Curriculum Vitae

Makoto Matsumoto

June 2, 2015

Makoto Matsumoto.
Professor.
Department of Mathematics, Graduate School of Science
Hiroshima University.
1-3-1 Kagamiyama, Higashi-Hiroshima, zip 739-8526.
Tel.+81-824-24-7348 Faximille +81-824-24-0710
URL: http://www.math.sci.hiroshima-u.ac.jp/~m-mat
email: m-mat at math.sci.hiroshima-u.ac.jp
Birth: 1965/2/18

1995/1/23 Ph.D (Mathematics, Kyoto Univ.)
2000/3/29 Doctor of Engineering (Mathematical Engineering, Univ. of Tokyo)

1990/10/1 Research Associate, RIMS, Kyoto Univ.
1995/9/1 Lecturer, Dept. of Math. Faculty of Science and Engineering, Keio Univ.
1998/4/1 Associate Professor, Keio Univ.
1999/9/1 Associate Professor, Dept. of Math. Graduate School of Sci. Kyushu Univ.
2000/4/1 Associate Professor, Dept. of Math. Fac. of IHS. Kyoto Univ.
2002/4/1 Professor, Dept. of Math. Graduate School of Science, Hiroshima Univ.
2010/4/1 Professor, Graduate School of Mathematical Sciences,
University of Tokyo.
2013/4/1 Professor, Dept. of Math. Graduate School of Science, Hiroshima Univ.

Awards

- 1997/3 Institute of Combinatorics and its Applications: Kirkman Medal
- 1997/10 Takebe Prize for young mathematicians (Mathematical Society of Japan)
- 1998/11 Gijuku Prize of Keio University
- 1999/12 Japan IBM Science Prize
- 2005/3 Funai Information Science Prize
- 2006/4 Ministry of Education Prize

- 2008/3 JSPS Prize
- 2008/11 Hiroshima University President Prize
- 2014/4 Ichimura Science Prize
- 2014/10 Fujiwara Mathematical Science Grand Prize

List of Publication

References

[1] M. Imori, M. Matsumoto and H. Yamada "The line digraph of a regular and pancircular digraph is also regular and pancircular," 1988 Graphs and Combinatorics 4(235–239)

[2] M. Matsumoto and N. Tokushige "The exact bound in the Erdös-Ko-Rado Theorem for cross-intersecting families," 1989 Journal of Combinatorial Theory Ser.A 52(90–97)

[3] M. Matsumoto and N. Tokushige "A generalization of the Katona Theorem for cross t-intersecting families," 1989 Graphs and Combinatorics 5(159–171)

[4] M. Matsumoto "Bounds for the vertex linear arboricity" 1990 Jounal of Graph Theory 14(117–126)

[5] Y. Egawa, K, Kaneko and M. Matsumoto "A mixed version of Menger's Theorem," 1991 Combinatorica 11(71–74)

[6] Y. Kurita and M. Matsumoto "Primitive t-nomial ($t = 3, 5$) over GF(2) whose degree is a Mersenne Exponent ≤ 44497," 1991 Mathematics of Computation 56(817–821)

[7] M. Matsumoto and Y. Kurita "Twisted GFSR Generators," 1992 ACM Transactions on Modeling and Computer Simulations 2(179–194)

[8] M. Asada, T. Oda and M. Matsumoto "Local monodromy on the fundamental groups of algebraic curves along a degenerate stable curve," 1995 Journal of Pure and Applied Algebra (103) 235–283

[9] P. Frankl, M. Matsumoto, I. Z. Ruzsa and N. Tokushige "Minimum shadows in uniform hypergraphs and a generalization of the Takagi function," 1994 Journal of Combinatorial Theory (A) 68(125–148)

[10] M. Matsumoto and Y. Kurita "Twisted GFSR Generators II,"

1994 ACM Transactions on Modeling and Computer Simulation, Vol.4, No. 3 (July, 1994) (254–266)

[11] B. Chen, M. Matsumoto J. Wang, Z. Zhang, and J. Zhang, "A Short Proof of Nash-Williams' Theorem for the Arboricity of a Graph" 1994 Graphs and Combinatorics 10(27–28)

[12] M. Matsumoto "On the Galois image in the derivation algebra of π_1 of the projective line minus three points" 1995 Contemporary Mathematics 186(201–213)

[13] Y. Ihara and M. Matsumoto "On Galois actions on profinite completion of braid groups" 1995 Contemporary Mathematics 186(173–200)

[14] M. Matsumoto "Galois representations on profinite braid groups on curves" 1996 J. reine. angew. Math. 474 (169–219)

[15] F. Jaeger, M. Matsumoto, and K. Nomura "Association schemes related with type II matrices and spin models" Journal of Algebraic Combinatorics 8 (1998), 39-72.

[16] M. Matsumoto and Y. Kurita "Strong Deviations from Randomness in m-sequences based on Trinomials" 1996 ACM Transactions on Modeling and Computer Simulation 6 (99–106)

[17] M. Matsumoto "Galois group $\mathrm{G}_{\mathbf{Q}}$, Singularity E_7, and Moduli $\mathcal{M}_3$" London Math. Soc. Lecture Note Series **243** Geometric Galois Actions 2. The Inverse Galois Problem, Moduli Spaces and Mapping class Groups. 1997 (179–218).

[18] H. Ashihara and M. Matsumoto "An Application of Finite Projective Space to Replicated Data Management" Computer Systems Science & Engineering, Vol.15 No.2 (Mar.2000) pp.87-91.

[19] M. Matsumoto and T. Nishimura "Mersenne Twister: a 623-dimensionally equidistributed uniform pseudorandom number generator" ACM Transactions on Modeling and Computer Simulation 8. (Jan. 1998) 3–30.

[20] Y. Kurita, H. Leeb and M. Matsumoto, An exercize (Exercize 14, Section 3.6, p.604) in Knuth's "The art of computer programming Vol.2, 3rd edtion" (1997).

[21] M. Matsumoto "A presentation of mapping class groups in terms of Artin groups and geometric monodromy of singularities" Mathematische Annalen 316, (2000) 401–418.

[22] M. Matsumoto "Simple cellular automata as pseudorandom m-sequence generators for built-in self-test" ACM Transactions on Modeling and Computer Simulation 8. (Jan. 1998) 31–42.

[23] H. Maehara and M. Matsumoto "Is there a circle that passes through a given number of lattice points?" European Journal of Combinatorics 19 (1998), 591-592.

[24] H. Enomoto, M. Hagita and M. Matsumoto, "A note on difference sets" Journal of Combinatorial Theory (A) 84 (1998) 133-144.

[25] T. Kumada, H. Leeb, Y. Kurita, and M. Matsumoto, “New primitive t-nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent” Mathematics of Computation Vol. 69 No. 230 (1999)) 811-814.

[26] M. Matsumoto, “A generalization of Jaeger-Nomura’s Bose Mesner algebra associated to type II matrices,” Ann. Inst. Fourier (Grenoble) 49 (1999), no. 3, 1027–1035.

[27] M. Matsumoto and T. Oda, “Combinatorial Dehn Twists” Far East J. Math. Sci. (FJMS) 1999, Special Volume, Part II, 137–198.

[28] M. Matsumoto and T. Nishimura, “Dynamic Creation of Pseudorandom number generator,” 56–69 in: Monte Carlo and Quasi-Monte Carlo Methods 1998, Ed. H. Niederreiter and J. Spanier, Springer 2000.

[29] S. Wegenkittl and M. Matsumoto, “Getting Rid of Correlations among Pseudorandom Numbers: Discarding versus Tempering,” ACM Trans. on Modeling and Computer Simulation **9**, 282–294 (1999).

[30] M. Matsumoto and A. Tamagawa “Mapping-Class-group action versus Galois action on profinite fundamental groups” American Journal of Mathematics 122 1017–1026 (2000).

[31] M. Matsumoto and T. Nishimura “A Nonempirical Test on the Weight of Pseudorandom Number Generators” 381–395 in: Monte Carlo and Quasi-Monte Carlo methods 2000, Ed. K.T. Fang, F.J.Hickernel, and H. Niederreiter, Springer-Verlag 2002.

[32] M. Matsumoto and T. Nishimura “Sum-discrepancy test on pseudorandom number generators” Mathematics and Computers in Simulation, Vol. 62 (2003), pp 431-442.

[33] R. Hain and M. Matsumoto “Weighted completion of Galois groups and Galois actions on the fundamental group of $P^1 - \{0, 1, \infty\}$” Compositio Mathematicae 139-2 (2003) 119–167.

[34] R. Hain and M. Matsumoto “Tannakian fundamental groups associated to Galois groups” MSRI Publications 41 (2003) 183–216.

[35] M. Matsumoto and S. Tagami “Practical fast algorithm for finite field arithmetics using group rings” Hiroshima Mathematical Journal 34 (2004), no. 2, 201–210

[36] R. Hain and M. Matsumoto Galois actions on fundamental groups of curves and the cycle C-C’ Journal of the Inst. Math. Jussieu 4 (2005), 363-403.

[37] F. Panneton, P. L’Ecuyer and M. Matsumoto “Improved Long-Period Generators Based on Linear Reccurences Modulo 2” ACM Transactions on Mathematical Software, 32 (1, March) 2006, 1–16.

[38] Makoto Matsumoto, Mutsuo Saito, Hiroshi Haramoto, Takuji Nishimura “Pseudorandom Number Generation: Impossibility and Compromise” Journal of Universal Computer Science, Vol. 12, No. 6, pp. 672-690, 2006.

[39] M. Matsumoto and T. Nishimura, Weight discrepancy tests on M-sequences, Bulltin of Yamagata University (Natural Science), Vol. 16, No.3, 2007, 105–112.

[40] Haramoto, H., Matsumoto, M., Nishimura, T. "Computing conditional probabilities for $\mathbf{F}_2$-linear pseudorandom bit generator by splitting Mac-Williams identity", International Journal of Pure and Applied Mathematics, Vol.38 No.1, 2007.

[41] Makoto Matsumoto, Isaku Wada, Ai Kuramoto, Hyo Ashihara, "Common Defects in Initialization of Pseudorandom Number Generators," ACM Trans. on Modeling and Computer Simulation 17(4): (2007). (21 pages)

[42] Mutsuo Saito and Makoto Matsumoto, "SIMD-oriented Fast Mersenne Twister: A 128-bit Pseudorandom Number Generator," in: Monte Carlo and Quasi-monte Carlo Methods 2006, pp. 617–632, Springer-Verlag, 2007.

[43] Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita. "A Fast Stream Cipher with Huge State Space and Quasigroup Filter for Software," in: Carlisle M. Adams, Ali Miri, Michael J. Wiener Ed. Selected Areas of Cryptography 2007 (SAC 2007), Lecture Notes in Computer Science 4876, pp.245–262, Springer-Verlag 2007.

[44] Haramoto, H., Nishimura, T., Matsumoto, M., Panneton, F, L'Ecuyer, P. "Efficient Jump Ahead for F_2-linear Random Number Generators" INFORMS Journal of Computing, 20 (3), pp.385-390 (2008).

[45] Mariko Hagita, Makoto Matsumoto, Fumio Natsu, Yuki Ohtsuka. "Error Correcting Sequence and Projective De Bruijn Graph," Graphs and Combinatorics 24, pp.185-194 (2008)

[46] Yuki Ohtsuka, Makoto Matsumoto, and Mariko Hagita. "Projective de Bruijn Sequences," Lecture Notes in Computer Science 5203, Sequences and Their Applications - SETA 2008, pp.167–174, 2008.

[47] Hiroshi Haramoto, Makoto Matsumoto, and Pierre L'Ecuyer. "A Fast Jump Ahead Algorithm for Linear Recurrences in a Polynomial Space," Lecture Notes in Computer Science 5203, Sequences and Their Applications - SETA 2008, pp.290–298, 2008.

[48] Hiroshi Haramoto, Makoto Matsumoto. "A p-adic algorithm for computing the inverse of integer matrices," Journal of Computational and Applied Mathematics 225 (2009), pp. 320-322. doi:10.1016/j.cam.2008.07.044

[49] Richard Hain, Makoto Matsumoto. "Relative Pro-ℓ Completions of Mapping Class Groups," Journal of Algebra, vol. 321 (2009), pp. 3335-3374.

[50] Mutsuo Saito, Makoto Matsumoto. "A PRNG specialized in double precision floating point numbers using an affine transition," in: Monte Carlo and Quasi-Monte Carlo Methods 2008, P. L'Ecuyer and A. Owen (Ed.), Springer-Verlag 2009. pp.589–602.

[51] Shin Harase, Makoto Matsumoto, Mutsuo Saito. “Fast lattice reduction for F_2-linear pseudorandom number generators,” Mathematics of Computation 80 (2011), 395-407.

[52] Makoto Matsumoto, “Difference between Galois representations in automorphism and outer-automorphism groups of a fundamental group,” Proceedings of the American Mathematical Society 139 (2011), 1215-1220.

[53] Su Chen, Makoto Matsumoto, Takuji Nishimura, and Art B. Owen, “New Inputs and Methods for Markov Chain Quasi-Monte Carlo,” in: Monte Carlo and Quasi-Monte Carlo Methods 2010, L. Plaskota and H. Woźniakowski (Ed.) Springer-Verlag 2012, pp.293–307.

[54] M. Saito, M. Matsumoto, “Variants of Mersenne Twister Suitable for Graphic Processors,” ACM Transactions on Mathematical Software, 39 (2), Feb. 2013 (Article Number 12, 20 pages). http://dx.doi.org/10.1145/2427023.2427029

[55] M. Matsumoto, “Introduction to Arithmetic Mapping Class Groups,” in IAS-Park City Mathematics Series 20, AMS, 2013, pp.317–351.

[56] M. Matsumoto, M. Saito, K. Matoba, “A computable figure of merit for quasi-monte carlo point sets,” Math. Comp. 83 (2014), 1233-1250 doi:10.1090/S0025-5718-2013-02774-3 Published electronically: September 23, 2013

[57] M. Matsumoto, Y. Yoshiki, “Existence of higher order convergent quasi-Monte Carlo rules via Walsh figure of merit,” in: Monte Carlo and Quasi-Monte Carlo Methods 2012, Springer (2013), 569-579. doi:10.1007/978-3-642-41095-6-29

[58] H. Haramoto, M. Matsumoto, T. Nishimura, Y. Otsuka, “A non-empirical test on the 2nd to the 6th least significant bits of PRNGs,” Monte Carlo and Quasi-Monte Carlo Methods 2012, Springer (2013), 417-426. doi:10.1007/978-3-642-41095-6-19

[59] J. Dick, M. Matsumoto, “On the fast computation of the weight enumerator polynomial and the t value of digital nets over finite abelian groups,” SIAM J. Discrete Math. 27-3 (2013), pp. 1335-1359 http://dx.doi.org/10.1137/120893677