zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Goltvanitsa, M. A.

Digit sequences of skew linear recurrences of maximal period over Galois rings. (English)
Zbl 1476.11025
Mat. Vopr. Kriptografii 6, No. 2, 19-27 (2015).

Summary: A pseudo-random sequences constructed as a digit sequence of a skew linear recurrence of maximal period over Galois ring are studied. We find the periods of such sequences and lower bounds for their ranks as a sequences over field. A rank of the first digit sequence of a skew linear recurrence of maximal period is determined exactly under certain conditions on the digit set.

MSC:

11B37 Recurrences
11B83 Special sequences and polynomials
11T99 Finite fields and commutative rings (number-theoretic aspects)

Cited in **4** Documents

Keywords:

skew linear recurrences; Galois ring; digit sequence

Full Text: DOI MNR

References:

[1] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., "Linear recurring sequences over rings and modules", J. Math. Sci., 76:6 (1995), 2793-2915 · Zbl 0859.11001 · doi:10.1007/BF02362772

[2] Nechaev A. A., "Kerdock code in a cyclic form", Diskretnaya matematika, 1:4 (1989), 123-139 (in Russian) · Zbl 0734.94023

[3] Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N., "Skew linear recurring sequences of maximal period over Galois rings", J. Math. Sci., 187:2 (2012), 115-128 · Zbl 1273.12003 · doi:10.1007/s10958-012-1054-2

[4] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyschev V. N., "Linear and polylinear recurring sequences over abelian groups and modules", J. Math. Sci., 102:6 (2000), 4598-4626 · Zbl 1036.11003

[5] Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N., "Skew LRS of maximal period over Galois rings", Matematicheskie voprosy kriptografii, 4:2 (2013), 59-72 · Zbl 1477.11025

[6] Tsaban B., Vishne U., "Efficient linear feedback shift registers with maximal period", Finite Fields and Their Applications, 8:2 (2002), 256-267 · Zbl 1015.94005 · doi:10.1006/ffta.2001.0339

[7] Zeng G., Han W., He K., Word-oriented feedback shift register: \(\sigma \)-LFSR, Cryptology ePrint Archive: Report 2007/114,

[8] Zeng G., He K. C., Han W., "A trinomial type of \(\sigma \)-LFSR oriented toward software implementation", Science in China, Series F - Information Sciences, 50:3 (2007), 359-372 · Zbl 1142.94008

[9] Zeng G., Yang Y., Han W., Fan Sh., "Word oriented cascade jump \(\sigma \)-LFSR", AAECC, 2009, 127-136 · Zbl 1273.94363

[10] Ghorpade S. R., Hasan S. U., Kumari M., "Primitive polynomials, Singer cycles, and word-oriented linear feedback shift registers", Des. Codes Cryptogr., 58:2 (2011), 123-134 · Zbl 1263.11108 · doi:10.1007/s10623-010-9387-7

[11] Ghorpade Sudhir R., Ram Samrith, "Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields", Finite Fields Appl., 17:5 (2011), 461-472 · Zbl 1263.11112 · doi:10.1016/j.ffa.2011.02.008

[12] Kuzmin A. S., Nechaev A. A., "Linear recurring sequences over Galois rings", Uspekhi matem. nauk, 48:1 (1993), 167-168 (in Russian) · Zbl 0811.11075

[13] Glukhov M. M., Elizarov V. P., Nechaev A. A., Algebra, v. II, Gelios ARV, 2003 (in Russian)

[14] Kurakin V. L., "The first coordinate sequence of a linear recurrence of maximum period over a Galois ring", Diskretnaya matematika, 6:2 (1994), 88-100 (in Russian) · Zbl 0824.11072

[15] Kuzmin A. S. Nechaev A. A., "Linear recurring sequences over Galois rings", Algebra i Logika, 3:2 (1995), 169-189 (in Russian) · Zbl 0872.11055

[16] Lidl R., Niederreiter H., Finite Fields, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, 1983 · Zbl 0554.12010

[17] Nechaev A. A., "Finite Rings with Applications", Handbook of Algebra, 5, ed. M. Hazewinkel, Elsevier B. V., 2008, 213-320 · Zbl 1197.16027

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically

Edited by FIZ Karlsruhe, the European Mathematical Society and the Heidelberg Academy of Sciences and Humanities
© 2023 FIZ Karlsruhe GmbH

matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.

© 2023 FIZ Karlsruhe GmbH