

LIST OF PUBLICATIONS

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

January 15, 2012

References

- [1] A characterization of the *Baby Monster* F_2 , including a note on ${}^2E_6(2)$, *Journal of Algebra* **56** (1979), 384-395.
- [2] A 2-local characterization of the Rudvalis simple group , *Journal of Algebra* **58** (1979), 563-571.
- [3] On a certain class of 2-local subgroups in finite simple groups, *Rend. Sem. Mat. Univ. Padova* **62** (1980), 137-163.
- [4] On minimal blocking sets, *Archiv der Mathematik* **35** (1980), 394-400.
- [5] Blocking sets of maximal type in finite projective planes, *Rend. Sem. Mat. Univ. Padova* **65** (1981), 85-101.
- [6] On the weight distribution in binary codes generated by projective planes, *Quarterly Journal of Mathematics Oxford* **33** (1982), 275-279.
- [7] Blocking sets of 16 points in projective planes of order 10 Part I, *manuscript*.
- [8] Blocking sets of 16 points in projective planes of order 10 Part II, *Quarterly Journal of Mathematics Oxford* **36** (1985), 383-391.

- [9] On projective planes of orders 28 or 32 whose binary code contains vectors of small weight, *Mitteilungen aus dem Mathematischen Seminar Giessen* **201** (1991), 25-33.
- [10] Necessary conditions for additive loops of finite projective planes, *Geometriae Dedicata* **19** (1985), 207-216.
- [11] On generalized Ramsey numbers for trees, (coauthor A.Brandis) *Combinatorica* **5** (1985), 95-107.
- [12] Blocking sets of 16 points in projective planes of order 10 Part III, *Rend. Sem. Mat. Univ. Padova* **74** (1985), 163-174.
- [13] Ramsey numbers for the path with three edges, *European Journal of Combinatorics* **7** (1986), 205-206.
- [14] The maximal size of a 3-arc in $PG(2, 8)$, *Journal of Combinatorial Mathematics and Combinatorial Computing* **45** (2003), 147-161, based upon (k, n) -arcs of maximal size in the plane of order 8, *Forschungsschwerpunkt Geometrie, Mathematisches Institut der Universität Heidelberg*.
- [15] On (n, k) -colorings of complete graphs, (with A. Gyárfás) *Congressus Numerantium* **58** (1987), 123-139.
- [16] Weighted arcs, the finite Radon transform and a Ramsey problem, *Graphs and Combinatorics* **7** (1991), 113-118.
- [17] A new family of 4-designs, *Graphs and Combinatorics* **11** (1995), 209-211.
- [18] A family of 4-designs with block size 9, *Discrete Mathematics* **138** (1995), 113-117.
- [19] Designs with block size 6 in projective planes of characteristic 2, *Graphs and Combinatorics* **8** (1992), 207-224.
- [20] Some friends of Alltop's designs $4 - (2^f + 1, 5, 5)$, *Journal of Combinatorial Mathematics and Combinatorial Computing* **36** (2001), 43-53.
- [21] A family of perpendicular arrays achieving perfect 4-fold secrecy, *Discrete Mathematics* **125** (1994), 63-66.

- [22] (coauthor Tran van Trung) Some highly symmetric authentication perpendicular arrays, *Designs, Codes and Cryptography* **1** (1992),307-319.
- [23] Halving $PGL(2, 2^f)$, f odd: a series of cryptocodes (coauthor Tran van Trung), *Designs, Codes and Cryptography* **1** (1991), 141-148.
- [24] Monotypical uniformly homogeneous sets of permutations, *Archiv der Mathematik* **58** (1992), 338-344.
- [25] The uniformly 3-homogeneous subsets of $PGL(2, q)$, *Journal of Algebraic Combinatorics* **4**(1995), 99-102.
- [26] Small islands, *Proceedings of the Conference on extremal problems in finite sets, Visegrad (Ungarn) 1991, Bolyai Society Mathematical Studies* **3**, pp. 93-110.
- [27] Some t -homogeneous sets of permutations (coauthors Stephen Black, Yves Edel), *Designs, Codes and Cryptography* **9** (1996),29-38.
- [28] Theory of perpendicular arrays (coauthor Yves Edel), *Journal of Combinatorial Designs* **6** (1994), 375-406.
- [29] Halving $PSL_2(q)$ (with Yves Edel), *Journal of Geometry* **64** (1999), 51-55.
- [30] Universal hashing and geometric codes, *Designs, Codes and Cryptography* **11** (1997), 207-221.
- [31] Construction of orthogonal arrays, *Journal of Statistical Planning and Inference* **56** (1996), 39-47.
- [32] Algebraic and geometric authentication systems, *manuscript*.
- [33] On families of hash functions via geometric codes and concatenation, (coauthors T.Johansson,G.Kabatiansky,B.Smeets), *Proceedings CRYPTO 93, Lecture Notes in Computer Science* **773** (1994),331-342.
- [34] Bounds on orthogonal arrays and resilient functions, *Journal of Combinatorial Designs* **3** (1995), 179-183.

- [35] (coauthors K. Gopalakrishnan, D. R. Stinson): Bounds for resilient functions and orthogonal arrays, Proceedings *CRYPTO 94*, Lecture Notes in Computer Science **839** (1994), 247-256.
- [36] A^2 -codes from universal hash classes, Proceedings *EUROCRYPT 95*, Lecture Notes in Computer Science **921** (1995), 311-318.
- [37] (with Y. Edel): New code parameters from Reed-Solomon subfield codes, *IEEE Transactions on Information Theory* **43** (1997), 953-968.
- [38] (coauthors K. Gopalakrishnan, D. R. Stinson) : Orthogonal Arrays, Resilient Functions, Error Correcting Codes and Linear Programming Bounds, *SIAM Journal on Discrete Mathematics* **6** (1996), 424-452.
- [39] (with Y. Edel) Extending and lengthening BCH-codes, *Finite Fields and Their Applications* **3** (1997), 314-333.
- [40] (with Y. Edel) Lengthening and the Gilbert-Varshamov bound, *IEEE Transactions on Information Theory* **43** (1997), 991-992.
- [41] (with Y. Edel) Twisted BCH-codes, *Journal of Combinatorial Designs* **5** (1997), 377-389.
- [42] (with Y. Edel) Some codes related to BCH-codes of low dimension, *Discrete Mathematics* **205** (1999), 57-64, reprinted in *Discrete Mathematics, Editors' Choice, Edition 1999*.
- [43] (with Y. Edel) Dense sphere packings from new codes, *Journal of Algebraic Combinatorics* **11** (2000), 95-100.
- [44] (with Y. Edel) A family of 2-weight codes related to BCH-codes, *Journal of Combinatorial Designs* **5** (1997), 391-396.
- [45] Chapters *Orthogonal Arrays of Strength more than Two* (coauthor Charles Colbourn) and *Ordered Designs and Perpendicular Arrays*, in *CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, New York, London Tokyo 1996.
- [46] (with Y. Edel) Inverting construction Y_1 , *IEEE Transactions on Information Theory* **44** (1998), 1993.

- [47] (with Y. Edel) Construction of digital nets from BCH-codes, *Monte Carlo and Quasi-Monte Carlo Methods 1996, Lecture Notes in Statistics* **127** (1997), 221-231.
- [48] Authentication via algebraic-geometric codes, in **Recent Progress in Geometry**, *Supplemento ai Rendiconti del Circolo Matematico di Palermo* **51** (1998), 139-152.
- [49] (coauthors K. Gopalakrishnan and D. R. Stinson) A note on the duality of linear programming bounds for orthogonal arrays and codes, *Bulletin of the Institute of Combinatorics and its Applications* **22**(1998),17-24.
- [50] (with Y. Edel) Families of ternary (t, m, s) -nets related to BCH-codes, *Monatshefte zur Mathematik* **132** (2001), 99-103.
- [51] (coauthors Y. Edel and L. Tolhuizen) New codes via the lengthening of BCH codes with UEP codes, *Finite Fields and Their Applications* **5** (1999), 345-353.
- [52] (with Y. Edel) A family of caps in projective 4-space in characteristic 2, *Congressus Numerantium* **141** (1999), 191-202.
- [53] (with Y. Edel) A family of caps in projective 4-space in odd characteristic, *Finite Fields and Their Applications* **6** (2000), 283-293.
- [54] (with Y. Edel) Recursive constructions for large caps, *Bulletin of the Belgian Mathematical Society - Simon Stevin* **6** (1999), 249-258.
- [55] (with Y. Edel) 41 is the largest size of a cap in $PG(4, 4)$, *Designs, Codes and Cryptography* **16** (1999), 151-160.
- [56] (with Y. Edel) Quantum twisted codes, *Journal of Combinatorial Designs* **8** (2000), 174-188.
- [57] (coauthor H. Schellwat) Weakly biased arrays, almost independent arrays and error-correcting codes, *Codes and Association Schemes*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science vol.56 (A.Barg, S.Litsyn, eds), 2001, pp.33-46.
- [58] (coauthor A. Gulliver) New linear codes over $GF(9)$, *Australasian Journal of Combinatorics* **21**(2000), 131-140.

- [59] An infinite family of 7-designs, *Discrete Mathematics* **240** (2001),1-11.
- [60] (with Y. Edel) Large caps in small spaces,
Designs, Codes and Cryptography **23** (2001), 197-212.
- [61] (coauthors Antonello Cossidente and Yves Edel)
Caps on classical varieties and their projections,
European Journal of Combinatorics **22** (2001), 135-143.
- [62] Direct constructions of additive codes ,
Journal of Combinatorial Designs **10** (2002), 207-216.
- [63] (coauthors S. Marcugini and F. Pambianco) The smallest size of a complete cap in $PG(3, 7)$, *Discrete Mathematics* **306** (2006), 1257-1263 .
- [64] (with H. Schellwat) Almost independent and weakly biased arrays: efficient constructions and cryptologic applications,
Advances in Cryptology - CRYPTO 2000 (M.Bellare,ed),
Lecture Notes in Computer Science **1880** (2000), 533-543.
- [65] The theory of cyclic codes and a generalization to additive codes,
Designs, Codes and Cryptography **25** (2002), 189-206.
- [66] (with Y. Edel) Bounds on affine caps,
Journal of Combinatorial Designs **10** (2002), 111-115.
- [67] (coauthors Y. Edel and W. Ch. Schmid) Coding-theoretic constructions for (t, m, s) -nets and ordered orthogonal arrays,
Journal of Combinatorial Designs **10** (2002), 403-418.
- [68] (with S. Marcugini and F. Pambianco) Projective planes, coverings and a network problem,
Designs, Codes and Cryptography **29** (2003), 71-89.
- [69] Large caps, *Combinatorics 2002* (G.Korchmaros, ed.), Topics in Combinatorics:geometry, graph theory and designs, Maratea (Potenza), June 2-8, 2002, pp. 7-38.
A revised version is in *Journal of Geometry* **76** (2003), 16-51.
- [70] (with Y. Edel) The largest cap in $AG(4, 4)$ and its uniqueness,
Designs, Codes and Cryptography **29** (2003), 99-104.

- [71] (with S. Marcugini, F. Pambianco) A family of highly symmetric codes, *IEEE Transactions on Information Theory* **51** (2005), 3665-3668.
- [72] (with Y. Edel) Caps of order $3q^2$ in affine 4-space in characteristic 2, *Finite Fields and Their Applications* **10** (2004), 168-182.
- [73] (with Y. Edel) A family of binary (t, m, s) -nets of strength 5, *Designs, Codes and Cryptography* **37** (2005), 211-214.
- [74] Nordstrom-Robinson code and A_7 -geometry, *Finite Fields and Their Applications* **13** (2007), 158-170.
- [75] Introduction to Coding Theory, *Chapman and Hall/CRC Press*, 2004.
- [76] (coauthor W. Ch. Schmid) An asymptotic Gilbert-Varshamov bound for (T, M, S) -nets, *Integers* **5** (2005), A04, 1-11.
- [77] (coauthor Y. Edel) Families of nets of low and medium strength, *Integers* **5** (2005), A03, 1-13.
- [78] A direct approach to linear programming bounds for codes and tms-nets, *Designs, Codes and Cryptography* **42** (2007), 127-143.
- [79] *Ordered Designs, Perpendicular Arrays and Permutation sets*, for the second edition of the *CRC Handbook of Combinatorial Designs*, pp. 542-546, published November 2006.
- [80] (coauthor Jessica Fridrich) Constructing good covering codes for applications in steganography, *LNCS Transactions on Data Hiding and Multimedia Security* (2008), 1-22.
- [81] (coauthor Gohar Kyureghyan) Crooked binomials, *Designs, Codes and Cryptography* **46** (2008), 261-301.
- [82] (coauthors G. Faina, S. Marcugini, F. Pambianco) Additive quaternary codes of small length, *Proceedings ACCT, Zvenigorod (Russia) September 2006*, 15-18.
- [83] (coauthors G. Faina, S. Marcugini, F. Pambianco) On the structure of the (n, r) -arcs in $PG(2, q)$, *Proceedings ACCT, Zvenigorod (Russia) September 2006*, 19-23.

- [84] Cyclic additive and quantum stabilizer codes, *Arithmetic of finite fields WAIFI, Madrid 2007 (C. Carlet and B. Sunar (eds), Lecture Notes in Computer Science 4547 (2007), 276-283.*
- [85] (coauthors Y. Edel, G. Faina, S. Marcugini, F. Pambianco) Short additive quaternary codes, *IEEE Transactions on Information Theory* **55** (2009), 952-954.
- [86] A family of crooked functions, *Designs, Codes and Cryptography* **50** (2009), 235-241.
- [87] (coauthors G. Faina, M. Giulietti, S. Marcugini, F. Pambianco) The geometry of quantum codes, *Innovations in Incidence Geometry* **6-7** (2009), 53-71.
- [88] (coauthors S. Marcugini and F. Pambianco) A geometric non-existence proof of an extremal additive code, *Journal of Combinatorial Theory, Series A*, **117** (2010), 128-137.
- [89] New semifields, PN and APN functions, *Designs, Codes and Cryptography* **54** (2010), 189-200. DOI: 10.1007/s10623-009-9318-7. Published online August 04, 2009.
- [90] New commutative semifields and their nuclei, Proceedings of AAECC-18 (Tarragona, Spain), M. Bras-Amorós and T. Høholdt (Eds), *Lecture Notes in Computer Science* **5527** (2009), 179-185.
- [91] *All the stabilizer codes of distance 3*, (coauthors S.Yu, Y. Dong, Q. Chen, C.H. Oh), submitted to *IEEE IT Transactions*.
- [92] (coauthor Yves Edel) *Large caps in projective Galois spaces*, in: **Current research topics in Galois geometry**, J. de Beule and L. Storme (eds), Nova Science Publishers 2011 (2nd quarter), pp. 81-94.
- [93] (coauthors R.D. Fears, S. Marcugini and F. Pambianco): *The non-existence of a $[[13, 5, 4]]$ quantum stabilizer code*, arXiv:0908.1348, *IEEE IT Transactions* **57** (2011), 4788-4793.
- [94] (coauthors D. Bartoli, S. Marcugini, F. Pambianco): *Geometric constructions of quantum codes*, *Error-Correcting Codes, Finite Geometries*

and Cryptography, Contemporary Mathematics, vol 523, Amer. Math. Soc, Providence, RI, 2010, pp. 149-154.

- [95] (coauthors D. Bartoli, S. Marcugini, F. Pambianco): *The structure of quaternary quantum caps*, in preparation.
- [96] *Commutative semifields from projection mappings*, *Designs, Codes and Cryptography* **61** (2011), 187-196.
- [97] (coauthor W. M. Kantor) *A projection construction for semifields*, submitted to *Journal of Algebraic Combinatorics*.
- [98] *Semifields, their substructures and commutativity*, submitted to the Proceedings of the Contact Forum, Brussels 2011.
- [99] *Cyclic additive codes*, manuscript.