Bibliography

Bil84. Elizabeth J. Billington, *Balanced n-ary designs: a combinatorial survey and some new results*, Ars Combin. **17** (1984), no. A, 37–72.

Bil89. Elizabeth J. Billington, *Designs with repeated elements in blocks: a survey and some recent results*, Congr. Numer. 68 (1989), 123–146, Eighteenth Manitoba Conference on Numerical Mathematics and Computing (Winnipeg, MB, 1988).

CD76. I. M. Chakravarti and A. Dey, *On the construction of balanced and orthogonal arrays*, Canad. J. Statist. **4** (1976), 109–117.

Cha56. I. M. Chakravarti, *Fractional replication in asymmetrical factorial designs and partially balanced arrays*, Sankhyā **17** (1956), 143–164.

Cha61. I. M. Chakravarti, *On some methods of construction of partially balanced arrays*, Ann. Math. Statist. **32** (1961), 1181–1185.

Cho82. D. V. Chopra, *A note on balanced arrays of strength four*, Sankhyā (B) **44** (1982), 71–75.

Cho83. D. V. Chopra, *A note on an upper bound for the constraints of balanced arrays with strength t*, Commun. Statist.-Theor. Meth. **12** (1983), 1755–1759.

CK96. T. Caliński and S. Kageyama, *Block designs: Their combinatorial and statistical properties*, Handbook of Statistics, vol. 13, ch. 22, pp. 809–873, North-Holland, 1996.

CLO98. David Cox, John Little, and Donal O'Shea, *Using algebraic geometry*, Springer-Verlag, New York, 1998.

Dey75. A. Dey, *A note on balanced designs*, Sankhyā Ser. B **37** (1975), 461–462.

DKS72. A. Dey, A. C. Kulshreshtha, and G. M. Saha, *Three symbol partially balanced arrays*, Ann. Inst. Statist. Math. **24** (1972), 525–528.

ElG85. T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inf. Theory **4** (1985), 469–472, IT-31.

FHJY89. R. Fuji-Hara, M. Jimbo, and F. Yuan, *A recursive construction of balanced arrays*, Utilitas Mathematica **36** (1989), 83–92.

FHK91. R. Fuji-Hara and S. Kuriki, *Mutually balanced nested designs*, Discrete Math. **97** (1991), 167–176.

FHKK$^+$. R. Fuji-Hara, S. Kageyama, S. Kuriki, Y. Miao, and S. Shinohara, *Balanced nested designs and balanced arrays*, submitted.

FHKM96. R. Fuji-Hara, S. Kuriki, and M. Miyake, *Cyclic orthogonal and balanced arrays*, J. Statist. Planning Inf. **56** (1996), 171–180.

FHKMS. R. Fuji-Hara, S. Kuriki, Y. Miao, and S. Shinohara, *Balanced nested designs and balanced n-ary designs*, J. Statist. Plann. Inference, to appear.

FHS99. Ryoh Fuji-Hara and Satoshi Shinohara, *Symmetric sets of curves and combinatorial arrays*, Finite Fields: Theory, Applications, and Algorithms (Ronald C. Mullin and Gary L.

Mullen, eds.), Comtemporary Mathematics, vol. 225, American Mathematical Society, 1999, pp. 225–230.

Ful69. William Fulton, *Algebraic curves. An introduction to algebraic geometry*, W. A. Benjamin, Inc., New York-Amsterdam, 1969, Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

GLK95. Sudhir Gupta, Woo-Sun Lee, and Sanpei Kageyama, *Nested balanced N-ary designs*, Metrika **42** (1995), 411–419.

Gop81. V. G. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24** (1981), 170–172.

Gop91. V. D. Goppa, *Geometry and Codes*, Kluwer Academic Publishers, Boston, 1991.

Hot44. H. Hotelling, *Some problems in weighing and other experimental techniques*, Ann. Math. Stat. **32** (1944), 297–306.

Hyo92. Y. Hyodo, *Characteristic-polynomials of information matrices of some balanced fractional 2^m factorial designs of resolution $2l+1$*, J. Statist. Planning Inf. **31** (1992), 245–252.

Kag75. S. Kageyama, *Note on the construction of partially balanced arrays*, Ann. Inst. Statist. Math. **27** (1975), 177–180.

Kag79. Sanpei Kageyama, *Mathematical expression of an inequality for a block design*, Ann. Inst. Statist. Math. **31** (1979), no. 2, 293–298.

Kag80. Sanpei Kageyama, *Characterization of certain balanced n-ary block designs*, Ann. Inst. Statist. Math. **32** (1980), no. 1, 107–110.

KDS72. A. C. Kulshreshtha, A. Dey, and G. M. Saha, *Balanced designs with unequal replications and unequal block sizes*, Ann. Math. Stats. **43** (1972), 1342–1345.

KFH94. S. Kuriki and R. Fuji-Hara, *Balanced arrays of strength two and nested (r, λ)-designs*, J. Combin. Designs 2 (1994), 407–414.

KN79. M. Kuwada and R. Nishii, *On a connection between balanced arrays and balanced fractional s^m factorial designs*, J. Japan Statist. Soc. 9 (1979), 93–101.

Kob87. N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.

Kob94. Neal Koblitz, *A course in number theory and cryptography*, second ed., Springer-Verlag, New York, 1994.

KT79. Sanpei Kageyama and Takumi Tsuji, *Inequality for equireplicated n-ary block designs with unequal block sizes*, J. Statist. Plann. Inference **3** (1979), no. 2, 101–107.

KT80. Sanpei Kageyama and Takumi Tsuji, *Characterization of equireplicated variance-balanced block designs*, Ann. Inst. Statist. Math. **32** (1980), no. 2, 263–273.

Kur84a. S. Kuriki, *Existence conditions for balanced arrays of strength t, $t+2$ constraints and s symbols*, TRU Math. **20** (1984), 139–161.

Kur84b. S. Kuriki, *General existence condition for balanced arrays of strength t, m constraints and s symbols*, TRU Math. **20** (1984), 191–211.

Kur88. S. Kuriki, *Existence of 2-symbol balanced arrays of strength-t and $t+2$ constraints*, J. Statist. Planning Inf. **20** (1988), 225–228.

Kuw79. M. Kuwada, *Balanced arrays of strength 4 and balanced fractional 3^m factorial designs*, J. Statist. Planning Inf. **3** (1979), 347–360.

LJ87. H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Annals of Math. **126** (1987), 649–673.

MD67. J. S. Murty and M. N. Das, *Balanced* $n-$ ary *block designs and their uses*, J. Indian Statist. Assoc. **5** (1967), 73–82.

Mil86. V. S. Miller, *Use of elliptic curves in cryptography*, CRYPTO '85: Lecture Notes in Computer Science, 1986, pp. 417–426.

Miy95. Nobuko Miyamoto, *The constructions of balanced arrays*, Master's thesis, University of Tsukuba, 1995.

Miy98. Nobuko Miyamoto, *Mutually M-intersecting varieties and combinatorial arrays*, Ph.D. thesis, University of Tsukuba, 1998.

Mor77. Elizabeth J. Morgan, *Construction of balanced n-ary designs*, Utilitas Math. **11** (1977), 3–31.

Mor79. Elizabeth J. Morgan, *Construction of balanced designs and related identities*, Combinatorial mathematics, VI (Proc. Sixth Austral. Conf., Univ. New England, Armidale, 1978), Springer, Berlin, 1979, pp. 79–91.

Mor91. Carlos Moreno, *Algebraic curves over finite fields*, Cambridge University Press, Cambridge, 1991.

Pan81. V. S. Soundara Pandian, *Some properties for balanced n-ary designs*, Estadística **35** (1981), no. 124, 77–86.

RS74. J. A. Rafter and E. Seiden, *Contributions to the theory and construction of balanced arrays*, Ann. Statist. **2** (1974), 1256–1273.

Rue86. R. A. Rueppel, *Analysis and design of stream ciphers*, Springer-Verlag, Berlin, Germany, 1986.

Rue92. R. A. Rueppel, *Stream ciphers*, Contemporary Cryptology – The Science of Information Integrity (G. J. Simmons, ed.), IEEE Press, New York, 1992, pp. 65–134.

SA70. J. N. Srivastava and D. A. Anderson, *Some basic properties of multidimensional partially balanced designs*, Ann. Math. Statist. **41** (1970), 1438–1445.

Sah75. G. M. Saha, *On construction of balanced ternary designs*, Sankhyā Ser. B **37** (1975), no. 2, 220–227.

SC73. J. N. Srivastava and D. V. Chopra, *Balanced arrays and orthogonal arrays*, A survey of combinatorial theory (J. N. et al. Srivastava, ed.), North-Holland publishing company, 1973, pp. 411–428.

SD73. G. M. Saha and A. Dey, *On construction and uses of balanced n-ary designs*, Ann. Inst. Statist. Math. **25** (1973), 439–445.

SF79. M. Shafiq and W. T. Federer, *Generalized N-ary balanced block designs*, Biometrika **66** (1979), no. 1, 115–123.

Shi75. T. Shirakura, *On balanced of 2 symbols, strength $2l$, m constraints and index set $\{\mu_0, \mu_1, \dots, \mu_{2l}\}$ with $\mu_l = 0$*, J. Japan Statist. Soc. **5** (1975), 53–56.

Shi76. T. Shirakura, *Optimal balanced fractional 2^m factorial designs of resolution VII, $6 \leq m \leq 8$*, Ann. Statist. **4** (1976), 515–531.

Shi77. T. Shirakura, *Contributions to balanced fractional 2^m factorial designs derived from balanced arrays of strength $2l$*, Hiroshima Math. J. **7** (1977), 217–285.

Shi96. Satoshi Shinohara, *Balanced arrays from algebraic curves over finite fields*, Master's thesis, University of Tsukuba, 1996.

SK75. T. Shirakura and M. Kuwada, *Note on balanced fractional 2^m factorial designs of resolution $2l + 1$*, Ann. Inst. Statist. Math. **27** (1975), 377–386.

SK76. T. Shirakura and M. Kuwada, *Covariance matrices of the estimates for balanced fractional 2^m factorial designs of resolution* $2l+1$, J. Japan Statist. Soc. **6** (1976), 27–31.

SMK88. G. M. Saha, R. Mukerjee, and S. Kageyama, *Bounds on the number of constraints for balanced arrays of strength t*, J. Statist. Planning Inf. **18** (1988), 255–265.

Sri70. J. N. Srivastava, *Optimal balanced 2^m fractional factorial designs*, S.N. Roy Memorial Volume, Univ. of North Carolina and Indian Statist. Institute (1970), 689–706.

Sri72. J. N. Srivastava, *Some general existence conditions for balanced arrays of strength t and 2 symbols*, J. Combinatorial Theory (A) **13** (1972), 198–206.

SS87. Anne Penfold Street and Deborah J. Street, *Combinatorics of experimental design*, The Clarendon Press Oxford University Press, New York, 1987.

ST92. Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Springer-Verlag, New York, 1992.

Sti95. Douglas R. Stinson, *Cryptography*, CRC Press, Boca Raton, FL, 1995, Theory and practice.

SW81. J. N. Srivastava and A. M. Wijetunga, *Balanced arrays of strength t with three symbols and $(t+1)$ rows*, J. Comb., Inf. & Syst. Sci. **6** (1981), 335–355.

Toc52. K. D. Tocher, *The design and analysis of block experiments*, J. Roy. Statist. Soc. (B) **14** (1952), 45–100.

TV91. M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht, 1991.

TVZ82. M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, *Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound*, Mathematische Nachrichten **109** (1982), 21–28.

Uen93. Kenji Ueno, *Daisuukika*, Iwanami Shoten, Tokyo, 1993, Iwanami Kouza Ōyou Sūgaku [Iwanami Lectures on Applied Mathematics], Kiso [Fundamental] 9.

Uen97. Kenji Ueno, *An introduction to algebraic geometry*, American Mathematical Society, Providence, RI, 1997, Translated from the 1995 Japanese original by Katsumi Nomizu.

vLvdG88. J. H. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, Birkhäuser Verlag, Basel, 1988.

XL99. C. P. Xing and K. Y. Lam, *Sequences with almost perfect complexity profiles and curves over finite fields*, IEEE Trans. Inf. Theory **45** (1999), no. 4, 1267–1270.

YKY83. S. Yamamoto, S. Kuriki, and F. Yuan, *Balanced arrays of strength t, $t+1$ constraints and s symbols*, TRU Math. (1983), 105–114.

YKY85. S. Yamamoto, M. Kuwada, and F. Yuan, *On the maximum number of constraints for s-symbol balanced arrays of strength t*, Commun. Statist.-Theor. Meth. **14** (1985), 2447–2456.

YSK75. S. Yamamoto, T. Shirakura, and M. Kuwada, *Balanced arrays of strength $2l$ and balanced fractional 2^m factorial designs*, Ann. Inst. Statist. Math. **27** (1975), 143–157.