Surveys in Mathematics and its Applications

ISSN 1842-6298 (electronic), 1843-7265 (print)
Volume **5** (2010), 17 – 34

ON ANOTHER TWO CRYPTOGRAPHIC IDENTITIES IN UNIVERSAL OSBORN LOOPS

T. G. Jaiyéọlá and J. O. Adéníran

Abstract. In this study, by establishing an identity for universal Osborn loops, two other identities (of degrees 4 and 6) are deduced from it and they are recognized and recommended for cryptography in a similar spirit in which the cross inverse property (of degree 2) has been used by Keedwell following the fact that it was observed that universal Osborn loops that do not have the 3-power associative property or weaker forms of; inverse property, power associativity and diassociativity to mention a few, will have cycles (even long ones). These identities are found to be cryptographic in nature for universal Osborn loops and thereby called cryptographic identities. They were also found applicable to security patterns, arrangements and networks which the CIP may not be applicable to.

Full text

References

[1] R. Artzy, *On loops with a special property*, Proc. Amer. Math. Soc. **6** (1955), 448–453. MR0069804(16,1083e). Zbl 0066.27101.

[2] R. Artzy, *Inverse-Cycles in Weak-Inverse Loops*, Proc. Amer. Math. Soc. **68**, 2 (1978), 132–134. MR0463340 (57#3293). Zbl 0353.20059.

[3] A. S. Basarab, *The Osborn loop*, Studies in the theory of quasigroups and loops, **193** (1973) Shtiintsa, Kishinev, 12–18. MR0369591 (51#5824).

[4] A. S. Basarab, *Osborn's $\mathcal{G}$-loop*, Quasigroups and Related Systems **1** (1994), 51–56. MR1327945 (96e:20098). Zbl 0951.20506.

[5] A. S. Basarab, *Generalised Moufang G-loops*, Quasigroups and Related Systems **3** (1996), 1–6. MR1745960. Zbl 0944.20051.

2000 Mathematics Subject Classification: 20NO5; 08A05.
Keywords: Universal Osborn loops; Cryptography.

[6] A. S. Basarab and A. I. Belioglo, *UAI Osborn loops*, Quasigroups and loops, Mat. Issled. **51** (1979), 8–13. MR0544327 (80h:20103b). Zbl 0439.20051.

[7] R. H. Bruck, *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1966. Zbl 0141.01401.

[8] B. F. Bryant and H. Schneider, *Principal loop-isotopes of quasigroups*, Canad. J. Math. **18** (1966), 120–125. MR0188333 (32#5772). Zbl 0132.26405.

[9] O. Chein, H. O. Pflugfelder and J. D. H. Smith, *Quasigroups and loops : Theory and applications*, Heldermann Verlag, 1990. MR1125806 (93g:20133). Zbl 0719.20036.

[10] V. O. Chiboka, *The study of properties and construction of certain finite order G-loops*, Ph.D thesis, Obafemi Awolowo University, Ile-Ife,1990.

[11] P. Csörgő, *Extending the structural homomorphism of LCC loops*, Comment. Math. Univ. Carolinae **46** (2005) 3, 385–389. MR2174517 (2006g:20114). Zbl 1106.20051.

[12] P. Csörgő and A. Drápal, *Left conjugacy closed loops of nilpotency class 2*, Results Math. **47** (2005), 242–265. MR2153496 (2006b:20095). Zbl 1097.20053.

[13] J. Dene and A. D. Keedwell, *Latin squares and their applications*, the English University press Lts, 1974. MR0351850 (50 #4338). Zbl 0283.05014.

[14] A. Drápal, *Conjugacy closed loops and their multiplication groups*, J. Alg. **272** (2004), 838–850. MR2028083 (2004i:20125). Zbl 1047.20049.

[15] A. Drápal, *Structural interactions of conjugacy closed loops*, Trans. Amer. Math. Soc. **360** (2008), 671–689. MR2346467 (2009a:20118). Zbl 1144.20043.

[16] A. Drápal, *On multiplication groups of left conjugacy closed loops*, Comment. Math. Univ. Carolinae **45** (2004), 223–236. MR2075271 (2005e:20102) Zbl 1101.20035.

[17] A. Drápal, *On extraspecial left conjugacy closed loops*, J. Alg. **302** (2) (2006), 771–792. MR2293781 (2008b:20081). Zbl 1109.20056.

[18] A. Drápal (2004), *On left conjugacy closed loops with a nucleus of index two*, Abh. Math. Sem. Univ. Hamburg **74** (2004), 205–221. MR2112832 (2005k:20173). Zbl 1084.20043.

[19] P. Csörgő and A. Drápal, *On left conjugacy closed loops in which the left multiplication group is normal*, Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, **76** (2006) 17–34. MR2293429 (2008g:20150). Zbl 1128.20052.

[20] E. G. Goodaire and D. A. Robinson, *A class of loops which are isomorphic to all loop isotopes*, Can. J. Math. **34** (1982), 662–672. MR0663308 (83k:20079). Zbl 0467.20052.

[21] E. G. Goodaire and D. A. Robinson, *Some special conjugacy closed loops*, Canad. Math. Bull. **33** (1990), 73–78. MR1036860(91a:20077). Zbl 0661.20046.

[22] E. G. Goodaire, E. Jespers and C. P. Milies (1996), *Alternative loop rings*, NHMS(184), Elsevier, 1996.MR1433590(98e:17041). Zbl 0878.17029.

[23] R. L. Jr. Griess, *Code loops*, J. Alg. **100** (1986), 224–234.MR0839580 (87i:20124). Zbl 0589.20051.

[24] E. D. Huthnance Jr., *A theory of generalised Moufang loops*, Ph.D. thesis, Georgia Institute of Technology, 1968.

[25] T. G. Jaíyéọlá, *A study of new concepts in Smarandache quasigroups and loops*, ProQuest Information and Learning (ILQ), Ann Arbor, USA, 2009. MR2489953. Zbl 1159.20035.

[26] T. G. Jaiyéọlá and J. O. Adéníran, *New identities in universal Osborn loops*, Quasigroups And Related Systems, Vol. 17 (2009). MR2536708. Zbl pre05578166.

[27] A. D. Keedwell, *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin. **20** (1999), 241—250. MR1723878 (2000h:20123). Zbl 0935.20061.

[28] M. K. Kinyon, *A survey of Osborn loops*, Milehigh conference on loops, quasigroups and non-associative systems, University of Denver, Denver, Colorado, 2005.

[29] M. K. Kinyon, K. Kunen, *The structure of extra loops*, Quasigroups and Related Systems **12** (2004), 39–60. MR2130578 (2006a:20121). Zbl 1076.20065.

[30] M. K. Kinyon, K. Kunen, J. D. Phillips, *Diassociativity in conjugacy closed loops*, Comm. Alg. 32 (2004), 767–786. MR2101839 (2005h:20159). Zbl 1077.20076 .

[31] M. K. Kinyon, K. Kunen, *Power-associative conjugacy closed loops*, J. Alg. **304** (2) (2006), 679–711. MR2264275 (2007h:20075). Zbl 1109.20057.

[32] K. Kunen, *G-loops and Permutation Groups*, J. Alg. **220** (1999), 694–708. MR1717366(2000j:20133). Zbl 0944.20056.

[33] K. Kunen, *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352** (2000), 2889–2911. MR1615991(2000j:20132). Zbl 0962.20048.

[34] P. T. Nagy and K. Strambach, *Loops as invariant sections in groups, and their geometry*, Canad. J. Math. **46** (1994), no. 5, 1027–1056. MR1295130 (95h:20088). Zbl 0814.20055.

[35] J. M. Osborn, *Loops with the weak inverse property*, Pac. J. Math. **10** (1961), 295–304. MR0111800 (22 #2660). Zbl 0091.02101.

[36] H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Sigma series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990. MR1125767 (93g:20132). Zbl 0715.20043.

[37] J. D. Phillips, *A short basis for the variety of WIP PACC-loops*, Quasigroups and Related Systems **1** (2006) 14, 73–80. MR2268827. Zbl 1123.20063.

[38] W. B. Vasantha Kandasamy, *Smarandache loops*, Department of Mathematics, Indian Institute of Technology, Madras, India, 2002. MR1958775 (2004a:20076). Zbl 1050.20045.

T. G. Jaiyéọlá
Obafemi Awolowo University,
Department of Mathematics,
Ile Ife 220005, Nigeria.
e-mail: jaiyeolatemitope@yahoo.com,tjayeola@oauife.edu.ng
http://www.oauife.edu.ng/faculties/science/mth/research.htm#jaiyeola

J. O. Adéníran
University of Agriculture,
Department of Mathematics,
Abeokuta 110101, Nigeria.
e-mail: ekenedilichineke@yahoo.com, adeniranoj@unaab.edu.ng
http://www.unaab.edu.ng/attachments/435_DR.%20Adeniran.pdf