Ermilov, D. M.; **Kozlitin, O. A.**

On the structure of graph of polynomial transformation of the Galois ring. (Russian. English summary) Zbl 1475.94116

Mat. Vopr. Kriptografii 6, No. 3, 47-73 (2015).

Summary: Graphs of polynomial transformations of Galois ring R having cardinality q^n and characteristic p^n are studied. A cyclic structure of polynomial permutations having maximal possible cycle length $q(q-1)p^{n-2}$ is described and an algorithm for the construction of such permutations is proposed. For graphs of nonbijective transformations some numerical characteristics of sets of noncyclic vertices are computed.

MSC:

94A60 Cryptography
94B25 Combinatorial codes

Keywords:

cyclic structure of graph; polynomial with maximal length cycle; polynomial transformation of the Galois ring

Full Text: DOI MNR

References:

[1] Glukhov M. M., Elizarov V. P., Nechaev A. A., Algebra, Gelios-ARV, M., 2003, 749 pp.

[2] Carlitz L., "Functions and polynomials \((\operatorname{mod}\,p^n)\)", Acta Arithmetica, 9 (1964), 66-78

[3] Knut D. E., Iskusstvo programmirovaniya, v. 2, Izd. dom Vilyams, Moskva-Sankt-Peterburg-Kiev, 2000, 828 pp.

[4] Anashin V. S., "O gruppakh i koltsakh, obladayuschikh tranzitivnymi polinomami", XVI Vsesoyuznaya algebraicheskaya konferentsiya, Tezisy, ch. II, 1981, 4-5

[5] Larin M. V., "Tranzitivnye polinomialnye preobrazovaniya kolets vychetov", Diskretn. matem., 14:2 (2002), 20-32 · Zbl 1054.11010 · doi:10.4213/dm238

[6] Nechaev A. A., "Polinomialnye preobrazovaniya konechnykh kommutativnykh kolets glavnykh idealov", Matematicheskie zametki, 27:6 (1980), 885-897 · Zbl 0448.13020

[7] Viktorenkov V. E., "Orgraf polinomialnogo preobrazovaniya nad kommutativnym lokalnym koltsom", Obozr. prikl. i promyshl. matem., 7:2 (2000), 327

[8] Viktorenkov V. E., "O nekotorykh kharakteristikakh tsiklovoi struktury sluchainykh ravnoveroyatnykh podstanovok s pomechennymi tsiklami i ikh primenenie dlya issledovaniya polinomialnykh preobrazovanii kolets", Obozr. prikl. i promyshl. matem., 10:3 (2003), 621

[9] Ermilov D. M., Kozlitin O. A., "Tsiklovaya struktura polinomialnogo generatora nad koltsom Galua", Matematicheskie voprosy kriptografii, 4:1 (2013), 27-57

[10] Elizarov V. P., Konechnye koltsa, Gelios-ARV, M., 2006, 304 pp.

[11] Asanov M. O., Baranskii V. A., Rasin V. V., Diskretnaya matematika: grafy, matroidy, algoritmy, NITs Regulyarnaya i khaoticheskaya dinamika, Izhevsk, 2001, 288 pp.