Farmer, D. G.; **Horadam, K. J.**

Equivalence classes of multiplicative central $(p^n, p^n, p^n, 1)$-relative difference sets. (English)

Zbl 1234.05047

Cryptogr. Commun. 3, No. 1, 17-28 (2011).

Summary: We show by explicit construction that the equivalence classes of multiplicative central $(p^n, p^n, p^n, 1)$-RDSs relative to $\mathbb{Z}_p^n$ in groups E with $E/\mathbb{Z}_p^n \cong \mathbb{Z}_p^n$ arein one-to-one correspondence with the strong isotopism classes of presemifields of order p^n. We also show there are $1,446$ equivalence classes of central (16, 16, 16, 1)-RDS relative to $\mathbb{Z}_2^4$, in groups E for which $E/\mathbb{Z}_2^4 \cong \mathbb{Z}_2^4$. Only one is abelian.

MSC:

05B10 Combinatorial aspects of difference sets (number-theoretic, group-theoretic, etc.)
05B25 Combinatorial aspects of finite geometries

Keywords:

relative difference set; equivalence class; presemifield

Software:

Magma

Full Text: DOI

References:

[1] Bonnecaze, A., Duursma, I.: Translates of linear codes over \$\{\(\backslash\)mathbb Z\}_4\$. IEEE Trans. Inf. Theory 43, 1–13 (1997) · Zbl 0885.94028

[2] Bosma, W., Cannon, J., Playoust, C.: The MAGMA algebra system I: the user language. J. Symbol. Comput. 24, 235–265 (1997) · Zbl 0898.68039 · doi:10.1006/jsco.1996.0125

[3] Colbourn, C.J., Dinitz, J.H. (eds.): The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton (1996) · Zbl 0836.00010

[4] Cordero, M., Wene, G.P.: A survey of finite semifields. Discrete Math. 208/209, 125–137 (1999) · Zbl 1031.12009 · doi:10.1016/S0012-365X(99)00068-0

[5] Coulter, R.S., Henderson, M.: Commutative presemifields and semifields. Adv. Math. 217, 282–304 (2008) · Zbl 1194.12007 · doi:10.1016/j.aim.2007.07.007

[6] Davis, J.A., Jedwab, J.: A unifying construction for difference sets. J. Comb. Theory A 80, 13–78 (1997) · Zbl 0884.05019 · doi:10.1006/jcta.1997.2796

[7] Dillon, J.F.: Personal correspondence, 27 February and 15 March 2010

[8] Dempwolff, U.: Semifield planes of order 81. J. Geom. 89, 1–16 (2008) · Zbl 1175.12003 · doi:10.1007/s00022-008-1995-2

[9] Elliott, J.E.H., Butson, A.T.: Relative difference sets. Ill. J. Math. 10, 517–531 (1966) · Zbl 0145.01503

[10] Farmer, D.G.: Presemifields, bundles and polynomials over GF(p n). Ph.D. thesis, RMIT University, Melbourne, Australia (2008)

[11] Farmer, D.G., Horadam, K.J.: Presemifield bundles over GF(p 3). In: Proc. ISIT 2008, Toronto, pp. 2613–2616. IEEE (2008)

[12] Horadam, K.J.: Equivalence classes of central semiregular relative difference sets. J. Comb. Des. 8, 330–346 (2000) · Zbl 0953.05009 · doi:10.1002/1520-6610(2000)8:5<330::AID-JCD3>3.0.CO;2-X

[13] Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton (2007) · Zbl 1145.05014

[14] Horadam, K.J., Farmer, D.G.: Bundles, presemifields and nonlinear functions. Designs Codes Cryptogr. 49, 79–94 (2008) · Zbl 1178.94190 · doi:10.1007/s10623-008-9172-z

[15] Horadam, K.J., Udaya, P.: A new construction of central relative (p a , p a , p a , 1)-difference sets. Designs Codes Cryptogr. 27, 281–295 (2002) · Zbl 1027.05013 · doi:10.1023/A:1019999223151

[16] Jungnickel, D.: On automorphism groups of divisible designs. Canad. J. Math. 24, 257–297 (1982) · Zbl 0488.05012 · doi:10.4153/CJM-1982-018-x

[17] Kantor, W.M.: Commutative semifields and symplectic spreads. J. Algebra 270, 96–114 (2003) · Zbl 1041.51002 · doi:10.1016/S0021-8693(03)00411-3

[18] Knuth, D.E.: Finite semifields and projective planes. J. Algebra 2, 182–217 (1965) · Zbl 0128.25604 · doi:10.1016/0021-8693(65)90018-9

[19] LeBel, A.: Shift actions on 2-cocycles. Ph.D. thesis, RMIT University, Melbourne, Australia (2005)

[20] LeBel, A., Horadam, K.J.: Direct sums of balanced functions, perfect nonlinear functions and orthogonal cocycles. J. Comb. Des. 16, 173–181 (2008) · Zbl 1136.94006 · doi:10.1002/jcd.20187

[21] Perera, A.A.I., Horadam, K.J.: Cocyclic generalised Hadamard matrices and central relative difference sets. Designs Codes Cryptogr. 15, 187–200 (1998) · Zbl 0919.05007 · doi:10.1023/A:1008367718018

[22] Pott, A.: Finite geometry and character theory. LNM, vol. 1601. Springer, Berlin (1995) · Zbl 0818.05001

[23] Pott, A.: A survey on relative difference sets. In: Groups, Difference Sets and the Monster. Walter de Gruyter, New York (1996) · Zbl 0847.05018

[24] Robinson, D.J.S.: A Course in the Theory of Groups, 2nd edn. Springer, New York (1996)

[25] Rua, I.F., Fernandez-Combarro, E., Ranilla, J.: Classification of semifields of order 64. J. Algebra 322, 4011–4029 (2009) · Zbl 1202.12003 · doi:10.1016/j.jalgebra.2009.02.020