Sage Reference Manual: References

Release 8.2

The Sage Development Team

May 06, 2018

CONTENTS

The references for Sage, sorted alphabetically by citation key.

REFERENCES:

BIBLIOGRAPHY

[ABBR2012] A. Abad, R. Barrio, F. Blesa, M. Rodriguez. Algorithm 924. *ACM Transactions on Mathematical Software*, *39* no. 1 (2012), 1-28.

[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.

[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.

[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.

[AJL2011] Susumu Ariki, Nicolas Jacon, and Cedric 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.

[AM1974] J. F. Adams and H. R. Margolis, "Sub-Hopf-algebras of the Steenrod algebra," Proc. Cambridge Philos. Soc. 76 (1974), 45-52.

[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

[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

[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

[Av2000] D. Avis, *A revised implementation of the reverse search vertex enumeration algorithm.* Polytopes-combinatorics and computation. Birkhauser Basel, 2000.

[Ava2017] R. Avanzi, *The QARMA block cipher family*; in ToSC, (2017.1), pp. 4-44.

[Ba1994] Kaushik Basu. *The Traveler's Dilemma: Paradoxes of Rationality in Game Theory*. The American Economic Review (1994): 391-395.

[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.

[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.

[BB2009] Tomas J. Boothby and Robert W. Bradshaw. *Bitslicing and the Method of Four Russians Over Larger Finite Fields*. Arxiv 0901.1413, 2009.

[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, Bjorner, Linusson, Shareshian, and Welker, "Complexes of not i-connected graphs," Topology 38 (1999), 271-299

[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.

[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.

[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

[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.

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

[BD2004] M. Becker and A. Desoky. *A study of the DVD content scrambling system (CSS) algorithm*; in Proceedings of ISSPIT, (2004), pp. 353-356.

[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.

[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.

[Bel2011] Belarusian State University, *Information technologies. Data protection. Cryptograpic algorithms for encryption and integrity control*; in STB 34.101.31-2011, (2011).

[Benasque2009] Fernando Rodriguez Villegas, *The L-function of the quintic*, http://users.ictp.it/~villegas/hgm/benasque-2009-report.pdf

[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

[Ber1991] C. Berger, "Une version effective du théorème de Hurewicz", https://tel.archives-ouvertes.fr/tel-00339314/en/.

[BeukersHeckman] F. Beukers and G. Heckman, *Monodromy for the hypergeometric function '{}_n F_{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).

[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.

[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

[BH1994] S. Billey, M. Haiman. *Schubert polynomials for the classical groups*. J. Amer. Math. Soc., 1994.

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

[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

[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

[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.

[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

[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 http://www.crypto.rub.de/imperia/md/content/texte/publications/conferences/present_ches2007.pdf

[BL2000] Anders Björner and Frank H. Lutz, "Simplicial manifolds, bistellar flips and a 16-vertex triangulation of the Poincaré homology 3-sphere", Experiment. Math. 9 (2000), no. 2, 275-289.

[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.

[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.

[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.

[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

[BP1982] H. Beker and F. Piper. *Cipher Systems: The Protection of Communications*. John Wiley and Sons, 1982.

[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

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

[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.

[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

[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

[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.

[BW1996] Anders Bjorner 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.

[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)

[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

[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

[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.

[CEW2011] Georgios Chalkiadakis, Edith Elkind, and Michael Wooldridge. *Computational Aspects of Cooperative Game Theory*. Morgan & Claypool Publishers, (2011). ISBN 9781608456529, doi:10.2200/S00355ED1V01Y201107AIM016.

[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

[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.

[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

[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.

[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)

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

[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.

[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.

[CLS2011] David A. Cox, John Little, and Hal Schenck. *Toric Varieties*. Volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.

[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. http://www.win.tue.nl/~amc/pub/papers/cmt.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.

[Coh1993] Henri Cohen. A Course in Computational Number Theory. Graduate Texts in Mathematics 138. Springer, 1993.

[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.

[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

[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/

[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.

[CPdA2014] Maria Chlouveraki and Loic Poulain d'Andecy. *Representation theory of the Yokonuma-Hecke algebra*. (2014) Arxiv 1302.6225v2.

[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.

[Crossproduct] Algebraic Properties of the Cross Product Wikipedia article Cross_product

[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.

[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

[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.

[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).

[De1973] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep., Suppl., vol. 10, 1973.

[De1974] M. Demazure, Desingularisation des varietes de Schubert, Ann. E. N. S., Vol. 6, (1974), p. 163-172

[Deh2011] P. Dehornoy, Le probleme 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.

[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.

[Dev2005] Devaney, Robert L. *An Introduction to Chaotic Dynamical Systems.* Boulder: Westview, 2005, 331.

[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

[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. http://dlmf.nist.gov/10

[DLMF-Error] N. M. Temme: 7. Error Functions, Dawson's and Fresnel Integrals, in NIST Digital Library of Mathematical Functions. http://dlmf.nist.gov/7

[DLMF-Struve] R. B. Paris: 11. Struve and Related Functions, in NIST Digital Library of Mathematical Functions. http://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'Ecole Normale Superieure, Ser. 4, 23, no. 3 (1990) p 469-494

[Do2009] P. Dobcsanyi et al. DesignTheory.org. http://designtheory.org/database/

[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

[Du2003] I. Duursma, "Extremal weight enumerators and ultraspherical polynomials", Discrete Mathematics 268 (2003), 103–127.

[Du2009] Du Ye. *On the Complexity of Deciding Degeneracy in Games*. Arxiv 0905.3012v1 (2009)

[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)

[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)

[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.

[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

[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.

[ESSS2012] 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.

[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

[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)

[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.

[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.

[FMV2014] Xander Faber, Michelle Manes, and Bianca Viray. Computing Conjugating Sets and Automorphism Groups of Rational Functions. Journal of Algebra, 423 (2014), 1161-1190.

[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.

[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)

[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.

[FRT1990] Faddeev, Reshetikhin and Takhtajan. *Quantization of Lie Groups and Lie Algebras*. Leningrad Math. J. vol. **1** (1990), no. 1.

[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.

[Fu1993] Wiliam Fulton, *Introduction to Toric Varieties*, Princeton University Press, 1993.

[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

[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).

[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.

[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.

[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.

[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).

[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.

[Go1967] Solomon Golomb, Shift register sequences, Aegean Park Press, Laguna Hills, Ca, 1967

[God1968] R. Godement: *Algebra*, Hermann (Paris) / Houghton Mifflin (Boston) (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. Bjorner 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] C.Godsil and G.Royle, *Algebraic Graph Theory*. Graduate Texts in Mathematics, Springer, 2001.

[Gr2007] J. Green, Polynomial representations of GL_n, Springer Verlag, 2007.

[GriRei16] Darij Grinberg, Victor Reiner, *Hopf Algebras in Combinatorics*, Arxiv 1409.8356v4.

[GR2013] Darij Grinberg, Tom Roby. *Iterative properties of birational rowmotion*. http://www.cip.ifi.lmu.de/~grinberg/algebra/skeletal.pdf

[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.

[GrS1967] Grunbaum and Sreedharan, "An enumeration of simplicial 4-polytopes with 8 vertices", J. Comb. Th. 2, 437-465 (1967)

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

[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

[GW2014] G. Gratzer and F. Wehrung, Lattice Theory: Special Topics and Applications Vol. 1, Springer, 2014.

[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.

[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

[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.

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

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

[Hes2002] F. Hess, "Computing Riemann-Roch spaces in algebraic function fields and related topics," J. Symbolic Comput. 33 (2002), no. 4, 425–445.

[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

[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

[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.

[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].

[Hoc] Winfried Hochstaettler, "About the Tic-Tac-Toe Matroid", preprint.

[HN2006] Florent Hivert and Janvier Nzeutchap. *Dual Graded Graphs in Combinatorial Hopf Algebras*. https://www.lri.fr/~hivert/PAPER/commCombHopfAlg.pdf

[HP2003] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge Univ. Press, 2003.

[HP2016] S. Hopkins, D. Perkinson. "Bigraphical Arrangements". Transactions of the American Mathematical Society 368 (2016), 709-725. Arxiv 1212.4398

[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

[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.

[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

[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)

[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).

[IK2010] Kenji Iohara and Yoshiyuki Koga. *Representation Theory of the Virasoro Algebra*. Springer, (2010).

[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.

[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.

[JL2009] Nicolas Jacon and Cedric Lecouvey. *Kashiwara and Zelevinsky involutions in affine type A*. Pac. J. Math. 243(2):287-311 (2009).

[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)

[JPdA15] N. Jacon and L. Poulain d'Andecy. *An isomorphism theorem for Yokonuma-Hecke algebras and applications to link invariants*. (2015) Arxiv 1501.06389v3.

[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.

[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.

[Kat1991] Nicholas M. Katz, *Exponential sums and differential equations*, Princeton University Press, Princeton NJ, 1991.

[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

[KB1983] W. Kühnel and T. F. Banchoff, "The 9-vertex complex projective plane", Math. Intelligencer 5 (1983), no. 3, 11-22.

[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.

[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.

[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

[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.

[KLS2013] Allen Knutson, Thomas Lam, and David Speyer. *Positroid Varieties: Juggling and Geometry* Compositio Mathematica, **149** (2013), no. 10. Arxiv 1111.3660.

[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.

[KN1963] S. Kobayashi & K. Nomizu : *Foundations of Differential Geometry*, vol. 1, Interscience Publishers (New York) (1963).

[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.

[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.

[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/

[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

[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

[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

[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 version: 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.

[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

[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)

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

[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)

[Lau2011] Alan G.B. Lauder, "Computations with classical and p-adic modular forms", LMS J. of Comput. Math. 14 (2011), 214-231.

[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

[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.

[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.

[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.

[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.

[LLMSSZ2013] Thomas Lam, Luc Lapointe, Jennifer Morse, Anne Schilling, Mark Shimozono and Mike Zabrocki. *k-Schur functions and affine Schubert calculus*. Arxiv 1301.3569.

[LM2006] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. ICALP, pp. 144–155, Springer, 2006.

[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

[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.

[Lot2005] M. Lothaire, *Applied combinatorics on words*. Cambridge University Press (2005).

[LP2007] G. Leander and A. Poschmann, *On the Classification of 4 Bit S-boxes*; in WAIFI, (2007), pp. 159-176.

[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

[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)

[LS2017] Xuan Liu and Travis Scrimshaw. *A uniform approach to soliton cellular automata using rigged configurations*. Preprint (2017) Arxiv 1706.02443

[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.

[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

[Lyo2003] R. Lyons, Determinantal probability measures. Publications Mathematiques de l'Institut des Hautes Etudes Scientifiques 98(1) (2003), pp. 167-212.

[Mac1987] 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.

[MagmaHGM] *Hypergeometric motives* in Magma, http://magma.maths.usyd.edu.au/~watkins/papers/HGM-chapter.pdf

[Mas94] 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.

[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

[Mas1969] James L. Massey, "Shift-Register Synthesis and BCH Decoding." IEEE Trans. on Information Theory, vol. 15(1), pp. 122-127, Jan 1969.

[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)

[McC1978] K. McCrimmon. *Jordan algebras and their applications*. Bull. Amer. Math. Soc. **84** 1978.

[McM1992] John McMillan. *Games, strategies, and managers*. Oxford University Press.

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

[MirMor2009] R. Miranda, D.R. Morrison, "Embeddings of Integral Quadratic Forms" http://www.math.ucsb.edu/~drm/manuscripts/eiqf.pdf .

[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.

[MoPa1994] P. Morton and P. Patel. The Galois theory of periodic points of polynomial maps. Proc. London Math. Soc., 68 (1994), 225-263.

[MR1989] G. Melançon and C. Reutenauer. *Lyndon words, free algebras and shuffles*, Can. J. Math., Vol. XLI, No. 4, 1989, pp. 577-591.

[MR2002] S. Murphy, M. Robshaw *Essential Algebraic Structure Within the AES*; in Advances in Cryptology - CRYPTO 2002; LNCS 2442; Springer Verlag 2002

[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.

[MSZ2013] Michael Maschler, Solan Eilon, and Zamir Shmuel. *Game Theory*. Cambridge: Cambridge University Press, (2013). ISBN 9781107005488.

[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.

[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.

[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.

[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/.

[Nij1955] A. Nijenhuis, *Jacobi-type identities for bilinear differential concomitants of certain tensor fields. I*, Indagationes Mathematicae (Proceedings) **58**, 390 (1955).

[NN2007] Nisan, Noam, et al., eds. *Algorithmic game theory.* Cambridge University Press, 2007.

[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/

[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)

[Or2016] M. Orlitzky. The Lyapunov rank of an improper cone. Citation: Optimization Methods and Software (accepted 2016-06-12). http://www.optimization-online.org/DB_HTML/2015/10/5135.html. doi:10.1080/10556788.2016.1202246

[Oxl1992] James Oxley, *Matroid theory*, Oxford University Press, 1992.

[Oxl2011] James Oxley, *Matroid Theory, Second Edition*. Oxford University Press, 2011.

[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

[PearsonTest] Wikipedia article Goodness_of_fit, accessed 13th October 2009.

[Pen2012] R. Pendavingh, On the evaluation at $(-i, i)$ of the Tutte polynomial of a binary matroid. Preprint: Arxiv 1203.0910

[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.

[Pon2010] S. Pon. *Types B and D affine Stanley symmetric functions*, unpublished PhD Thesis, UC Davis, 2010.

[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

[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

[PS2011] R. Pollack, and G. Stevens. *Overconvergent modular symbols and p-adic L-functions.* Annales scientifiques de l'Ecole normale superieure. Vol. 44. No. 1. Elsevier, 2011.

[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.

[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

[Raj1987] A. Rajan, Algorithmic applications of connectivity and related topics in matroid theory. Ph.D. Thesis, Northwestern university, 1987.

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

[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).

[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)

[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.

[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.

[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.

[Ros1999] K. Rosen *Handbook of Discrete and Combinatorial Mathematics* (1999), Chapman and Hall.

[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

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

[Rud1958] M. E. Rudin. *An unshellable triangulation of a tetrahedron*. Bull. Amer. Math. Soc. 64 (1958), 90-91.

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

[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.

[Sch1996] E. Schaefer. A simplified data encryption algorithm. Cryptologia, 20(1):77–84, 1996.

[Sch2006] Oliver Schiffmann. *Lectures on Hall algebras*, preprint, 2006. Arxiv 0611617v2.

[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).

[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.

[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.

[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.

[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.

[Sor1984] A. Sorkin, *LUCIFER: a cryptographic algorithm*; in Cryptologia, 8(1), pp. 22–35, 1984.

[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.

[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.

[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.

[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.

[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

[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/

[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

[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

[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.

[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.

[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

[SV2000] J. Stern and S. Vaudenay, *CS-Cipher*; in First Open NESSIE Workshop, (2000).

[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/

[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

[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.

[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.

[Tar1976] Robert E. Tarjan, *Edge-disjoint spanning trees and depth-first search*, Acta Informatica 6 (2), 1976, 171-185, doi:10.1007/BF00268499.

[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.

[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.

[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)

[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)

[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).

[UNITTEST] unittest – Unit testing framework – http://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

[Vat2008] D. Vatne, *The mutation class of 'D_n' quivers*, Arxiv 0810.4789v1.

[VB1996] E. Viterbo, E. Biglieri. *Computing the Voronoi Cell of a Lattice: The Diamond-Cutting Algorithm*. IEEE Transactions on Information Theory, 1996.

[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).

[Voe2003] V. Voevodsky, Reduced power operations in motivic cohomology, Publ. Math. Inst. Hautes Études Sci. No. 98 (2003), 1-57.

[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.

[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.

[WFYTP2008] D. Watanable, S. Furuya, H. Yoshida, K. Takaragi, and B. Preneel, *A new keystream generator MUGI*; in FSE, (2002), pp. 179-194.

[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.

[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

[WW2005] Ralf-Philipp Weinmann and Kai Wirt, *Analysis of the DVB Common Scrambling Algorithm*; in IFIP TC-6 TC-11, (2005).

[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).

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

[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).

[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.

[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.

[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.