Sage Reference Manual: References

Release 8.9

The Sage Development Team

Oct 02, 2019

CONTENTS

The references for Sage, sorted alphabetically by citation key.

REFERENCES:

BIBLIOGRAPHY

[AAGMRZ2019] M. Aagaard, R. AlTawy, G. Gong, K. Mandal, R. Rohit, N. Zidaric "WAGE: An Authenticated CipherSubmission 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

[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. Bogdanvo, O. Dunkelman, S. Huang, F. Regazzoni "Qameleonv. 1.0" https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/qameleon-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. Abdomnicai, 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 BlockCipher for Authenticated Encryption with AssociatedData" https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/LILLIPUT-AE-spec.pdf

[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.

[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)

[AHK2015] Karim Adiprasito, June Huh, and Eric Katz. *Hodge theory for combinatorial geometries*. arXiv 1511.02888.

[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

[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.

[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.

[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

[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.

[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.

[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. http://people.math.sfu.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. http://people.math.sfu.ca/~cbm/aands/page_435.htm

[AS-Struve] M. Abramowitz: 12. Struve Functions and Related Functions, in Abramowitz and Stegun: Handbook of Mathematical Functions. http://people.math.sfu.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 http://www.math.sfu.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

[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

[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.

[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.

[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.

[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

[Baz2011] Ivan Bazhov, On orbits of the automorphism group on a complete toric variety. Beitr Algebra Geom (2013) 54: 471, arXiv 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.

[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 AuthenticatedEncryption 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

[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.

[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-BeetleAuthenticated Encryption and Hash Family" https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/PHOTON-Beetle-spec.pdf

[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.

[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.

[BCN1989] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-Regular Graphs*, Springer, 1989.

[BdJ2008] Besser, Amnon, and Rob de Jeu. "Li^(p)-Service? An Algorithm for Computing p-Adic Polylogarithms." Mathematics of Computation (2008): 1105-1134.

[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

[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

[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.

[Bec1992] Bernhard Beckermann. "A reliable method for computing M-Padé approximants on arbitrary staircases". J. Comput. Appl. Math., 40(1):19-42, 1992. https://doi.org/10.1016/0377-0427(92)90039-Z.

[BeCoMe] Frits Beukers, Henri Cohen, Anton Mellit, *Finite hypergeometric functions*, arXiv 1505.02900

[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. Cryptograpic 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

[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

[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

[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* $\mathsf{P}_k(n)$ *with* $2k > n$ *and the fundamental theorems of invariant theory for the symmetric group* S_n. Preprint (2017). arXiv 1707.1410

[BHS2008] Robert Bradshaw, David Harvey and William Stein. strassen_window_multiply_c. strassen.pyx, Sage 3.0, 2008. http://www.sagemath.org

[BHNR2004] S. Brlek, S. Hamel, M. Nivat, C. Reutenauer, On the Palindromic Complexity of Infinite Words, in J. Berstel, J. Karhumaki, 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

[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. Iaggelonicae 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.

[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. Vikkelsoe. *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. http://dx.doi.org/10.1137/S0895479892230031

[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

[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.

[BL2008] Corentin Boissy and Erwan Lanneau, *Dynamics and geometry of the Rauzy-Veech induction for quadratic differentials* (arXiv 0710.5614) to appear in Ergodic Theory and Dynamical Systems.

[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. https://doi.org/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. https://doi.org/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.

[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).

[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.

[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.

[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, Francois Morain, Eric Schost. Fast algorithms for computing isogenies between elliptic curves. [Research Report] 2006, pp.28. <inria-00091441>

[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.

[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

[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

[BOR2009] Emmanuel Briand, Rosa Orellana, Mercedes Rosas. *The stability of the Kronecker products of Schur functions*. arXiv 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.

[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

[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

[BPS2008] Lubomira Balkova, Edita Pelantova, and Wolfgang Steiner. *Sequences with constant number of return words*. Monatsh. Math, 155 (2008) 251-263.

[BPU2016] Alex Biryukov, Léo Perrin, Aleksei Udovenko, *Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1*; in EuroCrypt'16, pp. 372-402.

[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" AAECC 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.

[Bro2011] Francis Brown, *Multiple zeta values and periods: From moduli spaces to Feynman integrals*, in Contemporary Mathematics vol 539, pages 27-52, 2011.

[Bro2016] A.E. Brouwer, Personal communication, 2016.

[Br1910] Bruckner, "Uber die Ableitung der allgemeinen Polytope und die nach Isomorphismus verschiedenen Typen der allgemeinen Achtzelle (Oktatope)", Verhand. Konik. Akad. Wetenschap, Erste Sectie, 10 (1910)

[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).

[Br2016] *Bresenham's Line Algorithm*, Python, 26 December 2016. http://www.roguebasin.com/index.php?title=Bresenham%27s_Line_Algorithm

[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

[Bruin-Molnar] 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.

[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.

[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. Zamboni, A connection between palindromic and factor complexity using return words," Advances in Applied Mathematics 42 (2009) 60-74.

[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

[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)

[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.

[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.

[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)

[CC2013] Mahir Bilen Can and Yonah Cherniavsky. *Omitting parentheses from the cyclic notation*. (2013). arXiv 1308.0936v2.

[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].

[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 Clingher 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]

[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 symmetricalgorithms 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.

[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

[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.

[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.

[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

[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. IBSN 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

[Cha22005] B. Cha. Vanishing of some cohomology goups 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*. Sém. Lothar. Combin. (2008). arXiv 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.

[Cha2006] Ruth Charney. *An introduction to right-angled Artin groups*. http://people.brandeis.edu/~charney/papers/RAAGfinal.pdf, arXiv 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

[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/

[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.

[CK2008] Derek G. Corneil and Richard M. Krueger, *A Unified View of Graph Searching*, SIAM Jounal 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/ (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.

[CL2013] Maria Chlouveraki and Sofia Lambropoulou. *The Yokonuma-Hecke algebras and the HOMFLYPT polynomial*. (2015) arXiv 1204.1871v4.

[Cle1872] Alfred Clebsch, *Theorie der binären 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. Labbé, 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.

[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

[Co1984] J. Conway, Hexacode and tetracode - MINIMOG and MOG. *Computational group theory*, ed. M. Atkinson, Academic Press, 1984.

[Co1999] John Conway, Neil Sloan. *Sphere Packings, Lattices and Groups*, Springer Verlag 1999.

[CO2010] Jonathan Comes, Viktor Ostrik. *On blocks of Deligne's category* $\underline{\mathrm{Rep}}(S_t)$. 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.

[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.

[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

[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

[Cox] David Cox, "What is a Toric Variety", https://dacox.people.amherst.edu/lectures/tutorial.ps

[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.

[CP2005] A. Cossidente and T. Penttila, *Hemisystems on the Hermitian surface*, Journal of London Math. Soc. 72(2005), 731–741. doi:10.1112/S0024610705006964.

[CP2012] Grégory Châtel, Viviane Pons. *Counting smaller trees in the Tamari order*, arXiv 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.

[CPdA2014] Maria Chlouveraki and Loïc Poulain d'Andecy. *Representation theory of the Yokonuma-Hecke algebra*. (2014) arXiv 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.

[Cro1983] M. Crochemore, Recherche linéaire d'un carré dans un mot, C. R. Acad. Sci. Paris Sér. I Math. 296 (1983) 14 781–784.

[CRS2016] Dean Crnković, Sanja Rukavina, and Andrea Švob. *Strongly regular graphs from orthogonal groups* $O^+(6,2)$ *and* $O^-(6,2)$. arXiv 1609.07133

[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.

[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.

[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.

[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 CC 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.

[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.

[CW2005] J. E. Cremona and M. Watkins. Computing isogenies of elliptic curves. preprint, 2005.

[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.

[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. Eichlseder, 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. Unterluggauer "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.

[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.

[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.

[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.

[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. MathSciNet 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.

[DK2013] John R. Doyle and David Krumm, *Computing algebraic numbers of bounded height*, arXiv 1111.4963v4 (2013).

[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-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.

[DN1990] Claude Danthony and Arnaldo Nogueira, *Measured foliations on nonorientable surfaces*, Annales scientifiques de l'École Normale Supérieure, Sér. 4, 23, no. 3 (1990) p 469-494

[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

[DPS2017] Kevin Dilks, Oliver Pechenik, and Jessica Striker, *Resonance in orbits of plane partitions and increasing tableaux*, JCTA 148 (2017), 244-274, https://doi.org/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).

[DR2002] Joan Daemen, Vincent Rijmen. *The Design of Rijndael*. Springer-Verlag Berlin Heidelberg, 2002.

[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.

[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 (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.

[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.

[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.

[Early2017] Nick Early. *Canonical bases for permutohedral plates*. Preprint (2017). arXiv 1712.08520v3.

[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)

[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)

[EGHLSVY] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, Elena Yudovina, "Introduction to representation theory", arXiv 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-ehrhardt.de/specialfunctions.pdf.

[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

[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.

[Eri1995] H. Erikson. Computational and Combinatorial Aspects of Coxeter Groups. Thesis, 1995.

[ER1959] Paul ErdH{o}s and Alfr'ed R'enyi. "On Random Graphs", Publicationes Mathematicae. 6: 290–297, 1959.

[ERH2015] Jorge Espanoza and Steen Ryom-Hansen. *Cell structures for the Yokonuma-Hecke algebra and the algebra of braids and ties*. (2015) arXiv 1506.00715.

[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.

[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

[Feu2009] T. Feulner. The Automorphism Groups of Linear Codes and Canonical Representatives of Their Semilinear Isometry Classes. Advances in Mathematics of Communications 3 (4), pp. 363-383, Nov 2009

[Feu2013] Feulner, Thomas, "Eine kanonische Form zur Darstellung aequivalenter Codes – Computergestuetzte Berechnung und ihre Anwendung in der Codierungstheorie, Kryptographie und Geometrie", Dissertation, University of Bayreuth, 2013.

[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.

[FM2014] Cameron Franc and Marc Masdeu, "Computing fundamental domains for the Bruhat-Tits tree for GL_2(Qp), 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.

[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.

[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 Préville-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.

[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] Wiliam 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.

[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

[Gallai] T. Gallai, Elementare Relationen bezueglich der Glieder und trennenden Punkte von Graphen, Magyar Tud. Akad. Mat. Kutato 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.

[Ge2005] Loukas Georgiadis, *Linear-Time Algorithms for Dominators and Related Problems*, PhD thesis, Princetown University, TR-737-05, (2005). ftp://ftp.cs.princeton.edu/reports/2005/737.pdf

[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

[GGD2011] E. Girondo, G. Gonzalez-Diez, *Introduction to Compact Riemann surfaces and Dessins d'enfant*, (2011) London Mathematical Society, Student Text 79.

[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.

[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, https://doi.org/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.

[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, https://doi.org/10.1007/11832225_20

[GJ2007] A. Glen, J. Justin, Episturmian words: a survey, Preprint, 2007, arXiv 0801.1655.

[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. Tarniţă. 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, https://doi.org/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

[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.

[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

[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. https://doi.org/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.

[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

[GR2001] Chris Godsil and Gordon Royle, *Algebraic Graph Theory*. Graduate Texts in Mathematics, Springer, 2001.

[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.

[GriRei18] Darij Grinberg, Victor Reiner, *Hopf Algebras in Combinatorics*, arXiv 1409.8356v5.

[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

[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)

[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/0001870884900057

[GS1999] Venkatesan Guruswami and Madhu Sudan, Improved Decoding of Reed-Solomon Codes and Algebraic-Geometric Codes, 1999

[Go1993] David M. Goldschmidt. *Group characters, symmetric functions, and the Hecke algebras*. AMS 1993.

[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)

[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, http://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 polyonmials*. Int. Math. Res. Notices **5** (1999), 251-275. arXiv math/9807014v1.

[GW2014] G. Gratzer 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.pysqlite.user/2005-11/msg00047.html

[Hac2016] M. Hachimori. http://infoshako.sk.tsukuba.ac.jp/~hachi/math/library/dunce_hat_eng.html

[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

[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

[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.

[HarPri] F. Harary and G. Prins. The block-cutpoint-tree of a graph. Publ. Math. Debrecen 13 1966 103-107.

[Hat2002] Allen Hatcher, "Algebraic Topology", Cambridge University Press (2002).

[HC2006] Mark van Hoeij and John Cremona, Solving Conics over function fields. J. Théor. Nombres Bordeaux, 2006.

[He2002] H. Heys *A Tutorial on Linear and Differential Cryptanalysis* ; 2002' available at http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf

[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

[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).

[Hig2008] N. J. Higham, "Functions of matrices: theory and computation", Society for Industrial and Applied Mathematics (2008).

[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.

[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 MathSciNet 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.

[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, Reykjav´k, 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.

[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.

[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.

[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

[HR2016] Clemens Heuberger and Roswitha Rissner, "Computing J-Ideals of a Matrix Over a Principal Ideal Domain", arXiv 1611.10308, 2016.

[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.

[HS2018] B. Hutz, M. Stoll. "Smallest representatives of $SL(2, \mathbf{Z})$-orbits of binary forms and endomorphisms of P1", arXiv 1805.08579, 2018.

[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.

[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.

[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.

[Huy2005] D. Huybrechts : *Complex Geometry*, Springer (Berlin) (2005).

[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

[IR1990] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, GTM volume 84, 1990.

[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.

[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 Jankoa 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

[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

[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). https://doi.org/10.1145/2930889.2930928

[Joh1980] D. Johnson, "Spin structures and quadratic forms on surfaces", J. London Math. Soc (2), 22, 1980, 365-373

[Joh1990] D.L. Johnson. *Presentations of Groups*. Cambridge University Press. (1990).

[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

[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.

[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.

[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.

[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.

[Kal1980] T. Kaliath, "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.

[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.

[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

[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

[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

[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.

[KKPSSSYYLLCHH2004] 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

[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.

[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).

[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

[Knu1995] Donald E. Knuth, *Overlapping Pfaffians*, arXiv math/9503234v1.

[Knu2005] Lars R. Knudsen, *SMASH - A Cryptographic Hash Function*; in FSE'05, (2005), pp. 228-242.

[Kob1993] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*. Springer GTM 97, 1993.

[Koe1999] Wolfram Koepf: Effcient 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

[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

[KP2011] Manuel Kauers and Peter Paule. The Concrete Tetrahedron. Springer-Verlag, 2011.

[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

[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/0012365X9290368P

[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

[KR2001] J. Kahane and A. Ryba. *The hexad game*, Electronic Journal of Combinatorics, **8** (2001). 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. Kreps. *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

[KS2002] A. Khare and U. Sukhatme. "Cyclic Identities Involving Jacobi Elliptic Functions", preprint 2002. arXiv 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.

[KS2019] J. Kliem and C. Stump. *A face iterator for polyhedra and more general finite locally branched lattices*. Preprint (2019): arXiv 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.

[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.

[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.

[Kuh1987] W. Kühnel, "Minimal triangulations of Kummer varieties", Abh. Math. Sem. Univ. Hamburg 57 (1987), 7-20.

[Kuh1995] Kuhnel, "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

[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)

[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

[KZ2003] M. Kontsevich, A. Zorich "Connected components of the moduli space of Abelian differentials with prescripebd singularities" Invent. math. 153, 631-678 (2003)

[Lab2008] S. Labbé, Propriétés combinatoires des f-palindromes, Mémoire de maîtrise en Mathématiques, Montréal, UQAM, 2008, 109 pages.

[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

[Lan2008] E. Lanneau "Connected components of the strata of the moduli spaces of quadratic differentials", Annales sci. de l'ENS, serie 4, fascicule 1, 41, 1-56 (2008)

[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.

[LB1988] Lee, P.J., Brickell, E.F. An observation on the security of McEliece's public-key cryptosystem. EuroCrypt 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)

[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.

[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.

[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.

[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

[LLM2014] Lee, Li, Mills, A combinatorial formula for certain elements in the upper cluster algebra, arXiv 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

[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.

[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

[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 doi:10.1016/j.aam.2011.01.002.

[LM2018] A. Lauve, M. Mastnak. *Bialgebra coverings and transfer of structure*. Preprint, arXiv 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

[LNSSS2013] 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

[Loe2007] David Loeffler, *Spectral expansions of overconvergent modular functions*, Int. Math. Res. Not 2007 (050). arXiv math/0701168.

[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

[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.

[LS] A. Lum, W. Stein. Verification of the Birch and Swinnerton-Dyer Conjecture for Elliptic Curves with Complex Multiplication (unpublished)

[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.

[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.

[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

[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.

[Mar2004] S. Marcus, Quasiperiodic infinite words, Bull. Eur. Assoc. Theor. Comput. Sci. 82 (2004) 170-174.

[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 MathSciNet MR1711316

[Mat2002] Jiří Matousek, "Lectures on Discrete Geometry", Springer, 2002

[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).

[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%2FBF00383950

[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.

[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

[MatroidDatabase] Database of Matroids

[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 (Castiglioncello, 1990), 313–334, Progr. Math., 94, Birkhauser Boston, Boston, MA, 1991.

[Mil1958] J. W. Milnor, *The Steenrod algebra and its dual*, Ann. of Math. (2) 67 (1958), 150-171.

[Mil1978] S. Milne, *A q-analog of restricted growth functions, Dobinsky's equality and Charlier polynomials*. Trans. Amer. Math. Soc., 245 (1978), 89-118.

[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 .

[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.

[MMY2003] Jean-Christophe Yoccoz, Stefano Marmi and Pierre Moussa "On the cohomological equation for interval exchange maps", C. R. Acad. Sci. Paris, projet de Note, 2003 Systèmes dynamiques/Dynamical Systems. arXiv math/0304469v1

[MM2015] J. Matherne and G. Muller, *Computing upper cluster algebras*, Int. Math. Res. Not. IMRN, 2015, 3121-3149.

[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.

[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.

[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

[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_022martinezc.pdf

[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

[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

[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.

[MSSY2001] Mateescu, A., Salomaa, A., Salomaa, K. and Yu, S., *A sharpening of the Parikh mapping*. Theoret. Informatics Appl. 35 (2001) 551-564.

[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.

[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.

[Muth2017] Robert Muth. *Super RSK correspondence with symmetry*. arXiv 1711.00420v1.

[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.

[Nas1950] John Nash. *Equilibrium points in n-person games.* Proceedings of the National Academy of Sciences 36.1 (1950): 48-49.

[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/.

[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.

[Nog1985] Arnaldo Nogueira, "Almost all Interval Exchange Transformations with Flips are Nonergodic" (Ergod. Th. & Dyn. Systems, Vol 5., (1985), 257-271

[Normaliz] Winfried Bruns, Bogdan Ichim, and Christof Soeger, Normaliz, http://www.mathematik.uni-osnabrueck.de/normaliz/

[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 withIntegrated 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.

[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.

[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

[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

[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

[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

[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

[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.

[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

[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

[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.

[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

[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

[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

[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.

[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. http://www.ms.unimelb.edu.au/~ram/Publications/1997PLMSv75p99.pdf

[Rau1979] Gerard Rauzy, *Échanges d'intervalles et transformations induites*, Acta Arith. 34, no. 3, 203-212, 1980

[Rea2004] Nathan Reading. *Cambrian Lattices*. arXiv math/0402086v2.

[Rea2009] Nathan Reading, *Noncrossing partitions and the shard intersection order*, DMTCS Proceedings of FPSAC 2009, 745–756

[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.pdfc

[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.

[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.

[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

[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

[Roc1970] R.T. Rockafellar, *Convex Analysis*. Princeton University Press, Princeton, 1970.

[Rog2018] Baptiste Rognerud, *Exceptional and modern intervals of the Tamari lattice*. arXiv 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.*

[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

[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.

[RSS] Wikipedia article Residual_sum_of_squares, accessed 13th October 2009.

[RSW2011] Victor Reiner, Franco Saliola, Volkmar Welker. *Spectra of Symmetrized Shuffling Operators*. arXiv 1102.2460v2.

[RT1975] 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.

[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.

[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/ruskeycombgen.pdf

[Rüt2014] Julian Rüth, *Models of Curves and Valuations*. Open Access Repositorium der Universität Ulm. Dissertation (2014). doi:10.18725/OPARU-3275

[RV2007] Fernando Rodriguez Villegas. Experimental Number Theory. Oxford Graduate Texts in Mathematics 13, 2007.

[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.

[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

[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

[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.

[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.

[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.

[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 $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. 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.

[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.

[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.

[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.

[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.

[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.

[Spe2013] D. Speyer, *An infinitely generated upper cluster algebra*, arXiv 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. Quisquarter, and J.-D. Legat, *ICEBERG: An involutional 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.

[SS1983] Shorey and Stewart. "On the Diophantine equation a x^{2t} + b x^t y + c y^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.

[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.

[SS2017] Ben Salisbury and Travis Scrimshaw. *Rigged configurations for all symmetrizable types*. Electron. J. Combin., **24(1)** (2017) #P1.30. arXiv 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.

[ST2010] Einar Steingrimmsson 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

[St1986] Richard Stanley. *Two poset polytopes*, Discrete Comput. Geom. (1986), doi:10.1007/BF02187680

[St2011b] W. Stein, "Toward a Generalization of the Gross-Zagier Conjecture", Int Math Res Notices (2011), doi:10.1093/imrn/rnq075

[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

[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

[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.

[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.

[STW2013] J. Schejbal, E. Tews, and J. Wälde, *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

[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.

[Sun2010] Yi Sun. *The McKay correspondence*. 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 Théorie des Nombres de Bordeaux, 2012.

[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

[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 Shareshian 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, 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.

[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.

[SYYTIYTT2002] 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.

[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. Shimozono, M. Zabrocki, Hall-Littlewood vertex operators and generalized Kostka polynomials. Adv. Math. 158 (2001), no. 1, 66-85.

[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.

[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 0710.3901v2.

[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.

[Tho2010] T. Thongjunthug, Computing a lower bound for the canonical height on elliptic curves over number fields, Math. Comp. 79 (2010), pages 2431-2449.

[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

[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/>.

[TW1980] A.D. Thomas and G.V. Wood, Group Tables (Exeter: Shiva Publishing, 1980)

[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. Indesteege, Ö. Kücük, 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).

[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 Hecek 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

[Vee1978] William Veech, "Interval exchange transformations", J. Analyse Math. 33 (1978), 222-272

[Ver] Helena Verrill, "Fundamental domain drawer", Java program, http://www.math.lsu.edu/~verrill/

[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 decryptiong 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.

[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.

[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

[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 Q and their L-functions*, http://magma.maths.usyd.edu.au/~watkins/papers/known.pdf

[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.

[Web2007] James Webb. *Game theory: decisions, interaction and Evolution*. Springer Science & Business Media, 2007.

[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 (2016).

[Wei1994] Charles A. Weibel, *An introduction to homological algebra*. Cambridge Studies in Advanced Math., vol. 38, Cambridge Univ. Press, 1994.

[Wel1988] Codes and Cryptography, Dominic Welsh, Oxford Sciences Publications, 1988

[Wer1998] Annette Werner, Local heights on abelian varieties and rigid analytic uniformization, Doc. Math. 3 (1998), 301-319.

[WFYTP2008] D. Watanable, 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

[Wie2000] B. Wieland. *A large dihedral symmetry of the set of alternating sign matrices*. Electron. J. Combin. 7 (2000).

[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.

[WP-Bessel] Wikipedia article Bessel_function

[WP-Error] Wikipedia article Error_function

[WP-Struve] Wikipedia article Struve_function

[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

[Wu2004] Wuthrich, C. (2004). On p-adic heights in families of elliptic curves. Journal of the London Mathematical Society, 70(1), 23-40.

[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

[Yoc2005] Jean-Christophe Yoccoz "Echange d'Intervalles", Cours au collège de France

[Yip2018] Yip, Martha. "Rook placements and Jordan forms of upper-triangular nilpotent matrices." Electronic J. Comb. 25(1) (2018) #P1.68. arXiv 1703.00057.

[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.

[YWHWXSW2014] 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.

[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.

[ZDYBXJZ2019] W. Zhang, T. Ding, B. Yang, Z. Bao, Z. Xiang, F. Ji, X. Zhao. "KNOT: Algorithm Speci cationsand 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.

[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.

[Zie1998] G. M. Ziegler. *Shelling polyhedral 3-balls and 4-polytopes*. Discrete Comput. Geom. 19 (1998), 159-174.

[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 "TheCiliPadiFamily of LightweightAuthenticated Encryption" https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/cilipadi-spec.pdf

[Zor2008] A. Zorich "Explicit Jenkins-Strebel representatives of all strata of Abelian and quadratic differentials", Journal of Modern Dynamics, vol. 2, no 1, 139-185 (2008) (http://www.math.psu.edu/jmd)

[Zor] Anton Zorich, "Generalized Permutation software" (http://perso.univ-rennes1.fr/anton.zorich)

[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.