UDC 512.7+519.7+681.3

Automata on Algebraic Structures

V. V. Skobelev

Institute of Applied Mathematics and Mechanics, National Academy of Sciences of Ukraine, Ukraine, 83114, Donetsk, R. Luxemburg st., 74, vv_skobelev@iamm.ac.donetsk.ua

A survey of results obtained in investigations of automata determined over finite algebraic structures. The objects of research are automata over some finite ring, automata determined in terms of ideals, automata over varieties, and families of hash-functions determined by automata without output function. Computational security, complexity of simulation and homomorphisms of investigated automata are characterized.

Key words: rings, automata, identification, computational security.

References

1. Gill A. *Lineinye posledovatel'nostnye mashiny* [Linear sequential machines]. Moscow, Nauka, 1974. 298 p. (in Russian).

2. Faradgev R. G. *Lineinye posledovatel'nostnye mashiny* [Linear sequential machines]. Moscow, Sovetskoje Radio, 1975, 248 p. (in Russian).

3. Agibalov G. P. Recognition of operators realized by linear autonomous automata. *Izv. AN USSR. Tech. Cybernetika*, 1970, no. 3, pp. 99–108 (in Russian).

4. Agibalov G. P., Jufit Ya.G. O prostykh eksperimentakh dlia lineinykh initsial'nykh avtomatov [On simple experiments for linear initial automata]. *Avtomatica i vychisliteljnaja technika*, 1972, no. 2, pp. 17–19 (in Russian).

5. Speranskij D. V. *Eksperimenty s lineinymi i bilineinymi konechnymi avtomatami* [Experiments with linear and bi-linear finite automata]. Saratov, Saratov. Univ. Press, 2004. 144 p. (in Russian).

6. Kurosh A.G. *Lektsii po obshchei algebre* [Lectures in general algebra]. Moscow, Nauka, 1973, 400 p. (in Russian).

7. Skobelev V. V., Skobelev V. G. Analiz shifrsistem [Analysis of ciphersystems]. Donetsk, IAMM NASU, 2009, 479 p. (in Russian).

8. Skobelev V. V., Glazunov N. M., Skobelev V. G. *Mnogoobraziia nad kol'tsami. Teoriia i prilozhenie* [Varieties over rings. Theory and applications]. Donetsk, IAMM NASU, 2011, 323 p. (in Russian).

9. Skobelev V. V., Skobelev V. G. Analysis of nonlinear automata with lag 2 over finite ring. *Prikladnaja discretnaja matematika*, 2010, no. 1, pp. 68–85 (in Russian).

10. Skobelev V. V. Complexity of identification of nonlinear 1-dimensional automata with lag 2 over finite ring. *Computernaja mathematika*, 2011, vol. 2, pp. 81–89 (in Russian).

11. Kuznetsov S. P. *Dinamicheskii khaos* [Dynamical chaos]. Moscow, Fizmatlit, 2001. 296 p. (in Russian).

12. Skobelev V. V., Skobelev V. G. On the complexity of analysis of automata over a finite ring. *Cybernet. Systems Anal.*, 2010, vol. 46, no. 4, pp. 533–545.

13. Skobelev V. V. On systems of polynomial equations over finite rings. *Naukovi zapysky NaU-KMA. Ser. Computerny nauky*, 2012, vol. 138, pp. 15–19.

14. Skobelev V. V. On subsets of automata over finite ring determined via terms of ideals. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2011, no. 3, pp. 212–218 (in Ukrainian).

15. Skobelev V. V. Simulation of automata over a finite ring by the automata with finite memory. *J. of Automation and Information Sci.* 2012, vol. 44, no. 5, pp. 57–66.

16. Skobelev V. V. Analysis of the problem of recognition of automaton over some ring. *Dopov. Nats. Akad. Nauk Ukr., Mat., Pryr., Tekh. Nauky*, 2012, no. 9, pp. 29–35 (in Russian).

17. Skobelev V. V. On automata determined over varieties over some ring. *Tr. Inst. Prikl. Mat. Mekh.*, 2012, vol. 24, pp. 190–201 (in Russian).

18. Skobelev V. V. Automata over vatieties with some algebra. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2012, no 2, pp. 234–238 (in Ukrainian).

19. Skobelev V. V. Analysis of automata determined over parametric varieties over an associative ring. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2012, no. 3, pp. 239–244.

20. Skobelev V. V. On automata determined over polynomially parametric varieties over some finite ring. *Tr. Inst. Prikl. Mat. Mekh.* 2012, vol. 25, pp. 185–195 (in Russian).

21. Skobelev V. V. On homomorphisms of automata over varieties over some ring. *Dopov. Nats. Akad. Nauk Ukr., Mat., Pryr., Tekh. Nauky*, 2013, no. 1, pp. 42–46 (in Russian).

22. Skobelev V. V. Analysis of automata determined over elliptic curves. *Visn., Ser. Fiz.-Mat. Nauky, Kyïv. Univ. Im. Tarasa Shevchenka*, 2012, no. 1, pp. 223–230 (in Ukrainian).

23. Skobelev V. V. Analysis of families of hash functions defined by automata over a finite ring. *Cybernet. Systems Anal.*, 2013, vol. 49, no. 2, pp. 209–216.