

Kamlovskii, O. V.

Distribution properties of rows and columns for matrix linear recurrent sequences of the first order. (Russian. English summary) [Zbl 1476.11027](#)

Mat. Vopr. Kriptografii 6, No. 4, 65-76 (2015).

Summary: We consider sequences of matrices over Galois ring satisfying linear recurrent equation of the first order. Estimates of the frequencies of rows and columns in such sequences are obtained. These results generalize previously known bounds.

MSC:

11B37 Recurrences

11B83 Special sequences and polynomials

11T99 Finite fields and commutative rings (number-theoretic aspects)

Keywords:

Galois rings; matrix sequences; matrix generators

Full Text: [DOI](#) [MNR](#)

References:

- [1] Nechaev A. A., "Kod Kerdoka v tsiklicheskoj forme", *Diskret. matem.*, 1:4 (1989), 123-139 · [Zbl 0734.94023](#)
- [2] Nechaev V. I., "Raspredelenie znakov v posledovatelnosti pryamougolnykh matrits nad konechnym polem", *Trudy Matematicheskogo instituta imeni V. A. Steklova*, 218, 1997, 335-342 · [Zbl 0932.11077](#)
- [3] Tsypyshev V. N., "Matrichnyi lineinyi kongruentnyi generator nad koltsom Galua nechetnoi kharakteristiki", *Chebyshevskii sbornik*, 4:1 (2003), 112-124 · [Zbl 1116.94009](#)
- [4] Gentle J. E., *Random number generation and Monte Carlo methods*, Springer-Verlag, New York, 2003 · [Zbl 1028.65004](#)
- [5] Afflerbach L., Grothe H., "The lattice structure of pseudo-random vectors generated by matrix generators", *J. Comput. Appl. Math.*, 23 (1988), 127-131 · [Zbl 0658.65006](#) · [doi:10.1016/0377-0427\(88\)90338-X](#)
- [6] Niederreiter H., "Statistical independence properties of pseudorandom vectors produced by matrix generators", *J. Comput. Appl. Math.*, 31 (1990), 139-151 · [Zbl 0708.65007](#) · [doi:10.1016/0377-0427\(90\)90345-Z](#)
- [7] Nechaev A. A., "Tsiklovye tipy lineinykh podstanovok nad konechnymi kommutativnymi koltsami", *Matem. sb.*, 184:3 (1993), 21-56 · [Zbl 0857.11066](#)
- [8] Kamlovskii O. V., "Chastotnye kharakteristiki lineinykh rekurrentnykh posledovatelnoei nad koltsami Galua", *Matem. sb.*, 200:4 (2009), 31-52 · [Zbl 1232.94013](#) · [doi:10.4213/sm4528](#)
- [9] Kamlovskii O. V., "Chastotnye kharakteristiki razryadnykh posledovatelnoei lineinykh rekurrent nad koltsami Galua", *Izv. RAN. Ser. matem.*, 77:6 (2013), 71-96 · [Zbl 1286.11018](#) · [doi:10.4213/im7799](#)
- [10] Korobov N. M., "Raspredelenie nevychetov i pervoobraznykh kornei v rekurrentnykh ryadakh", *Doklady AN SSSR*, 88:4 (1953), 603-606 · [Zbl 0050.04301](#)
- [11] Niederreiter H., "Distribution properties of feedback shift register sequences", *Probl. Control and Inform. Theory*, 15:1 (1986), 19-34 · [Zbl 0607.94012](#)
- [12] Nechaev A. A., "O podobii matrits nad kommutativnym lokalnym artinovym koltsom", *Trudy seminar im. Petrovskogo I. G.*, 184, no. 9, 1983, 81-101
- [13] Leng S., *Algebra*, Mir, M., 1968, 564 pp.
- [14] Glukhov M. M., Elizarov V. P., Nechaev A. A., *Algebra*, Uchebnyk, v. 2, Gelios ARV, M., 2003, 416 pp.

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