN 978-0-8218-6003-8.
- [Bond2007] P. Bonderson, Nonabelian anyons and interferometry, Dissertation (2007). <https://thesis.library.caltech.edu/2447/>
- [BDGRTW2019] Bonderson, Delaney, Galindo, Rowell, Tran, and Wang, On invariants of modular categories beyond modular data. J. Pure Appl. Algebra 223 (2019), no. 9, 4065–4088. [arXiv 1805.05736](https://arxiv.org/abs/1805.05736).
- [BM2004] John M. Boyer and Wendy J. Myrvold, *On the Cutting Edge: \*Simplified  $O(n)$  Planarity by Edge Addition*. Journal of Graph Algorithms and Applications, Vol. 8, No. 3, pp. 241-273, 2004. doi:10.7155/jgaa.00091.
- [BM2007] G. Brinkmann and B.D. McKay, *Fast generation of planar graphs*, MATCH-Communications in Mathematical and in Computer Chemistry, 58(2):323-357, 2007.
- [BM2012] N. Bruin and A. Molnar, *Minimal models for rational functions in a dynamical setting*, LMS Journal of Computation and Mathematics, Volume 15 (2012), pp 400-417.
- [BM2016] Gunnar Brinkmann, Brendan McKay, *Guide to using plantri*, version 5.0, 2016. <http://cs.anu.edu.au/~bdm/plantri/plantri-guide.txt>
- [BM2021] Alin Bostan and Ryuhei Mori, *A simple and fast algorithm for computing the  $N$ -th term of a linearly recurrent sequence*, Proceedings of Symposium on Simplicity in Algorithms (SOSA), pp. 118–132, 2021. doi:10.1137/1.9781611976496.14

- [BMBFLR2008] A. Blondin-Massé, S. Brlek, A. Frosini, S. Labbé, S. Rinaldi, *Reconstructing words from a fixed palindromic length sequence*, Proc. TCS 2008, 5th IFIP International Conference on Theoretical Computer Science (September 8-10 2008, Milano, Italia).
- [BMBL2008] A. Blondin-Massé, S. Brlek, S. Labbé, *Palindromic lacunas of the Thue-Morse word*, Proc. GASCOM 2008 (June 16-20 2008, Bibbiena, Arezzo-Italia), 53–67.
- [BMFPR] M. Bousquet-Melou, E. Fusy, L.-F. Preville Ratelle. *The number of intervals in the  $m$ -Tamari lattices*. [arXiv 1106.1498](https://arxiv.org/abs/1106.1498)
- [BMS2006] Bugeaud, Mignotte, and Siksek. “Classical and modular approaches to exponential Diophantine equations: I. Fibonacci and Lucas perfect powers.” *Annals of Math*, 2006.
- [BMSS2006] Alin Bostan, Bruno Salvy, François Morain, Éric Schost. Fast algorithms for computing isogenies between elliptic curves. [Research Report] 2006, pp.28. <inria-00091441> <https://arxiv.org/pdf/cs/0609020.pdf>
- [BN2010] D. Bump and M. Nakasuji. Integration on  $p$ -adic groups and crystal bases. *Proc. Amer. Math. Soc.* 138(5), pp. 1595–1605.
- [BN2008] Victor V. Batyrev and Benjamin Nill. Combinatorial aspects of mirror symmetry. In *Integer points in polyhedra — geometry, number theory, representation theory, algebra, optimization, statistics*, volume 452 of *Contemp. Math.*, pages 35–66. Amer. Math. Soc., Providence, RI, 2008. [arXiv math/0703456v2](https://arxiv.org/abs/math/0703456v2).
- [Bob2013] J.W. Bober. Conditionally bounding analytic ranks of elliptic curves. ANTS 10, 2013. <http://msp.org/obs/2013/1-1/obs-v1-n1-p07-s.pdf>
- [Bod1993] H. L. Bodlaender, *A Tourist Guide through Treewidth*, Acta Cybern. 1993.
- [Bod1998] Hans L. Bodlaender, *A partial  $k$ -arboretum of graphs with bounded treewidth*, Theoretical Computer Science 209(1-2):1-45, 1998. doi:10.1016/S0304-3975(97)00228-4.
- [Bo2009] Bosch, S., Algebra, Springer 2009
- [Bor1993] Lev A. Borisov, “Towards the mirror symmetry for Calabi-Yau complete intersections in Gorenstein Fano toric varieties”, 1993. [arXiv alg-geom/9310001v1](https://arxiv.org/abs/alg-geom/9310001v1)
- [Bor1995] Stephen P. Borgatti. *Centrality and AIDS*. (1995). *Connections* 18(1):112-115. [Online] Available: <http://www.analytictech.com/networks/centaids.htm>
- [BOR2009] Emmanuel Briand, Rosa Orellana, Mercedes Rosas. *The stability of the Kronecker products of Schur functions*. [arXiv 0907.4652v2](https://arxiv.org/abs/0907.4652v2).
- [Bou1989] N. Bourbaki. *Lie Groups and Lie Algebras*. Chapters 1-3. Springer. 1989.
- [BP1982] H. Beker and F. Piper. *Cipher Systems: The Protection of Communications*. John Wiley and Sons, 1982.
- [BP1993] Dominique Bernardi and Bernadette Perrin-Riou, Variante  $p$ -adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier), *C. R. Acad. Sci. Paris, Sér I. Math.*, 317 (1993), no. 3, 227-232.
- [BP1994] A. Berman and R. J. Plemmons. *Nonnegative Matrices in the Mathematical Sciences*. SIAM, Philadelphia, 1994.
- [BP2000] V. M. Bukhshtaber and T. E. Panov, “Moment-angle complexes and combinatorics of simplicial manifolds,” *Uspekhi Mat. Nauk* 55 (2000), 171–172.
- [BP2014] V. M. Bukhshtaber and T. E. Panov. “Toric Topology”, 2014. [arXiv 1210.2368](https://arxiv.org/abs/1210.2368)
- [BP2015] P. Butera and M. Pernici “Sums of permanental minors using Grassmann algebra”, *International Journal of Graph Theory and its Applications*, 1 (2015), 83–96. [arXiv 1406.5337](https://arxiv.org/abs/1406.5337)
- [BP2023] N. Brettell and R. Pendavingh, *Computing excluded minors for classes of matroids representable over partial fields*, arXiv preprint [arXiv 2302.13175](https://arxiv.org/abs/2302.13175) (2023).
- [BPRS2009] J. Bastian, T. Prellberg, M. Rubey, C. Stump, *Counting the number of elements in the mutation classes of  $\tilde{A}_n$ -quivers*; [arXiv 0906.0487](https://arxiv.org/abs/0906.0487)

- [BPS2008] Lubomira Balkova, Edita Pelantova, and Wolfgang Steiner. *Sequences with constant number of return words*. Monatsh. Math, 155 (2008) 251-263.
- [BPS2010] Anne Berry, Romain Pogorelcnik and Genevieve Simonet. *An Introduction to Clique Minimal Separator Decomposition*. Algorithms 3(2):197-215, 2010. doi:10.3390/a3020197
- [BPU2016] Alex Biryukov, Léo Perrin, Aleksei Udovenko, *Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1*; in EuroCrypt'16, pp. 372-402.
- [Br1910] Bruckner, "Über die Ableitung der allgemeinen Polytope und die nach Isomorphismus verschiedenen Typen der allgemeinen Achtzelle (Oktatope)", Verhand. Konik. Akad. Wetenschap, Erste Sectie, 10 (1910)
- [BR1998] Georgia Benkart and Tom Roby. *Down-up algebras*. J. Algebra, **209** no. 1 (1999), pp. 305-335. doi:10.1006/jabr.1998.7511.
- [Br2000] Kenneth S. Brown, *Semigroups, rings, and Markov chains*, arXiv math/0006145v1.
- [BR2000a] P. Barreto and V. Rijmen, *The ANUBIS Block Cipher*; in First Open NESSIE Workshop, (2000).
- [BR2000b] P. Barreto and V. Rijmen, *The Khazad legacy-level Block Cipher*; in First Open NESSIE Workshop, (2000).
- [BR2000c] P. Barreto and V. Rijmen, *The Whirlpool hashing function*; in First Open NESSIE Workshop, (2000).
- [BR2010] Matthew Baker and Robert Rumely. Potential theory and dynamics on the Berkovich projective line. Mathematical Surveys and Monographs, Volume 159. 2010.
- [BR2010a] Jean Berstel and Christophe Reutenauer, *Noncommutative Rational Series With Applications*. Cambridge, 2010.
- [BR2010b] Valérie Berthé and Michel Rigo, editors. Combinatorics, automata, and number theory, volume 135. Cambridge: Cambridge University Press, 2010.
- [Br2016] *Bresenham's Line Algorithm*, Python, 26 December 2016. [http://www.roguebasin.com/index.php?title=Bresenham%27s\\_Line\\_Algorithm](http://www.roguebasin.com/index.php?title=Bresenham%27s_Line_Algorithm)
- [Brandes01] Ulrik Brandes, A faster algorithm for betweenness centrality, Journal of Mathematical Sociology 25.2 (2001): 163-177, <http://www.inf.uni-konstanz.de/algo/publications/b-fabc-01.pdf>
- [Bra2011] Volker Braun, Toric Elliptic Fibrations and F-Theory Compactifications, arXiv 1110.4883
- [Bre1993] Richard P. Brent. *On computing factors of cyclotomic polynomials*. Mathematics of Computation. **61** (1993). No. 203. pp 131–149. arXiv 1004.5466v1. <http://www.jstor.org/stable/2152941>
- [Bre1997] T. Breuer "Integral bases for subfields of cyclotomic fields" AAEC 8, 279–289 (1997).
- [Bre2000] Enno Brehm, *3-Orientations and Schnyder 3-Tree-Decompositions*, 2000. <https://page.math.tu-berlin.de/~felsner/Diplomarbeiten/brehm.ps.gz>
- [Bre2008] A. Bretscher and D. G. Corneil and M. Habib and C. Paul (2008), "A simple Linear Time LexBFS Cograph Recognition Algorithm", SIAM Journal on Discrete Mathematics, 22 (4): 1277–1296, doi:10.1137/060664690.
- [Bre2023] N. Brettell, *The excluded minors for GF(5)-representable matroids on ten elements*, arXiv preprint arXiv 2307.14614 (2023).
- [Bro2011] Francis Brown, *Multiple zeta values and periods: From moduli spaces to Feynman integrals*, in Contemporary Mathematics vol 539, pages 27-52, 2011.
- [Bro2013] Francis Brown, *Single-valued motivic periods and multiple zeta values*, Forum Math. Sigma 2 (2014), doi:10.1017/fms.2014.18.
- [Bro2016] A.E. Brouwer, Personal communication, 2016.

- [Bro1982] A. Brouwer, *Polarities of G. Higman's symmetric design and a strongly regular graph on 176 vertices*, Aequationes mathematicae 25, no. 1 (1982): 77-82. doi:10.1007/BF02189599.
- [Bro1989] A. Broder, *Generating random spanning trees*, Proceedings of the 30th IEEE Symposium on Foundations of Computer Science, 1989, pp. 442-447. doi:10.1109/SFCS.1989.63516, <<http://www.cs.cmu.edu/~15859n/RelatedWork/Broder-GenRanSpanningTrees.pdf>>\_
- [Bro2009] R. Bröker: *Constructing supersingular elliptic curves*. Journal of Combinatorics and Number Theory 1.3 (2009), pp. 269–273.
- [Broder2000] Broder, A.Z., Kumar, R., Maghoul, F., Raghavan, P., Rajagopalan, S., Stata, R., Tomkins, A., Wiener, J.L.: Graph structure in the web. Computer Networks 33(1-6), 309–320 (2000)
- [BRS2015] A. Boussicault, S. Rinaldi et S. Socci. *The number of directed k-convex polyominoes* 27th Annual International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2015), 2015. arXiv 1501.00872
- [Bru1994] Richard A. Brualdi, Hyung Chan Jung, William T. Trotter Jr *On the poset of all posets on n elements* Volume 50, Issue 2, 6 May 1994, Pages 111-123 Discrete Applied Mathematics <http://www.sciencedirect.com/science/article/pii/0166218X9200169M>
- [Bru1998] J. Brundan. *Modular branching rules and the Mullineux map for Hecke algebras of type A*. Proc. London Math. Soc. (3) 77 (1998), 551–581. MathSciNet MR1643413
- [BS1969] D. Blatt, G. Szekeres. *A Skew Hadamard Matrix of Order 52*, Canadian Journal of Mathematics 21 (1969): 1319-1322. doi:10.4153/CJM-1969-144-2
- [BS1996] Eric Bach, Jeffrey Shallit. *Algorithmic Number Theory, Vol. 1: Efficient Algorithms*. MIT Press, 1996. ISBN 978-0262024051.
- [BS2003] I. Bouyukliev and J. Simonis, Some new results on optimal codes over  $F_5$ , Designs, Codes and Cryptography 30, no. 1 (2003): 97-111, [http://www.moi.math.bas.bg/moiuser/~iliya/pdf\\_site/gf5srev.pdf](http://www.moi.math.bas.bg/moiuser/~iliya/pdf_site/gf5srev.pdf).
- [BS2010] P. Baseilhac and K. Shigechi. *A new current algebra and the reflection equation*. Lett. Math. Phys. 92 (2010), pp. 47-65. arXiv 0906.1482.
- [BS2011] E. Byrne and A. Sneyd, On the Parameters of Codes with Two Homogeneous Weights. WCC 2011-Workshop on coding and cryptography, pp. 81-90. 2011. <https://hal.inria.fr/inria-00607341/document>
- [BS2012] Jonathan Bloom and Dan Saracino, *Modified growth diagrams, permutation pivots, and the BWX map  $Phi^*$* , Journal of Combinatorial Theory, Series A Volume 119, Number 6 (2012), pp. 1280-1298.
- [BSS2009] David Bremner, Mathieu Dutour Sikiric, Achill Schuermann: Polyhedral representation conversion up to symmetries, Proceedings of the 2006 CRM workshop on polyhedral computation, AMS/CRM Lecture Notes, 48 (2009), 45-71. arXiv math/0702239
- [BSV2010] M. Bolt, S. Snoeyink, E. Van Andel. “Visual representation of the Riemann map and Ahlfors map via the Kerzman-Stein equation”. Involve 3-4 (2010), 405-420.
- [BDLGZ2009] M. Bucci et al. A. De Luca, A. Glen, L. Q. Zamoni, A connection between palindromic and factor complexity using return words,” Advances in Applied Mathematics 42 (2009) 60-74.
- [BSZ2019] Nils Bruin, Jeroen Sijsling, and Alexandre Zotine, *Numerical Computation of Endomorphism Rings of Jacobians*, The Open Book Series, Vol. 2 (2019), No. 1, pp. 155-171, <https://msp.org/obs/2019/2-1/p10.xhtml>
- [BUVO2007] Johannes Buchmann, Ullrich Vollmer: Binary Quadratic Forms, An Algorithmic Approach, Algorithms and Computation in Mathematics, Volume 20, Springer (2007)
- [BV2004] Jean-Luc Baril, Vincent Vajnovszki. *Gray code for derangements*. Discrete Applied Math. 140 (2004) doi:10.1016/j.dam.2003.06.002 <http://jl.baril.u-bourgogne.fr/derange.pdf>

- [BV2009] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, Cambridge, 2009. ISBN 9780521833783.
- [BvR1982] Andries Brouwer and John van Rees, More mutually orthogonal Latin squares, *Discrete Mathematics*, vol.39, num.3, pages 263-281, 1982 <http://oai.cwi.nl/oai/asset/304/0304A.pdf>
- [BW1988] Anders Björner, Michelle L. Wachs, *Generalized quotients in Coxeter groups*. Transactions of the American Mathematical Society, vol. 308, no. 1, July 1988. <http://www.ams.org/journals/tran/1988-308-01/S0002-9947-1988-0946427-X/S0002-9947-1988-0946427-X.pdf>
- [BW1993] Thomas Becker and Volker Weispfenning. *Groebner Bases - A Computational Approach To Commutative Algebra*. Springer, New York, 1993.
- [BW1994] M. Burrows, D.J. Wheeler, “A block-sorting lossless data compression algorithm”, HP Lab Technical Report, 1994, available at <http://www.hpl.hp.com/techreports/Compaq-DEC/SRC-RR-124.html>
- [BW1996] Anders Björner and Michelle L. Wachs. *Shellable nonpure complexes and posets. I*. Trans. of Amer. Math. Soc. **348** No. 4. (1996)
- [BY2016] Pauline Baillet and Masahiko Yoshinaga. *Vanishing results for the Aomoto complex of real hyperplane arrangements via minimality*. J. Singularities. **14** (2016), 74-90.
- [BZ01] A. Berenstein, A. Zelevinsky *Tensor product multiplicities, canonical bases and totally positive varieties* Invent. Math. **143** No. 1. (2002), 77-128.
- [BZ2003] Vladimir Batagelj and Matjaz Zaversnik. *An  $O(m)$  Algorithm for Cores Decomposition of Networks*. 2003. [arXiv cs/0310049v1](https://arxiv.org/abs/cs/0310049v1).
- [Cal2005] D. Callan. *On Conjugates for Set Partitions and Integer Compositions*. Preprint, [arXiv math/0508052](https://arxiv.org/abs/math/0508052).
- [dCa2007] C. de Canniere: *Analysis and Design of Symmetric Encryption Algorithms*, PhD Thesis, 2007.
- [Can1990] J. Canny. Generalised characteristic polynomials. J. Symbolic Comput. Vol. 9, No. 3, 1990, 241–250.
- [Car1972] R. W. Carter. *Simple groups of Lie type*, volume 28 of Pure and Applied Mathematics. John Wiley and Sons, 1972.
- [Car1972a] R. W. Carter. *Conjugacy classes in the Weyl group*, Comp. Math. Vol 26 (1972) 1-59.
- [Cha2005] F. Chapoton, *Une Base Symétrique de l'algèbre des Coinvariants Quasi-Symétriques*, Electronic Journal of Combinatorics Vol 12(1) (2005) N16.
- [Che1944] S. Chern, *A simple intrinsic proof of the Gauss-Bonnet formula for closed Riemannian manifolds*, Ann. of Math. (2) 45 (1944), 747–752.
- [CP2023] M. Cati and D.V. Pasechnik. *Implementing Hadamard Matrices in SageMath*. Preprint, [arXiv 2306.16812](https://arxiv.org/abs/2306.16812), (2023).
- [CQ2019] A. Cassella and C. Quadrelli. *Right-angled Artin groups and enhanced Koszul properties*. Preprint, [arXiv 1907.03824](https://arxiv.org/abs/1907.03824), (2019).
- [CS1996] G. Call and J. Silverman. Computing the Canonical Height on K3 Surfaces. Mathematics of Comp. , 65 (1996), 259-290.
- [CB2007] Nicolas Courtois, Gregory V. Bard: Algebraic Cryptanalysis of the Data Encryption Standard, In 11-th IMA Conference, Cirencester, UK, 18-20 December 2007, Springer LNCS 4887. See also <http://eprint.iacr.org/2006/402/>.
- [CC1982] Chottin and R. Cori, *Une preuve combinatoire de la rationalité d'une série génératrice associée aux arbres*, RAIRO, Inf. Théor. 16, 113–128 (1982)
- [CC1995] Wei-Kuo Chiang, Rong-Jaye Chen: *The  $(n, k)$ -star graph: A generalized star graph*. Information Processing Letters 56(5): 259-264, 1995. doi:10.1016/0020-0190(95)00162-1

- [CC2013] Mahir Bilen Can and Yonah Cherniavsky. *Omitting parentheses from the cyclic notation*. (2013). [arXiv 1308.0936v2](#).
- [CC2023] C. Ceballos and C. Chenevière. *On linear intervals in the alt `nu`-Tamari lattices* [arXiv 2305.02250](#)
- [CCL2015] N. Cohen, D. Coudert, and A. Lancin. *On computing the Gromov hyperbolicity*. ACM Journal of Experimental Algorithmics, 20(1.6):1-18, 2015. doi:10.1145/2780652 or [<https://hal.inria.fr/hal-01182890>].
- [CS1999a] D. Cohen and A. Suciu. *Characteristic varieties of arrangements*. Math. Proc. Cambridge Philos. Soc. 127 (1999), no.1, 33–53. doi:10.1017/S03050004199003576.
- [CCLSV2005] M. Chudnovsky, G. Cornuejols, X. Liu, P. Seymour, K. Vuskovic. *Recognizing berge graphs*. Combinatorica vol 25 (2005), n 2, pages 143–186. doi:10.1007/s00493-005-0012-8.
- [CD1996] Charles Colbourn and Jeffrey Dinitz, Making the MOLS table, Computational and constructive design theory, vol 368, pages 67-134, 1996
- [CD2007] Adrian Clinger and Charles F. Doran, “Modular invariants for lattice polarized K3 surfaces”, Michigan Math. J. 55 (2007), no. 2, 355-393. [arXiv math/0602146v1](#) [math.AG]
- [CD2013] I. Cardinali and B. De Bruyn, *Spin-embeddings, two-intersection sets and two-weight codes*, Ars Comb. 109 (2013): 309-319. <https://biblio.ugent.be/publication/4241842/file/4241845.pdf>
- [CDJN2019] A. Chakraborti, N. Datta, A. Jha, M. Nandi “HyENA” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/hyena-spec.pdf>
- [CDL2015] A. Canteaut, Sebastien Duval, Gaetan Leurent *Construction of Lightweight S-Boxes using Feistel and MISTY Structures*; in Proceedings of SAC 2015; LNCS 9566; pp. 373-393; Springer-Verlag 2015; available at <http://eprint.iacr.org/2015/711.pdf>
- [CDLNPPS2019] A. Canteaut, S. Duval, G. Leurent, M. Naya-Plasencia, L. Perrin, T. Pornin, A. Schrottenloher. “Saturnin: a suite of lightweight symmetrical algorithms for post-quantum security” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/SATURNIN-spec.pdf>
- [CE2001] Raul Cordovil and Gwihen Etienne. *A note on the Orlik-Solomon algebra*. Europ. J. Combinatorics. **22** (2001). pp. 165-170. <http://www.math.ist.utl.pt/~rcordov/Ce.pdf>
- [CE2003] Henry Cohn and Noam Elkies, New upper bounds on sphere packings I, Ann. Math. 157 (2003), 689–714.
- [Cer1994] D. P. Cervone, “Vertex-minimal simplicial immersions of the Klein bottle in three-space”, Geom. Ded. 50 (1994) 117-141, <http://www.math.union.edu/~dpvc/papers/1993-03.kb/vmkb.pdf>.
- [CES2003] Brian Conrad, Bas Edixhoven, William Stein  $J_1(p)$  Has Connected Fibers Documenta Math. 8 (2003) 331–408
- [CEW2011] Georgios Chalkiadakis, Edith Elkind, and Michael Wooldridge. *Computational Aspects of Cooperative Game Theory*. Morgan & Claypool Publishers, (2011). ISBN 9781608456529, doi:10.2200/S00355ED1V01Y201107AIM016.
- [CF2005] Raul Cordovil and David Forge. *Gröbner and diagonal bases in Orlik-Solomon type algebras* Cubo **7** (2), (2005). pp. 1-20.
- [CFHM2013] Wei Chen, Wenjie Fang, Guangda Hu, Michael W. Mahoney, *On the Hyperbolicity of Small-World and Treelike Random Graphs*, Internet Mathematics **9**:4 (2013), 434-491. doi:10.1080/15427951.2013.828336, [arXiv 1201.1717](#).
- [CFI1992] Cai, JY., Fürer, M. & Immerman, N. Combinatorica (1992) 12: 389. doi:10.1007/BF01305232
- [CFKLMPPS15] Marek Cygan, Fedor V. Fomin, Łukasz Kowalik, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michał Pilipczuk, Saket Saurabh. *Parameterized Algorithms*. Springer International Publishing Switzerland 2015

- [CFKP1997] James W. Cannon, William J. Floyd, Richard Kenyon and Walter R. Parry. *Hyperbolic Geometry*. Flavors of Geometry, MSRI Publications, Volume 31, 1997.
- [CFKPR2010] Ioannis Caragiannis, Afonso Ferreira, Christos Kaklamanis, Stéphane Pérennes, Hervé Rivano. *Fractional Path Coloring in Bounded Degree Trees with Applications*. Algorithmica, Springer Verlag, 2010, 58 (2), pp.516-540. doi:10.1007/s00453-009-9278-3, <https://hal.archives-ouvertes.fr/hal-00371052/document>
- [CFL1958] K.-T. Chen, R.H. Fox, R.C. Lyndon, Free differential calculus, IV. The quotient groups of the lower central series, Ann. of Math. 68 (1958) 81–95.
- [CFZ2000] J. Cassaigne, S. Ferenczi, L.Q. Zamboni, Imbalances in Arnoux-Rauzy sequences, Ann. Inst. Fourier (Grenoble) 50 (2000) 1265–1276.
- [CFZ2002] Chapoton, Fomin, Zelevinsky - Polytopal realizations of generalized associahedra, [arXiv math/0202004](https://arxiv.org/abs/math/0202004).
- [CGHLM2013] P. Crescenzi, R. Grossi, M. Habib, L. LANZI, A. Marino. *On computing the diameter of real-world undirected graphs*. Theor. Comput. Sci. 514: 84-95 (2013). doi:10.1016/j.tcs.2012.09.018.
- [CGILM2010] P. Crescenzi, R. Grossi, C. Imbrenda, L. LANZI, and A. Marino. *Finding the Diameter in Real-World Graphs: Experimentally Turning a Lower Bound into an Upper Bound*. Proceedings of 18th Annual European Symposium on Algorithms. Lecture Notes in Computer Science, vol. 6346, 302-313. Springer (2010). doi:10.1007/978-3-642-15775-2\_26.
- [CGLM2012] Crescenzi P., Grossi R., LANZI L., Marino A. (2012) *On Computing the Diameter of Real-World Directed (Weighted) Graphs*. In: Klasing R. (eds) Experimental Algorithms. SEA 2012. Lecture Notes in Computer Science, vol 7276. Springer, Berlin, Heidelberg doi:10.1007/978-3-642-30850-5\_10.
- [CGW2013] Daniel Cabarcas, Florian Göpfert, and Patrick Weiden. Provably Secure LWE-Encryption with Uniform Secret. Cryptology ePrint Archive, Report 2013/164. 2013. 2013/164. <http://eprint.iacr.org/2013/164>
- [Conr] Keith Conrad, “Artin-Hasse-Type Series and Roots of Unity”, <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/AHrootofunity.pdf>
- [Coron2023] Basile Coron *Supersolvability of built lattices and Koszulness of generalized Chow rings*. Preprint, [arXiv 2302.13072](https://arxiv.org/abs/2302.13072) (2023).
- [CGMRV16] A. Conte, R. Grossi, A. Marino, R. Rizzi, L. Versari, “Directing Road Networks by Listing Strong Orientations.”, Combinatorial Algorithms, Proceedings of 27th International Workshop, IWOCA 2016, August 17-19, 2016, pages 83–95.
- [Ch2012] Cho-Ho Chu. *Jordan Structures in Geometry and Analysis*. Cambridge University Press, New York. 2012. ISBN 978-1-107-01617-0.
- [Cha92] Chameni-Nembua C. and Monjardet B. *Les Treillis Pseudocomplémentés* Finis Europ. J. Combinatorics (1992) 13, 89-107.
- [Cha18] Frédéric Chapoton, *Some properties of a new partial order on Dyck paths*, 2018, [arXiv 1809.10981](https://arxiv.org/abs/1809.10981)
- [Cha22005] B. Cha. Vanishing of some cohomology groups and bounds for the Shafarevich-Tate groups of elliptic curves. J. Number Theory, 111:154-178, 2005.
- [Cha2008] Frédéric Chapoton. *Sur le nombre d'intervalles dans les treillis de Tamari*. Sémin. Lothar. Combin. (2008). [arXiv math/0602368v1](https://arxiv.org/abs/math/0602368v1).
- [ChLi] F. Chapoton and M. Livernet, *Pre-Lie algebras and the rooted trees operad*, International Math. Research Notices (2001) no 8, pages 395-408. Preprint: [arXiv math/0002069v2](https://arxiv.org/abs/math/0002069v2).
- [Cha2006] Ruth Charney. *An introduction to right-angled Artin groups*. <http://people.brandeis.edu/~charney/papers/RAAGfinal.pdf>, [arXiv math/0610668](https://arxiv.org/abs/math/0610668).
- [ChenDB] Eric Chen, Online database of two-weight codes, <http://moodle.tec.hkr.se/~chen/research/2-weight-codes/search.php>

- [CHK2001] Keith D. Cooper, Timothy J. Harvey and Ken Kennedy. *A Simple, Fast Dominance Algorithm*, Software practice and Experience, 4:1-10 (2001). <http://www.hipersoft.rice.edu/grads/publications/dom14.pdf>
- [Chu2007] F. Chung, *Random walks and local cuts in graphs*, Linear Algebra and its Applications 423 (2007), no. 1, 22-32.
- [Chu2012] T. Church *Homological stability for configuration spaces of manifolds*, Inventiones Mathematicae, 2012(188), pp. 465-504.
- [CHPSS18] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song. *Boomerang Connectivity Table: A New Cryptanalysis Tool* (2018) IACR Transactions on Symmetric Cryptology. Vol 2017, Issue 4. pre-print available at <https://eprint.iacr.org/2018/161.pdf>
- [CIA] CIA Factbook 09 <https://www.cia.gov/library/publications/the-world-factbook/>
- [CK1986] R. Calderbank, W.M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. 18(1986) 97-122. doi:10.1112/blms/18.2.97.
- [CK1999] David A. Cox and Sheldon Katz. *Mirror symmetry and algebraic geometry*, volume 68 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1999.
- [Cox1989] David A. Cox. Primes of the form  $x^2 + ny^2$ . Wiley, 1989.
- [CK2008] Derek G. Corneil and Richard M. Krueger, *A Unified View of Graph Searching*, SIAM Journal on Discrete Mathematics, 22(4), 1259–1276, 2008. doi:10.1137/050623498
- [CK2001] M. Casella and W. Kühnel, “A triangulated K3 surface with the minimum number of vertices”, Topology 40 (2001), 753–772.
- [CKS1999] Felipe Cucker, Pascal Koiran, and Stephen Smale. *A polynomial-time algorithm for diophantine equations in one variable*, J. Symbolic Computation 27 (1), 21-29, 1999.
- [CK2015] J. Campbell and V. Knight. *On testing degeneracy of bi-matrix games*. [http://vknight.org/unpeudemath/code/2015/06/25/on\\_testing\\_degeneracy\\_of\\_games/](http://vknight.org/unpeudemath/code/2015/06/25/on_testing_degeneracy_of_games/) (2015)
- [CL1996] Chartrand, G. and Lesniak, L.: *Graphs and Digraphs*. Chapman and Hall/CRC, 1996.
- [CL2002] Chung, Fan and Lu, L. *Connected components in random graphs with given expected degree sequences*. Ann. Combinatorics (6), 2002 pp. 125-145. doi:10.1007/PL00012580.
- [CL2017] Xavier Caruso and J  r  my Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields* J. Symbolic Comput. 79 (2017), 411-443.
- [CL2013] Maria Chlouveraki and Sofia Lambropoulou. *The Yokonuma-Hecke algebras and the HOMFLYPT polynomial*. (2015) arXiv 1204.1871v4.
- [Cle1872] Alfred Clebsch, *Theorie der bin  ren algebraischen Formen*, Teubner, 1872.
- [CLG1997] Frank Celler and C. R. Leedham-Green, *Calculating the Order of an Invertible Matrix*, 1997
- [CLRS2001] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, *Section 22.4: Topological sort*, Introduction to Algorithms (2nd ed.), MIT Press and McGraw-Hill, 2001, 549-552, ISBN 0-262-03293-7.
- [CLO2005] D. Cox, J. Little, D. O’Shea. Using Algebraic Geometry. Springer, 2005.
- [CLS2011] David A. Cox, John Little, and Hal Schenck. *Toric Varieties*. Volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.
- [CLS2014] C. Ceballos, J.-P. Labb  , C. Stump, *Subword complexes, cluster complexes, and generalized multi-associahedra*, J. Algebr. Comb. 39 (2014) pp. 17-51. doi:10.1007/s10801-013-0437-x, arXiv 1108.1776.
- [CM2000] Paula A.A.B. Carvalho and Ian M. Musson. *Down-up algebras and their representation theory*. J. Algebra. 228 no. 1, (2000), pp. 286-310. doi:10.1006/jabr.1999.8263

- [CM2012] M. Cabanes, I. Marin, *On ternary quotients of cubic Hecke algebras*, Comm. Math. Phys. (2012), Volume 314, Issue 1, pp 57-92. doi:10.1007/s00220-012-1519-7, arXiv 1010.1465.
- [CMN2014] David Coudert, Dorian Mazauric, and Nicolas Nisse, *Experimental Evaluation of a Branch and Bound Algorithm for computing Pathwidth*. In Symposium on Experimental Algorithms (SEA), volume 8504 of LNCS, Copenhagen, Denmark, pages 46-58, June 2014, doi:10.1007/978-3-319-07959-2\_5, <https://hal.inria.fr/hal-00943549/document>
- [CMO2011] C. Chun, D. Mayhew, J. Oxley, A chain theorem for internally 4-connected binary matroids. J. Combin. Theory Ser. B 101 (2011), 141-189.
- [CMO2012] C. Chun, D. Mayhew, J. Oxley, Towards a splitter theorem for internally 4-connected binary matroids. J. Combin. Theory Ser. B 102 (2012), 688-700.
- [CMR2005] C. Cid, S. Murphy, M. Robshaw, *Small Scale Variants of the AES*; in Proceedings of Fast Software Encryption 2005; LNCS 3557; Springer Verlag 2005; available at <http://www.isg.rhul.ac.uk/~sean/smallAES-fse05.pdf>
- [CMR2006] C. Cid, S. Murphy, and M. Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*; Springer Verlag 2006
- [CMT2003] A. M. Cohen, S. H. Murray, D. E. Talyor. *Computing in groups of Lie type*. Mathematics of Computation. **73** (2003), no 247. pp. 1477–1498. <https://www.win.tue.nl/~amc/pub/papers/cmt.pdf>
- [CN2019] B. Chakraborty, M. Nandi “Orange” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/orange-spec.pdf>
- [CrNa2020] J.E. Cremona and F. Najman, *Q-curves over odd degree number fields*, arXiv 2004.10054.
- [CreSuth2023] J.E. Cremona and A.V. Sutherland. *Computing the endomorphism ring of an elliptic curve over a number field*. arXiv 2301.11169.
- [CoCo1] J.H. Conway, H.S.M. Coxeter *Triangulated polygons and frieze patterns*, The Mathematical Gazette (1973) 57 p.87-94
- [CoCo2] J.H. Conway, H.S.M. Coxeter *Triangulated polygons and frieze patterns (continued)*, The Mathematical Gazette (1973) 57 p.175-183
- [Co1984] J. Conway, Hexacode and tetracode - MINIMOG and MOG. *Computational group theory*, ed. M. Atkinson, Academic Press, 1984.
- [CO2010] Jonathan Comes, Viktor Ostrik. *On blocks of Deligne’s category  $\text{Rep}(S_t)$* . arXiv 0910.5695v2, <http://pages.uoregon.edu/jcomes/blocks.pdf>
- [Coh1981] A. M. Cohen, *A synopsis of known distance-regular graphs with large diameters*, Stichting Mathematisch Centrum, 1981. <http://persistent-identifier.org/?identifier=urn:nbn:nl:ui:18-6775>
- [Coh1993] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics 138. Springer, 1993.
- [Coh2000] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.
- [Coh2007I] Henri Cohen, *Number Theory, Vol. I: Tools and Diophantine Equations*. GTM 239, Springer, 2007.
- [Coh2007] Henri Cohen, *Number Theory, Volume II*. Graduate Texts in Mathematics 240. Springer, 2007.
- [Coh2019] Nathann Cohen, *Several Graph problems and their Linear Program formulations*, 2019. <https://hal.archives-ouvertes.fr/inria-00504914/en>
- [Coj2005] Alina Carmen Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves. With an appendix by Ernst Kani*. Canad. Math. Bull. 48 (2005), no. 1, 16–31.

- [Colb2004] C.J. Colbourn. “Combinatorial aspects of covering arrays”. *Matematiche (Catania)* 59 (2004), pp. 125–172.
- [Col2004] Pierre Colmez, Invariant  $\mathcal{L}$  et derivees de valeurs propres de Frobenius, preprint, 2004.
- [Col2013] Julia Collins. *An algorithm for computing the Seifert matrix of a link from a braid representation*. (2013). <http://www.maths.ed.ac.uk/~jcollins/SeifertMatrix/SeifertMatrix.pdf>
- [Com2019] Camille Combe, *Réalisation cubique du poset des intervalles de Tamari*, preprint [arXiv 1904.00658](https://arxiv.org/abs/1904.00658)
- [Com1974] Comtet Louis, *Identities and Expansions*. In: *Advanced Combinatorics*. 1974. pp. 127-175 [doi:10.1007/978-94-010-2196-8\\_3](https://doi.org/10.1007/978-94-010-2196-8_3)
- [Con] Keith Conrad, *Groups of order 12*, <http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/group12.pdf>, accessed 21 October 2009.
- [Con2013] Keith Conrad: *Exterior powers*, <http://www.math.uconn.edu/~kconrad/blurbs/>
- [Con2015] Keith Conrad: *Tensor products*, <http://www.math.uconn.edu/~kconrad/blurbs/>
- [Con2018] Anthony Conway, *Notes On The Levine-Tristram Signature Function*, July 2018 <http://www.unige.ch/math/folks/conway/Notes/LevineTristramSurvey.pdf>
- [Coo2006] K. Coolsaet, *The uniqueness of the strongly regular graph  $srg(105,32,4,12)$* , *Bull. Belg. Math. Soc.* 12(2006), 707-718. <http://projecteuclid.org/euclid.bbms/1136902608>
- [Cou2014] Alain Couvreur, *Codes and the Cartier operator*, *Proceedings of the American Mathematical Society* 142.6 (2014): 1983-1996.
- [Cox] David Cox, “What is a Toric Variety”, <https://dacox.people.amherst.edu/lectures/tutorial.ps>
- [Cox1957] H. S. M. Coxeter: *Factor groups of the braid groups*, *Proceedings of the Fourth Canadian Mathematical Congress (Vancouver 1957)*, pp. 95-122.
- [Cox1969] Harold S. M. Coxeter, *Introduction to Geometry*, 2nd ed. New York:Wiley, 1969.
- [CP2001] John Crisp and Luis Paris. *The solution to a conjecture of Tits on the subgroup generated by the squares of the generators of an Artin group*. *Invent. Math.* **145** (2001). No 1, 19-36. [arXiv math/0003133](https://arxiv.org/abs/math/0003133).
- [CP2005] A. Cossidente and T. Penttila, *Hemisystems on the Hermitian surface*, *Journal of London Math. Soc.* 72(2005), 731–741. [doi:10.1112/S0024610705006964](https://doi.org/10.1112/S0024610705006964).
- [CP2012] Grégory Châtel, Viviane Pons. *Counting smaller trees in the Tamari order*, [arXiv 1212.0751v1](https://arxiv.org/abs/1212.0751v1).
- [CP2015] Grégory Châtel and Viviane Pons. *Counting smaller elements in the tamari and m-tamari lattices*. *Journal of Combinatorial Theory, Series A*. (2015). [arXiv 1311.3922](https://arxiv.org/abs/1311.3922).
- [CP2016] N. Cohen, D. Pasechnik, *Implementing Brouwer’s database of strongly regular graphs*, *Designs, Codes, and Cryptography*, 2016 [doi:10.1007/s10623-016-0264-x](https://doi.org/10.1007/s10623-016-0264-x)
- [CPdA2014] Maria Chlouveraki and Loïc Poulain d’Andecy. *Representation theory of the Yokonuma-Hecke algebra*. (2014) [arXiv 1302.6225v2](https://arxiv.org/abs/1302.6225v2).
- [CPS2006] J.E. Cremona, M. Prickett and S. Siksek, Height Difference Bounds For Elliptic Curves over Number Fields, *Journal of Number Theory* 116(1) (2006), pages 42-68.
- [CR1962] Curtis, Charles W.; Reiner, Irving “Representation theory of finite groups and associative algebras.” *Pure and Applied Mathematics*, Vol. XI Interscience Publishers, a division of John Wiley & Sons, New York-London 1962, pp 545–547
- [Cre1997] J. E. Cremona, *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.
- [Cre2003] Cressman, Ross. *Evolutionary dynamics and extensive form games*. MIT Press, 2003.
- [Cre2020] Creedon, Samuel. *The center of the partition algebra*. Preprint, [arXiv 2005.00600](https://arxiv.org/abs/2005.00600) (2020).

- [Cro1983] M. Crochemore, Recherche linéaire d'un carré dans un mot, C. R. Acad. Sci. Paris Sér. I Math. 296 (1983) 14 781–784.
- [Cro2004] Peter R. Cromwell, *Knots and links*, Cambridge University Press (2004). doi:10.1017/CBO9780511809767
- [CRS2016] Dean Crnković, Sanja Rukavina, and Andrea Švob. *Strongly regular graphs from orthogonal groups  $O^+(6, 2)$  and  $O^-(6, 2)$* . arXiv 1609.07133
- [CRSKKY1989] G. Cohen, D. Rubie, J. Seberry, C. Koukouvinos, S. Kounias, M. Yamada, *A survey of base sequences, disjoint complementary sequences and  $OD(4t; t, t, t, t)$* . JCMCC. The Journal of Combinatorial Mathematics and Combinatorial Computing, 5 (1989), 69–104.
- [CRST2006] M. Chudnovsky, N. Robertson, P. Seymour, R. Thomas. *The strong perfect graph theorem*. Annals of Mathematics, vol 164, number 1, pages 51–230, 2006.
- [CRV2018] Xavier Caruso, David Roe and Tristan Vaccon. *ZpL: a p-adic precision package*, (2018) arXiv 1802.08532.
- [CRV2014] Xavier Caruso, David Roe and Tristan Vaccon. *Tracking p-adic precision*, LMS J. Comput. Math. 17 (2014), 274–294.
- [Connell1999] Ian Connell. *Elliptic Curve Handbook*. Online lecture notes, available at <https://git.hackade.org/ben/tinycrypt/raw/branch/master/docs/Elliptic%20Curve%20Handbook.pdf>
- [CS1986] J. Conway and N. Sloane. *Lexicographic codes: error-correcting codes from game theory*, IEEE Trans. Infor. Theory 32 (1986) 337–348.
- [CS1999] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd. ed., Grundlehren der Mathematischen Wissenschaften, vol. 290, Springer-Verlag, New York, 1999.
- [CS1988] Conway, J. H., and N. J. A. Sloane. *Low-Dimensional Lattices. IV. The Mass Formula*, Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, vol. 419, no. 1857, 1988, pp. 259–286.
- [CS2003] John E. Cremona and Michael Stoll. *On The Reduction Theory of Binary Forms*. Journal für die reine und angewandte Mathematik, 565 (2003), 79–99.
- [CS2006] J. E. Cremona, and S. Siksek, Computing a Lower Bound for the Canonical Height on Elliptic Curves over  $\mathbf{Q}$ , ANTS VII Proceedings: F.Hess, S.Pauli and M.Pohst (eds.), ANTS VII, Lecture Notes in Computer Science 4076 (2006), pages 275–286.
- [CS2018] Craig Costello and Benjamin Smith: Montgomery curves and their arithmetic. J. Cryptogr. Eng. 8 (2018), 227–240.
- [CST2010] Tullio Ceccherini-Silberstein, Fabio Scarabotti, Filippo Tolli. *Representation Theory of the Symmetric Groups: The Okounkov-Vershik Approach, Character Formulas, and Partition Algebras*. CUP 2010.
- [CT2013] J. E. Cremona and T. Thongjunthug, The Complex AGM, periods of elliptic curves over  $\mathbb{C}$  and complex elliptic logarithms. Journal of Number Theory Volume 133, Issue 8, August 2013, pages 2813–2841.
- [CTTL2014] C. Carlet, Deng Tang, Xiaohu Tang, and Qunying Liao: *New Construction of Differentially 4-Uniform Bijections*, Inscrypt, pp. 22–38, 2013.
- [CT1998] F. Chung and P. Tetali, *Isoperimetric inequalities for Cartesian products of graphs*, Combinatorics, Probability and Computing 7 (1998), no. 2, 141–148.
- [Cu1984] R. Curtis, The Steiner system  $S(5, 6, 12)$ , the Mathieu group  $M_{12}$ , and the kitten. *Computational group theory*, ed. M. Atkinson, Academic Press, 1984.
- [Cun1986] W. H. Cunningham, Improved Bounds for Matroid Partition and Intersection Algorithms. SIAM Journal on Computing 1986 15:4, 948–957.

- [CVV2019] Xavier Caruso, Tristan Vaccon and Thibaut Verron, *Gröbner bases over Tate algebras*, arXiv 1901.09574 (2019)
- [CVV2020] Xavier Caruso, Tristan Vaccon and Thibaut Verron, *Signature-based algorithms for Gröbner bases over Tate algebras*, arXiv 2002.04491 (2020)
- [CW1972] J. Cooper and J. Wallis. *A construction for Hadamard arrays*, Bulletin of the Australian Mathematical Society 7(2) (1972): 269-277. doi:10.1017/S0004972700045019
- [CW2005] J. E. Cremona and M. Watkins. Computing isogenies of elliptic curves. preprint, 2005.
- [CHW2015] Cui, Shawn X.; Hong, Seung-Moon; Wang, Zhenghan Universal quantum computation with weakly integral anyons. Quantum Inf. Process. 14 (2015), no. 8, 2687-2727.
- [CW2015] Cui, S. X. and Wang, Z. (2015). Universal quantum computation with metaplectic anyons. Journal of Mathematical Physics, 56(3), 032202. doi:10.1063/1.4914941
- [Dat2007] Basudeb Datta, “Minimal triangulations of manifolds”, J. Indian Inst. Sci. 87 (2007), no. 4, 429-449.
- [Dav1997] B.A. Davey, H.A. Priestley, *Introduction to Lattices and Order*, Cambridge University Press, 1997.
- [DJS2003] M. Davis, T. Januszkiewicz, and R. Scott. *Fundamental groups of blow-ups*. Selecta Math., Adv. Math. \*177 no. 1 (2002) pp. 115-179. arXiv math/0203127.
- [DB1996] K. Duggal, A. Bejancu, *Lightlike Submanifolds of Semi-Riemannian Manifolds and Applications*, Mathematics and Its Applications, 1996.
- [DCSW2008] C. De Canniere, H. Sato, D. Watanabe, *Hash Function Luffa: Specification*; submitted to NIST SHA-3 Competition, 2008. Available at <http://www.sdl.hitachi.co.jp/crypto/luffa/>
- [DCW2016] Dan-Cohen, Ishai, and Stefan Wewers. “Mixed Tate motives and the unit equation.” International Mathematics Research Notices 2016.17 (2016): 5291-5354.
- [DD1991] R. Dipper and S. Donkin. *Quantum  $GL_n$* . Proc. London Math. Soc. (3) 63 (1991), no. 1, pp. 165-211.
- [DD2010] Tim Dokchitser and Vladimir Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. Math. (2) 172 (2010), 567-596.
- [DDLL2013] Léo Ducas, Alain Durmus, Tancrède Lepoint and Vadim Lyubashevsky. *Lattice Signatures and Bimodal Gaussians*; in Advances in Cryptology – CRYPTO 2013; Lecture Notes in Computer Science Volume 8042, 2013, pp 40-56 <http://www.di.ens.fr/~lyubash/papers/bimodal.pdf>
- [Dec1998] W. Decker and T. de Jong. Groebner Bases and Invariant Theory in Groebner Bases and Applications. London Mathematical Society Lecture Note Series No. 251. (1998) 61–89.
- [DEMS2016] C. Dobraunig, M. Eichseder, F. Mendel, and M. Schläffer, *Ascon v1.2*; in CAESAR Competition, (2016).
- [DEMMMPU2019] C. Dobraunig, M. Eichseder, S. Mangard, F. Mendel, B. Mennink, R. Primas, T. Unterlugauer “ISAP v2.0” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/ISAP-spec.pdf>
- [De1973] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep., Suppl., vol. 10, 1973.
- [De1970] M. Demazure Sous-groupes algébriques de rang maximum du groupe de Cremona. Ann. Sci. Ecole Norm. Sup. 1970, 3, 507–588.
- [De1974] M. Demazure, *Désingularisation des variétés de Schubert*, Ann. E. N. S., Vol. 6, (1974), p. 163-172
- [Deh2011] P. Dehornoy, *Le problème d’isotopie des tresses*, in Leçons mathématiques de Bordeaux, vol. 4, pages 259-300, Cassini (2011).
- [deG2000] Willem A. de Graaf. *Lie Algebras: Theory and Algorithms*. North-Holland Mathematical Library. (2000). Elsevier Science B.V.

- [deG2005] Willem A. de Graaf. *Constructing homomorphisms between Verma modules*. Journal of Lie Theory. **15** (2005) pp. 415-428.
- [Dej1972] F. Dejean. Sur un théorème de Thue. J. Combinatorial Theory Ser. A 13:90–99, 1972.
- [Del1972] Ph. Delsarte, *Weights of linear codes and strongly regular normed spaces*, Discrete Mathematics (1972), Volume 3, Issue 1, Pages 47-64, doi:10.1016/0012-365X(72)90024-6
- [Den2012] Tom Denton. Canonical Decompositions of Affine Permutations, Affine Codes, and Split  $k$ -Schur Functions. Electronic Journal of Combinatorics, 2012.
- [Deo1987a] V. Deodhar, A splitting criterion for the Bruhat orderings on Coxeter groups. Comm. Algebra, 15:1889-1894, 1987.
- [Deo1987b] V.V. Deodhar, On some geometric aspects of Bruhat orderings II. The parabolic analogue of Kazhdan-Lusztig polynomials, J. Alg. 111 (1987) 483-506.
- [DesignHandbook] Handbook of Combinatorial Designs (2ed) Charles Colbourn, Jeffrey Dinitz Chapman & Hall/CRC 2012
- [DerZak1980] Nachum Dershowitz and Schmuel Zaks, *Enumerations of ordered trees*, Discrete Mathematics (1980), 31: 9-28.
- [Dev2005] Devaney, Robert L. *An Introduction to Chaotic Dynamical Systems*. Boulder: Westview, 2005, 331.
- [DeVi1984] M.-P. Delest, and G. Viennot, *Algebraic Languages and Polyominoes Enumeration*. Theoret. Comput. Sci. 34, 169-206, 1984.
- [DJP2014] Luca De Feo, David Jao and Jérôme Plût: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology, vol. 8, no. 3, 2014, pp. 209-247. <https://eprint.iacr.org/2011/506.pdf>
- [DFMS1996] Philippe Di Francesco, Pierre Mathieu, and David Sénéchal. *Conformal Field Theory*. Graduate Texts in Contemporary Physics, Springer, 1996.
- [DG1982] Louise Dolan and Michael Grady. *Conserved charges from self-duality*, Phys. Rev. D(3) **25** (1982), no. 6, 1587-1604.
- [DG1994] S. Dulucq and O. Guibert. Mots de piles, tableaux standards et permutations de Baxter, proceedings of Formal Power Series and Algebraic Combinatorics, 1994.
- [DG2006] Yon Dourisboure and Cyril Gavoille. *Tree-decompositions with bags of small diameter*. Discrete Mathematics, 307 (16) (2007), pp. 2008-2029. doi:10.1016/j.disc.2005.12.060
- [DGH2020] C. Donnot, A. Genitrini and Y. Herida. Unranking Combinations Lexicographically: an efficient new strategy compared with others, 2020, <https://hal.archives-ouvertes.fr/hal-02462764v1>
- [DGK2014] D. Đoković, O. Golubitsky and I.Kotsireas. *Some New Orders of Hadamard and Skew-Hadamard Matrices*, Journal of Combinatorial Designs 22(6) (2014): 270-277. doi:10.1002/jcd.21358
- [DGMPPS2019] N. Datta, A. Ghoshal, D. Mukhopadhyay, S. Patranabis, S. Picek, R. Sashukhan. “TRIFLE” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/trifle-spec.pdf>
- [DGRB2010] David Avis, Gabriel D. Rosenberg, Rahul Savani, Bernhard von Stengel. *Enumeration of Nash equilibria for two-player games*. <http://www.maths.lse.ac.uk/personal/stengel/ETissue/ARSVS.pdf> (2010)
- [DHSW2003] Dumas, Heckenbach, Saunders, Welker, “Computing simplicial homology based on efficient Smith normal form algorithms,” in “Algebra, geometry, and software systems” (2003), 177-206.
- [DI1989] Dan Gusfield and Robert W. Irving. *The stable marriage problem: structure and algorithms*. Vol. 54. Cambridge: MIT press, 1989.

- [DI1995] F. Diamond and J. Im, Modular forms and modular curves. In: V. Kumar Murty (ed.), Seminar on Fermat's Last Theorem (Toronto, 1993-1994), 39-133. CMS Conference Proceedings 17. American Mathematical Society, 1995.
- [Dil1940] Lattice with Unique Irreducible Decompositions R. P. Dilworth, 1940 (Annals of Mathematics 41, 771-777) With comments by B. Monjardet <http://cams.ehess.fr/docannexe.php?id=1145>
- [Di2000] L. Dissett, Combinatorial and computational aspects of finite geometries, 2000, <https://tspace.library.utoronto.ca/bitstream/1807/14575/1/NQ49844.pdf>
- [DJM1998] R. Dipper, G. James and A. Mathas *Cyclotomic  $q$ -Schur algebras*, Math. Z, **229** (1998), 385-416. [Math-SciNet MR1658581](#)
- [DJP2001] X. Droubay, J. Justin, G. Pirillo, *Episturmian words and some constructions of de Luca and Rauzy*, Theoret. Comput. Sci. 255 (2001) 539–553.
- [Djo1992a] D. Đoković. *Construction of some new Hadamard matrices*, Bulletin of the Australian Mathematical Society 45(2) (1992): 327-332. doi:10.1017/S0004972700030185
- [Djo1992b] D. Đoković. *Skew Hadamard matrices of order  $4 \times 37$  and  $4 \times 43$* , Journal of Combinatorial Theory, Series A 61(2) (1992): 319-321. doi:10.1016/0097-3165(92)90029-T
- [Djo1992c] D. Đoković. *Ten New Orders for Hadamard Matrices of Skew Type*, Publikacije Elektrotehničkog fakulteta. Serija Matematika 2 (1992): 47-59.
- [Djo1994a] D. Đoković. *Five New Orders for Hadamard Matrices of Skew Type*, Australasian Journal of Combinatorics 10 (1994): 259-264.
- [Djo1994b] D. Đoković. *Two Hadamard matrices of order 956 of Goethals-Seidel type*, Combinatorica 14(3) (1994): 375-377. doi:10.1007/BF01212983
- [Djo2008a] D. Đoković. *Skew-Hadamard matrices of orders 188 and 388 exist*, International Mathematical Forum 3 no.22 (2008): 1063-1068. [arXiv 0704.0640](#)
- [Djo2008b] D. Đoković. *Skew-Hadamard matrices of orders 436, 580 and 988 exist*, Journal of Combinatorial Designs 16 (2008): 493-498. [arXiv 0706.1973](#)
- [Djo2008c] D. Đoković. *Hadamard matrices of order 764 exist*, Combinatorica 28(4) (2008): 487-489. doi:10.1007/s00493-008-2384-z
- [Djo2023a] D. Đoković. *Skew-Hadamard matrices of order 276*. [arXiv 10.48550/ARXIV.2301.02751](#)
- [Djo2023b] D. Đoković, Email Communication. 26 January 2023.
- [Djo2024] D. Đoković. *Two classes of Hadamard matrices of Goethals-Seidel type* [arXiv 2404.14375](#)
- [DK2013] John R. Doyle and David Krumm, *Computing algebraic numbers of bounded height*, [arXiv 1111.4963v4](#) (2013).
- [DK2016] D. Đokovic, I. Kotsireas. *A class of cyclic  $(v; k_1, k_2, k_3; \lambda)$  difference families with  $v = 3 \pmod{4}$  a prime*, Special Matrices 4(1) (2016): 317-325. doi:10.1515/spma-2016-0029
- [DLHK2007] J. A. De Loera, D. C. Haws, M. Köppe, Ehrhart polynomials of matroid polytopes and polymatroids. Discrete & Computational Geometry, Volume 42, Issue 4. [arXiv 0710.4346](#), doi:10.1007/s00454-008-9120-8
- [DLMF-Bessel] F. W. J. Olver and L. C. Maximon: *10. Bessel Functions*, in NIST Digital Library of Mathematical Functions. <https://dlmf.nist.gov/10>
- [DLMF-Error] N. M. Temme: *7. Error Functions, Dawson's and Fresnel Integrals*, in NIST Digital Library of Mathematical Functions. <https://dlmf.nist.gov/7>
- [DLMF-Legendre] T. M. Dunster: *Legendre and Related Functions*, in NIST Digital Library of Mathematical Functions. <https://dlmf.nist.gov/14>

- [DLMF-Struve] R. B. Paris: *11. Struve and Related Functions*, in NIST Digital Library of Mathematical Functions. <https://dlmf.nist.gov/11>
- [DLRS2010] De Loera, Rambau and Santos, “Triangulations: Structures for Algorithms and Applications”, Algorithms and Computation in Mathematics, Volume 25, Springer, 2011.
- [DNB1996] Feodor F. Dragan, Falk Nicolai, Andreas Brandstat. *LexBFS-orderings and powers of graphs*. International Workshop on Graph-Theoretic Concepts in Computer Science, WG 1996. Lecture Notes in Computer Science, vol 1197. Springer, Berlin, Heidelberg. doi:10.1007/3-540-62559-3\_15
- [Do2009] P. Dobcsanyi et al. DesignTheory.org. <http://designtheory.org/database/>
- [Dob1999a] H. Dobbertin: *Almost perfect nonlinear power functions on  $GF(2^n)$ : the Niho case*. Information and Computation, 151 (1-2), pp. 57-72, 1999.
- [Dob1999b] H. Dobbertin: *Almost perfect nonlinear power functions on  $GF(2^n)$ : the Welch case*. IEEE Transactions on Information Theory, 45 (4), pp. 1271-1275, 1999.
- [Dol2009] Igor Dolgachev. *McKay Correspondence*. (2009). <http://www.math.lsa.umich.edu/~idolga/McKaybook.pdf>
- [dotspec] <http://www.graphviz.org/doc/info/lang.html>
- [DPS2017] Kevin Dilks, Oliver Pechenik, and Jessica Striker, *Resonance in orbits of plane partitions and increasing tableaux*, JCTA 148 (2017), 244-274, doi:10.1016/j.jcta.2016.12.007
- [DPV2001] J. Daemen, M. Peeters, and G. Van Assche, *Bitslice ciphers and power analysis attacks*; in FSE, (2000), pp. 134-149.
- [DP2008] Jean-Guillaume Dumas and Clement Pernet. Memory efficient scheduling of Strassen-Winograd’s matrix multiplication algorithm. *arXiv 0707.2347v1*, 2008.
- [DPVAR2000] J. Daemen, M. Peeters, G. Van Assche, and V. Rijmen, *Nessie proposal: NOEKEON*; in First Open NESSIE Workshop, (2000).
- [DR2001] J. Du and H. Rui. *Specht modules for Ariki-Koike algebras*, Comm. Alg., **29** (2001), 4710-4719.
- [DR2002] Joan Daemen, Vincent Rijmen. *The Design of Rijndael*. Springer-Verlag Berlin Heidelberg, 2002.
- [Dragan2018] Feodor Dragan, Michel Habib, Laurent Viennot. *Revisiting Radius, Diameter, and all Eccentricity Computation in Graphs through Certificates*. *arXiv 1803.04660*
- [Dro1987] Carl Droms. *Isomorphisms of graph groups*. Proc. of the Amer. Math. Soc. **100** (1987). No 3. <http://educ.jmu.edu/~dromscg/vita/preprints/Isomorphisms.pdf>
- [DS1994] J. Dalbec and B. Sturmfels. Invariant methods in discrete and computational geometry, chapter Introduction to Chow forms, pages 37-58. Springer Netherlands, 1994.
- [DS2004] Dan Gusfield, Jens Stoye, Linear time algorithms for finding and representing all the tandem repeats in a string, Journal of Computer and System Sciences, Volume 69, Issue 4, 2004, Pages 525-546, doi:10.1016/j.jcss.2004.03.004.
- [DS2009] W. Decker, F.-O. Schreyer, *Varieties, Gröbner Bases, and Algebraic Curves*, 2009. <https://www.math.uni-sb.de/ag/schreyer/images/PDFs/teaching/ws1617ag/book.pdf>
- [DS2010] K. Duggal, B. Sahin, *Differential Geometry of Lightlike Submanifolds*, Frontiers in Mathematics, 2010.
- [DSK2006] A. De Sole and V. Kac. “Finite vs Affine W-algebras”. Jpn. J. Math. (2006) vol. 1, no. 1, pp 137–261
- [Du2001] I. Duursma, “From weight enumerators to zeta functions”, in Discrete Applied Mathematics, vol. 111, no. 1-2, pp. 55-73, 2001.
- [Du2003] I. Duursma, “Extremal weight enumerators and ultraspherical polynomials”, Discrete Mathematics 268 (2003), 103–127.

- [Du2004] I. Duursma, “Combinatorics of the two-variable zeta function”, Finite fields and applications, 109-136, Lecture Notes in Comput. Sci., 2948, Springer, Berlin, 2004.
- [Du2009] Du Ye. *On the Complexity of Deciding Degeneracy in Games*. [arXiv 0905.3012v1](https://arxiv.org/abs/0905.3012v1) (2009)
- [Du2010] J. J. Duistermaat, Discrete integrable systems. QRT maps and elliptic surfaces. Springer Monographs in Mathematics. Berlin: Springer. xxii, 627 p., 2010
- [Du2018] O. Dunkelman, *Efficient Construction of the Boomerang Connection Table* (preprint); in Cryptology ePrint Archive, (2018), 631.
- [Duc1998] L. Ducos, Optimizations of the Subresultant Algorithm. <http://www-math.univ-poitiers.fr/~ducos/Travaux/sous-resultants.pdf>
- [Dur1998] F. Durand, *A characterization of substitutive sequences using return words*, Discrete Math. 179 (1998) 89-101.
- [Duv1983] J.-P. Duval, Factorizing words over an ordered alphabet, J. Algorithms 4 (1983) 363–381.
- [Duv1988] A. Duval. *A directed graph version of strongly regular graphs*, Journal of Combinatorial Theory, Series A 47(1) (1988): 71-100. doi:10.1016/0097-3165(88)90043-X
- [DW1995] Andreas W.M. Dress and Walter Wenzel, *A Simple Proof of an Identity Concerning Pfaffians of Skew Symmetric Matrices*, Advances in Mathematics, volume 112, Issue 1, April 1995, pp. 120-134. <http://www.sciencedirect.com/science/article/pii/S0001870885710298>
- [DW2007] I. Dynnikov and B. Wiest, On the complexity of braids, J. Europ. Math. Soc. 9 (2007)
- [Dy1993] M. J. Dyer. *Hecke algebras and shellings of Bruhat intervals*. Compositio Mathematica, 1993, 89(1): 91-115.
- [Dy1994] M. J. Dyer. *Bruhat intervals, polyhedral cones and Kazhdan-Lusztig-Stanley polynomials*. Math.Z., 215(2):223-236, 1994.
- [Dy2001] M. J. Dyer. *On minimal lengths of expressions of Coxeter group elements as products of reflections*. Proc. Amer. Math. Soc. Vol 129 (9) (Sep 2001) pp. 2591-2595
- [Early2017] Nick Early. *Canonical bases for permutohedral plates*. Preprint (2017). [arXiv 1712.08520v3](https://arxiv.org/abs/1712.08520v3).
- [EB1966] J. Elliot and A. Butson. *Relative difference sets*, Illinois Journal of Mathematics 10(3) (1966): 517-531. doi:10.1215/ijm/1256055004
- [Eb1989] W. Eberly, “Computations for algebras and group representations”. Ph.D. Thesis, University of Toronto, 1989. <http://www.cpsc.ucalgary.ca/~eberly/Research/Papers/phdthesis.pdf>
- [Ed1974] A. R. Edmonds, ‘Angular Momentum in Quantum Mechanics’, Princeton University Press (1974)
- [EDI2014] EDITH COHEN, DANIEL DELLING, THOMAS PAJOR and RENATO F. WERNECK Computing Classic Closeness Centrality, at Scale In Proceedings of the second ACM conference on Online social networks (COSN ‘14) doi:10.1145/2660460.2660465
- [Edix] Edixhoven, B., *Point counting after Kedlaya*, EIDMA-Stieltjes graduate course, Leiden (notes: [https://www.math.leidenuniv.nl/~edix/oww/mathofcrypt/carls\\_edixhoven/kedlaya.pdf](https://www.math.leidenuniv.nl/~edix/oww/mathofcrypt/carls_edixhoven/kedlaya.pdf))
- [Ega1981] Yoshimi Egawa, Characterization of  $H(n, q)$  by the parameters, Journal of Combinatorial Theory, Series A, Volume 31, Issue 2, 1981, Pages 108-125, ISSN 0097-3165; doi:10.1016/0097-3165(81)90007-8. (<http://www.sciencedirect.com/science/article/pii/0097316581900078>)
- [EGNO2015] Pavel Etingof, Shlomo Gelaki, Dmitri Nikshych and Victor Ostrik, *Tensor Categories*, AMS Mathematical Surveys and Monographs 205 (2015).
- [EGHLSVY] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, Elena Yudovina, “Introduction to representation theory”, [arXiv 0901.0827v5](https://arxiv.org/abs/0901.0827v5).

- [EKLP1992] N. Elkies, G. Kuperberg, M. Larsen, J. Propp, *Alternating-Sign Matrices and Domino Tilings*, Journal of Algebraic Combinatorics, volume 1 (1992), p. 111–132.
- [Eh2013] Ehrhardt, Wolfgang. “The AMath and DAMath Special Functions: Reference Manual and Implementation Notes, Version 1.3”. 2013. <http://www.wolfgang-ehhardt.de/specialfunctions.pdf>.
- [EL2002] Ekedahl, Torsten & Laksov, Dan. (2002). *Splitting algebras, Symmetric functions and Galois Theory*. J. Algebra Appl. 4, doi:10.1142/S0219498805001034
- [EM2001] Pavel Etingof and Xiaoguang Ma. *Lecture notes on Cherednik algebras*. <http://www-math.mit.edu/~etingof/73509.pdf> arXiv 1001.0432.
- [EMMN1998] P. Eaded, J. Marks, P. Mutzel, S. North. *Fifth Annual Graph Drawing Contest*; <http://www.merl.com/papers/docs/TR98-16.pdf>
- [Eny2012] J. Enyang. *Jucys-Murphy elements and a presentation for the partition algebra*. J. Algebraic Combin. **37** (2012) no 3, 401–454.
- [Eny2013] J. Enyang. *A seminormal form for partition algebras*. J. Combin. Theory Series A **120** (2013) 1737–1785.
- [EP2013] David Einstein, James Propp. *Combinatorial, piecewise-linear, and birational homomesy for products of two chains*. arXiv 1310.5294v1.
- [EP2013b] David Einstein, James Propp. *Piecewise-linear and birational toggling*. Extended abstract for FPSAC 2014. <http://faculty.uml.edu/jpropp/fpsac14.pdf>
- [Epp2008] David Eppstein, *Recognizing partial cubes in quadratic time*, J. Graph Algorithms and Applications 15 (2): 269–293, 2011. doi:10.7155/jgaa.00226, arXiv 0705.1025.
- [EPSV2023] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. *Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic*. LuCaNT 2023. <https://ia.cr/2023/106>
- [Eri1995] H. Erikson. *Computational and Combinatorial Aspects of Coxeter Groups*. Thesis, 1995.
- [ER1959] Paul Erdős and Alfred Rényi. “On Random Graphs”, Publicationes Mathematicae. 6: 290–297, 1959.
- [ERH2015] Jorge Espanoza and Steen Rym-Hansen. *Cell structures for the Yokonuma-Hecke algebra and the algebra of braids and ties*. (2015) arXiv 1506.00715.
- [ERT1979] Erdős, P. and Rubin, A.L. and Taylor, H. *Choosability in graphs*. Proc. West Coast Conf. on Combinatorics, Graph Theory and Computing, Congressus Numerantium, vol 26, pages 125–157, 1979.
- [ESSS2011] D. Engels, M.-J. O. Saarinen, P. Schweitzer, and E. M. Smith, *The Hummingbird-2 lightweight authenticated encryption algorithm*; in RFIDSec, (2011), pp. 19–31.
- [ETS2006a] ETSI/Sage, *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2*; in Document 5: Design and Evaluation Report, (2006).
- [ETS2011] ETSI/Sage, *Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3*; in Document 4: Design and Evaluation Report, (2011).
- [Ewa1996] Ewald, “Combinatorial Convexity and Algebraic Geometry”, vol. 168 of Graduate Texts in Mathematics, Springer, 1996
- [EZ1950] S. Eilenberg and J. Zilber, “Semi-Simplicial Complexes and Singular Homology”, Ann. Math. (2) 51 (1950), 499–513.
- [EPW14] Ben Elias, Nicholas Proudfoot, and Max Wakefield. *The Kazhdan-Lusztig polynomial of a matroid*. 2014. arXiv 1412.7408.
- [Fag1983] Fagin, Ronald. *Degrees of acyclicity for hypergraphs and relational database schemes*. Journal of the ACM (JACM) 30.3 (1983): 514–550.

- [Fayers2010] Matthew Fayers. *An LLT-type algorithm for computing higher-level canonical bases*. J. Pure Appl. Algebra **214** (2010), no. 12, 2186–2198. [arXiv 0908.1749v3](#).
- [Fedorov2015] Roman Fedorov, *Variations of Hodge structures for hypergeometric differential operators and parabolic Higgs bundles*, [arXiv 1505.01704](#)
- [Fe1997] Stefan Felsner, “On the Number of Arrangements of Pseudolines”, Proceedings SoCG 96, 30–37. Discrete & Computational Geometry 18 (1997), 257–267. <http://page.math.tu-berlin.de/~felsner/Paper/numarr.pdf>
- [FT00] Stefan Felsner, William T. Trotter, Dimension, Graph and Hypergraph Coloring, Order, 2000, Volume 17, Issue 2, pp 167–177, <http://link.springer.com/article/10.1023%2FA%3A1006429830221>
- [Feng2014] Gang Feng, *Finding  $k$  shortest simple paths in directed graphs: A node classification algorithm*. Networks, 64(1), 6–17, 2014. [doi:10.1002/net.21552](#)
- [Fe2012] Hans L. Fetter, “A Polyhedron Full of Surprises”, Mathematics Magazine 85 (2012), no. 5, 334–342.
- [Fed2015] Federal Agency on Technical Regulation and Metrology (GOST), GOST R 34.12-2015, (2015)
- [Feingold2004] Alex J. Feingold. *Fusion rules for affine Kac-Moody algebras*. Contemp. Math., **343** (2004), pp. 53–96. [arXiv math/0212387](#)
- [Fel2001] Yves Felix, Stephen Halperin and J.-C. Thomas. *Rational homotopy theory*, Graduate texts in mathematics 201, Springer, 2001.
- [Feu2009] T. Feulner. The Automorphism Groups of Linear Codes and Canonical Representatives of Their Semi-linear Isometry Classes. Advances in Mathematics of Communications 3 (4), pp. 363–383, Nov 2009
- [Feu2013] Feulner, Thomas, “Eine kanonische Form zur Darstellung äquivalenter Codes – Computergestützte Berechnung und ihre Anwendung in der Codierungstheorie, Kryptographie und Geometrie”, Dissertation, University of Bayreuth, 2013.
- [FG1965] Fulkerson, D.R. and Gross, OA, *Incidence matrices and interval graphs*. Pacific J. Math 1965, Vol. 15, number 3, pages 835–855. [doi:10.2140/pjm.1965.15.835](#).
- [FH2015] J. A. de Faria, B. Hutz. *Combinatorics of Cycle Lengths on Wehler  $K3$  Surfaces over finite fields*. New Zealand Journal of Mathematics 45 (2015), 19–31.
- [FIV2012] H. Fournier, A. Ismail, and A. Vigneron. *Computing the Gromov hyperbolicity of a discrete metric space*. 2012. [arXiv 1210.3323](#).
- [FK1991] I. A. Faradjev and M. H. Klin, *Computer package for computations with coherent configurations*, Proc. ISSAC-91, ACM Press, Bonn, 1991, pages 219–223; code, by I.A.Faradjev (with contributions by A.E.Brouwer, D.V.Pasechnik). <https://github.com/dimpase/coco>
- [FKS2004] R. J. Fletcher, C. Koukouvinos and J. Seberry. *New skew-Hadamard matrices of order  $4 \cdot 59$  and new  $D$ -optimal designs of order  $2 \cdot 59$* , Discrete Mathematics 286(3) (2004): 251–253. [doi:10.1016/j.disc.2004.05.009](#)
- [FL2001] David Forge and Michel Las Vergnas. *Orlik-Solomon type algebras*. European J. Combin. **22** (5), (2001). pp. 699–704.
- [FM2014] Cameron Franc and Marc Masdeu, *Computing fundamental domains for the Bruhat-Tits tree for  $GL_2(Q_p)$ ,  $p$ -adic automorphic forms, and the canonical embedding of Shimura curves*. LMS Journal of Computation and Mathematics (2014), volume 17, issue 01, pp. 1–23.
- [FMSS1995] Fulton, MacPherson, Sottile, Sturmfels: *Intersection theory on spherical varieties*, J. of Alg. Geometry 4 (1995), 181–193. <http://www.math.tamu.edu/~frank.sottile/research/ps/spherical.ps.gz>
- [FMV2014] Xander Faber, Michelle Manes, and Bianca Viray. *Computing Conjugating Sets and Automorphism Groups of Rational Functions*. Journal of Algebra, 423 (2014), 1161–1190.

- [FNO2019] Hans Fotsing Tetsing, Ferdinand Ngakeu and Benjamin Olea, *Rigging technique for 1-lightlike submanifolds and preferred rigged connections*, Mediterranean Journal of Mathematics, (2019).
- [Fog2002] N. Pytheas Fogg, *Substitutions in Dynamics, Arithmetics, and Combinatorics*, Lecture Notes in Mathematics 1794, Springer Verlag. V. Berthé, S. Ferenczi, C. Mauduit and A. Siegel, Eds. (2002).
- [Fom1994] Sergey V. Fomin, “Duality of graded graphs”. Journal of Algebraic Combinatorics Volume 3, Number 4 (1994), pp. 357-404.
- [Fom1995] Sergey V. Fomin, “Schensted algorithms for dual graded graphs”. Journal of Algebraic Combinatorics Volume 4, Number 1 (1995), pp. 5-45.
- [FoiMal14] Loic Foissy, Claudia Malvenuto, *The Hopf algebra of finite topologies and T-partitions*, Journal of Algebra, Volume 438, 15 September 2015, pp. 130–169, doi:10.1016/j.jalgebra.2015.04.024, arXiv 1407.0476v2.
- [FoSta1994] S. Fomin, R. Stanley. *Schubert polynomials and the nilCoxeter algebra*. Advances in Math., 1994.
- [FOS2009] G. Fourier, M. Okado, A. Schilling. *Kirillov-Reshetikhin crystals for nonexceptional types*. Advances in Mathematics. **222** (2009). Issue 3. 1080-1116. arXiv 0810.5067.
- [FOS2010] G. Fourier, M. Okado, A. Schilling. *Perfectness of Kirillov-Reshetikhin crystals for nonexceptional types*. Contemp. Math. 506 (2010) 127-143 ( arXiv 0811.1604 )
- [FP1996] Komei Fukuda, Alain Prodon: Double Description Method Revisited, Combinatorics and Computer Science, volume 1120 of Lecture Notes in Computer Science, page 91-111. Springer (1996)
- [FPR2015] Wenjie Fang and Louis-François Prévaille-Ratelle, *From generalized Tamari intervals to non-separable planar maps*. arXiv 1511.05937
- [FR1985] Friedl, Katalin, and Lajos Rónyai. “Polynomial time solutions of some problems of computational algebra”. Proceedings of the seventeenth annual ACM symposium on Theory of computing. ACM, 1985.
- [Fra2011] Cameron Franc, “Nearly rigid analytic modular forms and their values at CM points”, Ph.D. thesis, McGill University, 2011.
- [FRT1990] Faddeev, Reshetikhin and Takhtajan. *Quantization of Lie Groups and Lie Algebras*. Leningrad Math. J. vol. **1** (1990), no. 1.
- [Fru1977] Roberto Frucht. *A Canonical Representation of Trivalent Hamiltonian Graphs*. Journal of Graph Theory, 1:45-60, 1977. doi:10.1002/jgt.3190010111
- [FS1978] Dominique Foata, Marcel-Paul Schuetzenberger. *Major Index and Inversion Number of Permutations*. Mathematische Nachrichten, volume 83, Issue 1, pages 143-159, 1978. <http://igm.univ-mlv.fr/~berstel/Mps/Travaux/A/1978-3MajorIndexMathNachr.pdf>
- [FS1994] William Fulton, Bernd Sturmfels, *Intersection Theory on Toric Varieties*, arXiv alg-geom/9403002
- [FS2009] Philippe Flajolet and Robert Sedgewick, *Analytic combinatorics*. Cambridge University Press, Cambridge, 2009. See also the [Errata list](#).
- [FST2012] A. Felikson, M. Shapiro, and P. Tumarkin, *Cluster Algebras of Finite Mutation Type Via Unfoldings*, Int Math Res Notices (2012) 2012 (8): 1768-1804.
- [Fuchs1994] J. Fuchs. *Fusion Rules for Conformal Field Theory*. Fortsch. Phys. **42** (1994), no. 1, pp. 1-48. doi:10.1002/prop.2190420102, arXiv hep-th/9306162.
- [Ful1989] W. Fulton. Algebraic curves: an introduction to algebraic geometry. Addison-Wesley, Redwood City CA (1989).
- [Ful1993] William Fulton, *Introduction to Toric Varieties*, Princeton University Press, 1993.
- [Ful1997] William Fulton, *Young Tableaux*. Cambridge University Press, 1997.

- [FV2002] I. Fagnot, L. Vuillon, Generalized balances in Sturmian words, *Discrete Applied Mathematics* 121 (2002), 83–101.
- [FY2004] Eva Maria Feichtner and Sergey Yuzvinsky. *Chow rings of toric varieties defined by atomic lattices*. *Inventiones Mathematicae*. **155** (2004), no. 3, pp. 515–536.
- [FZ2001] S. Fomin and A. Zelevinsky. *Cluster algebras I. Foundations*, *J. Amer. Math. Soc.* **15** (2002), no. 2, pp. 497–529. [arXiv math/0104151](https://arxiv.org/abs/math/0104151) (2001).
- [FZ2007] S. Fomin and A. Zelevinsky, *Cluster algebras IV. Coefficients*, *Compos. Math.* 143 (2007), no. 1, 112–164.
- [Ga02] Shuhong Gao, A new algorithm for decoding Reed-Solomon Codes, January 31, 2002
- [Gabow1995] Harold N. Gabow. *A Matroid Approach to Finding Edge Connectivity and Packing Arborescences*. *Journal of Computer and System Sciences*, 50(2):259–273, 1995. doi:10.1006/jcss.1995.1022
- [Gallai] T. Gallai, Elementare Relationen bezüglich der Glieder und trennenden Punkte von Graphen, *Magyar Tud. Akad. Mat. Kutató Int. Kozl.* 9 (1964) 235–236
- [Gambit] Richard D. McKelvey, Andrew M. McLennan, and Theodore L. Turocy, *Gambit: Software Tools for Game Theory, Version 13.1.2.* <http://www.gambit-project.org> (2014).
- [Gans1981] Emden R. Gansner, *The Hillman-Grassl Correspondence and the Enumeration of Reverse Plane Partitions*, *Journal of Combinatorial Theory, Series A* 30 (1981), pp. 71–89. doi:10.1016/0097-3165(81)90041-8
- [Gar2015] V. Garg *Introduction to Lattice Theory with Computer Science Applications* (2015), Wiley.
- [GDR1999] R. González-Díaz and P. Réal, *A combinatorial method for computing Steenrod squares* in *J. Pure Appl. Algebra* 139 (1999), 89–108.
- [GDR2003] R. González-Díaz and P. Réal, *Computation of cohomology operations on finite simplicial complexes* in *Homology, Homotopy and Applications* 5 (2003), 83–93.
- [GCL1992] Geddes, Czapor, Labahn, *Algorithms for computer algebra*. Springer (1992). ISBN 0-7923-9259-0.
- [Ge2005] Loukas Georgiadis, *Linear-Time Algorithms for Dominators and Related Problems*, PhD thesis, Princeton University, TR-737-05, (2005). <ftp://ftp.cs.princeton.edu/reports/2005/737.pdf>
- [Gek1988] E.-U. Gekeler, On the coefficients of Drinfel’d modular forms. *Invent. Math.* 93 (1988), no. 3, 667–700
- [Gek1991] E.-U. Gekeler. On finite Drinfeld modules. *Journal of algebra*, 1(141):187–203, 1991.
- [Gek2017] E.-U. Gekeler. On Drinfeld modular forms of higher rank. *Journal de théorie des nombres de Bordeaux*, Volume 29 (2017) no. 3, pp. 875–902. doi:10.5802/jtnb.1005
- [GG2012] Jim Geelen and Bert Gerards, Characterizing graphic matroids by a system of linear equations, submitted, 2012. Preprint: [http://www.gerardsbase.nl/papers/geelen\\_gerards=testing-graphicness%5B2013%5D.pdf](http://www.gerardsbase.nl/papers/geelen_gerards=testing-graphicness%5B2013%5D.pdf)
- [GGD2011] E. Gironde, G. Gonzalez-Diez, *Introduction to Compact Riemann surfaces and Dessins d’enfant*, (2011) London Mathematical Society, Student Text 79.
- [GGMM2020] A. Garver, S. Grosser, J. Matherne, and A. Morales. *Counting linear extensions of posets with determinants of hook lengths*. Preprint, [arXiv 2001.08822](https://arxiv.org/abs/2001.08822) (2020).
- [GGNS2013] B. Gerard, V. Grosso, M. Naya-Plasencia, and F.-X. Standaert, *Block ciphers that are easier to mask: How far can we go?*; in *CHES*, (2013), pp. 383–399.
- [GGOR2003] V. Ginzberg, N. Guay, E. Opdam, R. Rouquier. *On the category  $\mathcal{O}$  for rational Cherednik algebras*. *Invent. Math.* **154** (2003). [arXiv math/0212036](https://arxiv.org/abs/math/0212036).
- [GHJ2016] Ewgenij Gawrilow, Simon Hampe, and Michael Joswig, The polymake XML file format, *Mathematical software – ICMS 2016. 5th international congress*, Berlin, Germany, July 11–14, 2016. *Proceedings*, Berlin: Springer, 2016, pp. 403–410, doi:10.1007/978-3-319-42432-3\_50, ISBN 978-3-319-42431-6/pbk.

- [GHJV1994] E. Gamma, R. Helm, R. Johnson, J. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley (1994). ISBN 0-201-63361-2.
- [Gil1959] Edgar Nelson Gilbert. “Random Graphs”, *Annals of Mathematical Statistics*. 30 (4): 1141–1144, 1959.
- [Gir2012] Samuele Giraudo, *Algebraic and combinatorial structures on pairs of twin binary trees*, [arXiv 1204.4776v1](#).
- [GiTr1996] P. Gianni and B. Trager. *Square-Free Algorithms in Positive Characteristic*. *Applicable Algebra In Engineering, Communication And Computing*, 7(1), p. 1-14.
- [GJ1997] Ewgenij Gawrilow and Michael Joswig, polymake: a framework for analyzing convex polytopes, *Polytopes—combinatorics and computation (Oberwolfach, 1997)*, DMV Sem., vol. 29, Birkhäuser, Basel, 2000, pp. 43–73.
- [GJ2006] Ewgenij Gawrilow and Michael Joswig, Flexible object hierarchies in polymake (extended abstract), *Mathematical software—ICMS 2006, Lecture Notes in Comput. Sci.*, vol. 4151, Springer, Berlin, 2006, pp. 219–221, [doi:10.1007/11832225\\_20](#)
- [GJ2007] A. Glen, J. Justin, Episturmian words: a survey, Preprint, 2007, [arXiv 0801.1655](#).
- [Goff1999] Christopher Goff. *Isomorphic fusion algebras of twisted quantum doubles of finite groups*. PhD Thesis, University of California, Santa Cruz. 1999.
- [GoMa2010] Christopher Goff and Geoffrey Mason, *Generalized twisted quantum doubles and the McKay correspondence*, *J. Algebra* 324 (2010), no. 11, 3007–3016.
- [GJ2016] Muddappa Seetharama Gowda and Juyoung Jeong. Spectral cones in Euclidean Jordan algebras. *Linear Algebra and its Applications*, 509:286-305, 2016. [doi:10.1016/j.laa.2016.08.004](#).
- [GJKPRSS2019] D. Goudarzi, J. Jean, S. Koelbl, T. Peyrin, M. Rivain, Y. Sasaki, S. M. Sim. “Pyjamask” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Pyjamask-spec.pdf>
- [GJK+2014] Dimitar Grantcharov, Ji Hye Jung, Seok-Jin Kang, Masaki Kashiwara, Myungho Kim. *Crystal bases for the quantum queer superalgebra and semistandard decomposition tableaux.*; *Trans. Amer. Math. Soc.*, 366(1): 457-489, 2014. [arXiv 1103.1456v2](#).
- [GJPST2009] G. Grigorov, A. Jorza, S. Patrikis, W. Stein, C. Tarniță. Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves. *Math. Comp.* 78 (2009), no. 268, 2397–2425.
- [GJRW2010] Ewgenij Gawrilow, Michael Joswig, Thilo Rörig, and Nikolaus Witte, Drawing polytopal graphs with polymake, *Comput. Vis. Sci.* 13 (2010), no. 2, 99–110, [doi:10.1007/s00791-009-0127-3](#)
- [GK1982] Daniel H. Greene and Donald E. Knuth (1982), “2.1.1 Constant coefficients - A) Homogeneous equations”, *Mathematics for the Analysis of Algorithms* (2nd ed.), Birkhauser, p. 17.
- [GK2013] Roland Grinis and Alexander Kasprzyk, Normal forms of convex lattice polytopes, [arXiv 1301.6641](#)
- [GKLP2021] Loukas Georgiadis, Dionysios Kefallinos, Luigi Laura, Nikos Parotsidis. *An Experimental Study of Algorithms for Computing the Edge Connectivity of a Directed Graph*. *SIAM Symposium on Algorithm Engineering and Experiments (ALENEX)*, pp 85-97, 2021. [doi:10.1137/1.9781611976472.7](#)
- [GKP2011] Sylvain Gravier, Matjaz Kovse and Aline Parreau. *Generalized Sierpinski graphs*. Poster, European Conference on Combinatorics, Graph Theory and Applications (EuroComb’11), Budapest, 2011. <https://www.renyi.hu/conferences/ec11/posters/parreau.pdf>
- [GKZ1994] Gelfand, I. M.; Kapranov, M. M.; and Zelevinsky, A. V. “Discriminants, Resultants and Multidimensional Determinants” Birkhauser 1994
- [GL1996] G. Golub and C. van Loan. *Matrix Computations*. 3rd edition, Johns Hopkins Univ. Press, 1996.
- [GL2019] J. Grbić and A. Linton. “Lowest-degree triple Massey products in moment-angle complexes”, 2019. [arXiv 1908.02222v2](#)

- [GrLe1996] J. Graham and G.I. Lehrer *Cellular algebras*. Invent. Math. 123 (1996), 1–34. [MathSciNet MR1376244](#)
- [GLR2008] A. Glen, F. Levé, G. Richomme, Quasiperiodic and Lyndon episturmian words, Preprint, 2008, [arXiv 0805.0730](#).
- [GLSV2014] V. Grosso, G. Leurent, F.-X. Standaert, and K. Varici: *LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations*, in FSE, 2014.
- [GLSVJGK2014] V. Grosso, G. Leurent, F.-X. Standaert, K. Varici, F. D. A. Journault, L. Gaspar, and S. Kerckhof, *SCREAM & iSCREAM Side-Channel Resistant Authenticated Encryption with Masking*; in CAESAR Competition, (2014).
- [GM1987] Peter B. Gibbons and Rudolf MATHON. *Construction methods for Bhaskar Rao and related designs*. J. Austral. Math. Soc. Ser. A 42 (1987), no. 1, 5–30. [http://journals.cambridge.org/article\\_S1446788700033929](http://journals.cambridge.org/article_S1446788700033929)
- [GM2002] Daniel Goldstein and Andrew Mayer. On the equidistribution of Hecke points. Forum Mathematicum, 15:2, pp. 165–189, De Gruyter, 2003.
- [GMN2008] Jordi Guardia, Jesus Montes, Enric Nart. *Newton polygons of higher order in algebraic number theory* (2008). [arXiv 0807.2620](#)
- [GNL2011] Z. Gong, S. Nikova, and Y. W. Law, *KLEIN: A new family of lightweight block ciphers*; in RFIDSec, (2011), p. 1-18.
- [GN2018] Pascal Giorgi and Vincent Neiger. Certification of Minimal Approximant Bases. In ISSAC 2018, pages 167-174. [doi:10.1145/3208976.3208991](#)
- [Go1967] Solomon Golomb, Shift register sequences, Aegean Park Press, Laguna Hills, Ca, 1967
- [God1968] R. Godement: *Algebra*, Hermann (Paris) / Houghton Mifflin (Boston) (1968)
- [God1993] Chris Godsil (1993): *Algebraic Combinatorics*.
- [Gol1968] R. Gold: *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*. IEEE Transactions on Information Theory, 14, pp. 154-156, 1968.
- [Gop1981] V. D. Goppa, “Codes on algebraic curves,” Sov. Math. Dokl., vol. 24, no. 1, pp. 170–172, 1981.
- [Gor2016] D. Gorodkov, *A 15-vertex triangulation of the quaternionic projective plane*, Discrete & Computational Geometry, vol. 62, pp. 348-373 (2019). [doi:10.1007/s00454-018-00055-w](#)
- [Gos1972] Bill Gosper, “Continued Fraction Arithmetic” <https://perl.plover.com/classes/cftalk/INFO/gosper.txt>
- [Gos1998] D. Goss. Basic structures of function field arithmetic. Springer, 1998.
- [Gor1980] Daniel Gorenstein, Finite Groups (New York: Chelsea Publishing, 1980)
- [Gor2009] Alexey G. Gorinov, “Combinatorics of double cosets and fundamental domains for the subgroups of the modular group”, preprint [arXiv 0901.1340](#)
- [GP2012] Eddy Godelle and Luis Paris. *Basic questions on Artin-Tits groups*. A. Björner et al. (eds) Configuration spaces, CRM series. (2012) pp. 299–311. Edizioni della Normale, Pisa. [doi:10.1007/978-88-7642-431-1\\_13](#)
- [GPV2008] Craig Gentry, Chris Peikert, Vinod Vaikuntanathan. *How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions*. STOC 2008. [http://www.cc.gatech.edu/~cpeikert/pubs/trap\\_lattice.pdf](http://www.cc.gatech.edu/~cpeikert/pubs/trap_lattice.pdf)
- [GR2001] Chris Godsil and Gordon Royle, *Algebraic Graph Theory*. Graduate Texts in Mathematics, Springer, 2001.
- [Gre2006] R. M. Green, *Star reducible Coxeter groups*, Glasgow Mathematical Journal, Volume 48, Issue 3, pp. 583-609.

- [Gri2021] O. Gritsenko, *On strongly regular graph with parameters (65; 32; 15; 16)*, [arXiv 2102.05432](#).
- [GX2020] R. M. Green, Tianyuan Xu, *Classification of Coxeter groups with finitely many elements of a-value 2*, Algebraic Combinatorics, Volume 3 (2020) no. 2, pp. 331-364.
- [Gr2006] Matthew Greenberg, “Heegner points and rigid analytic modular forms”, Ph.D. Thesis, McGill University, 2006.
- [Gr2007] J. Green, Polynomial representations of  $GL_n$ , Springer Verlag, 2007.
- [Graham1985] J. Graham, *Modular representations of Hecke algebras and related algebras*. PhD thesis, University of Sydney, 1985.
- [GriRei18] Darij Grinberg, Victor Reiner, *Hopf Algebras in Combinatorics*, [arXiv 1409.8356v6](#).
- [GR1989] A. M. Garsia, C. Reutenauer. *A decomposition of Solomon’s descent algebra*. Adv. Math. **77** (1989). <http://www.lacim.uqam.ca/~christo/Publi%C3%A9s/1989/Decomposition%20Solomon.pdf>
- [GR1993] Ira M. Gessel, Christophe Reutenauer. *Counting Permutations with Given Cycle Structure and Descent Set*. Journal of Combinatorial Theory, Series A, 64 (1993), pp. 189–215.
- [GR2013] Darij Grinberg, Tom Roby. *Iterative properties of birational rowmotion*. <http://www.cip.ifi.lmu.de/~grinberg/algebra/skeletal.pdf>
- [Gri2005] G. Grigorov, Kato’s Euler System and the Main Conjecture, Harvard Ph.D. Thesis (2005).
- [GroLar1] R. Grossman and R. G. Larson, *Hopf-algebraic structure of families of trees*, J. Algebra 126 (1) (1989), 184-210. Preprint: [arXiv 0711.3877v1](#)
- [Grinb2016a] Darij Grinberg, *Double posets and the antipode of QSym*, [arXiv 1509.08355v3](#).
- [Gro1987] M. Gromov. *Hyperbolic groups*. Essays in Group Theory, 8:75–263, 1987. doi:10.1007/978-1-4613-9586-7\_3.
- [GrS1967] Grunbaum and Sreedharan, “An enumeration of simplicial 4-polytopes with 8 vertices”, J. Comb. Th. 2, 437-465 (1967)
- [Gru2003] Branko Grünbaum. *Convex Polytopes* (2nd ed), volume 221 of Graduate Texts in Mathematics, Springer, 2003. (1st ed, 1967, Wiley New York). doi:10.1007/978-1-4613-0019-9
- [GS1984] A. M. Garsia, Dennis Stanton. *Group actions on Stanley-Reisner rings and invariants of permutation groups*. Adv. in Math. **51** (1984), 107-201. <http://www.sciencedirect.com/science/article/pii/001870884900057>
- [GS1999] Venkatesan Guruswami and Madhu Sudan, Improved Decoding of Reed-Solomon Codes and Algebraic-Geometric Codes, 1999
- [GS2010] Daniel Gourion and Alberto Seeger. Critical angles in polyhedral convex cones: numerical and statistical considerations. Mathematical Programming, 123:173-198, 2010. doi:10.1007/s10107-009-0317-2.
- [Go1993] David M. Goldschmidt. *Group characters, symmetric functions, and the Hecke algebras*. AMS 1993.
- [GS1970] J.-M. Goethals and J. J. Seidel, *Strongly regular graphs derived from combinatorial designs*, Can. J. Math. 22 (1970) 597-614. doi:10.4153/CJM-1970-067-9
- [GS70s] J.M. Goethals and J. J. Seidel, *A skew Hadamard matrix of order 36*, J. Aust. Math. Soc. 11(1970), 343-344
- [GS1975] J.M. Goethals, and J. J. Seidel, *The regular two-graph on 276 vertices*, Discrete Mathematics 12, no. 2 (1975): 143-158. doi:10.1016/0012-365X(75)90029-1
- [GSL] GNU Scientific Library. <https://www.gnu.org/software/gsl/doc/html/>
- [GT1996] P. Gianni and B. Trager. “Square-free algorithms in positive characteristic”. Applicable Algebra in Engineering, Communication and Computing, 7(1), 1-14 (1996)

- [GT2001] Michael T. Goodrich and Roberto Tamassia. *Data Structures and Algorithms in Java*. 2nd edition, John Wiley & Sons, 2001.
- [GT2014] M.S. Gowda and J. Tao. On the bilinearity rank of a proper cone and Lyapunov-like transformations. *Mathematical Programming*, 147 (2014) 155-170.
- [Gu] GUAVA manual, <https://www.gap-system.org/Packages/guava.html>
- [Gut2001] Carsten Gutwenger and Petra Mutzel. *A Linear Time Implementation of SPQR-Trees*, International Symposium on Graph Drawing, (2001) 77-90
- [GW1999] Frederick M. Goodman and Hans Wenzl. *Crystal bases of quantum affine algebras and affine Kazhdan-Lusztig polynomials*. *Int. Math. Res. Notices* **5** (1999), 251-275. [arXiv math/9807014v1](https://arxiv.org/abs/math/9807014v1).
- [GW2014] G. Gratzner and F. Wehrung, *Lattice Theory: Special Topics and Applications Vol. 1*, Springer, 2014.
- [GYLL1993] I. Gutman, Y.-N. Yeh, S.-L. Lee, and Y.-L. Luo. *Some recent results in the theory of the Wiener number*. *Indian Journal of Chemistry*, 32A:651-661, 1993.
- [GZ1983] Greene; Zaslavsky, “On the Interpretation of Whitney Numbers Through Arrangements of Hyperplanes, Zonotopes, Non-Radon Partitions, and Orientations of Graphs”. *Transactions of the American Mathematical Society*, Vol. 280, No. 1. (Nov., 1983), pp. 97-126.
- [GZ1986] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*. *Invent. Math.* 84 (1986), no. 2, 225-320.
- [Ha2005] Gerhard Haring. [Online] Available: <http://osdir.com/ml/python.db.pygresqlite.user/2005-11/msg00047.html>
- [Ha83] M. Hall, *Combinatorial Theory*, 2nd edition, Wiley, 1983
- [Hac2016] M. Hachimori. [http://infoshako.sk.tsukuba.ac.jp/~hachi/math/library/dunce\\_hat\\_eng.html](http://infoshako.sk.tsukuba.ac.jp/~hachi/math/library/dunce_hat_eng.html)
- [HadaWiki] Hadamard matrices on Wikipedia, [Wikipedia article Hadamard\\_matrix](#)
- [Haf2004] Paul R. Hafner. *On the Graphs of Hoffman-Singleton and Higman-Sims*. *The Electronic Journal of Combinatorics* 11 (2004), #R77. [http://www.combinatorics.org/Volume\\_11/PDF/v11i1r77.pdf](http://www.combinatorics.org/Volume_11/PDF/v11i1r77.pdf)
- [Hai1989] M.D. Haiman, *On mixed insertion, symmetry, and shifted Young tableaux*. *Journal of Combinatorial Theory, Series A* Volume 50, Number 2 (1989), pp. 196-225.
- [Hai1992] Mark D. Haiman, *Dual equivalence with applications, including a conjecture of Proctor*, *Discrete Mathematics* 99 (1992), 79-113, <http://www.sciencedirect.com/science/article/pii/0012365X9290368P>
- [Haj2000] M. Hajiaghayi, *Consecutive Ones Property*, 2000. <http://www-math.mit.edu/~hajiagha/pp11.ps>
- [Han1960] Haim Hanani, On quadruple systems, pages 145-157, vol. 12, *Canadian Journal of Mathematics*, 1960 <http://cms.math.ca/cjm/v12/cjm1960v12.0145-0157.pdf>
- [Har1962] Frank Harary. *The determinant of the adjacency matrix of a graph*. *SIAM Review* 4 (1962), pp. 202-210. [doi:10.1137/1004057](https://doi.org/10.1137/1004057)
- [Har1969] Frank Harary, *Graph Theory*, Addison-Wesley, 1969.
- [Har1977] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.
- [Har1994] Frank Harary. *Graph Theory*. Reading, MA: Addison-Wesley, 1994.
- [Har2009] Harvey, David. *Efficient computation of p-adic heights*. *LMS J. Comput. Math.* **11** (2008), 40-59.
- [Harako2020] Shuichi Harako. *The second homology group of the commutative case of Kontsevich's symplectic derivation Lie algebra*. Preprint, 2020, [arXiv 2006.06064](https://arxiv.org/abs/2006.06064).
- [HarPri] F. Harary and G. Prins. The block-cutpoint-tree of a graph. *Publ. Math. Debrecen* 13 1966 103-107.
- [Harv2007] David Harvey. *Kedlaya's algorithm in larger characteristic*, [arXiv math/0610973](https://arxiv.org/abs/math/0610973).

- [BGS2007] Alin Bostan, Pierrick Gaudry, and Eric Schost, *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator*, SIAM Journal on Computing 36 (2007), no. 6, 1777-1806
- [Hat2002] Allen Hatcher, "Algebraic Topology", Cambridge University Press (2002).
- [Hayashi1990] T. Hayashi. *q-analogues of Clifford and Weyl algebras - spinor and oscillator representations of quantum enveloping algebras*. Comm. Math. Phys. **127** (1990) pp. 129-144.
- [HC2006] Mark van Hoeij and John Cremona, Solving Conics over function fields. J. Théor. Nombres Bordeaux, 2006.
- [He2006] Pinar Heggernes. *Minimal triangulations of graphs: A survey*. Discrete Mathematics, 306(3):297-317, 2006. doi:10.1016/j.disc.2005.12.003
- [He2002] H. Heys *A Tutorial on Linear and Differential Cryptanalysis* ; 2002' available at [http://www.engr.mun.ca/~howard/PAPERS/ldc\\_tutorial.pdf](http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf)
- [Hes2004] Florian Hess, "Computing relations in divisor class groups of algebraic curves over finite fields," Preprint, 2004.
- [Hes2002] Florian Hess, "Computing Riemann-Roch spaces in algebraic function fields and related topics," J. Symbolic Comput. 33 (2002), no. 4, 425-445.
- [Hes2002b] Florian Hess, "An algorithm for computing Weierstrass points," International Algorithmic Number Theory Symposium (pp. 357-371). Springer Berlin Heidelberg, 2002.
- [HH2012] Victoria Horan and Glenn Hurlbert, *Overlap Cycles for Steiner Quadruple Systems*, 2012, [arXiv 1204.3215](https://arxiv.org/abs/1204.3215)
- [HHL2009] T. Huang, L. Huang, M.I. Lin, *On a class of strongly regular designs and quasi-semisymmetric designs*. In: Recent Developments in Algebra and Related Areas, ALM vol. 8, pp. 129-153. International Press, Somerville (2009).
- [Hig2002] Nicholas J. Higham. Accuracy and Stability of Numerical Algorithms, Second Edition. Society for Industrial and Applied Mathematics, Philadelphia, 2002.
- [Hig2008] N. J. Higham, "Functions of matrices: theory and computation", Society for Industrial and Applied Mathematics (2008).
- [HIK2011] R. Hammack, W. Imrich, S. Klavzar, *Handbook of Product Graphs*, CRC press, 2011
- [HJ2004] Tom Hoeholdt and Joern Justesen, A Course In Error-Correcting Codes, EMS, 2004
- [HK2002a] Holme, P. and Kim, B.J. *Growing scale-free networks with tunable clustering*, Phys. Rev. E (2002). vol 65, no 2, 026107. doi:10.1103/PhysRevE.65.026107.
- [HKL2022] Clemens Heuberger, Daniel Krenn, Gabriel F. Lipnik, "Asymptotic Analysis of  $q$ -Recursive Sequences". Algorithmica **84** (2022), 2480-2532. doi:10.1007/s00453-022-00950-y.
- [HKOTY1999] G. Hatayama, A. Kuniba, M. Okado, T. Tagaki, and Y. Yamada, *Remarks on fermionic formula*. Contemp. Math., **248** (1999).
- [HKP2010] T. J. Haines, R. E. Kottwitz, A. Prasad, Iwahori-Hecke Algebras, J. Ramanujan Math. Soc., 25 (2010), 113-145. [arXiv 0309168v3](https://arxiv.org/abs/0309168v3) [MathSciNet MR2642451](https://mathscinet.ams.org/mathscinet/item.aspx?infocode=MR&id=MR2642451)
- [HL1999] L. Heath and N. Loehr (1999). New algorithms for generating Conway polynomials over finite fields. Proceedings of the tenth annual ACM-SIAM symposium on discrete algorithms, pp. 429-437.
- [HL2008] J. Hong and H. Lee. Young tableaux and crystal  $B(\infty)$  for finite simple Lie algebras. J. Algebra 320, pp. 3680-3693, 2008.
- [HL2014] Thomas Hamilton and David Loeffler, "Congruence testing for odd modular subgroups", LMS J. Comput. Math. 17 (2014), no. 1, 206-208, doi:10.1112/S1461157013000338.

- [HL2018] Mustafa Hajij and Jesse Levitt, “An Efficient Algorithm to Compute the Colored Jones Polynomial” [arXiv 1804.07910v2](#).
- [Hli2006] Petr Hlineny, “Equivalence-free exhaustive generation of matroid representations”, *Discrete Applied Mathematics* 154 (2006), pp. 1210-1222.
- [HLT1993] F. Harary, E. Loukakis, C. Tsouros, *The geodetic number of a graph*. Mathematical and computer modelling, vol. 17 n11 pp.89–95, 1993. doi:10.1016/0895-7177(93)90259-2.
- [HLY2002] Yi Hu, Chien-Hao Liu, and Shing-Tung Yau. Toric morphisms and fibrations of toric Calabi-Yau hypersurfaces. *Adv. Theor. Math. Phys.*, 6(3):457-506, 2002. [arXiv math/0010082v2](#) [math.AG].
- [HM2011] Florent Hivert and Olivier Mallet. *Combinatorics of k-shapes and Genocchi numbers*, in FPSAC 2011, Reykjavík, Iceland DMTCS proc. AO, 2011, 493-504.
- [HoDaCG17] Toth, Csaba D., Joseph O’Rourke, and Jacob E. Goodman. *Handbook of Discrete and Computational Geometry* (3rd Edition). Chapman and Hall/CRC, 2017.
- [Hoc] Winfried Hochstaettler, “About the Tic-Tac-Toe Matroid”, preprint.
- [HJ18] Thorsten Holm and Peter Jorgensen *A p-angulated generalisation of Conway and Coxeter’s theorem on frieze patterns*, *International Mathematics Research Notices* (2018)
- [Hopcroft1973] J. E. Hopcroft and R. E. Tarjan. *Dividing a Graph into Triconnected Components*, *SIAM J. Comput.*, 2(3), 135–158
- [Hopkins2017] Sam Hopkins, *RSK via local transformations*, <http://web.mit.edu/~shopkins/docs/rsk.pdf>
- [HilGra1976] A. P. Hillman, R. M. Grassl, *Reverse plane partitions and tableau hook numbers*, *Journal of Combinatorial Theory, Series A* 21 (1976), pp. 216–221. doi:10.1016/0097-3165(76)90065-0
- [HK2002] *Introduction to Quantum Groups and Crystal Bases*. Jin Hong and Seok-Jin Kang. 2002. Volume 42. Graduate Studies in Mathematics. American Mathematical Society.
- [HM1979] M. Habib, and M.C. Maurer On the X-join decomposition for undirected graphs *Discrete Applied Mathematics* vol 1, issue 3, pages 201-207
- [HMPV2000] Michel Habib, Ross McConnell, Christophe Paul, and Laurent Viennot. *Lex-BFS and partition refinement, with applications to transitive orientation, interval graph recognition and consecutive ones testing*. *Theoretical Computer Science*, 234(1-2): 59-84, 2000. doi:10.1016/S0304-3975(97)00241-7.
- [HN2006] Florent Hivert and Janvier Nzeutchap. *Dual Graded Graphs in Combinatorial Hopf Algebras*. <https://www.lri.fr/~hivert/PAPER/commCombHopfAlg.pdf>
- [HNT2005] Florent Hivert, Jean-Christophe Novelli, and Jean-Yves Thibon. *The algebra of binary search trees*, [arXiv math/0401089v2](#).
- [Hora] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, 2006.
- [HP2003] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, 2003.
- [HP2010] Michel Habib and Christophe Paul, *A survey of the algorithmic aspects of modular decomposition*. *Computer Science Review* vol 4, number 1, pages 41–59, 2010, <http://www.lirmm.fr/~paul/md-survey.pdf>, doi:10.1016/j.cosrev.2010.01.001.
- [HP2016] S. Hopkins, D. Perkinson. “Bigraphical Arrangements”. *Transactions of the American Mathematical Society* 368 (2016), 709-725. [arXiv 1212.4398](#)
- [HPR2010] Gary Haggard, David J. Pearce and Gordon Royle. *Computing Tutte Polynomials*. In *ACM Transactions on Mathematical Software*, Volume 37(3), article 24, 2010. Preprint: <http://homepages.ecs.vuw.ac.nz/~djp/files/TOMS10.pdf>
- [HPS2008] J. Hoffstein, J. Pipher, and J.H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.

- [HPS2017] Graham Hawkes, Kirill Paramonov, and Anne Schilling. *Crystal analysis of type C Stanley symmetric functions*. Electronic J. Comb. 24(3) (2017) #P3.51. [arXiv 1704.00889](#).
- [HOLM2016] Tristan Holmes and J. B. Nation, *Inflation of finite lattices along all-or-nothing sets*. <http://www.math.hawaii.edu/~jb/inflation.pdf>
- [Hor1972] E. Horowitz, “Algorithms for Rational Function Arithmetic Operations”, Annual ACM Symposium on Theory of Computing, Proceedings of the Fourth Annual ACM Symposium on Theory of Computing, pp. 108–118, 1972
- [HR2005] Tom Halverson and Arun Ram. *Partition algebras*. Euro. J. Combin. **26** (2005) 869–921.
- [HR2016] Clemens Heuberger and Roswitha Rissner, “Computing  $J$ -Ideals of a Matrix Over a Principal Ideal Domain”, [arXiv 1611.10308](#), 2016.
- [HR2017] Patricia Hersh and Victor Reiner, “Representation Stability for Cohomology of Configuration Spaces in  $\mathbb{R}^d$ ”, International Mathematics Research Notices, Vol 2017, No. 5, pp. 1433-1486. [doi:10.1093/imrn/rnw060](#)
- [HRS1993] C. D. Hodgson, I. Rivin and W. D. Smith. *A characterization of convex hyperbolic polyhedra and of convex polyhedra inscribed in the sphere*. Bulletin of the American Mathematical Society 27.2 (1992): 246-251.
- [HRS2016] J. Haglund, B. Rhoades, M. Shimozono. *Ordered set partitions, generalized coinvariant algebras, and the Delta Conjecture*. Preprint, [arXiv 1609.07575](#).
- [HRT2000] R.B. Howlett, L.J. Rylands, and D.E. Taylor. *Matrix generators for exceptional groups of Lie type*. J. Symbolic Computation. **11** (2000). <http://www.maths.usyd.edu.au/u/bobh/hrt.pdf>
- [HRW2015] J. Haglund, J. B. Remmel, A. T. Wilson. *The Delta Conjecture*. Preprint, [arXiv 1509.07058](#).
- [HS1968] Donald G. Higman and Charles C. Sims. *A simple group of order 44,352,000*. Mathematische Zeitschrift 105(2): 110-113, 1968. [doi:10.1007/BF01110435](#).
- [HS2010] Rene Henrion and Alberto Seeger. *Inradius and Circumradius of Various Convex Cones Arising in Applications*. Set-Valued and Variational Analysis, 18(3-4):483-511, 2010. [doi:10.1007/s11228-010-0150-z](#).
- [HS2018] B. Hutz, M. Stoll. “Smallest representatives of  $SL(2, \mathbf{Z})$ -orbits of binary forms and endomorphisms of  $P^1$ ”, [arXiv 1805.08579](#), 2018.
- [HSS] Aric Hagberg, Dan Schult and Pieter Swart. *NetworkX documentation*. [Online] Available: <http://networkx.github.io/documentation/latest/reference/index.html>
- [Hsu1996] Tim Hsu, “Identifying congruence subgroups of the modular group”, Proc. AMS 124, no. 5, 1351-1359 (1996)
- [Hsu1997] Tim Hsu, “Permutation techniques for coset representations of modular subgroups”, in L. Schneps (ed.), Geometric Galois Actions II: Dessins d’Enfants, Mapping Class Groups and Moduli, volume 243 of LMS Lect. Notes, 67-77, Cambridge Univ. Press (1997)
- [HST2001] Matthew D. Horton, H. M. Stark, and Audrey A. Terras, *What are zeta functions of graphs and what are they good for?*, in Quantum graphs and their applications, 173-189, Contemp. Math., Vol. 415.
- [HST2008] F. Hivert, A. Schilling, N. Thiery, *Hecke group algebras as quotients of affine Hecke algebras at level 0*, Journal of Combinatorial Theory, Series A 116 (2009) 844-863 ([arXiv 0804.3781](#))
- [HSV2006] Hess, Smart, Vercauteren, “The Eta Pairing Revisited”, IEEE Trans. Information Theory, 52(10): 4595-4602, 2006.
- [HT1972] Samuel Huang and Dov Tamari. *Problems of associativity: A simple proof for the lattice property of systems ordered by a semi-associative law*. J. Combinatorial Theory Ser. A. (1972). <http://www.sciencedirect.com/science/article/pii/0097316572900039> .

- [Hub1975] X. L. Hubaut. *Strongly regular graphs*. Disc. Math. 13(1975), pp 357–381. doi:10.1016/0012-365X(75)90057-6.
- [HT1996] W. H. Haemers and V. D. Tonchev, *Spreads in strongly regular graphs*, Designs, Codes and Cryptography 8 (1996) 145–157. doi:10.1023/A:1018037025910.
- [HMMS2019] June Huh, Jacob P. Matherne, Karola Mészáros, Avery St. Dizier. *Logarithmic concavity of Schur and related polynomials*. Trans. Am. Math. Soc. 375, No. 6, 4411–4427 (2022). arXiv 1906.09633, doi:10.1090/tran/8606.
- [Hutz2007] B. Hutz. Arithmetic Dynamics on Varieties of dimension greater than one. PhD Thesis, Brown University 2007
- [Hutz2009] B. Hutz. Good reduction of periodic points, Illinois Journal of Mathematics 53 (Winter 2009), no. 4, 1109–1126.
- [Hutz2015] B. Hutz. Determination of all rational preperiodic points for morphisms of PN. Mathematics of Computation, 84:291 (2015), 289–308.
- [Hutz2019] B. Hutz. Multipliers and invariants of endomorphisms of projective space in dimension greater than 1, Journal de Théorie des Nombres de Bordeaux, Tome 32 (2020) no. 2, pp. 439–469.
- [Huy2005] D. Huybrechts : *Complex Geometry*, Springer (Berlin) (2005).
- [HX2010] W. Haemers and Q. Xiang, Strongly regular graphs with parameters  $(4m^4, 2m^4 + m^2, m^4 + m^2, m^4 + m^2)$  exist for all  $m > 1$ , European Journal of Combinatorics, Volume 31, Issue 6, August 2010, Pages 1553–1559, doi:10.1016/j.ejc.2009.07.009
- [HZ1999] C. Holton, L. Q. Zamboni, *Descendants of primitive substitutions*, Theory Comput. Syst. 32 (1999) 133–157.
- [IEEEP1363] IEEE P1363 / D13 (Draft Version 13). Standard Specifications for Public Key Cryptography Annex A (Informative). Number-Theoretic Background. Section A.2.4
- [IJ1960] Igusa, Jun-ichi. *Arithmetic variety of moduli for genus two*. Ann. of Math. (2) 72 1960 612–649.
- [II1983] M. Imase and M. Itoh. “A design for directed graphs with minimum diameter”, *IEEE Trans. Comput.*, vol. C-32, pp. 782–784, 1983.
- [IK2010] Kenji Iohara and Yoshiyuki Koga. *Representation Theory of the Virasoro Algebra*. Springer, (2010).
- [IK2003] Yury Ionin and Hadi Kharaghani. *New families of strongly regular graphs*. Journal of Combinatorial Designs, 11(3):208–217, 2003. doi:10.1002/jcd.10038
- [IKMP2019A] T. Iwata, M. Khairallah, K. Minematsu, T. Peyrin “Remus v1.0” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Remus-spec.pdf>
- [IKMP2019B] T. Iwata, M. Khairallah, K. Minematsu, T. Peyrin “Romulus v1.0” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Romulus-spec.pdf>
- [IKMPSSS2019] T. Iwata, M. Khairallah, K. Minematsu, T. Peyrin, Y. Sasaki, S. M. Sim, L. Sun “Thank Goodness It’s Friday(TGIF)” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/TGIF-spec.pdf>
- [ILS2012] Giuseppe F. Italiano, Luigi Laura, and Federico Santaroni. *Finding strong bridges and strong articulation points in linear time*. Theoretical Computer Science, 447, 74–84 (2012). doi:10.1016/j.tcs.2011.11.011
- [ILZ2018] K. Iohara, G. Lehrer, and R. Zhang. *Schur-Weyl duality for certain infinite dimensional  $U_q(\mathfrak{sl}_2)$ -modules*. Preprint, arXiv 1811.01325 (2018).
- [IR1990] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, GTM volume 84, 1990.

- [IS2005] Alfredo Iusem and Alberto Seeger. On pairs of vectors achieving the maximal angle of a convex cone. *Mathematical Programming*, 104(2-3):501-523, 2005. doi:10.1007/s10107-005-0626-z.
- [ISSK2009] M. Izadi, B. Sadeghiyan, S. S. Sadeghian, H. A. Khanooki, *MIBS: A new lightweight block cipher*; in CANS, (2009), pp. 334-348.
- [Ive2012] S. Iveson, *Tableaux on  $k + 1$ -cores, reduced words for affine permutations, and  $k$ -Schur expansions*, Operators on  $k$ -tableaux and the  $k$ -Littlewood-Richardson rule for a special case, UC Berkeley: Mathematics, Ph.D. Thesis, <https://escholarship.org/uc/item/7pd1v1b5>
- [Iwa1964] N. Iwahori, On the structure of a Hecke ring of a Chevalley group over a finite field, *J. Fac. Sci. Univ. Tokyo Sect. I*, 10 (1964), 215–236 (1964). MathSciNet MR0165016
- [Iwa1972] K. Iwasawa, *Lectures on  $p$ -adic  $L$ -functions*, Princeton University Press, 1972.
- [Ja1971] N. Jacobson. *Exceptional Lie Algebras*. Marcel Dekker, Inc. New York. 1971. IBSN No. 0-8247-1326-5.
- [Jet2008] D. Jetchev. Global divisibility of Heegner points and Tamagawa numbers. *Compos. Math.* 144 (2008), no. 4, 811–826.
- [Jeong2017] Juyoung Jeong. Spectral sets and functions on Euclidean Jordan algebras. University of Maryland, Baltimore County, Ph.D. thesis, 2017.
- [JK1981] Gordon James, Adalbert Kerber, *The Representation Theory of the Symmetric Group*, Encyclopedia of Mathematics and its Applications, vol. 16, Addison-Wesley 1981.
- [JK2002] Zvonimir Janko and Hadi Kharaghani. *A Block Negacyclic Bush-Type Hadamard Matrix and Two Strongly Regular Graphs*. *J. Combin. Theory Ser. A* 98 (2002), no. 1, 118–126. doi:10.1006/jcta.2001.3231
- [JK2003] L. K. Jørgensen, M. Klin, M., *Switching of edges in strongly regular graphs. I. A family of partial difference sets on 100 vertices*, *Electronic Journal of Combinatorics* 10(1), 2003.
- [JKT2001] Zvonimir Janko, Hadi Kharaghani, and Vladimir D. Tonchev. *The existence of a Bush-type Hadamard matrix of order 324 and two new infinite classes of symmetric designs*. *Des. Codes Cryptogr.* 24(2):225–232, 2001. doi:10.1023/A:1011212922844
- [JL2009] Nicolas Jacon and Cedric Lecouvey. *Kashiwara and Zelevinsky involutions in affine type A*. *Pac. J. Math.* 243(2):287–311 (2009).
- [JL2016] M. Jones and L. Lapointe. *Pieri rules for Schur functions in superspace*. Preprint, arXiv 1608.08577
- [JMP2009] Michael Joswig, Benjamin Müller, and Andreas Paffenholz, polymake and lattice polytopes, 21st International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2009), Discrete Math. Theor. Comput. Sci. Proc., AK, Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2009, pp. 491–502
- [JNC2010] David Joyner, Minh Van Nguyen, and Nathann Cohen. *Algorithmic Graph Theory*. 2010, <http://code.google.com/p/graph-theory-algorithms-book/>
- [JNSV2016] Claude-Pierre Jeannerod, Vincent Neiger, Eric Schost, and Gilles Villard. Fast Computation of Minimal Interpolation Bases in Popov Form for Arbitrary Shifts. In *Proceedings ISSAC 2016* (pages 295-302). doi:10.1145/2930889.2930928
- [Joh1990] D.L. Johnson. *Presentations of Groups*. Cambridge University Press. (1990).
- [Joh1999] Anna M. Johnston. A generalized  $q$ th root algorithm. *Proceedings of the tenth annual ACM-SIAM symposium on Discrete algorithms*. Baltimore, 1999: pp. 929-930.
- [Jon1987] V. Jones, Hecke algebra representations of braid groups and link polynomials. *Ann. of Math.* (2) 126 (1987), no. 2, 335–388. doi:10.2307/1971403 MathSciNet MR0908150
- [Jon2005] V. Jones, The Jones Polynomial, 2005. <https://math.berkeley.edu/~vfr/jones.pdf>

- [JPD2018] Átila A. Jones, Fábio Protti and Renata R. Del-Vecchio: *Cograph generation with linear delay*. Theoretical Computer Science, 713:1-10, 2018. doi:10.1016/j.tcs.2017.12.037
- [JRJ94] Jourdan, Guy-Vincent; Rampon, Jean-Xavier; Jard, Claude (1994), “Computing on-line the lattice of maximal antichains of posets”, Order 11 (3) p. 197-210, doi:10.1007/BF02115811
- [Joy2004] D. Joyner, Toric codes over finite fields, Applicable Algebra in Engineering, Communication and Computing, 15, (2004), p. 63-79.
- [Joy2006] D. Joyner, *On quadratic residue codes and hyperelliptic curves*, (preprint 2006)
- [JP2002] J. Justin, G. Pirillo, Episturmian words and episturmian morphisms, Theoret. Comput. Sci. 276 (2002) 281–313.
- [JPdA15] N. Jacon and L. Poulain d’Andecy. *An isomorphism theorem for Yokonuma-Hecke algebras and applications to link invariants*. (2015) arXiv 1501.06389v3.
- [IS2006] Y.J. Ionin, S. Shrikhande, *Combinatorics of symmetric designs*. Cambridge University Press, 2006.
- [JS2000] A. Joellenbeck, M. Schocker. “Cyclic Characters of Symmetric Groups”. J. Algebraic Combin., **12** (2000), 155-161. doi:10.1023/A:1026592027019.
- [JS2010] B. Jones, A. Schilling. “Affine structures and a tableau model for  $E_6$  crystals”, J. Algebra. **324** (2010). 2512-2542. doi:10.1016/j.bbr.2011.03.031, arXiv 0909.2442.
- [JS2021] D. Jahn, C. Stump. *Bruhat intervals, subword complexes and brick polyhedra for finite Coxeter groups*, 2021, arXiv 2103.03715.
- [JV2000] J. Justin, L. Vuillon, *Return words in Sturmian and episturmian words*, Theor. Inform. Appl. 34 (2000) 343–356.
- [Ka1990] Victor G. Kac. *Infinite-dimensional Lie Algebras*. Third edition. Cambridge University Press, Cambridge, 1990.
- [Kac1997] V. Kac, “Vertex algebras for beginners”. Second Edition. vol 10. university lecture series. AMS, Cambridge, 1997.
- [Kal1992] B. Kaliski, *The MD2 message-digest algorithm*; in RFS 1319, (1992).
- [Ka1993] Masaki Kashiwara, The crystal base and Littelmann’s refined Demazure character formula, Duke Math. J. 71 (1993), no. 3, 839–858.
- [Ka2003] M. Kashiwara. Realizations of Crystals. Combinatorial and geometric representation theory (Seoul, 2001), Contemp. Math. **325**, Amer. Math. Soc., pp. 133–139, 2003.
- [Kai1980] Thomas Kailath. “Linear Systems”, Prentice-Hall, 1980.
- [Kai2012] Thomas Kaiser, *A short proof of the tree-packing theorem*, J. Discrete Math. 312(10): 1689-1691, 2012. doi:10.1016/j.disc.2012.01.020, arXiv 0911.2809.
- [Kal1980] T. Kailath, “Linear Systems”, Prentice-Hall, 1980, 383–386.
- [Kam2007] Joel Kamnitzer, *The crystal structure on the set of Mirković-Vilonen polytopes*, Adv. Math. **215** (2007), 66-93.
- [Kam2010] Joel Kamnitzer, *Mirković-Vilonen cycles and polytopes*, Ann. Math. (2) **171** (2010), 731-777.
- [Kan1958] D. M. Kan, *A combinatorial definition of homotopy groups*, Ann. Math. (2) 67 (1958), 282-312.
- [Kar1993] Vahid Karimipour. *Representations of the coordinate ring of  $GL_q(n)$* . (1993). arXiv hep-th/9306058.
- [Kas1971] T. Kasami: *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes*. Information and Control, 18, pp. 369-394, 1971.
- [Kas1966a] T. Kasami: *Weight Distributions of Bose-Chaudhuri-Hocquenghem Codes*. Coordinated Science Laboratory, University of Illinois at Urbana-Champaign. 1966 <http://hdl.handle.net/2142/74459>

- [Kas1966b] T. Kasami: *Weight Distribution Formula for Some Class of Cyclic Codes*. Coordinated Science Laboratory, University of Illinois at Urbana-Champaign. 1966
- [Kas2018] András Kaszanyitzky. *The GraftalLace Cellular Automata*. Preprint, [arXiv 1805.11532](#).
- [Kat1991] Nicholas M. Katz, *Exponential sums and differential equations*, Princeton University Press, Princeton NJ, 1991.
- [Kat2004] Kayuza Kato, *p*-adic Hodge theory and values of zeta functions of modular forms, *Cohomologies p*-adiques et applications arithmétiques III, *Astérisque* vol 295, SMF, Paris, 2004.
- [Kau1968] W. H. Kautz. “Bounds on directed (d, k) graphs”. *Theory of cellular logic networks and machines*, AFCRL-68-0668, SRI Project 7258, Final Rep., pp. 20-28, 1968.
- [Kau1991] Louis Kauffman. *Knots and Physics*, World Scientific, 1991 [doi:10.1142/4256](#).
- [Kaw2009] Kawahira, Tomoki. *An algorithm to draw external rays of the Mandelbrot set*, Nagoya University, 23 Apr. 2009. [math.titech.ac.jp/~kawahira/programs/mandel-exray.pdf](#)
- [Kir2016] M. Kirschmer, *Definite quadratic and hermitian forms with small class number*, Habilitationsschrift, RWTH Aachen University, 2016. [http://www.math.rwth-aachen.de/~Markus.Kirschmer/papers/herm.pdf](#)
- [KV2010] M. Kirschmer, J. Voight: *Algorithmic enumeration of ideal classes for quaternion orders*. *SIAM J. Comput.* 39(5): 1714-1747 (2010) [https://math.dartmouth.edu/~jvoight/articles/73446.pdf](#)
- [KB1983] W. Kühnel and T. F. Banchoff, “The 9-vertex complex projective plane”, *Math. Intelligencer* 5 (1983), no. 3, 11-22.
- [KB1995] A. N. Kirillov, A. D. Berenstein, *Groups generated by involutions, Gelfand–Tsetlin patterns, and combinatorics of Young tableaux*, *Algebra i Analiz*, 1995, Volume 7, Issue 1, pp. 92–152. [http://math.uoregon.edu/~arkadiy/bk1.pdf](#)
- [Ke1991] A. Kerber. *Algebraic combinatorics via finite group actions*, 2.2 p. 70. BI-Wissenschaftsverlag, Mannheim, 1991.
- [Ke2008] B. Keller, *Cluster algebras, quiver representations and triangulated categories*, [arXiv 0807.1960](#).
- [Ked2001] Kedlaya, K., *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, *J. Ramanujan Math. Soc.* 16 (2001) no 4, 323-338
- [KeSm1998] S. Keller and M. Smid, *Modes of Operation Validation System (MOVS): Requirements and Procedures* NIST Special Publication 800-17, 1998 [doi:10.6028/NIST.SP.800-17](#)
- [KG2016] P. Karpmann and Benjamin Gregoire, *The LITTLUN S-box and the FLY block cipher*, *Lightweight Cryptography Workshop*, 2016. [https://www.nist.gov/sites/default/files/documents/2016/10/18/karpman-paper-lwc2016.pdf](#)
- [Khu2004] K. Khuri-Makdisi. *Linear algebra algorithms for divisors on an algebraic curve*, *Mathematics of Computation* 73, no. 245 (2004) pp. 333-357.
- [Kin1992] Nancy G. Kinnarsley, *The vertex separation number of a graph equals its path-width*, *Information Processing Letters* 42(6):345-350, 1992. [doi:10.1016/0020-0190\(92\)90234-M](#).
- [KK1995] Victor Klee and Peter Kleinschmidt, *Convex polytopes and related complexes.*, in R. L. Graham, M. Grötschel, L Lovász, *Handbook of combinatorics*, Vol. 1, Chapter 18, 1995
- [KKMMNN1992] S-J. Kang, M. Kashiwara, K. C. Misra, T. Miwa, T. Nakashima, and A. Nakayashiki. *Affine crystals and vertex models*. *Int. J. Mod. Phys. A*, 7 (suppl. 1A), (1992) pp. 449-484.
- [KKPSSSYLLCHH2004] D. Kwon, J. Kim, S. Park, S. H. Sung, Y. Sohn, J. H. Song, Y. Yeom, E-J. Yoon, S. Lee, J. Lee, S. Chee, D. Han, and J. Hong, *New block cipher: ARIA*; in *ICISC*, (2004), pp. 432-445.

- [KKS2007] S.-J. Kang, J.-A. Kim, and D.-U. Shin. Modified Nakajima Monomials and the Crystal  $B(\infty)$ . *J. Algebra* **308**, pp. 524–535, 2007.
- [KL1979] D. Kazhdan and G. Lusztig. *Representations of Coxeter groups and Hecke algebras*. *Invent. Math.* **53** (1979), no. 2, 165–184. doi:10.1007/BF01390031 MathSciNet MR0560412
- [KL1990] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*. Cambridge University Press, 1990.
- [KL2008] Chris Kurth and Ling Long, “Computations with finite index subgroups of  $\mathrm{PSL}_2(\mathbf{Z})$  using Farey symbols”, *Advances in algebra and combinatorics*, 225–242, World Sci. Publ., Hackensack, NJ, 2008. Preprint version: arXiv 0710.1835
- [Kle1995] A. Kleshchev. *Branching rules for modular representations of symmetric groups. I*. *J. Algebra* **178** (1995), 493–511.
- [Kle1996] A. Kleshchev, *Branching rules for modular representations of symmetric groups III: Some corollaries and a problem of Mullineux*, *J. London Math. Soc.* **54** (1996) 25–38. MathSciNet MR1395065
- [Kle2009] A. Kleshchev. *Representation theory of symmetric groups and related Hecke algebras*. *Bull. Amer. Math. Soc.* **47** (2010), 419–481. arXiv 0909.4844.
- [KLLRSY2014] E. B. Kavun, M. M. Lauridsen, G. Leander, C. Rechberger, P. Schwabe, and T. Yalcin, *Prost v1*; CAESAR Competition, (2014).
- [KLPR2010] L. R. Knudsen, G. Leander, A. Poschmann, and M. J. B. Robshaw, *PRINTcipher: A block cipher for IC-printing*; in CHES, (2010), pp. 16-32.
- [KLRS2016] S.-J. Kang, K.-H. Lee, H. Ryu, and B. Salisbury. *A combinatorial description of the affine Gindikin-Karpelevich formula of type  $A_n^{(1)}$* . *Lie Algebras, Lie Superalgebras, Vertex Algebras and Related Topics*, *Proc. Sympos. Pure Math.*, vol. 92, Amer. Math. Soc., Providence, RI, 2016, pp. 145–165.
- [KLS2013] Allen Knutson, Thomas Lam, and David Speyer. *Positroid Varieties: Juggling and Geometry* *Compositio Mathematica*, **149** (2013), no. 10. arXiv 1111.3660.
- [Kly1990] Klyachko, Aleksandr Anatolevich. *Equivariant Bundles on Toral Varieties*, *Math USSR Izv.* **35** (1990), 337-375. [http://iopscience.iop.org/0025-5726/35/2/A04/pdf/0025-5726\\_35\\_2\\_A04.pdf](http://iopscience.iop.org/0025-5726/35/2/A04/pdf/0025-5726_35_2_A04.pdf)
- [KM1994] S.-J. Kang and K. C. Misra. *Crystal bases and tensor product decompositions of  $U_q(G_2)$ -modules*. *J. Algebra* **163**, pp. 675–691, 1994.
- [KM1997] Sandi Klavžar and Uroš Milutinović. *Graphs  $S(n,k)$  and a variant of the Tower of Hanoi problem*, *Czechoslovak Mathematical Journal*, 47:95-104, 1997. doi:10.1023/A:1022444205860
- [KMAUTOM2000] Masayuki Kanda, Shiho Moriai, Kazumaro Aoki, Hiroki Ueda, Youichi Takashima, Kazuo Ohta, and Tsutomu Matsumoto, *E2 - a new 128-bit block cipher*; in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E83-A(1):48–59, 12 2000.
- [KMM2004] Tomasz Kaczynski, Konstantin Mischaikow, and Marian Mrozek, “Computational Homology”, Springer-Verlag (2004).
- [KMN2012] On the trace of the antipode and higher indicators. Yevgenia Kashina and Susan Montgomery and Richard Ng. *Israel J. Math.*, v.188, 2012.
- [KMOY2007] M. Kashiwara, K. C. Misra, M. Okado, D. Yamada. *Perfect crystals for  $U_q(D_4^{(3)})$* , *J. Algebra*. **317** (2007).
- [Klaise2012] Janis Klaise. *Orders in imaginary quadratic fields of small class number* University of Warwick Undergraduate Masters thesis, unpublished (2012). [https://warwick.ac.uk/fac/cross\\_fac/complexity/people/students/dtc/students2013/klaise/janis\\_klaise\\_ug\\_report.pdf](https://warwick.ac.uk/fac/cross_fac/complexity/people/students/dtc/students2013/klaise/janis_klaise_ug_report.pdf)
- [KMR2012] A. Kleshchev, A. Mathas, and A. Ram, *Universal Specht modules for cyclotomic Hecke algebras*, *Proc. London Math. Soc.* (2012) **105** (6): 1245-1289. arXiv 1102.3519v1

- [KN1963] S. Kobayashi & K. Nomizu : *Foundations of Differential Geometry*, vol. 1, Interscience Publishers (New York) (1963).
- [KN1994] M. Kashiwara and T. Nakashima. Crystal graphs for representations of the  $q$ -analogue of classical Lie algebras. *J. Algebra* **165**, no. 2, pp. 295–345, 1994.
- [KNS2011] Atsuo Kuniba and Tomoki Nakanishi and Junji Suzuki, *T-systems and Y-systems in integrable systems*. *J. Phys. A*, **44** (2011), no. 10.
- [KnotAtlas] The Knot atlas. [http://katlas.org/wiki/Main\\_Page](http://katlas.org/wiki/Main_Page)
- [Knu1995] Donald E. Knuth, *Overlapping Pfaffians*, [arXiv math/9503234v1](https://arxiv.org/abs/math/9503234v1).
- [Knu1998] Donald E. Knuth *The Art of Computer Programming. Volume 2*
- [Knu2011] Donald E. Knuth, *The Art of Computer Programming. Volume 4A. Combinatorial Algorithms, Part 1*.
- [Knu2005] Lars R. Knudsen, *SMASH - A Cryptographic Hash Function*; in FSE'05, (2005), pp. 228-242.
- [KO2000] Yuji Kobayashi and Friedrich Otto, *Repetitiveness of languages generated by morphisms*. *Theoret. Comp. Sci.* 240 (2000) 337–378. doi:10.1016/S0304-3975(99)00238-8
- [Kob1993] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*. Springer GTM 97, 1993.
- [Koe1999] Wolfram Koepf: Efficient Computation of Chebyshev Polynomials in Computer Algebra Systems: A Practical Guide. John Wiley, Chichester (1999): 79-99.
- [Koh1996] Kohel, “Endomorphism Rings of Elliptic Curves over Finite Fields”, UC Berkeley PhD thesis 1996.
- [Koh2000] David Kohel, *Hecke Module Structure of Quaternions*, in *Class Field Theory — Its Centenary and Prospect* (Tokyo, 1998), *Advanced Studies in Pure Mathematics*, 30, 177-196, 2000.
- [Koh2004] E. Kohler. *Recognizing graphs without asteroidal triples*. *Journal of Discrete Algorithms* 2(4):439-452, Dec. 2004, doi:10.1016/j.jda.2004.04.005.
- [KohECHIDNA] Kohel, David. ECHIDNA: Databases for Elliptic Curves and Higher Dimensional Analogues. Available at <http://echidna.maths.usyd.edu.au/~kohel/dbs/>
- [Koh2007] A. Kohnert, *Constructing two-weight codes with prescribed groups of automorphisms*, *Discrete applied mathematics* 155, no. 11 (2007): 1451-1457. <http://linearcodes.uni-bayreuth.de/twoweight/>
- [Kol1991] V. A. Kolyvagin. On the structure of Shafarevich-Tate groups. *Algebraic geometry*, 94–121, *Lecture Notes in Math.*, 1479, Springer, Berlin, 1991.
- [Kos1985] J.-L. Koszul, *Crochet de Schouten-Nijenhuis et cohomologie*, in *Élie Cartan et les mathématiques d'aujourd'hui*, *Astérisque hors série* (1985), p. 257
- [KoSt08] C. Koukouvinos, S. Stylianou, *On skew-Hadamard matrices*, *Discrete Math.* **308** (2008) 2723-2731
- [KP2002] Volker Kaibel and Marc E. Pfetsch, “Computing the Face Lattice of a Polytope from its Vertex-Facet Incidences”, *Computational Geometry: Theory and Applications*, Volume 23, Issue 3 (November 2002), 281-290. Available at <http://portal.acm.org/citation.cfm?id=763203> and free of charge at [arXiv math/0106043](https://arxiv.org/abs/math/0106043)
- [KP2002b] James Kuzmanovich; Andrey Pavlichenkov, *Finite Groups of Matrices Whose Entries Are Integers*, *The American Mathematical Monthly*, Vol. 109, No. 2. (2002) pp. 173-186
- [KP2011] Manuel Kauers and Peter Paule. *The Concrete Tetrahedron*. Springer-Verlag, 2011.
- [KP2020] Lars Kastner and Marta Panizzut, *Hyperplane arrangements in polymake*, [arXiv 2003.13548](https://arxiv.org/abs/2003.13548).
- [KPRWZ2010] M. H. Klin, C. Pech, S. Reichard, A. Woldar, M. Zvi-Av, *Examples of computer experimentation in algebraic combinatorics*, *ARS MATHEMATICA CONTEMPORANEA* 3 (2010) 237–258. doi:10.26493/1855-3974.119.60b. <http://amc-journal.eu/index.php/amc/article/viewFile/119/118>

- [Kra1999] C. Krattenthaler, *Another Involution Principle-Free Bijective Proof of Stanley's Hook Content Formula*, Journal of Combinatorial Theory, Series A, **88** (1999), 66-92, <http://www.sciencedirect.com/science/article/pii/S0012365X9290368P>
- [Kra1999det] C. Krattenthaler, *Advanced determinant calculus*, Sémin. Lothar. Combin. **42** (1999), Art. B42q, 67pp.
- [Kra2006] Christian Krattenthaler, *Growth diagrams, and increasing and decreasing chains in fillings of Ferrers shapes*. Advances in Applied Mathematics Volume 37, Number 3 (2006), pp. 404-431.
- [Kr1971] D. Kraines, "On excess in the Milnor basis," Bull. London Math. Soc. **3** (1971), 363-365.
- [Kr2016] Stefan Kranich, An epsilon-delta bound for plane algebraic curves and its use for certified homotopy continuation of systems of plane algebraic curves, [arXiv 1505.03432](https://arxiv.org/abs/1505.03432)
- [Krumm2016] Daid Krumm, *Computing Points of Bounded Height in Projective Space over a Number Field*, MATHEMATICS OF COMPUTATION, Volume 85, Number 297, January 2016, Pages 423-447. <http://dx.doi.org/10.1090/mcom/2984>
- [KR2001] J. Kahane and A. Ryba. *The hexad game*, Electronic Journal of Combinatorics, **8** (2001). [http://www.combinatorics.org/Volume\\_8/Abstracts/v8i2r11.html](http://www.combinatorics.org/Volume_8/Abstracts/v8i2r11.html)
- [KR2001b] P.L. Krapivsky and S. Redner. "Organization of Growing Random Networks", Phys. Rev. E vol. 63 (2001), p. 066123.
- [KR2005] P.L. Krapivsky and S. Redner. "Network Growth by Copying", Phys. Rev. E vol. 71 (2005), p. 036118.
- [Kra1989] Kraus, Alain, Quelques remarques à propos des invariants  $(c_4)$ ,  $(c_6)$  et  $(\Delta)$  d'une courbe elliptique, Acta Arith. **54** (1989), 75-80.
- [Kre2002] V. Krops. *Social Network Analysis* (2002). [Online] Available: <http://www.orgnet.com/sna.html>
- [KRG1996] S. Klavzar, A. Rajapakse, and I. Gutman. *The Szeged and the Wiener index of graphs*. Applied Mathematics Letters, **9**(5):45-49, 1996. doi:10.1016/0893-9659(96)00071-7.
- [KS] Sheldon Katz and Stein Arild Stromme, "Schubert", A Maple package for intersection theory and enumerative geometry.
- [KS1998] Maximilian Kreuzer and Harald Skarke, *Classification of Reflexive Polyhedra in Three Dimensions*, [arXiv hep-th/9805190](https://arxiv.org/abs/hep-th/9805190)
- [KS2002] A. Khare and U. Sukhatme. "Cyclic Identities Involving Jacobi Elliptic Functions", preprint 2002. [arXiv math-ph/0201004](https://arxiv.org/abs/math-ph/0201004)
- [KS2006] Atsuo Kuniba and Reiho Sakamoto, *The Bethe ansatz in a periodic box-ball system and the ultradiscrete Riemann theta function*, J. Stat. Mech., P09005 (2006).
- [KS2010] J.-A. Kim and D.-U. Shin. *Generalized Young walls and crystal bases for quantum affine algebra of type A*. Proc. Amer. Math. Soc. **138** (2010), no. 11, 3877-3889.
- [KS2012] Jerome Kelleher, Barry O'Sullivan, *Generating all partitions: A Comparison of encodings*, Journal of Mathematical Modelling and Algorithms, **11**:89-104, 2012. doi:10.1007/s10852-011-9168-y [arXiv 0909.2331](https://arxiv.org/abs/0909.2331)
- [KS2015] Karel Klouda and Štěpán Starosta, *An Algorithm Enumerating All Infinite Repetitions in a DOL System*. Journal of Discrete Algorithms, **33** (2015), 130-138. doi:10.1016/j.jda.2015.03.006
- [KS2019] J. Kliem and C. Stump. *A face iterator for polyhedra and more general finite locally branched lattices*. Preprint (2019): [arXiv 1905.01945](https://arxiv.org/abs/1905.01945).
- [KSV2011] Ian Kiming, Matthias Schuett and Helena Verrill, "Lifts of projective congruence groups", J. London Math. Soc. (2011) **83** (1): 96-120, doi:10.1112/jlms/jdq062, [arXiv 0905.4798](https://arxiv.org/abs/0905.4798).
- [KT1986] N. Kerzman and M. R. Trummer. "Numerical Conformal Mapping via the Szego kernel". Journal of Computational and Applied Mathematics, **14**(1-2): 111-123, 1986.

- [KT2013] K. Tsukazaki, Explicit Isogenies of Elliptic Curves, PhD thesis, University of Warwick, 2013.
- [KTR2005] H. Kharaghani and B. Tayfeh-Rezaie. *A Hadamard matrix of order 428*, Journal of Combinatorial Designs 13(6) (2005): 435-440. doi:10.1002/jcd.20043
- [KTT2006] A. Kuniba, T. Takagi, and A. Takenouchi, *Bethe ansatz and inverse scattering transform in a periodic box-ball system*, Nuclear Phys. B **747**, no. 3 (2006), 354–397.
- [KTZ1987] Kierstead, H.A., Trotter, W.T. & Zhou, B. Representing an ordered set as the intersection of super greedy linear extensions. Order 4, 293-311 (1987). doi:10.1007/BF00337892
- [Kuh1987] W. Kühnel, “Minimal triangulations of Kummer varieties”, Abh. Math. Sem. Univ. Hamburg 57 (1987), 7-20.
- [Kuh1995] Kühnel, “Tight Polyhedral Submanifolds and Tight Triangulations” Lecture Notes in Mathematics Volume 1612, 1995
- [Kul1991] Ravi Kulkarni, “An arithmetic geometric method in the study of the subgroups of the modular group”, American Journal of Mathematics 113 (1991), no 6, 1053-1133
- [Kuniba2022] Atsuo Kuniba, *Quantum Groups in Three-Dimensional Integrability*. Theoretical and Mathematical Physics, Springer. 2022. doi:10.1007/978-981-19-3262-5.
- [Kur2008] Chris Kurth, “K Farey package for Sage”, <http://wayback.archive-it.org/855/20100510123900/http://www.public.iastate.edu/~kurthc/research/index.html>
- [KV2003] Kim, Jeong Han and Vu, Van H. *Generating random regular graphs*. Proc. 35th ACM Symp. on Thy. of Comp. 2003, pp 213-222. ACM Press, San Diego, CA, USA. doi:10.1145/780542.780576.
- [Kwon2012] Jae-Hoon Kwon. *Crystal bases of  $q$ -deformed Kac Modules over the Quantum Superalgebra  $U_q(\mathfrak{gl}(m|n))$* . International Mathematics Research Notices. Vol. 2014, No. 2, pp. 512-550 (2012)
- [Kwon2014] Jae-Hoon Kwon.  *$q$ -deformed Clifford algebra and level zero fundamental representations of quantum affine algebras*. J. Algebra, **399** (2014), pp. 927–947. doi:10.1016/j.jalgebra.2013.10.026.
- [KX1998] S. König and C. Xi. *On the structure of cellular algebras*. Algebras and modules, II (Geiranger, 1996), 365–386, CMS Conf. Proc., **24**, Amer. Math. Soc., Providence, RI, 1998. MathSciNet MR1648638
- [KY2019] Jang Soo Kim, Meesue Yoo. *Hook length property of  $d$ -complete posets via  $q$ -integrals*. J. Combin. Theory Ser. A, **162** (2019), pp. 167-221.
- [Lab2008] S. Labbé, *Propriétés combinatoires des  $f$ -palindromes*, Mémoire de maîtrise en Mathématiques, Montréal, UQAM, 2008, 109 pages.
- [Labelle2008] G. Labelle. *New combinatorial computational methods arising from pseudo-singletons*. DMTCS Proceedings 1, 2008.
- [Lak2010] Dan Laksov. *Splitting algebras and Gysin homomorphisms*. Journal of Commutative Algebra, Volume 2, Number 3, Fall 2010
- [Lam1996] T. K. Lam. *B and D analogues of stable Schubert polynomials and related insertion algorithms*. PhD Thesis, MIT, 1996.
- [Lam2004] Thomas Lam, *Growth diagrams, domino insertion and sign-imbalance*. Journal of Combinatorial Theory, Series A Volume 107, Number 1 (2004), pp. 87-115.
- [Lam2005] T. Lam, *Affine Stanley symmetric functions*, Amer. J. Math. 128 (2006), no. 6, 1553–1586.
- [Lam2008] T. Lam. *Schubert polynomials for the affine Grassmannian*. J. Amer. Math. Soc., 2008.
- [Lan2002] S. Lang : *Algebra*, 3rd ed., Springer (New York) (2002); doi:10.1007/978-1-4613-0041-0
- [Lasc] A. Lascoux. *Chern and Yang through ice*. Preprint.

- [Lau2011] Alan G.B. Lauder, *Computations with classical and  $p$ -adic modular forms*, LMS J. of Comput. Math. 14 (2011), 214-231.
- [Laz1992] Daniel Lazard, *Solving Zero-dimensional Algebraic Systems*, in Journal of Symbolic Computation (1992) vol. 13, pp. 117-131
- [Laz2004] Robert Lazarsfeld: Positivity in algebraic geometry II; Positivity for Vector Bundles, and Multiplier Ideals, Modern Surveys in Mathematics volume 49 (2004).
- [LB1962] C. G. Lekkerkerker, J. Ch. Boland. *Representation of a finite graph by a set of intervals on the real line*. Fundamenta Mathematicae, 51:45-64, 1962; doi:10.4064/fm-51-1-45-64.
- [LBO2014] Kwankyu Lee, Maria Bras-Amorós, and Michael E. O'Sullivan, *Unique decoding of general AG codes*, IEEE Transactions on Information Theory, vol 60, no. 4 (2014), pp. 2038–2053.
- [LB1988] Lee, P.J., Brickell, E.F. An observation on the security of McEliece's public-key cryptosystem. Euro-Crypt 1988. LNCS, vol. 330, pp. 275–280.
- [LdB1982] A. Liberato de Brito, 'FORTRAN program for the integral of three spherical harmonics', Comput. Phys. Commun., Volume 25, pp. 81-85 (1982)
- [LD2021] David Lowry-Duda. *Visualizing modular forms*. Arithmetic Geometry, Number Theory, and Computation. Simons Symposia, Springer, 2021. arXiv 2002.05234
- [Led1965] Joshua Lederberg. *DENDRAL-64: A System for Computer Construction, Enumeration and Notation of Organic Molecules as Tree Structures and Cyclic Graphs. Part II. Topology of Cyclic Graphs*. Interim Report to the National Aeronautics and Space Administration. Grant NsG 81-60. December 15, 1965. <https://ntrs.nasa.gov/api/citations/19660004785/downloads/19660004785.pdf>
- [Lee2016] Kwankyu Lee, *Decoding of differential AG codes*, Advances in Mathematics of Communications, vol. 10, no. 2 (2016), pp. 307–319.
- [Lee1996] Marc van Leeuwen. *The Robinson-Schensted and Sch'utzenberger algorithms, an elementary approach*. Electronic Journal of Combinatorics 3, no. 2 (1996): Research Paper 15, approx. 32 pp. (electronic)
- [Lee1997] J. M. Lee, *Riemannian Manifolds*, Springer (New York) (1997); doi:10.1007/b98852
- [Lee2011] J. M. Lee, *Introduction to Topological Manifolds*, 2nd ed., Springer (New York) (2011); doi:10.1007/978-1-4419-7940-7
- [Lee2013] J. M. Lee, *Introduction to Smooth Manifolds*, 2nd ed., Springer (New York) (2013); doi:10.1007/978-1-4419-9982-5
- [Lei2013] Tom Leinster, *The magnitude of metric spaces*. Doc. Math. 18 (2013), 857-905.
- [Ler2022] Antonin Leroux: *Quaternion algebras and isogeny-based cryptography*, PhD Thesis, 2022. [https://www.lix.polytechnique.fr/Labo/Antonin.LEROUX/manuscrit\\_these.pdf](https://www.lix.polytechnique.fr/Labo/Antonin.LEROUX/manuscrit_these.pdf)
- [Lev2014] Lionel Levine. *Threshold state and a conjecture of Poghosyan, Poghosyan, Priezzhev and Ruelle*, Communications in Mathematical Physics.
- [Lew2000] Robert Edward Lewand. *Cryptological Mathematics*. The Mathematical Association of America, 2000.
- [Li1995] Peter Littelmann, Crystal graphs and Young tableaux, J. Algebra 175 (1995), no. 1, 65–87.
- [Li1995b] P. Littelmann, Paths and root operators in representation theory. Ann. of Math. (2) 142 (1995), no. 3, 499-525.
- [Li2005] H. Li, *Abelianizing vertex algebras*. Comm. Math. Phys. vol. 259, no. 2, pp. 391–411 (2005)
- [Lic1977] A. Lichnerowicz, *Les variétés de Poisson et leurs algèbres de Lie associées*, Journal of Differential Geometry 12, 253 (1977); doi:10.4310/jdg/1214433987
- [Lic1997] William B. Raymond Lickorish. An Introduction to Knot Theory, volume 175 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1997. ISBN 0-387-98254-X

- [Lim] C. H. Lim, *CRYPTON: A New 128-bit Block Cipher*; available at <http://next.sejong.ac.kr/~chlim/pub/cryptonv05.ps>
- [Lim2001] C. H. Lim, *A Revised Version of CRYPTON: CRYPTON V1.0*; in FSE'01, pp. 31–45.
- [Lin1999] J. van Lint, *Introduction to coding theory*, 3rd ed., Springer-Verlag GTM, 86, 1999.
- [Liv1993] Charles Livingston, *Knot Theory*, Carus Mathematical Monographs, number 24.
- [Liv2006] M. Livernet, *A rigidity theorem for pre-Lie algebras*, J. Pure Appl. Algebra 207 (2006), no 1, pages 1-18. Preprint: [arXiv math/0504296v2](https://arxiv.org/abs/math/0504296v2).
- [LKOL2002] Hyeong-Ok Lee, Jong-Seok Kim, Eunseuk Oh and Hyeong-Seok Lim, *Hyper-Star Graph: A New Inter-connection Network Improving the Network Cost of the Hypercube*, Eurasian Conference on Information and Communication Technology, LNCS 2510, pp 858-865, 2002. doi:10.1007/3-540-36087-5\_99
- [LLM2003] A. Lascoux, L. Lapointe, and J. Morse. *Tableau atoms and a new Macdonald positivity conjecture*. Duke Math Journal, **116** (1), 2003. [arXiv math/0008073](https://arxiv.org/abs/math/0008073)
- [LLM2014] Lee, Li, Mills, A combinatorial formula for certain elements in the upper cluster algebra, [arXiv 1409.8177](https://arxiv.org/abs/1409.8177)
- [LLMS2006] T. Lam, L. Lapointe, J. Morse, M. Shimozono, *Affine insertion and Pieri rules for the affine Grassmannian*, Memoirs of the AMS, 208 (2010), no. 977, [arXiv math.CO/0609110](https://arxiv.org/abs/math.CO/0609110)
- [LLMS2013] Thomas Lam, Luc Lapointe, Jennifer Morse, and Mark Shimozono (2013). *The poset of k-shapes and branching rules for k-Schur functions* <<http://breakfreerun.org/index.php/ebooks/the-poset-of-k-shapes-and-branching-rules-for-k-schur-functions>>\_. Memoirs of the American Mathematical Society, 223(1050), 1-113. DOI: 10.1090/S0065-9266-2012-00655-1
- [LLMSSZ2013] Thomas Lam, Luc Lapointe, Jennifer Morse, Anne Schilling, Mark Shimozono and Mike Zabrocki. *k-Schur functions and affine Schubert calculus*, 2013. [arXiv 1301.3569](https://arxiv.org/abs/1301.3569).
- [LLT1996] Alain Lascoux, Bernard Leclerc, and Jean-Yves Thibon. *Hecke algebras at roots of unity and crystal bases of quantum affine algebras*. Comm. Math. Phys. **181** (1996), pp 205-263. [MathSciNet MR1410572](https://mathscinet.ams.org/mathscinet/item.aspx?infid=1410572)
- [LLT] A. Lascoux, B. Leclerc, and J.Y. Thibon. *The Plactic Monoid*. Survey article available at [<http://www-igm.univ-mlv.fr/~jyt/ARTICLES/plactic.ps>]
- [LLWC2011] Chien-Hung Lin, Jia-Jie Liu, Yue-Li Wang, William Chung-Kung Yen, *The Hub Number of Sierpinski-Like Graphs*, Theory Comput Syst (2011), vol 49, doi:10.1007/s00224-010-9286-3
- [LLYCL2005] H. J. Lee, S. J. Lee, J. H. Yoon, D. H. Cheon, and J. I. Lee, *The SEED Encryption Algorithm*; in RFC 4269, (2005).
- [LLZ2014] K. Lee, L. Li, and A. Zelevinsky, *Greedy elements in rank 2 cluster algebras*, Selecta Math. 20 (2014), 57-82.
- [LM2004] Lapointe, L. and Morse, J. 'Order Ideals in Weak Subposets of Young's Lattice and Associated Unimodality Conjectures'. Ann. Combin. (2004)
- [LM2006] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. ICALP, pp. 144–155, Springer, 2006.
- [LM2006b] L. Lapointe, J. Morse. Tableaux on  $k + 1$ -cores, reduced words for affine permutations, and  $k$ -Schur expansions. J. Combin. Theory Ser. A 112 (2005), no. 1, 44–81. MR2167475 (2006j:05214)
- [LM2011] A. Lauve, M. Mastnak. *The primitives and antipode in the Hopf algebra of symmetric functions in noncommuting variables*. Advances in Applied Mathematics. **47** (2011). 536-544. [arXiv 1006.0367v3](https://arxiv.org/abs/1006.0367v3) doi:10.1016/j.aam.2011.01.002.
- [LM2018] A. Lauve, M. Mastnak. *Bialgebra coverings and transfer of structure*. Preprint, [arXiv 1803.02691](https://arxiv.org/abs/1803.02691).
- [LMR2010] N. Linial, R. Meshulam and M. Rosenthal, "Sum complexes – a new family of hypertrees", Discrete & Computational Geometry, 2010, Volume 44, Number 3, Pages 622-636

- [LNSS2013] C. Lenart, S. Naito, D. Sagaki, A. Schilling, M. Shimozono, *A uniform model for Kirillov-Reshetikhin crystals. Extended abstract*. DMTCS proc, to appear ( [arXiv 1211.6019](#) )
- [Lod1995] Jean-Louis Loday. *Cup-product for Leibniz cohomology and dual Leibniz algebras*. Math. Scand., pp. 189–196 (1995). [http://www.math.uiuc.edu/K-theory/0015/cup\\_product.pdf](http://www.math.uiuc.edu/K-theory/0015/cup_product.pdf)
- [Loe2007] David Loeffler, *Spectral expansions of overconvergent modular functions*, Int. Math. Res. Not 2007 (050). [arXiv math/0701168](#).
- [Loksh2009] Daniel Lokshantov. *On the complexity of computing treelength*. Discrete Applied Mathematics. 158(7):820-827, 2009. doi:10.1016/j.dam.2009.10.007
- [Lom2019] Davide Lombardo, *Computing the geometric endomorphism ring of a genus 2 Jacobian*, Mathematics of Computation 88 (2019), 889-929. doi:10.1090/mcom/3358.
- [Lon2013] S. London, *Constructing New Turyn Type Sequences, T-Sequences and Hadamard Matrices*. PhD Thesis, University of Illinois at Chicago, 2013. <https://hdl.handle.net/10027/9916>
- [LOS2012] C. Lecouvey, M. Okado, M. Shimozono. “Affine crystals, one-dimensional sums and parabolic Lusztig  $q$ -analogues”. Mathematische Zeitschrift. **271** (2012). Issue 3-4. 819-865. doi:10.1007/s00209-011-0892-9, [arXiv 1002.3715](#).
- [Lot1983] M. Lothaire, *Combinatorics on Words*, vol. 17 of Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, Massachusetts (1983)
- [Lot1997] M. Lothaire, *Combinatorics on Words*, Cambridge University Press, (1997).
- [Lot2002] M. Lothaire, *Algebraic combinatorics on words*. Cambridge University Press (2002).
- [Lot2005] M. Lothaire, *Applied combinatorics on words*. Cambridge University Press (2005).
- [Lov1979] László Lovász, *On the Shannon capacity of a graph*, IEEE Trans. Inf. Th. 25(1979), 1-7. doi:10.1109/TIT.1979.1055985.
- [LP2007] G. Leander and A. Poschmann, *On the Classification of 4 Bit S-boxes*; in WAIFI, (2007), pp. 159-176.
- [LP2008] C. Lenart and A. Postnikov. *A combinatorial model for crystals of Kac-Moody algebras*. Trans. Amer. Math. Soc. 360 (2008), 4349-4381.
- [LP2011] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. in Proceeding of the 11th international conference on Topics in cryptology: CT-RSA 2011. Springer 2011, doi:10.1007/978-3-642-19074-2\_21
- [LPR2010] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On Ideal Lattices and Learning with Errors over Rings. in Advances in Cryptology – EUROCRYPT 2010. Springer 2010. doi:10.1007/978-3-642-13190-5\_1
- [LR1997] Robert Leduc and Arun Ram, A ribbon Hopf algebra approach to the irreducible representations of centralizer algebras: the Brauer, Birman-Wenzl, and type A Iwahori-Hecke algebras. Adv. Math. 125 (1997), no. 1, 1–94.
- [LR1998] Jean-Louis Loday and Maria O. Ronco. *Hopf algebra of the planar binary trees*, Advances in Mathematics, volume 139, issue 2, 10 November 1998, pp. 293-309. <http://www.sciencedirect.com/science/article/pii/S0001870898917595>
- [LR0102066] Jean-Louis Loday and Maria O. Ronco. Order structure on the algebra of permutations and of planar binary trees. [arXiv math/0102066v1](#).
- [LR2004] Dingjun Lou and Dongning Rao. *Characterizing factor critical graphs and an algorithm*, The Australasian Journal of Combinatorics, 30: 51–56, 2004. [http://ajc.maths.uq.edu.au/pdf/30/ajc\\_v30\\_p051.pdf](http://ajc.maths.uq.edu.au/pdf/30/ajc_v30_p051.pdf)
- [LRS2017] Julien Leroy, Michel Rigo, Manon Stipulanti, *Counting the number of non-zero coefficients in rows of generalized Pascal triangles*, Discrete Math. 340 (2017), no. 5, 862–881.

- [LS] A. Lum, W. Stein. Verification of the Birch and Swinnerton-Dyer Conjecture for Elliptic Curves with Complex Multiplication (unpublished)
- [LS1981] J. H. van Lint, and A. Schrijver, *Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields*, *Combinatorica*, 1(1), 1981, 63-73. doi:10.1007/BF02579178.
- [LS1986] G. I. Lehrer, L. Solomon, *On the action of the symmetric group on the cohomology of the complement of its reflecting hyperplanes*. *J. Algebra*, 104(2), 1986, 410-424. doi:10.1016/0021-8693(86)90225-5.
- [LS1990] A. Lascoux, M.-P. Schutzenberger. Keys and standard bases, invariant theory and tableaux. *IMA Volumes in Math and its Applications* (D. Stanton, ED.). Southend on Sea, UK, 19 (1990). 125-144.
- [LS1994] Eike Lau and Dierk Schleicher. *Internal addresses in the Mandelbrot set and irreducibility of polynomials*. Stony Brook Preprint #19 (1994). <https://www.math.stonybrook.edu/theses/thesis94-2/part1.pdf>
- [LS1998] Pierre Liardet, Pierre Stambul *Algebraic Computation with Continued Fractions*. *J. Number Th.* 73, 92-121, 1998.
- [LS2007] Thomas Lam and Mark Shimozono. *Dual graded graphs for Kac-Moody algebras*. *Algebra & Number Theory* 1.4 (2007) pp. 451-488.
- [LSS2009] T. Lam, A. Schilling, M. Shimozono. *Schubert polynomials for the affine Grassmannian of the symplectic group*. *Mathematische Zeitschrift* 264(4) (2010) 765-811 (arXiv 0710.2720)
- [LS2012] K.-H. Lee and B. Salisbury. Young tableaux, canonical bases, and the Gindikin-Karpelevich formula. arXiv 1205.6006.
- [LS2017] Xuan Liu and Travis Scrimshaw. *A uniform approach to soliton cellular automata using rigged configurations*. Preprint (2017) arXiv 1706.02443
- [LSW2012] Svante Linusson, John Shareshian and Michelle L. Wachs, *Rees products and lexicographic shellability*, *J. Comb.* 3 (2012), no. 3, 243-276.
- [LT1998] B. Leclerc, J.-Y. Thibon, Littlewood-Richardson coefficients and Kazhdan-Lusztig polynomials, <http://front.math.ucdavis.edu/9809.5122>
- [LT2009] G. I. Lehrer and D. E. Taylor. *Unitary reflection groups*. Australian Mathematical Society Lecture Series, 2009.
- [LT2012] Dan Laksov, Anders Thorup. *Splitting algebras and Schubert calculus*, *Indiana Univ. Math. J.* 61 (2012), 1253-1312 doi:10.1512/iumj.2012.61.4791
- [DeLuca2006] A. De Luca, *Pseudopalindrome closure operators in free monoids*, *Theoret. Comput. Sci.* 362 (2006) 282-300.
- [LT2018] Zhiqiang Li, Shaobin Tan. *Verma modules for rank two Heisenberg-Virasoro algebra*. Preprint, (2018). arXiv 1807.07735.
- [Lut2002] Frank H. Lutz, Császár's Torus, *Electronic Geometry Model No.* 2001.02.069 (2002). [http://www.eg-models.de/models/Classical\\_Models/2001.02.069/\\_direct\\_link.html](http://www.eg-models.de/models/Classical_Models/2001.02.069/_direct_link.html)
- [Lus1985] George Lusztig, *Cells in affine Weyl groups*, *Algebraic Groups and Related Topics*, *Advanced Studies in Pure mathematics* 6, 1985, pp. 255-287.
- [Lus2013] George Lusztig, *Hecke algebras with unequal parameters*, arXiv math/0208154.
- [Lut2005] Frank H. Lutz, "Triangulated Manifolds with Few Vertices: Combinatorial Manifolds", preprint (2005), arXiv math/0506372
- [LV2012] Jean-Louis Loday and Bruno Vallette. *Algebraic Operads*. Springer-Verlag Berlin Heidelberg (2012). doi:10.1007/978-3-642-30362-3.
- [Ltd06] Beijing Data Security Technology Co. Ltd, *Specification of SMS4, Block Cipher for WLAN Products - SMS4* (in Chinese); Available at <http://www.oscca.gov.cn/UpFile/200621016423197990.pdf>, (2006).

- [LTV1999] Bernard Leclerc, Jean-Yves Thibon, and Eric Vasserot. *Zelevinsky's involution at roots of unity*. J. Reine Angew. Math. 513:33-51 (1999).
- [LW2012] David Loeffler and Jared Weinstein, *On the computation of local components of a newform*, Mathematics of Computation **81** (2012) 1179-1200. doi:10.1090/S0025-5718-2011-02530-5
- [LW2015] T. Lawson and C. Wuthrich, Vanishing of some Galois cohomology groups for elliptic curves, arXiv 1505.02940
- [LY2001] K. Lauter and T. Yang, "Computing genus 2 curves from invariants on the Hilbert moduli space", Journal of Number Theory 131 (2011), pages 936 - 958
- [Lyo2003] R. Lyons, *Determinantal probability measures*. Publications Mathématiques de l'Institut des Hautes Études Scientifiques 98(1) (2003), pp. 167-212.
- [LZ2004] S. Lando and A. Zvonkine, "Graphs on surfaces and their applications", Springer-Verlag, 2004.
- [LZ2011] Bin Li and Hechun Zhang. *Path realization of crystal  $B(\infty)$* . Front. Math. China, **6** (4), (2011) pp. 689–706. doi:10.1007/s11464-010-0073-x
- [Mac1916] F.S. Macaulay. The algebraic theory of modular systems Cambridge university press, 1916.
- [Mac1995] I. G. Macdonald, Symmetric functions and Hall polynomials, second ed., The Clarendon Press, Oxford University Press, New York, 1995, With contributions by A. Zelevinsky, Oxford Science Publications.
- [MagmaHGM] *Hypergeometric motives in Magma*, <http://magma.maths.usyd.edu.au/~watkins/papers/HGM-chapter.pdf>
- [Mar1980] Jacques Martinet, Petits discriminants des corps de nombres, Journ. Arithm. 1980, Cambridge Univ. Press, 1982, 151–193.
- [Mar1983] H. R. Margolis, *Spectra and the Steenrod Algebra: Modules over the Steenrod Algebra and the Stable Homotopy Category*, North-Holland Mathematical Library. Vol. (29), Elsevier, 1983.
- [Mar2004] S. Marcus, Quasiperiodic infinite words, Bull. Eur. Assoc. Theor. Comput. Sci. 82 (2004) 170-174.
- [Mar2012] I. Marin, *The cubic Hecke algebra on at most 5 strands*, Journal of Pure and Applied Algebra 216 (2012) 2754-2782. doi:10.1016/j.jpaa.2012.04.013, arXiv 1110.6621.
- [Mar2018] I. Marin, *Maximal cubic quotient of the braid algebra*, preprint, 2018. available at <http://www.lamfa.u-picardie.fr/marin/arts/GQ.pdf>
- [Mas1994] James L. Massey, *SAFER K-64: A byte-oriented block-ciphering algorithm*; in FSE'93, Volume 809 of LNCS, pages 1-17. Springer, Heidelberg, December 1994.
- [Mat1992] O. Mathieu. *Classification of Harish-Chandra modules over the Virasoro Lie algebra*. Invent. Math. **107**(2) (1992), pp. 225-234.
- [Mat1999] A. Mathas. *Iwahori-Hecke algebras and Schur algebras of the symmetric group*. University Lecture Series, **15**. American Mathematical Society, Providence, RI, 1999. xiv+188 pp. ISBN: 0-8218-1926-7 Math-SciNet MR1711316
- [Mathas2002] Andrew Mathas. *The representation theory of the Ariki-Koike and cyclotomic  $q$ -Schur algebras*. Representation Theory of Algebraic Groups and Quantum Groups, Adv. Stud. Pure Math., vol. 40, Math. Soc. Japan, Tokyo (2004), pp. 261-320. arXiv math/0204025.
- [Mathas2004] Andrew Mathas. *Matrix units and generic degrees for the Ariki-Koike algebras*. J. Algebra. **281** (2004) pp. 695-730.
- [Mat2002] Jiří Matousek, "Lectures on Discrete Geometry", Springer, 2002
- [Mas1995] Mason, Geoffrey. *The quantum double of a finite group and its role in conformal field theory*. Groups '93 Galway/St. Andrews, Vol. 2, 405-417, London Math. Soc. Lecture Note Ser., 212, Cambridge, 1995.

- [Ma2009] Sarah Mason, An Explicit Construction of Type A Demazure Atoms, *Journal of Algebraic Combinatorics*, Vol. 29, (2009), No. 3, p.295-313. [arXiv 0707.4267](#)
- [Mac1936I] Saunders MacLane, *A construction for prime ideals as absolute values of an algebraic field*. *Duke Mathematical Journal*, 2(3) (1936), 492-510.
- [Mac1936II] Saunders MacLane, *A construction for absolute values in polynomial rings*. *Transactions of the American Mathematical Society*, 40(3)(1936), 363-395.
- [Mac1915] Percy A. MacMahon, *Combinatory Analysis*, Cambridge University Press (1915–1916). (Reprinted: Chelsea, New York, 1960).
- [Man2019] V. Manero and M. Marco, *Effective computation of degree bounded minimal models of GCDA's*, [arXiv 1909.07761](#)
- [MAR2009] H. Molina-Abril and P. Réal, *Homology computation using spanning trees* in *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, *Lecture Notes in Computer Science*, volume 5856, pp 272-278, Springer, Berlin (2009).
- [Mar1997] C.-M. Marle, *The Schouten-Nijenhuis bracket and interior products*, *Journal of Geometry and Physics* **23**, 350 (1997); doi:10.1016/S0393-0440(97)80009-5
- [Mark1992] George Markowsky, *Primes, irreducibles and extremal lattices*, *Order* 9 (1992), no. 3, 265-290. doi:10.1007%2FBBF00383950
- [Mar1994] George Markowsky. *Permutation lattices revisited*. *Mathematical Social Sciences*, 27 (1994), 59–72.
- [Mar2009a] Matilde Marcolli, *Feynman Motives*, Chapter 3, *Feynman integrals and algebraic varieties*, <http://www.its.caltech.edu/~matilde/LectureN3.pdf>
- [Mas1969] James L. Massey, “Shift-Register Synthesis and BCH Decoding.” *IEEE Trans. on Information Theory*, vol. 15(1), pp. 122-127, Jan 1969.
- [Mat1978] R. A. Mathon, *Symmetric conference matrices of order  $pq^2 + 1$* , *Canad. J. Math.* 30 (1978) 321-331, doi:10.4153/CJM-1978-029-1.
- [Mat2012] Yoshitake Matsumoto, *Database of Matroids*, 2012, <https://www-imai.is.s.u-tokyo.ac.jp/~ymatsu/matroid/index.html>
- [Mat2015] A. Mathas. *Cyclotomic quiver Hecke algebras of type A*, in “Modular representation theory of finite and p-adic groups”, 165–266, *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, **30**, World Sci. Publ., Hackensack, NJ, 2015. [MathSciNet MR3495747](#)
- [May1964] J. P. May, “The cohomology of restricted Lie algebras and of Hopf algebras; application to the Steenrod algebra.” Thesis, Princeton Univ., 1964.
- [May1967] J. P. May, *Simplicial Objects in Algebraic Topology*, University of Chicago Press (1967)
- [Maz1978] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* No. 47 (1977), 33–186 (1978).
- [Maz1978b] B. Mazur. Rational Isogenies of Prime Degree. *Inventiones Mathematicae* 44, 129-162 (1978).
- [MBRe2011] Patricia Muldoon Brown and Margaret A. Readdy, *The Rees product of posets*, *J. Comb.* 2 (2011), no. 2, 165-191
- [McC1978] K. McCrimmon. *Jordan algebras and their applications*. *Bull. Amer. Math. Soc.* **84** 1978.
- [McE1987] Robert J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.
- [McK1998] Brendan D. McKay, “Isomorph-Free Exhaustive generation”. *Journal of Algorithms*, 26(2): 306-324, February 1998.

- [McK2015] McKay, Brendan. *Description of graph6 and sparse6 encodings.*, updated Jun 2015. <http://cs.anu.edu.au/~bdm/data/formats.txt> (2019-08-25)
- [McM1992] John McMillan. *Games, strategies, and managers*. Oxford University Press.
- [Me1997] G. Melançon, *Factorizing infinite words using Maple*, MapleTech journal, vol. 4, no. 1, 1997, pp. 34-42.
- [MeNoTh11] Frédéric Menous, Jean-Christophe Novelli, Jean-Yves Thibon, *Mould calculus, polyhedral cones, and characters of combinatorial Hopf algebras*, Advances in Applied Mathematics, Volume 51, Issue 2, July 2013, Pages 177–227, doi:10.1016/j.aam.2013.02.003, arXiv 1109.1634v2.
- [MF1999] J.H. Mathews and K.D. Fink. *Numerical Methods Using MATLAB*. 3rd edition, Prentice-Hall, 1999.
- [Mes1991] Mestre, Jean-François. *Construction de courbes de genre 2 à partir de leurs modules*. Effective methods in algebraic geometry (Castiglione, 1990), 313–334, Progr. Math., 94, Birkhäuser Boston, Boston, MA, 1991.
- [MG1992] J. Misra and D. Gries. *A constructive proof of Vizing's theorem*. Information Processing Letters, (3) 41 (1992), 131-133. doi:10.1016/0020-0190(92)90041-S.
- [Mil1958] J. W. Milnor, *The Steenrod algebra and its dual*, Ann. of Math. (2) 67 (1958), 150-171.
- [Mil1974] J. W. Milnor and J. D. Stasheff, *Characteristic Classes*, University Press, Princeton and Tokyo, 1974.
- [Mil2006] J. W. Milnor, *On Lattes maps*, Dynamics on the Riemann sphere, Eur. Math. Soc., 9–43
- [Mil1978] S. Milne, *A  $q$ -analog of restricted growth functions, Dobinsky's equality and Charlier polynomials*. Trans. Amer. Math. Soc., 245 (1978), 89-118.
- [MilStu2005] Ezra Miller and Bernd Sturmfels, *Combinatorial Commutative Algebra*, GTM Vol. 227, Springer Science & Business Media, 2005.
- [Mil2004] Victor S. Miller, “The Weil pairing, and its efficient calculation”, J. Cryptol., 17(4):235-261, 2004
- [Mil2017] Arthur Milchior, *(Quasi-)linear time algorithm to compute LexDFS, LexUP and LexDown orderings*. (2017) arXiv 1701.00305
- [MirMor2009] R. Miranda, D.R. Morrison, “Embeddings of Integral Quadratic Forms” <http://www.math.ucsb.edu/~drm/manuscripts/eiqf.pdf>.
- [Mit2008] A. Mitra. *On the construction of  $M$ -sequences via primitive polynomials with a fast identification method*, International Journal of Electronics and Communication Engineering 2(9) (2008): 1991-1996.
- [Miy1991] M. Miyamoto. *A construction of Hadamard matrices*, Journal of Combinatorial Theory, Series A 57(1) (1991): 86-108. doi:10.1016/0097-3165(91)90008-5
- [MKO1998] Hans Munthe-Kaas and Brynjulf Owren. *Computations in a free Lie algebra*. (1998). Downloadable from Munthe-Kaas's website
- [MLH2008] C. Magnien, M. Latapy, and M. Habib. *Fast computation of empirically tight bounds for the diameter of massive graphs*. ACM Journal of Experimental Algorithms 13 (2008). doi:10.1145/1412228.1455266.
- [MMIB2012] Y. Matsumoto, S. Moriyama, H. Imai, D. Bremner: *Matroid Enumeration for Incidence Geometry*, Discrete and Computational Geometry, vol. 47, issue 1, pp. 17-43, 2012.
- [MM1998] Gunter Malle and Andrew Mathas. *Symmetric cyclotomic Hecke algebras* J. Algebra. **205** (1998) pp. 275-293.
- [MM2008] Manel Maia and Miguel Méndez. *On the arithmetic product of combinatorial species*. Discrete Mathematics (2008), Volume 308, Issue 23, pp. 5407-5427, arXiv math/0503436v2.
- [MM2015] J. Matherne and G. Muller, *Computing upper cluster algebras*, Int. Math. Res. Not. IMRN, 2015, 3121-3149.

- [MMRS2022] Ruslan G. Marzo, Rafael A. Melo, Celso C. Ribeiro and Marcio C. Santos: *New formulations and branch-and-cut procedures for the longest induced path problem*. Computers & Operations Research. 139, 105627 (2022) doi:10.1016/j.cor.2021.105627
- [Moh1988] B. Mohar, *Isoperimetric inequalities, growth, and the spectrum of graphs*, Linear Algebra and its Applications 103 (1988), 119–131.
- [Most2019] Jacob Mostovoy. *The pure cactus group is residually nilpotent*. Archiv der Math., **113** (2019). pp. 229-235. arXiv 1804.09165.
- [MNO1994] Alexander Molev, Maxim Nazarov, and Grigori Olshanski. *Yangians and classical Lie algebras*. (1994) arXiv hep-th/9409025
- [Mol2007] Alexander Ivanovich Molev. *Yangians and Classical Lie Algebras*. Mathematical Surveys and Monographs. Providence, RI: American Mathematical Society. (2007)
- [Mol2015] A. Molnar, Fractional Linear Minimal Models of Rational Functions, M.Sc. Thesis.
- [Mon1998] K. G. Monks, “Change of basis, monomial relations, and  $P_t^s$  bases for the Steenrod algebra,” J. Pure Appl. Algebra 125 (1998), no. 1-3, 235-260.
- [Mon2010] T. Monteil, The asymptotic language of smooth curves, talk at LaCIM2010.
- [Mont1987] Peter L. Montgomery: Speeding the Pollard and elliptic curve methods of factorization. Math. Comp. 48 (1987), 243-264.
- [Mo2009] D. Moody, Des. Codes Cryptogr. (2009) 52: 381. doi:10.1007/s10623-009-9287-x
- [MoPa1994] P. Morton and P. Patel. The Galois theory of periodic points of polynomial maps. Proc. London Math. Soc., 68 (1994), 225-263.
- [Motsak2006] Olekasandr Motsak. *Computation of the central elements and centralizers of sets of elements in non-commutative polynomial algebras*. PhD Thesis, 2006. <https://kluedo.ub.rptu.de/frontdoor/deliver/index/docId/2308/file/Thesis.pdf>
- [MP2019] M. Montes, D. Penazzi “Yarara and Coral v1” [https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/yarara\\_and\\_coral-spec.pdf](https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/yarara_and_coral-spec.pdf)
- [MPP2008] Conrado Martinez, Alois Panholzer and Helmut Prodinger, *Generating random derangements* doi:10.1137/1.9781611972986.7 [http://www.siam.org/proceedings/analco/2008/anl08\\_022martinez.pdf](http://www.siam.org/proceedings/analco/2008/anl08_022martinez.pdf)
- [MPPS2020] Jennifer Morse, Jianping Pan, Wencin Poh, Anne Schilling. *A Crystal on Decreasing Factorizations in the 0-Hecke Monoid* Electron. J. Combin., **27(2)** (2020) #P2.29. arXiv 1911.08732.
- [MR1985] R. Mathon and A. Rosa, *A new strongly regular graph*, Journal of Combinatorial Theory, Series A 38, no. 1 (1985): 84-86. doi:10.1016/0097-3165(85)90025-1
- [MR1989] G. Melançon and C. Reutenauer. *Lyndon words, free algebras and shuffles*, Can. J. Math., Vol. XLI, No. 4, 1989, pp. 577-591.
- [MR1995] C. Malvenuto, C. Reutenauer, *Duality between quasi-symmetric functions and the Solomon descent algebra*, Journal of Algebra 177 (1995), no. 3, 967-982. <http://www.lacim.uqam.ca/~christo/Publi%C3%A9s/1995/Duality.pdf>
- [MR1998] P. P. Martin and G. Rollet. *The Potts model representation and a Robinson-Schensted correspondence for the partition algebra*. Compositio Math., **112** (1998), pp. 237-254.
- [MR2002] S. Murphy, M. Robshaw *Essential Algebraic Structure Within the AES*; in Advances in Cryptology - CRYPTO 2002; LNCS 2442; Springer Verlag 2002
- [MRR1983] W. H. Mills, David P Robbins, Howard Rumsey Jr., *Alternating sign matrices and descending plane partitions*, Journal of Combinatorial Theory, Series A, Volume 34, Issue 3, May 1983, Pages 340–359. <http://www.sciencedirect.com/science/article/pii/0097316583900687>

- [MR2016] B. Malmskog, C. Rasmussen, *Picard curves over  $\mathbb{Q}$  with good reduction away from 3*. LMS Journal of Computation and Mathematics 19 (2016), no. 2, 382–408. doi:10.1112/S1461157016000413.
- [MS1977] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
- [MS1994] P. Martin and H. Saleur. *The blob algebra and the periodic Temperley-Lieb algebra*. Lett. Math. Phys., **30** (1994), no. 3. pp. 189–206.
- [MS2003] T. Mulders, A. Storjohann, “On lattice reduction for polynomial matrices”, J. Symbolic Comput. 35 (2003), no. 4, 377–401.
- [MS2011] G. Musiker and C. Stump, *A compendium on the cluster algebra and quiver package in sage*, arXiv 1102.4844.
- [MS2015] Jennifer Morse and Anne Schilling. *Crystal approach to affine Schubert calculus*. Int. Math. Res. Not. (2015). doi:10.1093/imrn/rnv194, arXiv 1408.0320.
- [MS2019] Y. Musleh and 'E. Schost. *Computing the characteristic polynomial of a finite rank two Drinfeld module*. In Proceedings of the 2019 ACM on International Symposium on Symbolic and Algebraic Computation, pages 307–314. ACM, 2019.
- [MS2023] Y. Musleh and 'E. Schost. *Computing the Characteristic Polynomial of Endomorphisms of a finite Drinfeld Module using Crystalline Cohomology*. In Proceedings of the 2023 ACM on International Symposium on Symbolic and Algebraic Computation, pages 461–469. ACM, 2023.
- [MSSY2001] Mateescu, A., Salomaa, A., Salomaa, K. and Yu, S., *A sharpening of the Parikh mapping*. Theoret. Informatics Appl. 35 (2001) 551–564.
- [MST2006] Barry Mazur, William Stein, John Tate. *Computation of  $p$ -adic heights and log convergence*. Doc. Math. 2006, Extra Vol., 577–614.
- [MSZ2013] Michael Maschler, Solan Eilon, and Zamir Shmuel. *Game Theory*. Cambridge: Cambridge University Press, (2013). ISBN 9781107005488.
- [MT1991] Mazur, B., & Tate, J. (1991). *The  $p$ -adic sigma function*. Duke Mathematical Journal, **62** (3), 663–688.
- [MTT1986] B. Mazur, J. Tate, and J. Teitelbaum, *On  $p$ -adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inventiones Mathematicae **84**, (1986), 1–48.
- [Mu1997] Murty, M. Ram. *Congruences between modular forms*. In “Analytic Number Theory” (ed. Y. Motohashi), London Math. Soc. Lecture Notes 247 (1997), 313–320, Cambridge Univ. Press.
- [Mul2004] Siguna Muller, “On the Computation of Square Roots in Finite Fields”, in Designs, Codes and Cryptography, Volume 31, Issue 3 (March 2004)
- [Mur1983] G. E. Murphy. *The idempotents of the symmetric group and Nakayama’s conjecture*. J. Algebra **81** (1983). 258–265.
- [Muth2019] Robert Muth. *Super RSK correspondence with symmetry*. Electron. J. Combin. **26** (2019), no. 2, Paper 2.27, 29 pp. <https://www.combinatorics.org/ojs/index.php/eljc/article/view/v26i2p27>, arXiv 1711.00420.
- [Muz2007] M. Muzychuk. *A generalization of Wallis-Fon-Der-Flaass construction of strongly regular graphs*. J. Algebraic Combin., 25(2):169–187, 2007. doi:10.1007/s10801-006-0030-7.
- [MV2010] D. Micciancio, P. Voulgaris. *A Deterministic Single Exponential Time Algorithm for Most Lattice Problems based on Voronoi Cell Computations*. Proceedings of the 42nd ACM Symposium Theory of Computation, 2010.
- [MvOV1996] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

- [MW1990] Brendan D. McKay and Nicholas C. Worland. “Uniform Generation of Random Regular Graphs of Moderate Degree”. *Journal of Algorithms*, 11(1):52-67, 1990. doi:10.1016/0196-6774(90)90029-E.
- [MW1994] Yiu-Kwong Man and Francis J. Wright. *Fast Polynomial Dispersion Computation and its Application to Indefinite Summation*. ISSAC 1994.
- [MW2009] Meshulam and Wallach, “Homological connectivity of random  $k$ -dimensional complexes”, preprint, math.CO/0609773.
- [MW2012] Ivan Marin and Emmanuel Wagner, *A CUBIC DEFINING ALGEBRA FOR THE LINKS-GOULD POLYNOMIAL* (arXiv 1203.5981v1 [mathGT] 27. Mar 2012)
- [NaiRow2011] Naidu and Rowell, A finiteness property for braided fusion categories. *Algebr. Represent. Theory* 14 (2011), no. 5, 837–855. arXiv 0903.4157.
- [NAR2018] Jamie R. Nunez, Christopher R. Anderson, Ryan S. Renslow *Optimizing colormaps with consideration for color vision deficiency to enable accurate interpretation of scientific data*. PLoS ONE 13(7), 2018: e0199239.
- [Nas1950] John Nash. *Equilibrium points in  $n$ -person games*. *Proceedings of the National Academy of Sciences* 36.1 (1950): 48-49.
- [Neu2018] Christian Neurohr, *Efficient Integration on Riemann Surfaces & Applications*, PhD Thesis, Carl von Ossietzky Universität Oldenburg <http://oops.uni-oldenburg.de/3607>.
- [New2003] Newman, M.E.J. *The Structure and function of complex networks*, SIAM Review vol. 45, no. 2 (2003), pp. 167-256. doi:10.1137/S003614450342480.
- [Nie2013] Johan S. R. Nielsen, *List Decoding of Algebraic Codes*, Ph.D. Thesis, Technical University of Denmark, 2013
- [Nie] Johan S. R. Nielsen, Codinglib, <https://bitbucket.org/jsrn/codinglib/>.
- [Niez1998] Marek Niezgoda. Group majorization and Schur type inequalities. *Linear Algebra and its Applications*, 268(1):9-30, 1998. doi:10.1016/S0024-3795(97)89322-6.
- [NW1978] A. Nijenhuis and H. Wilf, *Combinatorial Algorithms*, Academic Press (1978).
- [Nij1955] A. Nijenhuis, *Jacobi-type identities for bilinear differential concomitants of certain tensor fields. I*, *Indagationes Mathematicae (Proceedings)* **58**, 390 (1955).
- [Nik1977] V. V. Nikulin, “Integral symmetric bilinear forms and some of their applications” *Izv. Akad. Nauk SSSR Ser. Mat.*, 1979, Volume 43, Issue 1, Pages 111–177.
- [Nil2005] Benjamin Nill, “Gorenstein toric Fano varieties”, *Manuscripta Math.* 116 (2005), no. 2, 183-210. arXiv math/0405448v1 [math.AG]
- [NN2007] Nisan, Noam, et al., eds. *Algorithmic game theory*. Cambridge University Press, 2007.
- [NO2003] Sampo Niskanen and Patric R. J. Ostergard, *Cliquer User’s Guide, Version 1.0*, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. T48, 2003.
- [Normaliz] Winfried Bruns, Bogdan Ichim, and Christof Soeger, Normaliz, <http://www.mathematik.uni-osnabrueck.de/normaliz/>
- [NormalizMan] Winfried Bruns, Max Horn, *Normaliz 3.8.5*, 2020, <https://github.com/Normaliz/Normaliz/blob/master/doc/Normaliz.pdf>.
- [NoThWi08] J.-C. Novelli, J.-Y. Thibon, L. K. Williams, *Combinatorial Hopf algebras, noncommutative Hall-Littlewood functions, and permutation tableaux*. *Advances in Mathematics*, Volume 224, Issue 4, 10 July 2010, pp. 1311–1348, doi:10.1016/j.aim.2010.01.006, arXiv 0804.0995v3.
- [NovThi06] Jean-Christophe Novelli, Jean-Yves Thibon, *Polynomial realizations of some trialgebras*, FPSAC 2006. arXiv math/0605061v1.

- [NP2007] Nikolopoulos, S.D. and Palios, L., *Detecting holes and antiholes in graphs*, Algorithmica, 2007, Vol. 47, number 2, pages 119–138, doi:10.1007/s00453-006-1225-y, <http://www.cs.uoi.gr/~stavros/C-Papers/C-2004-SODA.pdf>
- [NWS2002] Newman, M.E.J., Watts, D.J. and Strogatz, S.H. *Random graph models of social networks*. Proc. Nat. Acad. Sci. USA 99:1 (2002), 2566–2572. doi:10.1073/pnas.012582999
- [NX2019] E. M. d. Nascimento, J. A. M. Xexeo “Name of Submission: FlexAEAD -A Lightweight Cipher with Integrated Authentication” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/FlexAEAD-spec.pdf>
- [NZ1997] T. Nakashima and A. Zelevinsky. Polyhedral Realizations of Crystal Bases for Quantized Kac-Moody Algebras. Adv. Math. **131**, pp. 253–278, 1997.
- [NZ2012] T. Nakanishi and A. Zelevinsky, *On tropical dualities in cluster algebras*, Algebraic groups and quantum groups, Contemp. Math., vol. 565, Amer. Math. Soc., Providence, RI, 2012, pp. 217–226.
- [Nze2007] Janvier Nzeutchap. *Binary Search Tree insertion, the Hypoplactic insertion, and Dual Graded Graphs*. arXiv 0705.2689 (2007).
- [OGKRKGBDDP2015] R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko, A. Boiko, O. Dyrda, V. Dolgov, and A. Pushkaryov, *A new standard of ukraine: The kupyna hash function*; in Cryptology ePrint Archive, (2015), 885.
- [Oha2011] R.A. Ohana. On Prime Counting in Abelian Number Fields. [http://wstein.org/home/ohanar/papers/abelian\\_prime\\_counting/main.pdf](http://wstein.org/home/ohanar/papers/abelian_prime_counting/main.pdf).
- [OLJ2014] Paul W. Olsen, Alan G. Labouseur, Jeong-Hyon Hwang. *Efficient Top-k Closeness Centrality Search*, Proceedings of the IEEE 30th International Conference on Data Engineering (ICDE), 2014. doi:10.1109/ICDE.2014.6816651.
- [ONe1983] B. O’Neill : *Semi-Riemannian Geometry*, Academic Press (San Diego) (1983)
- [Onsager1944] Lars Onsager. *Crystal statistics. I. A two-dimensional model with an order-disorder transition*, Phys. Rev. (2) **65** (1944), pp. 117–149.
- [Ore1933] Oystein Ore. *Theory of Non-Commutative Polynomials* Annals of Mathematics, Second Series, Volume 34, Issue 3 (Jul., 1933), 480–508.
- [Or2017] M. Orlitzky. The Lyapunov rank of an improper cone. Optimization Methods and Software, 32(1):109–125, 2017, doi:10.1080/10556788.2016.1202246.
- [Or2018a] M. Orlitzky. Lyapunov rank of polyhedral positive operators. Linear and Multilinear Algebra, 66(5):992–1000, 2018, doi:10.1080/03081087.2017.1331998.
- [Or2018b] M. Orlitzky. Positive and Z-operators on closed convex cones. Electronic Journal of Linear Algebra, 34:444–458, 2018, doi:10.13001/1081-3810.3782.
- [Or2020] M. Orlitzky. When a maximal angle among cones is nonobtuse. Computational and Applied Mathematics 39(2), 2020. doi:10.1007/s40314-020-1115-y.
- [Or2024] M. Orlitzky. Continuity of the conic hull. Journal of Convex Analysis 31(1):255–264, 2024.
- [ORS2013] Peter Ozsvath, Jacob Rasmussen, Zoltan Szabo, *Odd Khovanov homology*, Algebraic & Geometric Topology 13 (2013) 1465–1488, doi:10.2140/agt.2013.13.1465.
- [ORV] Grigori Olshanski, Amitai Regev, Anatoly Vershik, *Frobenius-Schur functions*, arXiv math/0110077v1. Possibly newer version at <http://www.wisdom.weizmann.ac.il/~regev/papers/FrobeniusSchurFunctions.ps>
- [OT1994] Peter Orlik and Hiroaki Terao. *Commutative algebras for arrangements*. Nagoya Math. J. **134** (1994), 65–73.

- [OS2018] Se-jin Oh and Travis Scrimshaw. *Categorical relations between Langlands dual quantum affine algebras: Exceptional cases*. Preprint: [arXiv 1802.09253](#) (2018).
- [OSS2009] Vitaly Osipov, Peter Sanders, Johannes Singler: *The Filter-Kruskal Minimum Spanning Tree Algorithm*. SIAM ALENEX, 2009: 52-61 [doi:10.1137/1.9781611972894.5](#)
- [Oum2009] Sang-il Oum, *Computing rank-width exactly*, Information Processing Letters, 2009, vol. 109, n. 13, p. 745–748, Elsevier. [doi:10.1016/j.ipl.2009.03.018](#). <http://mathsci.kaist.ac.kr/~sangil/pdf/2008exp.pdf>
- [Oxl1987] James Oxley, *The binary matroids with no 4-wheel minor*, 1987, Transactions of the American Mathematical Society, 301(1), 63-75.
- [Oxl1992] James Oxley, *Matroid theory*, Oxford University Press, 1992.
- [Oxl2011] James Oxley, *Matroid Theory, Second Edition*. Oxford University Press, 2011.
- [Pak2002] Igor Pak, *Hook length formula and geometric combinatorics*, Seminaire Lotharingien de Combinatoire, 46 (2001), B46f, <https://eudml.org/doc/121696>
- [Pap2023] Mihran Papikian, *Drinfeld modules*. Graduate Texts in Mathematics, 206, Springer International Publishing, Cham, 2023.
- [PALP] Maximilian Kreuzer, Harald Skarke: “PALP: A Package for Analyzing Lattice Polytopes with Applications to Toric Geometry” *omput.Phys.Commun.* 157 (2004) 87-106 [arXiv math/0204356](#)
- [Pana2002] F. Panaite, *Relating the Connes-Kreimer and Grossman-Larson Hopf algebras built on rooted trees*, Lett. Math. Phys. 51 (2000), no. 3, pages 211-219. Preprint: [arXiv math/0003074v1](#)
- [Pas1992] D. V. Pasechnik, *Skew-symmetric association schemes with two classes and strongly regular graphs of type  $L_{2n-1}/(4n-1)$* , Acta Applicanda Math. 29(1992), 129-138. [doi:10.1007/BF00053382](#).
- [Pau2006] Sebastian Pauli, “Constructing Class Fields over Local Fields”, *Journal de Théorie des Nombres de Bordeaux*, Vol. 18, No. 3 (2006), pp. 627-652.
- [PearsonTest] [Wikipedia article Goodness\\_of\\_fit](#), accessed 13th October 2009.
- [Pec2014] Oliver Pechenik, *Cyclic sieving of increasing tableaux and small Schroeder paths*, JCTA 125 (2014), 357-378, [doi:10.1016/j.jcta.2014.04.002](#)
- [Pei2010] Peikert, C. (2010). An Efficient and Parallel Gaussian Sampler for Lattices. In: Rabin, T. (eds) *Advances in Cryptology – CRYPTO 2010*. CRYPTO 2010. Lecture Notes in Computer Science, vol 6223. Springer, Berlin, Heidelberg. [doi:10.1007/978-3-642-14623-7\\_5](#)
- [Pen2012] R. Pendavingh, *On the evaluation at  $(-i, i)$  of the Tutte polynomial of a binary matroid*. Preprint: [arXiv 1203.0910](#)
- [Per2007] Markus Perling, *Divisorial Cohomology Vanishing on Toric Varieties*, [arXiv 0711.4836v2](#)
- [Pet2010] Christiane Peters, *Information-set decoding for linear codes over  $GF(q)$* , Proc. of PQCrypto 2010, pp. 81-94.
- [Pha2002] R. C.-W. Phan. *Mini advanced encryption standard (mini-AES): a testbed for cryptanalysis students*. Cryptologia, 26(4):283–306, 2002.
- [Piz1980] A. Pizer. *An Algorithm for Computing Modular Forms on  $\Gamma_0(N)$* , J. Algebra 64 (1980), 340-390.
- [Platt1976] C. R. Platt, *Planar lattices and planar graphs*, Journal of Combinatorial Theory Series B, Vol 21, no. 1 (1976): 30-39.
- [PoiReu95] Stephane Poirier, Christophe Reutenauer, *Algèbres de Hopf de tableaux*, Ann. Sci. Math. Québec, 19 (1): 79–90. <http://www.lacim.uqam.ca/~christo/Publi%C3%A9s/1995/Alg%C3%A8bres%20de%20Hopf%20de%20tableaux.pdf>
- [PM2019] D. Penazzi, M. Montes. “Shamash (and Shamashash)” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/ShamashAndShamashash-spec.pdf>

- [Pol2003] Robert Pollack, *On the  $p$ -adic  $L$ -function of a modular form at a supersingular prime*, Duke Math. J. 118 (2003), no. 3, 523-558.
- [Pol2009] J. Polhill, *Negative Latin square type partial difference sets and amorphic association schemes with Galois rings*, Journal of Combinatorial Designs 17, no. 3 (2009): 266-282. doi:10.1002/jcd.20206. <http://onlinelibrary.wiley.com/doi/10.1002/jcd.20206/abstract>
- [Pon2010] S. Pon. *Types B and D affine Stanley symmetric functions*, unpublished PhD Thesis, UC Davis, 2010.
- [Pons2013] Viviane Pons, *Combinatoire algébrique liée aux ordres sur les permutations*. PhD Thesis. (2013). arXiv 1310.1805v1.
- [Pons2018] Viviane Pons, *The Rise-Contact involution on Tamari intervals*. arXiv 1802.08335
- [Pop1972] V. M. Popov. "Invariant description of linear, time-invariant controllable systems". SIAM Journal on Control, 10(2):252-264, 1972. doi:10.1137/0310020
- [Pos1988] H. Postl. 'Fast evaluation of Dickson Polynomials' Contrib. to General Algebra, Vol. 6 (1988) pp. 223-225
- [Pos2005] A. Postnikov, Affine approach to quantum Schubert calculus, Duke Math. J. 128 (2005) 473-509
- [Pot1998] Potemine, I.Y., Minimal Terminal Q-Factorial Models of Drinfeld Coarse Moduli Schemes. Mathematical Physics, Analysis and Geometry 1, 171-191 (1998). doi:10.1023/A:1009724323513
- [PPW2013] D. Perkinson, J. Perlman, and J. Wilmes. *Primer for the algebraic geometry of sandpiles*. Tropical and Non-Archimedean Geometry, Contemp. Math., 605, Amer. Math. Soc., Providence, RI, 2013. arXiv 1112.6163
- [Proc1999] R. A. Proctor, *Minuscule elements of Weyl groups, the numbers game, and  $d$ -complete posets*. J. Algebra, 213(1):272-303, 1999.
- [PDynk1999] R. A. Proctor. *Dynkin diagram classification of  $\lambda$ -minuscule Bruhat lattices and of  $d$ -complete posets*. J. Algebraic Combin., 9(1):61-94, 1999.
- [Proc2014] R. A. Proctor.  *$d$ -complete posets generalize Young diagrams for the hook product formula: Partial Presentation of Proof*. RIMS Kôkyûroku, 1913:120-140, 2014.
- [PR2003] Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en  $p$* , Experiment. Math. 12 (2003), no. 2, 155-186.
- [PR2015] P. Pilarczyk and P. Réal, *Computation of cubical homology, cohomology, and (co)homological operations via chain contraction*, Adv. Comput. Math. 41 (2015), pp 253-275.
- [PRC2012] G. Piret, T. Roche, and C. Carlet, *PICARO - a block cipher allowing efficient higher-order side-channel resistance*; in ACNS, (2012), pp. 311-328.
- [PRV2017] L.-F. Préville-Ratelle and X. Viennot, *The enumeration of generalized Tamari intervals*. Trans. Amer. Math. Soc. 369 (2017), pp 5219-5239
- [Prototype\_pattern] Prototype pattern, [Wikipedia article Prototype\\_pattern](#)
- [PeSt2011] E. Pelantová, Š. Starosta, Infinite words rich and almost rich in generalized palindromes, in: G. Mauri, A. Leporati (Eds.), Developments in Language Theory, volume 6795 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 406-416
- [PS2002] Jim Pitman, Richard Stanley, *A polytope related to empirical distributions, plane trees, parking functions, and the associahedron*, J. Discrete Comput. Geom. (2002), 27:4, 603-634, doi:10.1007/s00454-002-2776-6, arXiv math/9908029.
- [PS2006] Dominique Poulalhon and Gilles Schaeffer, *Optimal coding and sampling of triangulations*, Algorithmica 46 (2006), no. 3-4, 505-527, doi:10.1007/s00453-006-0114-8, [http://www.lix.polytechnique.fr/~poulalho/Articles/PoSc\\_Algorithmica06.pdf](http://www.lix.polytechnique.fr/~poulalho/Articles/PoSc_Algorithmica06.pdf)

- [PS2011] R. Pollack, and G. Stevens. *Overconvergent modular symbols and  $p$ -adic  $L$ -functions*. Annales scientifiques de l'École normale supérieure. Vol. 44. No. 1. Elsevier, 2011.
- [PSW1996] Boris Pittel, Joel Spencer and Nicholas Wormald. *Sudden Emergence of a Giant  $k$ -Core in a Random Graph*. (1996). J. Combinatorial Theory. Ser B 67. pages 111-151. doi:10.1006/jctb.1996.0036. [Online] Available: <http://cs.nyu.edu/cs/faculty/spencer/papers/k-core.pdf>
- [PT2009] S. Payne, J. A. Thas. *Finite generalized quadrangles*. European Mathematical Society, 2nd edition, 2009.
- [PUNTOS] Jesus A. De Loera [http://www.math.ucdavis.edu/~deloera/RECENT\\_WORK/puntos2000](http://www.math.ucdavis.edu/~deloera/RECENT_WORK/puntos2000)
- [PvZ2010] R. A. Pendavingh, S. H. M. van Zwam, Lifts of matroid representations over partial fields, Journal of Combinatorial Theory, Series B, Volume 100, Issue 1, January 2010, Pages 36-67
- [PZ2008] J. H. Palmieri and J. J. Zhang, "Commutators in the Steenrod algebra," New York J. Math. 19 (2013), 23-37.
- [Pro2001] James Propp. *The Many Faces of Alternating Sign Matrices*, Discrete Mathematics and Theoretical Computer Science 43 (2001): 58 [arXiv math/0208125](https://arxiv.org/abs/math/0208125)
- [Propp1997] James Propp, *Generating Random Elements of Finite Distributive Lattices*, Electron. J. Combin. 4 (1997), no. 2, The Wilf Festschrift volume, Research Paper 15. <http://www.combinatorics.org/ojs/index.php/eljc/article/view/v4i2r15>
- [PW2013] Robin Pemantle and Mark C. Wilson. *Analytic Combinatorics in Several Variables*. Cambridge University Press, 2013.
- [PWZ1997] Marko Petkovsek, Herbert S. Wilf, Doron Zeilberger, *A = B*, AK Peters, Ltd., Wellesley, MA, USA, 1997, pp. 73-100
- [PZGH1999] Petho A., Zimmer H.G., Gebel J. and Herrmann E., Computing all S-integral points on elliptic curves Math. Proc. Camb. Phil. Soc. (1999), 127, 383-402
- [Rai2012] Alexander Raichev. *Leinartas's partial fraction decomposition*. [arXiv 1206.4740](https://arxiv.org/abs/1206.4740).
- [Raj1987] A. Rajan, Algorithmic applications of connectivity and related topics in matroid theory. Ph.D. Thesis, Northwestern university, 1987.
- [Ram1991] Arun Ram, *A Frobenius formula for the characters of the Hecke algebras*. Invent. Math. **106** (1991), pp. 461-488.
- [Ram1997] Arun Ram. *Seminormal representations of Weyl groups and Iwahori-Hecke algebras*. Proc. London Math. Soc. (3) **75** (1997). 99-133. [arXiv math/9511223v1](https://arxiv.org/abs/math/9511223v1). <http://www.ms.unimelb.edu.au/~ram/Publications/1997PLMSv75p99.pdf>
- [RCES1994] Ruskey, R. Cohen, P. Eades, A. Scott. *Alley CATs in search of good homes*. Congressus numerantium, 1994. Pages 97-110
- [Rea2004] Nathan Reading. *Cambrian Lattices*. [arXiv math/0402086v2](https://arxiv.org/abs/math/0402086v2).
- [Rea2009] Nathan Reading, *Noncrossing partitions and the shard intersection order*, DMTCS Proceedings of FPSAC 2009, 745-756
- [ReSt2020] Nathan Reading and Salvatore Stella, *An affine almost positive roots model*, J. Comb. Algebra Volume 4, Issue 1, 2020, pp. 1-59
- [Red2001] Maria Julia Redondo. *Hochschild cohomology: some methods for computations*. Resenhas IME-USP 5 (2), 113-137 (2001). <http://inmabb.criba.edu.ar/gente/mredondo/crasp.pdf>
- [Reg09] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. in Journal of the ACM 56(6). ACM 2009, doi:10.1145/1060590.1060603
- [Reg1958] T. Regge, 'Symmetry Properties of Clebsch-Gordan Coefficients', Nuovo Cimento, Volume 10, pp. 544 (1958)

- [Reg1959] T. Regge, ‘Symmetry Properties of Racah Coefficients’, *Nuovo Cimento*, Volume 11, pp. 116 (1959)
- [Reg2005] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC, pp. 84–93, ACM, 2005.
- [Ren2018] Joost Renes: Computing Isogenies Between Montgomery Curves Using the Action of  $(0, 0)$ . PQCrypto 2018, pp. 229–247. <https://eprint.iacr.org/2017/1198.pdf>
- [Reu1993] C. Reutenauer. *Free Lie Algebras*. Number 7 in London Math. Soc. Monogr. (N.S.). Oxford University Press. (1993).
- [Reu2003] Christophe Reutenauer. *Free Lie algebras*. Preprint of a chapter in the Handbook of Algebra, 2003. [Downloadable from Reutenauer’s website](#)
- [Rho69] John Rhodes, *Characters and complexity of finite semigroups* J. Combinatorial Theory, vol 6, 1969
- [RH2003] J. Rasch and A. C. H. Yu, ‘Efficient Storage Scheme for Pre-calculated Wigner 3j, 6j and Gaunt Coefficients’, *SIAM J. Sci. Comput.* Volume 25, Issue 4, pp. 1416-1428 (2003)
- [RH2003b] G. G. Rose and P. Hawkes, *Turing: A fast stream cipher*; in FSE, (2003), pp. 290-306.
- [Rio1958] J. Riordan, “An Introduction to Combinatorial Analysis”, Dover Publ. (1958)
- [Rio2019] S. Riou, “DryGASCON: Lightweight Cryptography Standardization Process round 1 submission” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/drygascon-spec.pdf>
- [Ris2016] Roswitha Rissner, “Null ideals of matrices over residue class rings of principal ideal domains”. *Linear Algebra Appl.*, **494** (2016) 44–69. [doi:10.1016/j.laa.2016.01.004](https://doi.org/10.1016/j.laa.2016.01.004).
- [RL1971] J. Rokne, P. Lancaster. Complex interval arithmetic. *Communications of the ACM* 14. 1971.
- [RMA2009] P. Réal and H. Molina-Abril, *Cell AT-models for digital volumes* in Torsello, Escolano, Brun (eds.), *Graph-Based Representations in Pattern Recognition*, Lecture Notes in Computer Science, volume 5534, pp. 314-3232, Springer, Berlin (2009).
- [RNPA2011] G. Rudolf, N. Noyan, D. Papp, and F. Alizadeh. Bilinear optimality constraints for the cone of positive polynomials. *Mathematical Programming, Series B*, 129 (2011) 5-31.
- [RPK1980] S. M. Reddy, D. K. Pradhan, and J. Kuhl. “Directed graphs with minimal diameter and maximal connectivity”, School Eng., Oakland Univ., Rochester MI, Tech. Rep., July 1980.
- [RPK1983] S. Reddy, P. Raghavan, and J. Kuhl. “A Class of Graphs for Processor Interconnection”. *IEEE International Conference on Parallel Processing*, pages 154-157, Los Alamitos, Ca., USA, August 1983.
- [Rob1991] Tom Roby, “Applications and extensions of Fomin’s generalization of the Robinson-Schensted correspondence to differential posets”. Ph.D. Thesis, M.I.T., Cambridge, Massachusetts, 1991.
- [Roberts2015] David P. Roberts, *Hypergeometric Motives I*, [https://icerm.brown.edu/materials/Slides/sp-f15-offweeks/Hypergeomteric\\_Motives,\\_I\\_{}\\_David\\_Roberts,\\_University\\_of\\_Minnesota\\_-\\_Morris.pdf](https://icerm.brown.edu/materials/Slides/sp-f15-offweeks/Hypergeomteric_Motives,_I_{}_David_Roberts,_University_of_Minnesota_-_Morris.pdf)
- [Roberts2017] David P. Roberts, *Hypergeometric motives and an unusual application of the Guinand-Weil-Mestre explicit formula*, [https://www.matrix-inst.org.au/wp\\_Matrix2016/wp-content/uploads/2016/04/Roberts-2.pdf](https://www.matrix-inst.org.au/wp_Matrix2016/wp-content/uploads/2016/04/Roberts-2.pdf)
- [Roc1970] R.T. Rockafellar, *Convex Analysis*. Princeton University Press, Princeton, 1970.
- [Roe1988] John Roe, *Elliptic operators, topology and asymptotic methods*. 2nd edition. CRC Press, 1988.
- [Rog2018] Baptiste Rognerud, *Exceptional and modern intervals of the Tamari lattice*. [arXiv 1801.04097](https://arxiv.org/abs/1801.04097)
- [Ros1999] K. Rosen *Handbook of Discrete and Combinatorial Mathematics* (1999), Chapman and Hall.
- [Ros2002] Rosenfeld, Vladimir Raphael, 2002: Enumerating De Bruijn Sequences. *Communications in Math. and in Computer Chem.*
- [Rosen2002] M. Rosen. Number theory in function fields. Springer, 2022.

- [Rot2001] Gunter Rote, *Division-Free Algorithms for the Determinant and the Pfaffian: Algebraic and Combinatorial Approaches*, H. Alt (Ed.): Computational Discrete Mathematics, LNCS 2122, pp. 119–135, 2001. <http://page.mi.fu-berlin.de/rote/Papers/pdf/Division-free+algorithms.pdf>
- [Rot2006] Ron Roth, *Introduction to Coding Theory*, Cambridge University Press, 2006
- [Row2006] Eric Rowell, *From quantum groups to unitary modular tensor categories*. In Representations of algebraic groups, quantum groups, and Lie algebras, Contemp. Math., **413**, Amer. Math. Soc., Providence, RI, 2006. [arXiv math/0503226](https://arxiv.org/abs/math/0503226).
- [RoStWa2009] Eric Rowell, Richard Stong and Zhenghan Wang, *On classification of modular tensor categories*, Comm. Math. Phys. 292, 343–389, 2009.
- [RR1997] Arun Ram and Jeffrey Remmel. *Applications of the Frobenius formulas and the characters of the symmetric group and the Hecke algebras of type A*. J. Algebraic Combin. **6** (1997), 59–87.
- [RRV2022] David P. Roberts and Fernando Rodriguez Villegas, *Hypergeometric motives*, Notices Amer. Math. Soc., **69** vol. 6 (2022). [doi:10.1090/noti2491](https://doi.org/10.1090/noti2491).
- [RSS] [Wikipedia article Residual\\_sum\\_of\\_squares](#), accessed 13th October 2009.
- [RS1995] Victor Reiner, Mark Shimozono, *Plactification*, J. Algebraic Combin. **4** (1995), pp. 331–351.
- [RS2012] G. Rudolph and M. Schmidt, “Differential Geometry and Mathematical Physics. Part I. Manifolds, Lie Groups and Hamiltonian Systems”, Springer, 2012.
- [RSW2011] Victor Reiner, Franco Saliola, Volkmar Welker. *Spectra of Symmetrized Shuffling Operators*. [arXiv 1102.2460v2](https://arxiv.org/abs/1102.2460v2).
- [RT1975a] Read, R. C. and Tarjan, R. E. *Bounds on Backtrack Algorithms for Listing Cycles, Paths, and Spanning Trees*. Networks, Volume 5 (1975), numer 3, pages 237–252. [doi:10.1002/net.1975.5.3.237](https://doi.org/10.1002/net.1975.5.3.237).
- [RT1975] Rose, D.J. and Tarjan, R.E., *Algorithmic aspects of vertex elimination*, Proceedings of seventh annual ACM symposium on Theory of computing, Pages 245–254, ACM 1975. [doi:10.1145/800116.803775](https://doi.org/10.1145/800116.803775).
- [RT1985] James Roskind and Robert Endre Tarjan. *A note on finding minimum-cost edge-disjoint spanning trees*. Mathematics of Operations Research, 10(4):701–708, 1985. [doi:10.1287/moor.10.4.701](https://doi.org/10.1287/moor.10.4.701)
- [RTL76] Donald J. Rose, Robert Endre Tarjan and George S. Lueker. *Algorithmic aspects of vertex elimination on graphs*. SIAM J. Comput., 5(2), 266–283 (1976).
- [Rub1991] K. Rubin. The “main conjectures” of Iwasawa theory for imaginary quadratic fields. Invent. Math. 103 (1991), no. 1, 25–68.
- [RS2010] RUBIN, K., & SILVERBERG, A. (2010). CHOOSING THE CORRECT ELLIPTIC CURVE IN THE CM METHOD. Mathematics of Computation, 79(269), 545–561. [doi:10.1090/S0025-5718-09-02266-2](https://doi.org/10.1090/S0025-5718-09-02266-2)
- [Rud1958] M. E. Rudin. *An unshellable triangulation of a tetrahedron*. Bull. Amer. Math. Soc. 64 (1958), 90–91.
- [Rus2003] Frank Ruskey. *Combinatorial Generation*. (2003). <http://www.1stworks.com/ref/ruskeycombggen.pdf>
- [Rüt2014] Julian Rütth, *Models of Curves and Valuations*. Open Access Repositorium der Universität Ulm. Dissertation (2014). [doi:10.18725/OPARU-3275](https://doi.org/10.18725/OPARU-3275)
- [RV2007] Fernando Rodriguez Villegas. *Experimental Number Theory*. Oxford Graduate Texts in Mathematics 13, 2007.
- [RV2019] Fernando Rodriguez Villegas. *Mixed Hodge numbers and factorial ratios*. [arXiv 1907.02722](https://arxiv.org/abs/1907.02722), 2019.
- [RW2008] Alexander Raichev and Mark C. Wilson. *Asymptotics of coefficients of multivariate generating functions: improvements for smooth points*, Electronic Journal of Combinatorics, Vol. 15 (2008). R89 [arXiv 0803.2914](https://arxiv.org/abs/0803.2914).

- [RW2012] Alexander Raichev and Mark C. Wilson. *Asymptotics of coefficients of multivariate generating functions: improvements for smooth points*. Online Journal of Analytic Combinatorics. Issue 6, (2011). [arXiv 1009.5715](#).
- [Saa2011] M-J. O. Saarinen, *Cryptographic Analysis of All 4 x 4-Bit S-Boxes*; in SAC, (2011), pp. 118-133.
- [Sag1987] Bruce E. Sagan. *Shifted tableaux, Schur Q-functions, and a conjecture of R. Stanley*. Journal of Combinatorial Theory, Series A Volume 45 (1987), pp. 62-103.
- [Sag2001] Bruce E. Sagan. *The Symmetric Group*, 2nd edition, New York 2001.
- [Sag2011] Bruce E. Sagan, *The cyclic sieving phenomenon: a survey*, [arXiv 1008.0790v3](#)
- [Sah2000] Sartaj Sahni. *Data Structures, Algorithms, and Applications in Java*. McGraw-Hill, 2000.
- [Sal1954] G. Salmon: “A Treatise on Conic Sections”, Chelsea Publishing Co., New York, 1954.
- [Sal1958] G. Salmon: “A Treatise on the Analytic Geometry of Three Dimensions”, Vol. I, Chelsea Publishing Company, New York, 1958.
- [Sal1965] G. Salmon: “A Treatise on the Analytic Geometry of Three Dimensions”, Vol II, Chelsea Publishing Co., New York, 1965.
- [Sal2014] B. Salisbury. The flush statistic on semistandard Young tableaux. [arXiv 1401.1185](#)
- [Sam2012] P. Samanta: *Antipodal Graphs* [doi:10.13140/RG.2.2.28238.46409](#)
- [Saw1985] K. Sawade. *A Hadamard matrix of order 268*, Graphs and Combinatorics 1(1) (1985): 185-187. [doi:10.1007/BF02582942](#)
- [Sch1961] Craige Schensted. *Longest increasing and decreasing subsequences*, Canadian Journal of Mathematics, Vol 13 (1961), pp. 179–191.
- [Sch1990] Schnyder, Walter. *Embedding Planar Graphs on the Grid*. Proc. 1st Annual ACM-SIAM Symposium on Discrete Algorithms, San Francisco (1994), pp. 138-147.
- [Sch1996] E. Schaefer. A simplified data encryption algorithm. Cryptologia, 20(1):77–84, 1996.
- [Scha1996] Richard D. Schaefer. *An Introduction to Nonassociative Algebras*. Dover, New York, 1996.
- [Sch1999] Gilles Schaeffer, *Random Sampling of Large Planar Maps and Convex Polyhedra*, Annual ACM Symposium on Theory of Computing (Atlanta, GA, 1999). [doi:10.1145/301250.301448](#).
- [Sch2003] Alexander Schrijver, *Combinatorial optimization: polyhedra and efficiency*, 2003.
- [Sch2003b] Manfred Schocker, *Multiplicities of Higher Lie Characters*. J. Aust. Math. Soc. 75 (2003), pp. 9-21. [doi:10.1017/S144678870000344X](#)
- [Sch2004] Manfred Schocker, *The descent algebra of the symmetric group*. Fields Inst. Comm. 40 (2004), pp. 145-161. <http://www.mathematik.uni-bielefeld.de/~ringel/schocker-neu.ps>
- [Sch2006] Oliver Schiffmann. *Lectures on Hall algebras*, preprint, 2006. [arXiv 0611617v2](#).
- [Sch2008] A. Schilling. “Combinatorial structure of Kirillov-Reshetikhin crystals of type  $D_n(1)$ ,  $B_n(1)$ ,  $A_{2n-1}(2)$ ”. J. Algebra. **319** (2008). 2938-2962. [arXiv 0704.2046](#).
- [Sch2013] Schmidt, Jens M “A Simple Test on 2-Vertex- and 2-Edge-Connectivity”, Information Processing Letters, 113 (7): 241–244 [doi:10.2307/2303897](#)
- [Sch2015] George Schaeffer. *Hecke stability and weight 1 modular forms*. Math. Z. 281:159–191, 2015. [doi:10.1007/s00209-015-1477-9](#)
- [Sco1985] R. Scott, *Wide-open encryption design offers flexible implementations*; in Cryptologia, (1985), pp. 75-91.
- [Seb1978] J. Seberry. *On Skew Hadamard Matrices*, Ars Combinatoria 6 (1978): 255-276.

- [Seb2017] J. Seberry, *Orthogonal designs: Hadamard matrices, quadratic forms and algebras*. Springer 2017. doi:10.1007/978-3-319-59032-5
- [SE1962] N. E. Steenrod and D. B. A. Epstein, Cohomology operations, Ann. of Math. Stud. 50 (Princeton University Press, 1962).
- [Ser1972] Jean-Pierre Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), no. 4, 259–331.
- [Ser1987] Jean-Pierre Serre, Sur les représentations modulaires de degré 2 de  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ . Duke Math. J. 54 (1987), no. 1, 179–230.
- [Ser1985] C. Series. The geometry of Markoff numbers. The Mathematical Intelligencer, 7(3):20–29, 1985.
- [Ser1992] J.-P. Serre : *Lie Algebras and Lie Groups*, 2nd ed., Springer (Berlin) (1992); doi:10.1007/978-3-540-70634-2
- [Ser2010] F. Sergeraert, *Triangulations of complex projective spaces* in Scientific contributions in honor of Mirian Andrés Gómez, pp 507-519, Univ. La Rioja Serv. Publ., Logroño (2010).
- [Sey1981] P. D. Seymour, Nowhere-zero 6-flows, J. Comb. Theory Ser B, 30 (1981), 130-135. doi:10.1016/0095-8956(81)90058-7
- [SH1995] C. P. Schnorr and H. H. Hörner. *Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction*. Advances in Cryptology - EUROCRYPT '95. LNCS Volume 921, 1995, pp 1-12.
- [SH1995b] Bernd Sturmfels, Serkan Hosten: GRIN: An implementation of Grobner bases for integer programming, in “Integer Programming and Combinatorial Optimization”, [E. Balas and J. Clausen, eds.], Proceedings of the IV. IPCO Conference (Copenhagen, May 1995), Springer Lecture Notes in Computer Science 920 (1995) 267-276.
- [Sha1997] Ron Shamir, *Advanced Topics in Graph Algorithms*, Course material, 1997, <http://www.cs.tau.ac.il/~rshamir/atga/atga.html>
- [SHET2018] O. Seker, P. Heggernes, T. Ekim, and Z. Caner Taskin. *Generation of random chordal graphs using subtrees of a tree*, arXiv 1810.13326v1.
- [Shi2002] M. Shimozono *Affine type A crystal structure on tensor products of rectangles, Demazure characters, and nilpotent varieties*, J. Algebraic Combin. **15** (2002). no. 2. 151-187. arXiv math.QA/9804039.
- [Shim2016] Shimada, Ichiro, *Connected components of the moduli of elliptic K3 surfaces*, arXiv 1610.04706.
- [Shi1971] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan and Princeton University Press, 1971.
- [Sho1999] Victor Shoup: *Efficient computation of minimal polynomials in algebraic extensions of finite fields*. In ISSAC '99, pp. 53–58. ACM, 1999. doi:10.1145/309831.309859, <https://shoup.net/papers/mpol.pdf>
- [Shr2004] S. Shreve, *Stochastic Calculus for Finance II: Continuous-Time Models*. New York: Springer, 2004
- [SIHMAS2011] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, *Piccolo: An ultra-lightweight block-cipher*; in CHES, (2011), pp. 342-457.
- [Sil1988] Joseph H. Silverman, Computing heights on elliptic curves. Mathematics of Computation, Vol. 51, No. 183 (Jul., 1988), pp. 339-358.
- [Sil1994] Joseph H. Silverman, Advanced topics in the arithmetic of elliptic curves. GTM 151, Springer-Verlag, New York, 1994.
- [Sil2007] Joseph H. Silverman. The Arithmetic of Dynamics Systems. GTM 241, Springer-Verlag, New York, 2007.
- [Sil2009] Joseph H. Silverman, The Arithmetic of Elliptic Curves. Second edition. Graduate Texts in Mathematics, 106. Springer, 2009.

- [Sim2004] Aron Simis, “Cremona transformations and some related algebras”. *Journal of Algebra* 280.1 (2004), 162-179.
- [SK2011] J. Spreer and W. Kühnel, “Combinatorial properties of the K3 surface: Simplicial blowups and slicings”, *Experimental Mathematics*, Volume 20, Issue 2, 2011.
- [SKWWHF1998] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, *Twofish: A 128-bit block cipher*; in AES Submission, (1998).
- [Sky2003] Brian Skyrms. *The stag hunt and the evolution of social structure*. Cambridge University Press, 2003.
- [SLB2008] Shoham, Yoav, and Kevin Leyton-Brown. *Multiagent systems: Algorithmic, game-theoretic, and logical foundations*. Cambridge University Press, 2008.
- [SloaHada] N.J.A. Sloane’s Library of Hadamard Matrices, at <https://neilsloane.com/hadamard/>
- [SMC2006] G.B. Sherwood, S.S. Martirosyan, and C.J. Colbourn, “Covering arrays of higher strength from permutation vectors”. *J. Combin. Designs*, 14 (2006) pp. 202-213.
- [SMMK2013] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, *TWINE: A lightweight block cipher for multiple platforms*; in SAC, (2012), pp. 338-354.
- [SMS2019] S. Sarkar, K. Mandal, D. Saha “Sycon v1.0 Submission to LightweightCryptographic Standards” <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/sycon-spec.pdf>
- [Sor1984] A. Sorkin, *LUCIFER: a cryptographic algorithm*; in *Cryptologia*, 8(1), pp. 22–35, 1984.
- [Sma1995] N.P. Smart, *The Solution of Triangularly Connected Decomposable Form Equations*. *Math. Comp.* 64 (1995), 819-840. doi:10.1090/S0025-5718-1995-1277771-4.
- [Sma1998] N.P. Smart, *The algorithmic resolution of Diophantine equations*, Number 41 in Student Texts. London Mathematical Society, 1998.
- [Sma1999] N.P. Smart, *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, *Journal of Cryptology*. 12. 193-196. 1999. doi:10.1007/s001459900052.
- [Smi2023] D. Smith, J. S. Myers, C. S. Kaplan and C. Goodman-Strauss, *An aperiodic monotile*, [arXiv 2303.10798](https://arxiv.org/abs/2303.10798)
- [SP2010] Fernando Solano and Michal Pioro, *Lightpath Reconfiguration in WDM networks*, *IEEE/OSA Journal of Optical Communication and Networking* 2(12):1010-1021, 2010. doi:10.1364/JOCN.2.001010.
- [Sot2011] M. A. Soto Gomez. 2011. *Quelques propriétés topologiques des graphes et applications à internet et aux réseaux*. Ph.D. Dissertation. Univ. Paris Diderot (Paris 7). <https://tel.archives-ouvertes.fr/tel-01259904/document>
- [Spa1966] Edwin H. Spanier, *Algebraic Topology*, Springer-Verlag New York, 1966. doi:10.1007/978-1-4684-9322-1, ISBN 978-1-4684-9322-1.
- [Spe1975] E. Spence. *Hadamard matrices from relative difference sets*, *Journal of Combinatorial Theory, Series A* 19(3) (1975): 287-300. doi:10.1016/0097-3165(75)90054-0
- [Spe1975b] E. Spence. *Skew-Hadamard Matrices of the Goethals-Seidel Type*, *Canadian Journal of Mathematics* 27(3) (1975): 555-560. doi:10.4153/cjm-1975-066-9
- [Spe1977] E. Spence. *Skew-Hadamard matrices of order  $2(q + 1)$* , *Discrete Mathematics* 18(1) (1977): 79-85. doi:10.1016/0012-365X(77)90009-7
- [Spe2013] D. Speyer, *An infinitely generated upper cluster algebra*, [arXiv 1305.6867](https://arxiv.org/abs/1305.6867).
- [SPGQ2006] F.-X. Standaert, G. Piret, N. Gershenfeld, and J.-J. Quisquater, *Sea: A scalable encryption algorithm for small embedded applications*; in CARDIS, (2006), pp. 222-236.
- [SPRQL2004] F.-X. Standaert, G. Piret, G. Rouvroy, J.-J. Quisquater, and J.-D. Legat, *ICEBERG: An involutonal cipher efficient for block encryption in reconfigurable hardware*; in FSE, (2004), pp. 279-299.

- [Squ1984] C. C. Squier. *The Burau representation is unitary*. Proceedings of the American Mathematical Society, Volume 90. Number 2, February 1984, pp. 199-202.
- [Sq1998] Matthew B. Squire. *Generating the acyclic orientations of a graph*. Journal of Algorithms, Volume 26, Issue 2, Pages 275 - 290, 1998. (<https://doi.org/10.1006/jagm.1997.0891>)
- [SS1983] Shorey and Stewart. "On the Diophantine equation  $ax^{2t} + bx^ty + cy^2 = d$  and pure powers in recurrence sequences." *Mathematica Scandinavica*, 1983.
- [SS1990] Bruce E. Sagan and Richard P. Stanley. *Robinson-Schensted algorithms for skew tableaux*. Journal of Combinatorial Theory, Series A 55.2 (1990) pp. 161-193.
- [SS1992] M. A. Shtan'ko and M. I. Shtogrin, "Embedding cubic manifolds and complexes into a cubic lattice", *Uspekhi Mat. Nauk* 47 (1992), 219-220.
- [SS2008] Geoffrey Scott and Christopher Storm, *The coefficients of the Ihara zeta function*, *Involve*, Vol. 1 (2008), No. 2, 217-233, doi:10.2140/involve.2008.1.217 (<http://msp.org/involve/2008/1-2/involve-v1-n2-p08-p.pdf>)
- [SS2015] Anne Schilling and Travis Scrimshaw. *Crystal structure on rigged configurations and the filling map*. *Electron. J. Combin.*, **22(1)** (2015) #P1.73. [arXiv 1409.2920](https://arxiv.org/abs/1409.2920).
- [SS2015II] Ben Salisbury and Travis Scrimshaw. *A rigged configuration model for  $B(\infty)$* . *J. Combin. Theory Ser. A*, **133** (2015) pp. 29-75. [arXiv 1404.6539](https://arxiv.org/abs/1404.6539).
- [SS2016] Alberto Seeger and David Sossa. Critical angles between two convex cones I. General theory. *TOP*, 24(1):44-65, 2016. doi:10.1007/s11750-015-0375-y.
- [SS2017] Ben Salisbury and Travis Scrimshaw. *Rigged configurations for all symmetrizable types*. *Electron. J. Combin.*, **24(1)** (2017) #P1.30. [arXiv 1509.07833](https://arxiv.org/abs/1509.07833).
- [SS2018] Ben Salisbury and Travis Scrimshaw. *Description of crystals for generalized Kac–Moody algebras using rigged configurations*. *Sém. Lothar. Combin.* **80B** (2018), Art. #20, 12 pp.
- [SSAMI2007] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, *The 128-bit blockcipher CLEFIA (extended abstract)*; in *FSE*, (2007), pp. 181-195.
- [ST1993] P. D. Seymour and Robin Thomas, *Graph searching and a min-max theorem for tree-width*, *J. Comb. Theory Ser. B* 58, 1 (May 1993), 22-33. doi:10.1006/jctb.1993.1027.
- [ST1994] Simon, K. and Trunz, P., *A cleanup on transitive orientation*, *Orders, Algorithms, and Applications*, 1994, doi:10.1007/BFb0019427, <ftp://ftp.inf.ethz.ch/doc/papers/ti/ga/ST94.ps.gz>
- [ST2010] Einar Steingrímsson and Bridget Tenner. *The Moebius Function of the Permutation Pattern Poset*, *Journal of Combinatorics* 1 (2010), 39-52
- [ST2011] A. Schilling, P. Tingley. *Demazure crystals, Kirillov-Reshetikhin crystals, and the energy function*. *Electronic Journal of Combinatorics*. **19(2)**. 2012. [arXiv 1104.2359](https://arxiv.org/abs/1104.2359)
- [Sta1979] Richard Stanley. *Invariants of Finite Groups and their applications to combinatorics*. *Bulletin (New Series) of the American Mathematical Society*, **\*1\*** no.3 (1979), 457-511.
- [St1986] Richard Stanley. *Two poset polytopes*, *Discrete Comput. Geom.* (1986), doi:10.1007/BF02187680
- [Stap2011] Alan Stapledon. *Equivariant Ehrhart Theory*. *Advances in Mathematics* 226 (2011), no. 4, 3622-3654
- [Sta1973] H. M. Stark, *Class-Numbers of Complex Quadratic Fields*. In: Kuijk W. (eds) *Modular Functions of One Variable I*. *Lecture Notes in Mathematics*, vol 320. (1973), Springer, Berlin, Heidelberg
- [Sta1993] Stahl, Saul: *The Poincaré Half-plane: A Gateway to Modern Geometry* Jones & Bartlett Learning, 1993. ISBN 086720298X, 9780867202984
- [Sta1995] R. P. Stanley, *A symmetric function generalization of the chromatic polynomial of a graph*, *Adv. Math.*, **\*111\*** no.1 (1995), 166-194. doi:10.1006/aima.1995.1020.

- [Sta2002] Richard P. Stanley, *The rank and minimal border strip decompositions of a skew partition*, J. Combin. Theory Ser. A 100 (2002), pp. 349-375. [arXiv math/0109092v1](#).
- [Sta2007] Stanley, Richard: *Hyperplane Arrangements*, Geometric Combinatorics (E. Miller, V. Reiner, and B. Sturmfels, eds.), IAS/Park City Mathematics Series, vol. 13, American Mathematical Society, Providence, RI, 2007, pp. 389-496.
- [EnumComb1] Stanley, Richard P. *Enumerative Combinatorics, volume 1*, Second Edition, Cambridge University Press (2011). <http://math.mit.edu/~rstan/ec/ec1/>
- [EnumComb2] Stanley, Richard P. *Enumerative Combinatorics, volume 2*. Cambridge University Press (1999). <http://math.mit.edu/~rstan/ec/>
- [Star2011] Š. Starosta, *On Theta-palindromic Richness*, Theoret. Comp. Sci. 412 (2011) 1111–1121
- [St2011b] W. Stein, *Toward a Generalization of the Gross-Zagier Conjecture*, Int Math Res Notices (2011), [doi:10.1093/imrn/rnq075](#)
- [St2007] W. Stein. *Modular Forms, a Computational Approach*. With an appendix by Paul E. Gunnells. AMS Graduate Studies in Mathematics, Volume 79, 2007. [doi:10.1090/gsm/079](#)
- [Sei2002] T. R. Seifullin, *Computation of determinants, adjoint matrices, and characteristic polynomials without division* [doi:10.1023/A:1021878507303](#)
- [ST1981] J. J. Seidel and D. E. Taylor, *Two-graphs, a second survey*. Algebraic methods in graph theory, Vol. I, II (Szeged, 1978), pp. 689–711, Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam-New York, 1981.
- [Stan2009] Richard Stanley, *Promotion and evacuation*, Electron. J. Combin. 16 (2009), no. 2, Special volume in honor of Anders Björner, Research Paper 9, 24 pp.
- [Ste1996] John R. Stembridge, *On the fully commutative elements of Coxeter groups*, Journal of Algebraic Combinatorics, 5, pp. 355-385
- [Ste1998] John R. Stembridge, *The enumeration of the fully commutative elements of Coxeter groups*, Journal of Algebraic Combinatorics, 7, pp. 291-320.
- [Ste2003] John R. Stembridge, *A local characterization of simply-laced crystals*, Transactions of the American Mathematical Society, Vol. 355, No. 12 (Dec., 2003), pp. 4807–4823
- [Stich2009] Stichtenoth, Henning. *Algebraic function fields and codes*. Vol. 254. Springer Science & Business Media, 2009.
- [Sti2006] Douglas R. Stinson. *Cryptography: Theory and Practice*. 3rd edition, Chapman & Hall/CRC, 2006.
- [Sto1998] A. Storjohann, An  $O(n^3)$  algorithm for Frobenius normal form. Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC'98), ACM Press, 1998, pp. 101-104.
- [Sto2000] A. Storjohann, Algorithms for Matrix Canonical Forms. PhD Thesis. Department of Computer Science, Swiss Federal Institute of Technology – ETH, 2000.
- [Sto2011] A. Storjohann, Email Communication. 30 May 2011.
- [Str1969] Volker Strassen. Gaussian elimination is not optimal. Numerische Mathematik, 13:354-356, 1969.
- [Striker2011] J. Striker. *A unifying poset perspective on alternating sign matrices, plane partitions, Catalan objects, tournaments, and tableaux*, Advances in Applied Mathematics 46 (2011), no. 4, 583-609. [arXiv 1408.5391](#)
- [Str2015] Jessica Striker. *The toggle group, homomesy, and the Razumov-Stroganov correspondence*, Electron. J. Combin. 22 (2015) no. 2 [arXiv 1503.08898](#)
- [Stu1987] J. Sturm, On the congruence of modular forms, Number theory (New York, 1984-1985), Springer, Berlin, 1987, pp. 275-280.
- [Stu1993] B. Sturmfels, Algorithms in invariant theory, Springer-Verlag, 1993.

- [Stu1995] Bernd Sturmfels, *Grobner Bases and Convex Polytopes* AMS University Lecture Series Vol. 8 (01 December 1995)
- [Stu1997] Bernd Sturmfels, Equations defining toric varieties, *Algebraic Geometry - Santa Cruz 1995*, Proc. Sympos. Pure Math., 62, Part 2, Amer. Math. Soc., Providence, RI, 1997, pp. 437-449.
- [Stu2008] C. Stump – More bijective Catalan combinatorics on permutations and on colored permutations, Preprint. [arXiv 0808.2822](https://arxiv.org/abs/0808.2822).
- [STW2013] J. Schejbal, E. Tews, and J. Walde, *Reverse engineering of chiasmus from gstool*; in 30c3, (2013).
- [STW2016] C. Stump, H. Thomas, N. Williams. *Cataland II*, in preparation, 2016.
- [STW2018] Christian Stump, Hugh Thomas and Nathan Williams, *Cataland: why the fuss?*, 2018. [arXiv 1503.00710](https://arxiv.org/abs/1503.00710)
- [SU2014] Christopher Skinner and Eric Urban, The Iwasawa main conjectures for GL2. *Invent. Math.* 195 (2014), no. 1, 1-277.
- [sudoku:escargot] “Al Escargot”, due to Arto Inkala, <http://timemaker.blogspot.com/2006/12/ai-escargot-vwv.html>
- [sudoku:norvig] Perter Norvig, “Solving Every Sudoku Puzzle”, <http://norvig.com/sudoku.html>
- [sudoku:royle] Gordon Royle, “Minimum Sudoku”, <http://people.csse.uwa.edu.au/gordon/sudokumin.php>
- [sudoku:top95] “95 Hard Puzzles”, <http://magictour.free.fr/top95>, or <http://norvig.com/top95.txt>
- [sudoku:wikipedia] “Near worst case”, [Wikipedia article Algorithmics\\_of\\_sudoku](#)
- [Sulzgr2017] Robin Sulzgruber, *Inserting rim-hooks into reverse plane partitions*, [arXiv 1710.09695v1](https://arxiv.org/abs/1710.09695v1).
- [Sun1994] Sheila Sundaram, *The Homology Representations of the Symmetric Group on Cohen-Macaulay Subposets of the Partition Lattice*, *Advances in Mathematics*, 1994 (104), 225-296.
- [Sun2010] Yi Sun. *The McKay correspondence*. [http://www.math.miami.edu/~armstrong/686sp13/McKay\\_Yi\\_Sun.pdf](http://www.math.miami.edu/~armstrong/686sp13/McKay_Yi_Sun.pdf) 2010
- [Sut2002] Ruedi Suter. *Young’s Lattice and Dihedral Symmetries*. *Europ. J. Combinatorics* (2002) 23, 233–238. <http://www.sciencedirect.com/science/article/pii/S0195669801905414>
- [Sut2012] Sutherland. A local-global principle for rational isogenies of prime degree. *Journal de Theorie des Nombres de Bordeaux*, 2012.
- [Suth2007] Andrew V. Sutherland, *Order Computations in Generic Groups*. PhD Thesis, Massachusetts Institute of Technology, June 2007. <https://math.mit.edu/~drew/sutherland-phd.pdf>
- [Suth2008] Andrew V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*. *Mathematics of Computation* **80** (2011), pp. 477-500. [arXiv 0809.3413v3](https://arxiv.org/abs/0809.3413v3).
- [RouSuthZur2022] Jeremy Rouse, Andrew V. Sutherland, David Zureick-Brown. *ℓ-adic images of Galois for elliptic curves over  $\mathbb{Q}$*  (and an appendix with John Voight). *Forum of Mathematics, Sigma* , Volume 10 , 2022. :doi: 10.1017/fms.2022.38. [arXiv 2106.11141](https://arxiv.org/abs/2106.11141).
- [Ryom2015] Steen Ryom-Hansen. *Projective modules for the symmetric group and Young’s seminormal form*. *J. Algebra* **439** (2015) pp. 515-541.
- [SV1970] H. Schneider and M. Vidyasagar. Cross-positive matrices. *SIAM Journal on Numerical Analysis*, 7:508-519, 1970.
- [SV2000] J. Stern and S. Vaudenay, *CS-Cipher*; in First Open NESSIE Workshop, (2000).
- [SV2013] Silliman and Vogt. “Powers in Lucas Sequences via Galois Representations.” *Proceedings of the American Mathematical Society*, 2013. [arXiv 1307.5078v2](https://arxiv.org/abs/1307.5078v2)
- [SW1999] Steger, A. and Wormald, N. *Generating random regular graphs quickly*. *Prob. and Comp.* 8 (1999), pp 377-396. doi:10.1017/S0963548399003867.

- [SW2002] William Stein and Mark Watkins, *A database of elliptic curves—first report*. In *Algorithmic number theory (ANTS V)*, Sydney, 2002, Lecture Notes in Computer Science 2369, Springer, 2002, p267–275. <http://modular.math.washington.edu/papers/stein-watkins/>
- [SW2012] John Shreshian and Michelle Wachs. *Chromatic quasisymmetric functions and Hessenberg varieties*. Configuration Spaces. CRM Series. Scuola Normale Superiore. (2012) pp. 433-460. doi:10.1007/978-88-7642-431-1\_20. <http://www.math.miami.edu/~wachs/papers/chrom.pdf>
- [SW2013] W. Stein and C. Wuthrich, Algorithms for the Arithmetic of Elliptic Curves using Iwasawa Theory Mathematics of Computation 82 (2013), 1757-1792.
- [St1922] Ernst Steinitz, *Polyeder und Raumeinteilungen*. In *Encyclopädie der Mathematischen Wissenschaften*, Franz Meyer and Hand Mohrmann, eds., volume 3, *Geometrie, erster Teil, zweite Hälfte*, pp. 1–139, Teubner, Leipzig, 1922
- [SU2009] J. Smillie and C. Ulcigrai. Symbolic coding for linear trajectories in the regular octagon, [arXiv 0905.0871](https://arxiv.org/abs/0905.0871), 2009.
- [Swe1969] Moss Sweedler. Hopf algebras. W.A. Benjamin, Math Lec Note Ser., 1969.
- [SWJ2008] Fatima Shaheen, Michael Wooldridge, and Nicholas Jennings. *A linear approximation method for the Shapley value*. Artificial Intelligence 172.14 (2008): 1673-1699.
- [SWW1972] A. Street, W. Wallis, J. Wallis, Combinatorics: Room squares, sum-free sets, Hadamard matrices. Lecture notes in Mathematics 292 (1972).
- [Sys1987] Maciej M. SysŁo, *Minimizing the jump number for partially-ordered sets: a graph-theoretic approach, II*. Discrete Mathematics, Volume 63, Issues 2-3, 1987, Pages 279-295.
- [SYTYTYT2002] T. Shimoyama, H. Yanami, K. Yokoyama, M. Takenaka, K. Itoh, J. Yajima, N. Torii, and H. Tanaka, *The block cipher SC2000*; in FSE, (2001), pp. 312-327.
- [Sz1969] G. Szekeres, Tournaments and Hadamard matrices, Enseignement Math. (2) 15(1969), 269-278
- [SZ1994] Bruno Salvy and Paul Zimmermann. Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. ACM transactions on mathematical software, 20.2:163-177, 1994.
- [SZ2001] M. Shimozone, M. Zabrocki, Hall-Littlewood vertex operators and generalized Kostka polynomials. Adv. Math. 158 (2001), no. 1, 66-85.
- [Sze1971] G. Szekeres. *Cyclotomy and complementary difference sets*, Acta Arithmetica 18 (1971): 349-353. doi:10.4064/aa-18-1-349-353
- [Sze1988] G. Szekeres. *A note on skew type orthogonal  $\pm 1$  matrices*, Combinatorics, Colloquia Mathematica Societatis, Janos Bolyai, 52 (1988): 489-498.
- [Tak1999] Kisao Takeuchi, Totally real algebraic number fields of degree 9 with small discriminant, Saitama Math. J. 17 (1999), 63–85 (2000).
- [Tam1962] Dov Tamari. *The algebra of bracketings and their enumeration*. Nieuw Arch. Wisk. (1962).
- [Tar1976] Robert E. Tarjan, *Edge-disjoint spanning trees and depth-first search*, Acta Informatica 6 (2), 1976, 171-185, doi:10.1007/BF00268499.
- [Tarjan72] R.E. Tarjan. Depth-First Search and Linear Graph Algorithms. SIAM J. Comput. 1(2): 146-160 (1972).
- [Tate1975] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil. Modular functions of one variable*, IV, pp. 33–52. Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.
- [Tate1966] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*. Seminaire Bourbaki, Vol. 9, Exp. No. 306, 1966.
- [Tate1966b] John Tate, *Endomorphisms of Abelian Varieties over Finite Fields*. Inventiones Math. 2, 134-144, 1966.
- [TB1997] Lloyd N. Trefethen and David Bau III, *Numerical Linear Algebra*, SIAM, Philadelphia, 1997.

- [TCHP2008] Marc Tedder, Derek Corneil, Michel Habib and Christophe Paul, *Simple, linear-time modular decomposition*, 2008. [arXiv 0710.3901](#).
- [Tee1997] Tee, Garry J. “Continuous branches of inverses of the 12 Jacobi elliptic functions for real argument”. 1997. <https://researchspace.auckland.ac.nz/bitstream/handle/2292/5042/390.pdf>.
- [Ter2011] Audrey Terras, *Zeta functions of graphs: a stroll through the garden*, Cambridge Studies in Advanced Mathematics, Vol. 128, 2011.
- [Terwilliger2011] Paul Terwilliger. *The universal Askey-Wilson algebra*. SIGMA **7** (2011), 069, 24 pages. [arXiv 1104.2813](#).
- [Ter2021] Paul Terwilliger. *The alternating central extension of the  $q^* - \text{Onsager algebra}$* . Preprint, [arxiv : 2103.03028](#) (2021).
- [Ter2021b] Paul Terwilliger. *The alternating central extension of the Onsager Lie algebra*. Preprint, [arXiv 2104.08106](#) (2021).
- [TP1994] J. Thas, S. Payne, *Spreads and ovoids in finite generalized quadrangles*. Geometriae Dedicata, Vol. 52, pp. 227-253, 1994.
- [Tho2010] T. Thongjunthug, Computing a lower bound for the canonical height on elliptic curves over number fields, Math. Comp. 79 (2010), pages 2431-2449.
- [Tho2011] Anders Thorup. *ON THE INVARIANTS OF THE SPLITTING ALGEBRA*, 2011, [arXiv 1105.4478](#)
- [TIDES] A. Abad, R. Barrio, F. Blesa, M. Rodriguez. TIDES tutorial: Integrating ODEs by using the Taylor Series Method (<http://www.unizar.es/acz/05Publicaciones/Monografias/MonografiasPublicadas/Monografia36/IndMonogr36.htm>)
- [TingleyLN] Peter Tingley. *Explicit  $\widehat{\mathfrak{sl}}_n$  crystal maps between cylindric plane partitions, multi-partitions, and multi-segments*. Lecture notes. [http://webpages.math.luc.edu/~ptingley/lecturenotes/explicit\\_bijections.pdf](http://webpages.math.luc.edu/~ptingley/lecturenotes/explicit_bijections.pdf)
- [Tingley2007] Peter Tingley. *Three combinatorial models for  $\widehat{\mathfrak{sl}}_n$  crystals, with applications to cylindric plane partitions*. International Mathematics Research Notices. (2007). [arXiv 0702062v3](#).
- [TK2013] F. W. Takes and W. A. Kosters. *Computing the eccentricity distribution of large graphs*. Algorithms 6:100-118 (2013). doi:10.3390/a6010100.
- [TOPCOM] J. Rambau, TOPCOM <<http://www.rambau.wm.uni-bayreuth.de/TOPCOM/>>.
- [TT2023] Tan Nhat Tran and Shuheì Tsujie. *A type B analog of Ish arrangement*. Preprint, [arXiv 2304.12022](#). (2023)
- [TTWL2009] Trebst, Troyer, Wang and Ludwig, A short introduction to Fibonacci anyon models, [arXiv 0902.3275](#).
- [Tur1974] R. J. Turyn *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings*. Journal of Combinatorial Theory, Series A 16.3 (1974), pp 313–333. doi:10.1016/0097-3165(74)90056-9
- [TVY2020] N. V. Tsilevich, A. M. Vershik, and S. Yuzvinsky. *The intrinsic hyperplane arrangement in an arbitrary irreducible representation of the symmetric group*, Arnold Math. J. **6** no. 2 (2020) pp. 173-187.
- [TW1980] A.D. Thomas and G.V. Wood, Group Tables (Exeter: Shiva Publishing, 1980)
- [TY1984] Robert Endre Tarjan, Mihalis Yannakakis. *Simple linear-time algorithms to test chordality of graphs, test acyclicity of hypergraphs, and selectively reduce acyclic hypergraphs*. SIAM Journal on Computing, 13:566-579, 1984. doi:10.1137/0213035
- [TY2009] Hugh Thomas and Alexander Yong, *A jeu de taquin theory for increasing tableaux, with applications to K-theoretic Schubert calculus*, Algebra and Number Theory 3 (2009), 121-148, <https://projecteuclid.org/euclid.ant/1513797353>

- [UDCIKMP2011] M. Ullrich, C. De Canniere, S. Indestege, Ö. Küçük, N. Mouha, and B. Preenel, *Finding Optimal Bitsliced Implementations of 4 x 4-bit S-boxes*; in SKEW, (2011).
- [Ukko1995] E. Ukkonen, *On-line construction of suffix trees*, Algorithmica, 1995, volume **14**, number 3, pages 249–260.
- [UNITTEST] unittest – Unit testing framework – <https://docs.python.org/library/unittest.html>
- [U.S1998] U.S. Department Of Commerce/National Institute of Standards and Technology, *Skipjack and KEA algorithms specifications*, v2.0, (1998).
- [U.S1999] U.S. Department Of Commerce/National Institute of Standards and Technology, *Data Encryption Standard*, (1999). <https://csrc.nist.gov/CSRC/media/Publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf>
- [Vai1994] I. Vaisman, *Lectures on the Geometry of Poisson Manifolds*, Springer Basel AG (Basel) (1994); doi:10.1007/978-3-0348-8495-2
- [Var1984] V. S. Varadarajan. *Lie groups, Lie algebras, and their representations*. Reprint of the 1974 edition. Graduate Texts in Mathematics, 102. Springer-Verlag, New York, 1984.
- [Vat2008] D. Vatne, *The mutation class of  $D_n$  quivers*, arXiv 0810.4789v1.
- [Vazirani2002] Monica Vazirani. *Parameterizing Hecke algebra modules: Bernstein-Zelevinsky multisegments, Kleshchev multipartitions, and crystal graphs*. Transform. Groups **7** (2002). pp. 267-303. arXiv 0107052v1, doi:10.1007/s00031-002-0014-1.
- [VB1996] E. Viterbo, E. Biglieri. *Computing the Voronoi Cell of a Lattice: The Diamond-Cutting Algorithm*. IEEE Transactions on Information Theory, 1996.
- [VBB1992] Marc Van Barel and Adhemar Bultheel. “A general module theoretic framework for vector M-Padé and matrix rational interpolation.” Numer. Algorithms, 3:451-462, 1992. doi:10.1007/BF02141952
- [VDKT2016] E. R. van Dam, J. H. Koolen, H. Tanaka, *Distance Regular graphs* The Electronic Journal of Combinatorics. 2016
- [Ver] Helena Verrill, “Fundamental domain drawer”, Java program, <http://www.math.lsu.edu/~verrill/>
- [Vie1979] Gérard Viennot. *Permutations ayant une forme donnée*. Discrete Mathematics 26.3 (1979): 279-284.
- [Vie1983] Xavier G. Viennot. *Maximal chains of subwords and up-down sequences of permutations*. Journal of Combinatorial Theory, Series A Volume 34, (1983), pp. 1-14.
- [VJ2004] S. Vaudenay and P. Junod, *Device and method for encrypting and decrypting a block of data Fox, a New Family of Block Ciphers*, (2004).
- [VO2005] A. M. Vershik, A. Yu. Okounkov. *A New Approach to the Representation Theory of the Symmetric Groups*. 2, 2005. arXiv math/0503040v3.
- [Voe2003] V. Voevodsky, Reduced power operations in motivic cohomology, Publ. Math. Inst. Hautes Études Sci. No. 98 (2003), 1-57.
- [Voi2008] John Voight, Enumeration of totally real number fields of bounded root discriminant, Lect. Notes in Comp. Sci. 5011 (2008).
- [Voi2012] J. Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms, to appear.
- [Voi2021] J. Voight. Quaternion Algebras. Graduate Texts in Mathematics 288. Springer Cham, 2021.
- [VS06] G.D. Villa Salvador. Topics in the Theory of Algebraic Function Fields. Birkhäuser, 2006.
- [VW1994] Leonard Van Wyk. *Graph groups are biautomatic*. J. Pure Appl. Alg. **94** (1994). no. 3, 341-352.
- [Wac2003] Wachs, “Topology of Matching, Chessboard and General Bounded Degree Graph Complexes” (Algebra Universalis Special Issue in Memory of Gian-Carlo Rota, Algebra Universalis, 49 (2003) 345-385)

- [Wal1960] C. T. C. Wall, “Generators and relations for the Steenrod algebra,” *Ann. of Math. (2)* **72** (1960), 429-444.
- [Wal1970] David W. Walkup, “The lower bound conjecture for 3- and 4-manifolds,” *Acta Math.* 125 (1970), 75-107.
- [Wal1970b] J. Wallis.  $(v, k, \lambda)$  Configurations and Hadamard matrices, *Journal of the Australian Mathematical Society* 11(3) (1970): 297-309. doi:10.1017/S1446788700006674
- [Wal2001] Timothy Walsh, *Gray codes for involutions*, *J. Combin. Math. Combin. Comput.* **36** (2001), 95-118. [http://www.info2.uqam.ca/~walsh\\_t/papers/Involutions%20paper.pdf](http://www.info2.uqam.ca/~walsh_t/papers/Involutions%20paper.pdf)
- [Walton1990] Mark A. Walton. *Fusion rules in Wess-Zumino-Witten models*. *Nuclear Phys. B* **340** (1990).
- [Wam1999] van Wamelen, Paul. *Examples of genus two CM curves defined over the rationals*. *Math. Comp.* 68 (1999), no. 225, 307–320.
- [Wam1999b] P. van Wamelen, Pari-GP code, section “thecubic” <https://www.math.lsu.edu/~wamelen/Genus2/FindCurve/igusa2curve.gp>
- [Wan1998] Daqing Wan, “Dimension variation of classical and p-adic modular forms”, *Invent. Math.* 133, (1998) 449-463.
- [Wan2010] Zhenghan Wang. *Topological quantum computation*. Providence, RI: American Mathematical Society (AMS), 2010. ISBN 978-0-8218-4930-9
- [Was1997] L. C. Washington, *Cyclotomic Fields*, Springer-Verlag, GTM volume 83, 1997.
- [Watkins] Mark Watkins, *Hypergeometric motives over  $\mathbb{Q}$  and their  $L$ -functions*, <http://magma.maths.usyd.edu.au/~watkins/papers/known.pdf>
- [Watkins2004] Mark Watkins. *Class numbers of imaginary quadratic fields*. *Math. Comp.* 73 (2004), 907-938. <https://www.ams.org/journals/mcom/2004-73-246/S0025-5718-03-01517-5/>
- [Wat2003] Joel Watson. *Strategy: an introduction to game theory*. WW Norton, 2002.
- [Wat2010] Watkins, David S. *Fundamentals of Matrix Computations*, Third Edition. Wiley, Hoboken, New Jersey, 2010.
- [WC2007] R.A. Walker II, and C.J. Colbourn, “Perfect Hash Families: Constructions and Existence”. *J. Math. Crypt.* 1 (2007), pp.125-150
- [Web2007] James Webb. *Game theory: decisions, interaction and Evolution*. Springer Science & Business Media, 2007.
- [WegSem2010] Elias Wegert and Gunter Semmler. *Phase plots of complex functions: a journey in illustration*. *Notices of the AMS*, 58: 768–780, 2010.
- [Weh1998] J. Wehler. *Hypersurfaces of the Flag Variety: Deformation Theory and the Theorems of Kodaira-Spencer, Torelli, Lefschetz, M. Noether, and Serre*. *Math. Z.* 198 (1988), 21-38.
- [WELLS] Elliot Wells. *Computing the Canonical Height of a Point in Projective Space*. [arXiv 1602.04920v1](https://arxiv.org/abs/1602.04920) (2016).
- [Wei1994] Charles A. Weibel, *An introduction to homological algebra*. Cambridge Studies in Advanced Math., vol. 38, Cambridge Univ. Press, 1994.
- [Wel1988] Dominic Welsh, *Codes and Cryptography*. Oxford Sciences Publications, 1988
- [Wer1998] Annette Werner, *Local heights on abelian varieties and rigid analytic uniformization*, *Doc. Math.* 3 (1998), 301-319.
- [Wes2017] Bruce Westbury. *Coboundary categories and local rules*, *The Electronic Journal of Combinatorics*, 25 (2018)
- [West2001] Douglas B. West. *Introduction to Graph Theory*. 2nd Edition, Prentice Hall, 2001, p. 150–151.
- [WFYTP2008] D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi, and B. Preneel, *A new keystream generator MUGI*; in *FSE*, (2002), pp. 179-194.

- [Whi1932] H. Whitney, *Congruent graphs and the connectivity of graphs*, American Journal of Mathematics, pages 150–168, 1932, [available on JSTOR](#)
- [Whi1971] A. Whiteman. *An infinite family of skew Hadamard matrices*, Pacific Journal of Mathematics 38(3) (1971): 817-822. doi:10.2140/pjm.1971.38.817
- [White2015] Noah White. *The monodromy of real Bethe vectors for the Gaudin model*. J. Combin. Algebra, **2** no. 3 (2018). pp. 259-300. arXiv 1511.04740.
- [Wich1997] Tim Wichmann. Der FGLM Algorithmus - verallgemeinert und implementiert in Singular Diploma Thesis (University of Kaiserslautern), 1997.
- [Wie2000] B. Wieland. *A large dihedral symmetry of the set of alternating sign matrices*. Electron. J. Combin. 7 (2000).
- [Wilson2008] Steve Wilson. *Rose Window Graphs*. Ars Mathematica Contemporanea 1(1):7-19, 2008. doi:10.26493/1855-3974.13.5bb
- [Wilson2016] A. T. Wilson. *An extension of MacMahon's Equidistribution Theorem to ordered multiset partitions*. Electron. J. Combin., **23** (1) (2016).
- [Wil2010] M. Willis. A direct way to find the right key of a semistandard Young tableau. arXiv 1110.6184v1.
- [Wil2013] Harold Williams. *Q-systems, factorization dynamics, and the twist automorphism*. Int. Math. Res. Not. (2015) no. 22, 12042–12069. doi:10.1093/imrn/rnv057.
- [Wol1974] W. A. Wolovich. "Linear Multivariable Systems", Applied Mathematical Sciences (volume 11). Springer-Verlag New-York, 1974. doi:10.1007/978-1-4612-6392-0
- [Woo1998] R. M. W. Wood, "Problems in the Steenrod algebra," Bull. London Math. Soc. 30 (1998), no. 5, 449-517.
- [Wor1984] Worley, Dale Raymond, *A theory of shifted Young tableaux*. Dissertation, Massachusetts Institute of Technology, 1984.
- [WPNBBAtl] R. A. Wilson, R. A. Parker, S. Nickerson, J. N. Bray, T. Breuer, *AtlasRep, a GAP interface to the atlas of group representations*. <http://www.math.rwth-aachen.de/~Thomas.Breuer/atlasrep>
- [WP-Bessel] [Wikipedia article Bessel\\_function](#)
- [WP-Error] [Wikipedia article Error\\_function](#)
- [WP-Struve] [Wikipedia article Struve\\_function](#)
- [WROM1986] Wright, Robert Alan; Richmond, Bruce; Odlyzko, Andrew; McKay, Brendan D. *Constant time generation of free trees*. SIAM J. Comput. 15 (1986), no. 2, 540–548. doi:10.1137/0215039.
- [WSK1997] D. Wagner, B. Schneier, and J. Kelsey, *Cryptoanalysis of the cellular encryption algorithm*; in CRYPTO, (1997), pp. 526-537.
- [Wu2009] Hongjun Wu, *The Hash Function JH*; submitted to NIST, (2008), available at [http://www3.ntu.edu.sg/home/wuhj/research/jh/jh\\_round3.pdf](http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf)
- [Wu2004] Wuthrich, Christian. *On p-adic heights in families of elliptic curves*. Journal of the London Mathematical Society, 70(1), 23-40, (2004).
- [Wu2018] Wuthrich, Christian. *Numerical modular symbols for elliptic curves*. Math. Comp. 87 (2018), no. 313, 2393–2423.
- [Wall71] J. Wallis, *A skew-Hadamard matrix of order 92*, Bull. Aust. Math. Soc. **5** (1971), 203-204
- [WW1972] J. Wallis and A.L. Whiteman, *Some classes of Hadamard matrices with constant diagonal*, Bull. Austral. Math. Soc. **7** (1972), 233-249
- [WW1991] Michelle Wachs and Dennis White, *p, q-Stirling numbers and set partition statistics*, Journal of Combinatorial Theory, Series A 56.1 (1991): 27-46.

- [WW2005] Ralf-Philipp Weinmann and Kai Wirt, *Analysis of the DVB Common Scrambling Algorithm*; in IFIP TC-6 TC-11, (2005).
- [WZ2011] W. Wu and L. Zhang, *The LBlock family of block ciphers*; in ACNS, (2011), pp. 327-344.
- [WZY2015] Wenling Wu, Lei Zhang, and Xiaoli Yu, *The DBlock family of block ciphers*; in Science China Information Sciences, (2015), pp. 1-14.
- [XP1994] Deng Xiaotie, and Christos Papadimitriou. *On the complexity of cooperative solution concepts*. Mathematics of Operations Research 19.2 (1994): 257-266.
- [Yamada2007] Daisuke Yamada. *Scattering rule in soliton cellular automaton associated with crystal base of  $U_q(D_4^{(3)})$* . J. Math. Phys., **48** (4):043509, 28, (2007).
- [Yen1970] Yen, Jin Y. (1970). *An algorithm for finding shortest routes from all source nodes to a given destination in general networks*. Quarterly of Applied Mathematics. 27 (4): 526–530. doi:10.1090/qam/253822
- [Yip2018] Yip, Martha. “Rook placements and Jordan forms of upper-triangular nilpotent matrices.” Electronic J. Comb. 25(1) (2018) #P1.68. arXiv 1703.00057.
- [Yu2007] K. Yu, *p-adic logarithmic forms and group varieties. III*. Forum Math., 19(2):187–280, 2007.
- [Yu2022] Runze Yu. *linearity of generalized cactus groups*. Preprint, arXiv 2202.00860 (2022).
- [Yun1976] Yun, David YY. On square-free decomposition algorithms. In Proceedings of the third ACM symposium on Symbolic and algebraic computation, pp. 26-35. ACM, 1976.
- [Yuz1993] Sergey Yuzvinsky, “The first two obstructions to the freeness of arrangements”, Transactions of the American Mathematical Society, Vol. 335, **1** (1993) pp. 231–244.
- [YWHWXS2014] D. Ye, P. Wang, L. Hu, L. Wang, Y. Xie, S. Sun, and P. Wang, *Panda v1*; in CAESAR Competition, (2014).
- [YT2002] F. Yura and T. Tokihiro, *On a periodic soliton cellular automaton*, J. Phys. A: Math. Gen. **35** (2002) 3787-3801.
- [YYT2003] D. Yoshihara, F. Yura, and T. Tokihiro, *Fundamental cycle of a periodic box-ball system*, J. Phys. A: Math. Gen. **36** (2003) 99-121.
- [Zag2008] D. Zagier, *Elliptic Modular Forms and Their Applications*, In: Ranestad K. (eds) The 1-2-3 of Modular Forms. Universitext. Springer, Berlin, Heidelberg. (2008) doi:10.1007/978-3-540-74119-0\_1
- [ZBLRYV2015] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, *RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms*; in Science China Information Sciences, (2015), pp. 1-15.
- [ZBN1997] C. Zhu, R. H. Byrd and J. Nocedal. L-BFGS-B: Algorithm 778: L-BFGS-B, FORTRAN routines for large scale bound constrained optimization. ACM Transactions on Mathematical Software, Vol 23, Num. 4, pp.550–560, 1997.
- [ZC2005] Afra Zomorodian and Gunnar Carlsson “Computing Persistent Homology”, Discrete and Computational Geometry (2005) doi:10.1007/s00454-004-1146-y
- [ZDYBXJZ2019] W. Zhang, T. Ding, B. Yang, Z. Bao, Z. Xiang, F. Ji, X. Zhao. *KNOT: Algorithm Specifications and Supporting Document* <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/KNOT-spec.pdf>
- [Zei2011] Doron Zeilberger. *The C-finite ansatz*. The Ramanujan Journal (2011): 1-10. doi:10.1007/s11139-012-9406-6
- [Zha2019] Bin Zhang. *Fountain: A Lightweight Authenticated Cipher (v1)* <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/fountain-spec.pdf>

- [Zhedanov1991] A.S. Zhedanov. “Hidden symmetry” of the Askey–Wilson polynomials, Theoret. and Math. Phys. **89** (1991), 1146–1157. doi:10.1007/BF01015906
- [ZF2012] Jin-Xin Zhou and Yan-Quan Feng. *Cubic Vertex-Transitive Non-Cayley Graphs of Order 8p*. The Electronic Journal of Combinatorics, 19(1), P53, 2012. doi:10.37236/2087
- [Zie1959] N. Zierler. *Linear Recurring Sequences*. Journal of the Society for Industrial and Applied Mathematics 7(1) (1959): 31-48. doi:10.1137/0107003
- [Zie1998] G. M. Ziegler. *Shelling polyhedral 3-balls and 4-polytopes*. Discrete Comput. Geom. 19 (1998), 159-174. doi:10.1007/PL00009339
- [Zie2007] G. M. Ziegler. *Lectures on polytopes*, Volume 152 of Graduate Texts in Mathematics, 7th printing of 1st edition, Springer, 2007.
- [ZJRRS2019] M. R. Z’aba, N. Jamil, M. S. Rohmad, H. A. Rani, S. Shamsuddin *The CiliPadi Family of Lightweight Authenticated Encryption* <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/cilipadi-spec.pdf>
- [ZL2014] Wei Zhou and George Labahn. “Unimodular completion of polynomial matrices”. In Proceedings ISSAC 2014, pages 413-420. ACM, 2014. doi:10.1145/2608628.2608640
- [ZS1998] Antoine Zoghbi, Ivan Stojmenovic, *Fast Algorithms for Generating Integer Partitions*, Intern. J. Computer Math., Vol. 70., pp. 319–332, 1998. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.1287>
- [ZZ2005] Hechun Zhang and R. B. Zhang. *Dual canonical bases for the quantum special linear group and invariant subalgebras*. Lett. Math. Phys. **73** (2005), pp. 165-181. arXiv math/0509651, doi:10.1007/s11005-005-0015-9