Design and Analysis of a New Logistic Chaotic Digital Generation Circuit

Juan Wang(✉), Liu Wenbin, Han Tongzhuang, and Zhou Xin

Electronic and Information Engineering Institute, Heilongjiang University of Science and Technology, Harbin 150027, People's Republic of China
76115347@qq.com

Abstract. Chaotic signals have the characteristics of noise-like, difficult to predict, and very sensitive to the initial state. They have broad application prospects in the fields of communication and cryptography. Aiming at the shortcomings of the traditional one-dimensional discrete logistic chaotic map, the full mapping space is small, and the complexity is not high. In this paper, a new type of logistic digital chaos generation circuit with better performance is modeled and simulated. By testing and analyzing the initial value sensitivity, autocorrelation and other characteristics of the generated sequence, the influence and rules of circuit parameter setting on the randomness of digital chaotic sequences are obtained, so as to provide the necessary theoretical basis for the application of digital chaotic sequences.

Keywords: New logistic chaos · Digital circuit · NIST test

1 Introduction

Chaos is a common motion form of nonlinear dynamics, and is a seemingly random behavior generated by deterministic nonlinear systems. This random behavior is different from the general random phenomenon and is determined only by the randomness of the system [1]. Owing to the unpredictability, anti-interception, high randomness, high complexity and easy implementation of chaotic signals, it has an excellent application prospect in secure communication [2]. Although the traditional logistic mapping is simple in form, it has the problems of small chaotic parameter range, small full mapping space, uneven iterative distribution, and low complexity, etc., poor security greatly limits the application of chaotic circuits in practice [3–6]. A new type of logistic mapping can be proposed in Literature [7], which has the advantages of high complexity, difficult prediction, strong sensitivity, full mapping parameter range, uniform iterative distribution, and strong randomness, and can better meet the chaotic secure communication field application requirements.

Due to Field Programmable Gate Array (FPGA) has the advantages of short development cycle, low input cost, reprogrammable, erasable, etc. [8], Many researchers have tried to use digital circuit technology to implement chaotic systems and applications

X. Jiang and P. Li (Eds.): GreeNets 2020, LNICST 333, pp. 66–74, 2020.
https://doi.org/10.1007/978-3-030-62483-5_8

in FPGA circuit boards. In this paper, the new logistic digital chaotic circuit in Matlab/Simulink environment can be achieved by modeling and simulating via using the DSP-Builder toolbox. Via reasonable circuit design and parameter setting, simulation analysis and NIST test of the new logistic chaotic circuit can be experimented, and the potential security risks are reduced and eliminated by studying the influence of the circuit parameter settings on the randomness of the chaotic sequence and its regularity. Thus, the digital chaotic signals generated by the system model can better meet the requirements in the application of chaotic secure communication systems.

2 New Logistic Chaotic Map

Discrete chaotic mapping refers to a system described by a difference equation, capable of generating discrete time domain and continuous amplitude chaotic signals. Owing to only through mapping functions, generation rules, and initial conditions, chaotic sequences can be generated. Thus, it has the advantages of simple, rapid, and easy control, and is widely used in the field of secure communications.

The traditional logistic chaotic map has become a widely studied and applied chaotic map because of its simple mathematical model. Although it has good pseudo-randomness and correlation and simple circuit implementation, there are still many problems, such as infinitely many fixed point attractors, small mapping space, small chaotic parameter range, uneven iterative distribution, and low complexity. Thereby reducing system security and anti-interference [9]. The new logistic chaotic mapping equation is:

$$x_{n+1} = \mu x_n(1 - x_n^2) \qquad n = 1, 2, 3 \ldots \tag{1}$$

In Eq. (1), initial value $x_0 \in (0, 1)$, x_n is the value of the n iteration, x_{n+1} is the value of the $n + 1$ iteration, $x_n \in (-1, 1)$, system parameters $\mu \in (0, 4]$, when $\mu \in [2.38, 4]$, the new logistic map is in a chaotic state.

3 Circuit Design of New Logistic Chaotic Map

As shown in Fig. 1, the new logistic chaotic circuit is built using the DSP Builder component library in the Matlab/Simulink environment. When the input pulse of the data selector is high, Constant = 0.15 is used as the initial value of the chaotic circuit. When the input pulse of the data selector is low, the new logistic chaotic iteration is started. The delayer ensures stable data output. The multiplier completes the data multiplication, the adder completes the data addition, the amplifier completes the data amplification and completes an iterative output, and finally realizes the interval quantization output through the barrel shift register and the bit decimator. The interval quantization function is defined as follows:

$$T[\mathrm{x}(n)] = \begin{cases} 0, x(n) \in \bigcup_{k=0}^{2^{\mathrm{m}}-1} I_{2k}^{m} \\ 1, x(n) \in \bigcup_{k=0}^{2^{\mathrm{m}}-1} I_{2k-1}^{m} \end{cases} \tag{2}$$

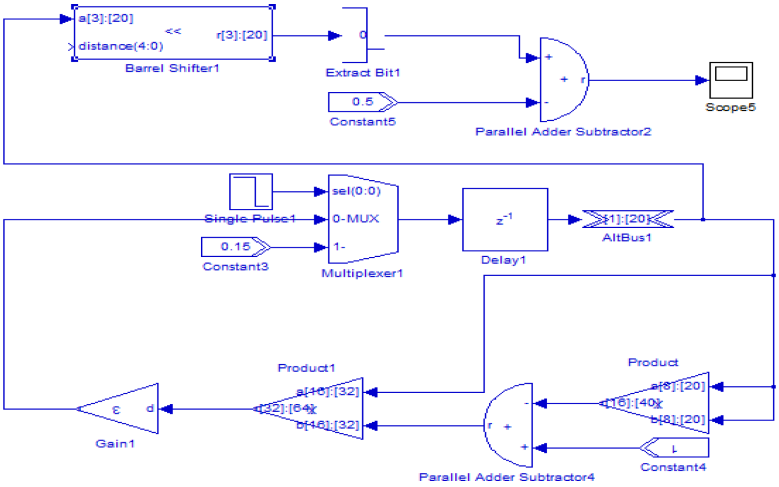


Fig. 1. Digital generation circuit of new logistic chaotic map

In Eq. (2), $m > 0$ and any positive integer. $I_0^m, I_1^m, I_2^m, \ldots$ is 0, 1 interval 2^m consecutive equal molecular interval. If the conversion value falls in the odd interval, it is quantized to 1, and if the conversion value falls in the even interval, it is quantized to 0.

In the case of ensuring that the bit width is sufficient and data will not overflow, minimizing the width of the bit width as much as possible can save resources inside the FPGA chip. The Altbus module (a:b) can map floating-point signals to fixed-point data. a represents the number of binary digits before the decimal point, and b represents the number of binary digits after the decimal point. By changing the settings of the Altbus module, the optimal parameter settings of the system are obtained, and achieve circuit design on target hardware.

4 Characteristics Analysis of New Logistic Chaotic Map

4.1 Numerical Distribution of New Logistic Chaotic Map

The numerical distribution of chaotic sequences is the criterion for judging the system's pseudo-randomness and the ability to resist statistical analysis attacks. The more uniform the distribution, the stronger its performance [10]. The new logistic numerical distribution is simulated. As shown in Fig. 2, the simulation time is set to 100, the gain is set to 3, and the initial value is set to 0.15. Through simulation analysis, it can be seen that when the Altbus module parameter $b < 20$, the numerical distribution of the new logistic chaotic sequence is not ideal; when the Altbus module parameter $b \geq 20$, the new logistic chaotic sequence has a relatively ideal numerical distribution. Therefore, it is concluded that the larger the b value of the Altbus module parameter is set, the better the numerical distribution of the new logistic. In order to balance system performance and hardware resources, the b value should generally be set to 20.

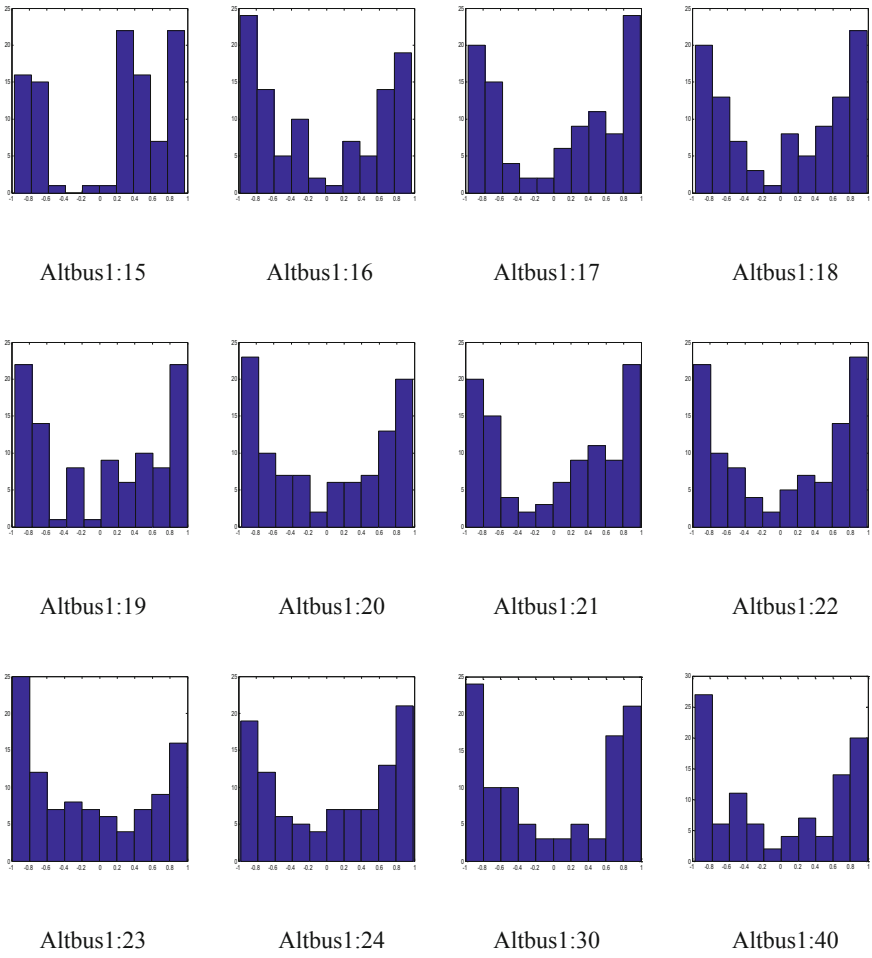
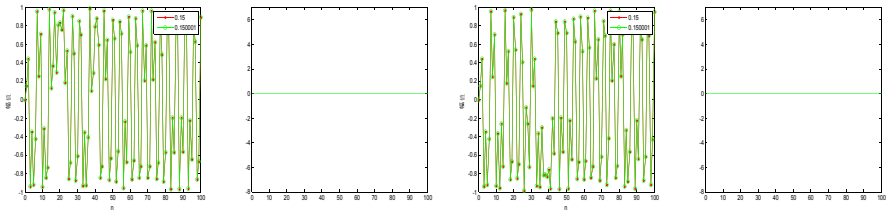


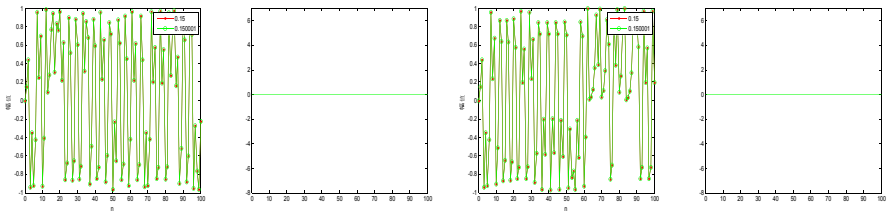
Fig. 2. Numerical distribution of new logistic chaotic map

4.2 Initial Value Sensitivity of New Logistic Chaotic Map

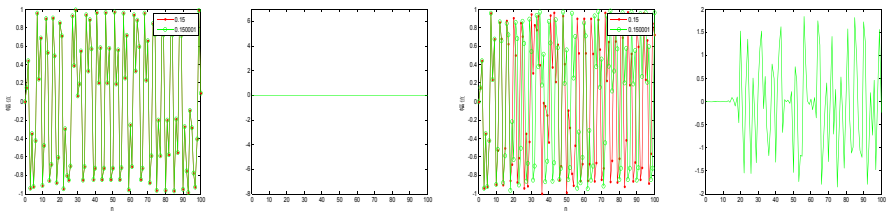
The initial value sensitivity of chaos is an objective reflection of the change of the system trajectory when the system undergoes small changes in the initial conditions [11]. The strength of the randomness of the system depends on the initial value sensitivity. Simulation experiments are performed on the initial sensitivity of the new logistic chaotic model. As shown in Fig. 3, the simulation time is set to 100, the gain is set to 3, and the initial values are set to 0.15 and 0.150001. Fig(a) shows the iteration values, and Fig(b) shows the difference between the two. Through simulation analysis, it can be seen that when the parameter *b* of the Altbus module is less than 20, the initial value sensitivity of the new logistic chaotic sequence is not ideal; when the parameter *b* of the Altbus module is greater than or equal to 20, the initial chaotic value differs only by 0.000001 and its iterative output will be completely different. Therefore, it is concluded that the



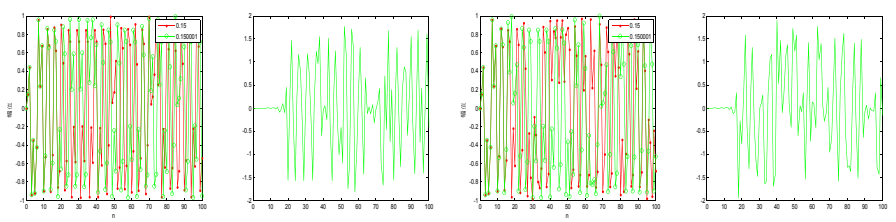
(a) Altbus1:15 (b) (a) Altbus1:16 (b)



(a) Altbus1:17 (b) (a) Altbus1:18 (b)

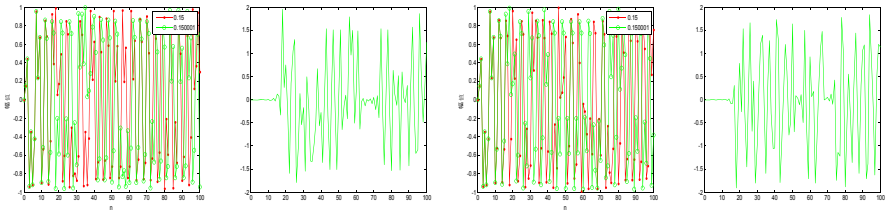


(a) Altbus1:19 (b) (a) Altbus1:20 (b)

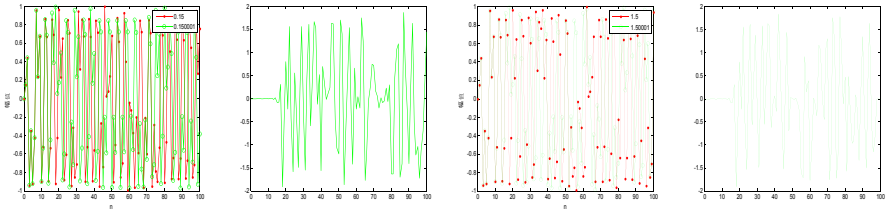


(a) Altbus1:21 (b) (a) Altbus1:22 (b)

Fig. 3. Initial value iteration of new logistic chaotic map



(a) Altbus1:23 (b) (a) Altbus1:24 (b)



(a) Altbus1:30 (b) (a) Altbus1:40 (b)

Fig. 3. (*continued*)

larger the b value of the Altbus module parameter, the better the initial value sensitivity of the new logistic. In order to balance system performance and hardware resources, the b value should generally be set to 20.

4.3 Autocorrelation of New Logistic Chaotic Map

Autocorrelation is a measure of the time-delay sequence similarity of the random sequence itself, and is an important index for measuring the security of chaotic systems [12]. In order to verify the influence of autocorrelation on the random characteristics of chaotic systems, a simulation experiment is performed on the autocorrelation of the new logistic chaotic model. As shown in Fig. 4, the simulation time is set to 1000, the gain is set to 3, and the initial value is set to 0.15. The simulation analysis shows that when the Altbus module parameter $b < 20$, the autocorrelation of the new logistic chaotic sequence is not ideal; when the Altbus module parameter $b \geq 20$, the new logistic chaotic sequence has ideal autocorrelation. Therefore, it is concluded that the larger the b value of the Altbus module parameter, the better the autocorrelation of the new logistic. In order to balance system performance and hardware resources, the b value should generally be set to 20.

4.4 NIST Test of New Logistic Chaotic Map

In order to further verify that the performance of the new logistic chaotic sequence is affected by the Altbus module parameter settings, according to the 16 test standards

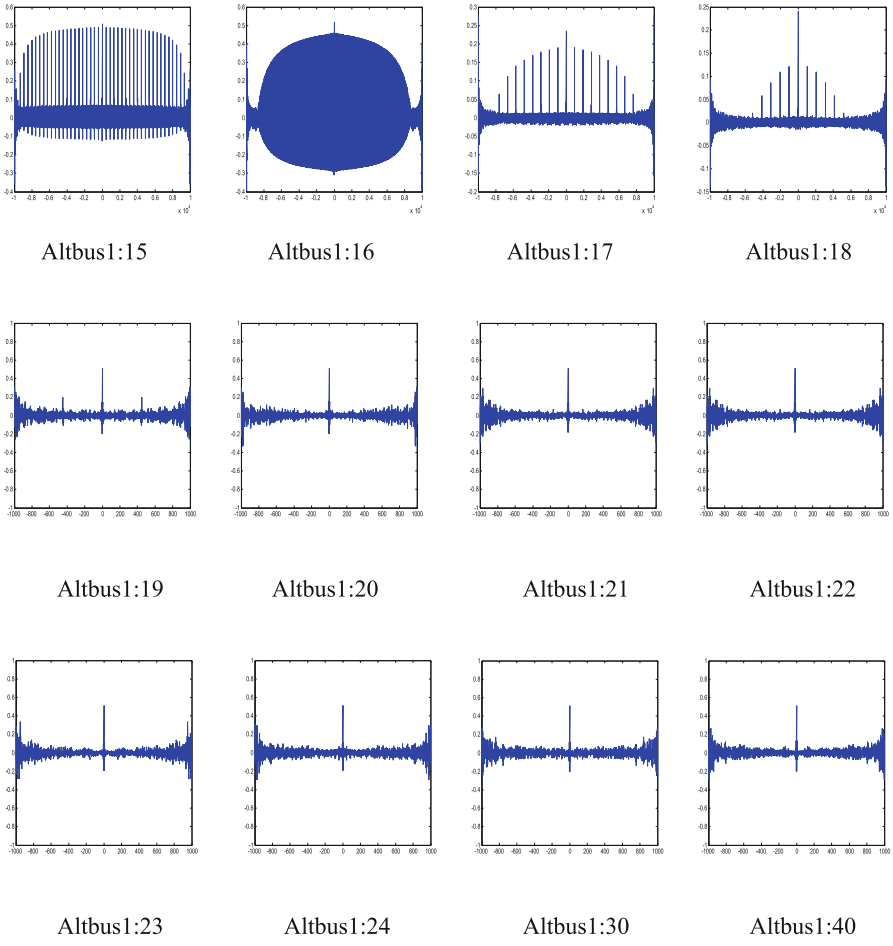


Fig. 4. Autocorrelation analysis of new logistic chaotic map

prepared by the National Institute of Standards and Technology (NIST), this paper conducts four tests: single-bit frequency, block frequency, runs, and longest run [13]. Among them, the p value * indicates that it does not meet the test requirements. If the p value is a number, it indicates that the test is passed. A larger p value indicates a better test result [14]. As can be seen from Table 1, when the b value of the Altbus module is set to 15–19, the test result of the new logistic chaotic sequence is poor, and the test result is better when the b value of the Altbus module is set to 20–25. Therefore, it is concluded that the larger the b value of the Altbus module parameter is set, the better the test result of the new logistic. In order to balance system performance and hardware resources, the b value should be set to 20 in combination with the above experiments.

Table 1. NIST test of new logistic chaotic map

Altbus a:b	Single-bit frequency		Block frequency		Runs		Longest run	
	p value	Proportion	*p* value	Proportion	*p* value	Proportion	*p* value	Proportion
1:15	*	100/100	*	100/100	*	100/100	*	99/100
1:16	*	100/100	*	100/100	*	98/100	*	100/100
1:17	*	98/100	*	97/100	*	98/100	*	98/100
1:18	*	99/100	*	100/100	0.304126	100/100	*	99/100
1:19	*	100/100	*	98/100	0.401996	100/100	*	100/100
1:20	0.381557	100/100	0.897762	100/100	0.237811	100/100	0.350485	100/100
1:21	0.319084	97/100	0.534146	97/100	0.162606	97/100	0.201998	97/100
1:22	0.619747	98/100	0.595549	98/100	0.334408	98/100	0.384125	98/100
1:23	0.712603	100/100	0.616305	100/100	0.498671	100/100	0.667396	100/100
1:24	0.892042	98/100	0.743126	98/100	0.868922	98/100	0.732411	98/100
1:25	0.912033	99/100	0.754439	99/100	0.877469	99/100	0.886579	99/100

5 Conclusion

Traditional logistic chaos, which has its unique characteristics and simple calculation rules, has very significant advantages in practical applications. The design and implementation of chaotic circuits is the key to the research of chaotic applications. This paper utilizes DSP-Builder toolbox to realize the modeling and simulation of the new logistic digital simulation circuit in matlab/simulink environment. It overcomes the difficulty and instability of the design of the analog chaotic circuit, and focus on the influence of chaotic circuit characteristics on the Altbus parameters setting of the conversion module, thereby reducing and eliminating potential safety hazards. The conclusions in this paper provide a certain theoretical basis for the generation of digital chaotic circuits, and have excellent application prospects in chaotic secure communication systems. The next step is to study the frequency domain characteristics of the new logistic digital circuit by changing the parameter settings, and obtain more accurate and comprehensive new logistic chaotic circuit characteristics.

Funding. This work was supported by Heilongjiang Fundamental Research Foundation for the Local Universities (2018KYYWF1189) and Science and Technology Innovation Foundation of Harbin (2017RAQXJ082).

References

1. Qin, J.C.: Realization of chaotic system and its control digital circuit. Masterundefineds degree thesis of Yunnan University (2014)
2. Wang, J., Ding, Q.: Dynamic rounds chaotic block cipher based on keyword abstract extraction. Entropy **20**(9), 693 (2018)
3. Li, Z.B., Li, F.Q., Zhu, X.M.: Chaotic secure communication simulation of deformed Chua's circuit. J. West Anhui Univ. **05**, 61–64 (2014)

4. Wu, Y.: Improvement of encryption scheme of classic logistic map image and exploration of double chaos encryption technology of digital image. Xinjiang University of Finance and Economics (2016)
5. Xu, D., Cui, X.X., Tian, W., et al.: Research on chaotic random number generator based on Logistic mapping. Microelectr. Comput. **33**(2), 1–6 (2016)
6. Jia, Y.J., Wang, Y.Y.: Design and implementation of improved logistic chaotic sequence generator. Mach. Electr. **37**(04), 24–29 (2019)
7. Wang, J., Ding, Q.: Excellent Performances of the Third-Level disturbed chaos in the cryptography algorithm and the spread spectrum communication. J. Inf. Hiding Multimed. Signal Process **7**, 826–835 (2016)
8. Wang, J., Wang, Y., Yin, C., et al.: Investigation on the simulation of one-dimensional discrete chaotic digital generation circuit. In: 2015 Third International Conference on Robot, Vision and Signal Processing (RVSP), pp. 195–199. IEEE (2015)
9. Wang, J., Yang, T., Li, Y., et al.: Design of integer chaotic key generator for wireless sensor network. Int. J. Future Gen. Commun. Network. **9**(11), 327–336 (2016)
10. Chen, Z.G., Liang, D.Q., Deng, X., et al.: Performance analysis and improvement of Logistic chaotic mapping. J. Electr. Inf. Technol. **38**(6), 1547–1551 (2016)
11. Dang, X.Y., Li, H.T., Yuan, Z., et al.: Implementation of chaotic mapping based on digital-analog mixing. Acta Phys. Sin **64**(16), 160501–160501 (2015)
12. Fan, C.L., Ding, Q.: Improved algorithm based on Logistic chaotic sequence and its performance analysis. Electr. Device **38**(4), 759–763 (2015)
13. Cai, D., Ji, X.Y., Shi, H., et al.: Improved method and performance analysis of piecewise Logistic chaotic mapping. J. Nanjing Univ. (Nat. Sci.) **52**(5), 809–815 (2016)
14. Qi, Y.B., Sun, K.H., Wang, H.H., et al.: Design and performance analysis of a hyperchaotic pseudorandom sequence generator. Comput. Eng. Appl. 135–139 (2017)