ETU THE FIRST ELECTROTECHNICAL UNIVERSITY

IEEE

Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering

(ElConRus)

January 29- February 1, 2018

Saint Petersburg, Russia

Preface

The IEEE Russia North West Section, IEEE Russia Section, Saint Petersburg Electrotechnical University “LETI”, National Research University of Electronic Technology "MIET", and Glyndwr University, UK are pleased to present the Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (2018 ElConRus) held in St. Petersburg and Moscow, Russia on January 29 - February 1, 2018. This conference is proudly hosted by two universities - Saint Petersburg Electrotechnical University “LETI” and the National Research University of Electronic Technology "MIET". The Organising Committee believes and trusts that we have been true to the spirit of collegiality that members of IEEE value whilst also maintaining a high standard as we reviewed papers, provided feedback and now present a strong body of published work in this collection of proceedings.

The themes for this year's conference were chosen as a means of bringing together the many orientations of electrical and electronic engineering research and teaching, and providing a basis for discussion of issues arising across the engineering community in relation to electrical and electronic engineering.

The aim in these proceedings has been to present high quality work in an accessible medium, for use in the teaching and further research of all people associated with electrical and electronic engineering studies. To achieve this aim, all abstracts were blind reviewed, and full papers submitted for publication in this journal of proceedings were subjected to a rigorous reviewing process.

Dr. Michael Shestopalov
Co-chair of the Conference Organizing Committee, Chair of the IEEE Russia NW Section

Publishing Details
Proceedings Edited by S. Shaposhnikov 2017 St. Petersburg, Russia: Saint Petersburg Electrotechnical University “LETI”
Prof. Popov str. 5, Saint Petersburg, 197376, Russia
Telephone: +7 (812) 234 28 91
Fax: +7 (812) 234 28 91

ISBN 978-1-5386-4339-6.

978-1-5386-4340-2/18/$31.00 ©2018 IEEE

Quasi-Chaotic Mode Detection and Prevention in Digital Chaos Generators

Timur I. Karimov, Denis N. Butusov, Dmitrii O. Pesterev, Dmitry V. Predtechenskii, Roman S. Tedoradze
Department of Computer Aided Design
Saint Petersburg Electrotechnical University "LETI"
Saint Petersburg, Russia
dnbutusov@etu.ru

***Abstract*—Numerical solutions of chaotic differential equations can exhibit quasi-chaotic behavior when implemented in short word length computers. Quasi-chaotic signal is a periodic waveform with extremely long period that looks chaotic on shorter time intervals. In many practical applications of chaos, it is assumed that chaotic waveform is non-recurring, thus quasi-chaotic regime is strongly undesirable. This especially affects embedded applications, where processors with short data types are common because of their low power consumption. In our work, we describe conditions under which quasi-chaotic oscillations can occur and study numerical methods from the point of robustness to the quasi-chaotic mode. An algorithm for quasi-chaotic mode detection is described. We also propose a quasi-chaotic regime elimination technique based on parameter shift approach. The simulation of Rössler chaotic system with 16-bit data representation is given as an experimental study. The obtained results show the theoretical possibility to substantially reduce the influence of the quasi-chaotic regime on low-precision chaos oscillators.**

Keywords—quasi-chaos detection; bifurcation analysis; numerical integration method; Rössler system; chaos generatorIntroduction

Nowadays, chaotic waveform generators are common in various technical applications. Most important of them are cryptographic systems, where computers with minimal possible word length are used to encrypt data and generate pseudo-random sequences [1–4]. When we simulate the chaotic system with finite precision on computers or FPGA some discretization effects appear, e.g. a quasi-chaotic mode. A quasi-chaotic waveform period highly depends on a chosen word length, as well as on initial conditions and nonlinearity parameters. Emergence of this mode reduces the security of the system and thus is strongly undesirable [5, 6]. To solve mentioned problem, it is necessary to create methods for detection and prevention of quasi-chaotic behavior.

This paper is organized as follows. A mathematical model of the test system is presented in Section II. An analysis of bifurcation step diagrams made for various discrete maps of the test system, obtained by different integration methods, is proposed in Section III. Section IV describes the quasi-chaotic mode detection algorithm. The quasi-chaotic regime prevention technique is considered in Section V. Finally, Section VI contains conclusion and discussion.

I. Chaos generator based on Rössler system

The well-known and commonly used in chaos generation [3] Rössler hyper-chaotic system [7] is described by the following system of ordinary differential equations

$$\begin{aligned} \dot{x} &= -y - z; \\ \dot{y} &= x + ay; \\ \dot{z} &= b + z(x - c), \end{aligned} \tag{1}$$

where $a = 0.1$, $b = 0.1$, $c = 5.6$ are nonlinearity parameters corresponding to the chaotic mode of oscillations.

To solve problem (1) we consider the list of numerical integration methods that include the explicit (*Euler*) and implicit Euler (*IEuler*) algorithms, the Euler-Cromer method (*Cromer*), the semi-implicit *D* and *CD* methods [8], the explicit midpoint method (*EMP*), its modification with Gragg's smoothing step (*MEMP*) and the linearly implicit midpoint (*LIMP*) method. Further, we will note the commutation order for semi-implicit methods as the number after the numerical method abbreviation, e.g. "*CD2"*.

The finite-difference schemes were constructed for all investigated algorithms with double data precision (*DBL*) and fixed-poin representation with total word length of 16 bits and integer word length of 8 bits (*FXP*).

II. Step diagram analysis

The traditional approach of chaotic dynamical systems investigation is a bifurcation analysis. The most common tool is a bifurcation diagram, a chart showing the maxima of the chosen variable in time domain plotted versus a nonlinearity parameter. If we use the integration step as the nonlinearity parameter, the diagram is called a step-diagram or an *h*-diagram.

Let us consider *h*-diagrams of the investigated finite-difference schemes for *DBL* and *FXP* implementations. One can see stair structure on *FXP* *h*-diagrams that indicates identity of attractors for relatively close step sizes. This means that the topological richness of the prototype system significantly decreases with the reduction of a word length. Thus, the system trajectories will be inevitably trapped in one of these "bins" during the oscillations, which will cause the quasi-chaotic regime to appear.

The analysis of step diagrams also allow us to choose the integration step sizes, which are most suitable for all studied methods to perform chaotic oscillations: $h_0 = 0.02734375$, $h_1 = 0.0390625$ and $h_2 = 0.0625$.

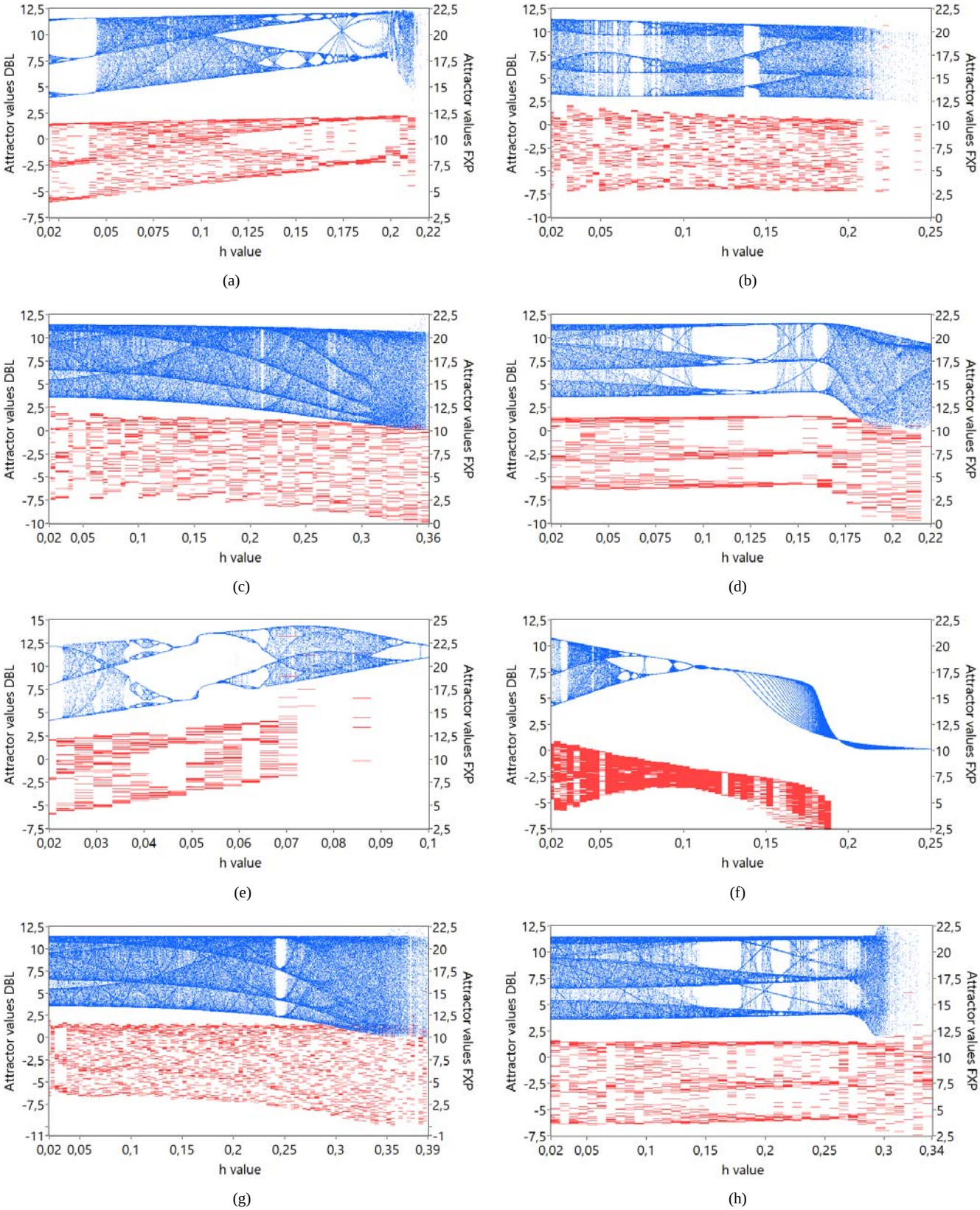

Fig. 1. The *h*-diagrams of Rössler system discretized by *Cromer* (a), *D* (b), *CD* (c), *EMP* (d), *Euler* (e), *IEuler* (f), *LIMP* (g) and *MEMP* (h) methods for *DBL* (blue) and *FXP* (red) data representation

III. QUASI-CHAOTIC MODE DETECTION

A. Quasi-chaotic mode detection algorithm

Here we present the algorithm, which allows us to detect and measure a start point and a period of quasi-chaotic oscillations. The proposed method consists of following steps:

1. Find $n + 1$ points of a numerical solution.

2. Take the values of state variables in a last point of the numerical solution $\mathbf{x}_n = \mathbf{x}(t_n)$.

3. Search for a point $\mathbf{x}(t_i) \equiv \mathbf{x}(t_n)$ at discrete time moments $t_0, t_1, \ldots, t_{n-1}$, where $t_i < t_{i+1}$.

4. Define a quasi-chaos period $T = t_1 - t_0$.

5. Find the point $S=t_q$, such that $x(t_q + T) = x(t_q)$, $x(t + T) \neq x(t), \forall t < t_q$ using binary search. This point is the starting point of quasi-chaos behavior.

The proposed algorithm was used to plot a series of 2D charts illustrating the values of quasi-chaos period and start time for sets of initial conditions with step sizes h_0, h_1, h_2. A color represents the length of the quasi-chaotic period or a time when quasi-chaos started. One basic square on the image corresponds to the one set of initial conditions $(x_i, y_j, 0)$. The white color corresponds to cases when *FXP* overflows. In our research, the finite-difference models of Rössler system were simulated on the time interval of 30 000 sec varying x and y initial conditions within the range [–10; 10] with increment of 1. In Fig. 2. the diagrams of a quasi-chaotic mode period T are represented. For the majority of numerical methods tested, these diagrams have similar circular shape except the square shape of *D* method diagram, because this numerical model is more stable with defined precision. In addition, the different methods have shown a different dependencies from the step size: forward (*Cromer1*, *Cromer2*, *CD1*, *EMP*, *MEMP*, *LIMP*), forward-backward (*IEuler*, *D1*, *D2*, *SIMP*) and backward dependency (*CD2*). This observation shows that some trivial dependences from step size, as one would expect, do not exist.

Average period of the quasi-chaotic mode for *Cromer*, *D*, *SIMP*, *EMP* and *ECD* methods are closer to maximal period value, and average period of *IEuler* and *MEMP* methods are closer to minimal period value.

B. Investigation of quasi-chaos mode starting points

In Fig. 3, the diagrams of the quasi-chaotic mode starting points *S* are presented. These plots are constructed and colored similarly to the period diagrams. One can see that quasi-chaos starting point dependency to the step size *h* differs from the same dependency of quasi-chaos period. For example, for the method *D* a forward dependency can be observed. Thus, we divided the numerical methods under consideration into three groups: the methods with forward dependency from step size (*D1*, *D2*), methods with forward-backward dependency (*IEuler*, *Cromer1*, *Cromer2*, *CD1*, *CD2*, *CD3*, *SIMP*, *LIMP*) and methods with backward dependency (*CD4*, *MEMP*). Moreover, one can notice that most of the starting point diagrams exhibit less variety of values than the period diagrams.

Now let us introduce a complex quality characteristic $Q = T + S$, which shows the supremum time where the system preserves a chaotic motion without repeating any solution points. One can see that *D* and *Cromer* semi-implicit methods have shown the good results (Fig.4).

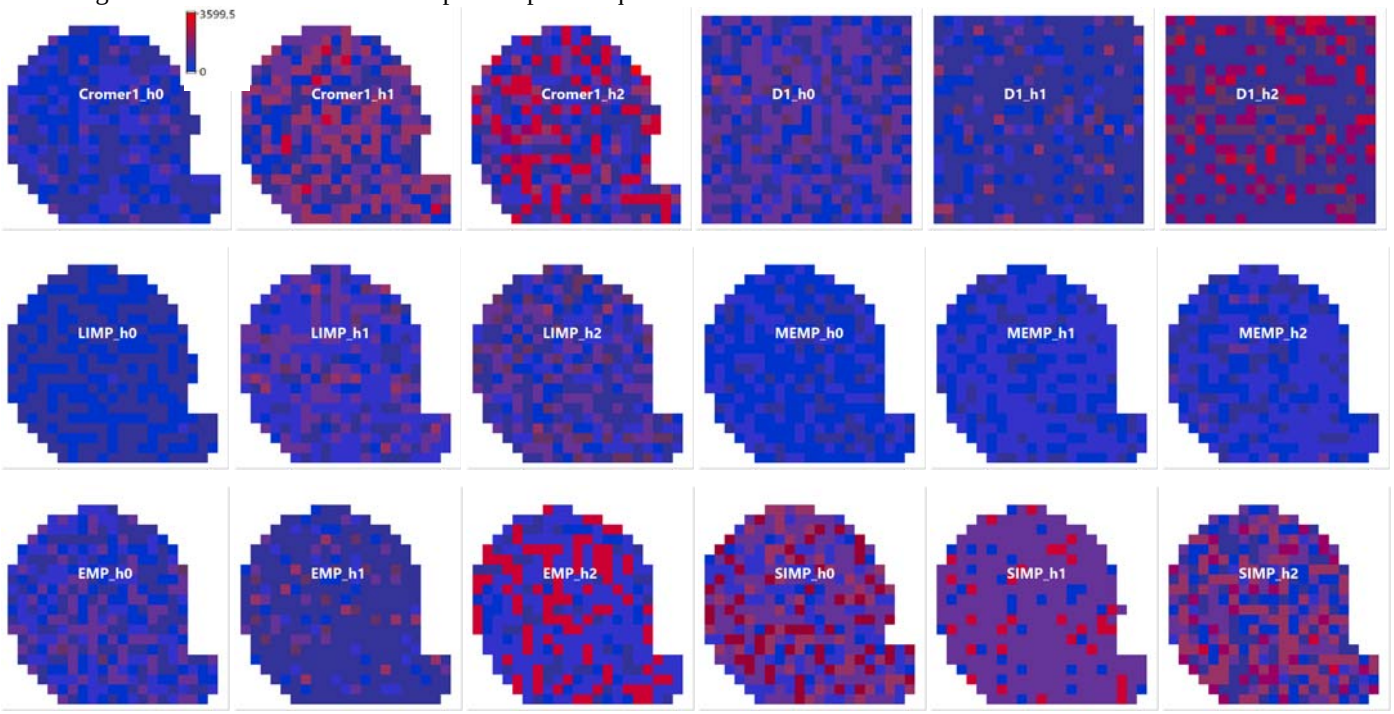

Fig. 2. The dependency of the quasi-chaotic regime period T to the initial conditions for four different numerical methods and three step sizes

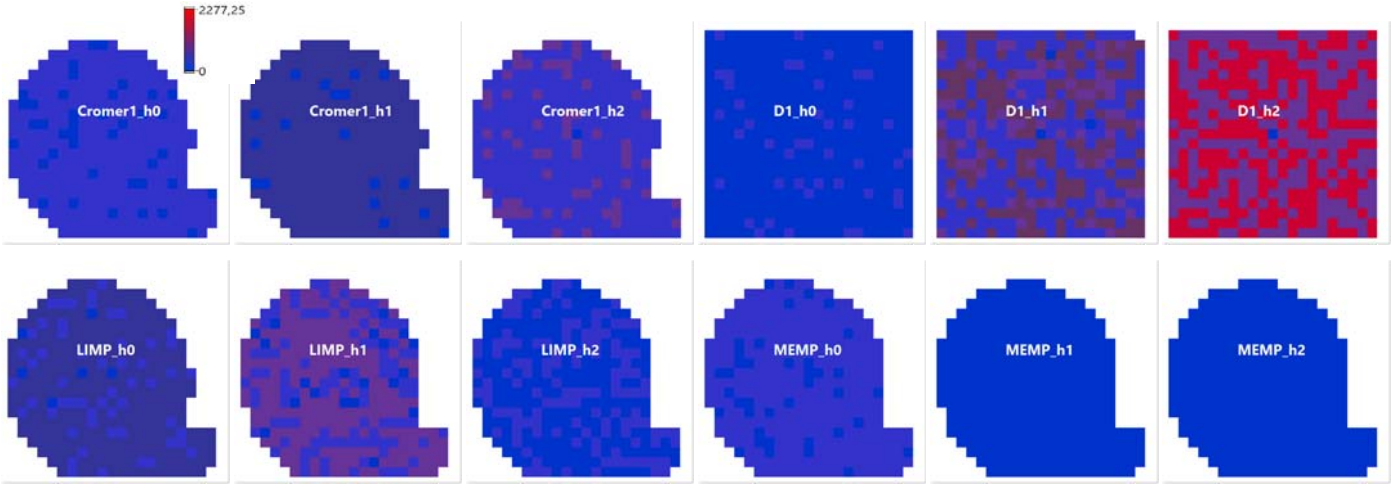

Fig.3. The dependency of the quasi-chaos starting point *S* to the initial conditions for four different numerical methods and three step sizes

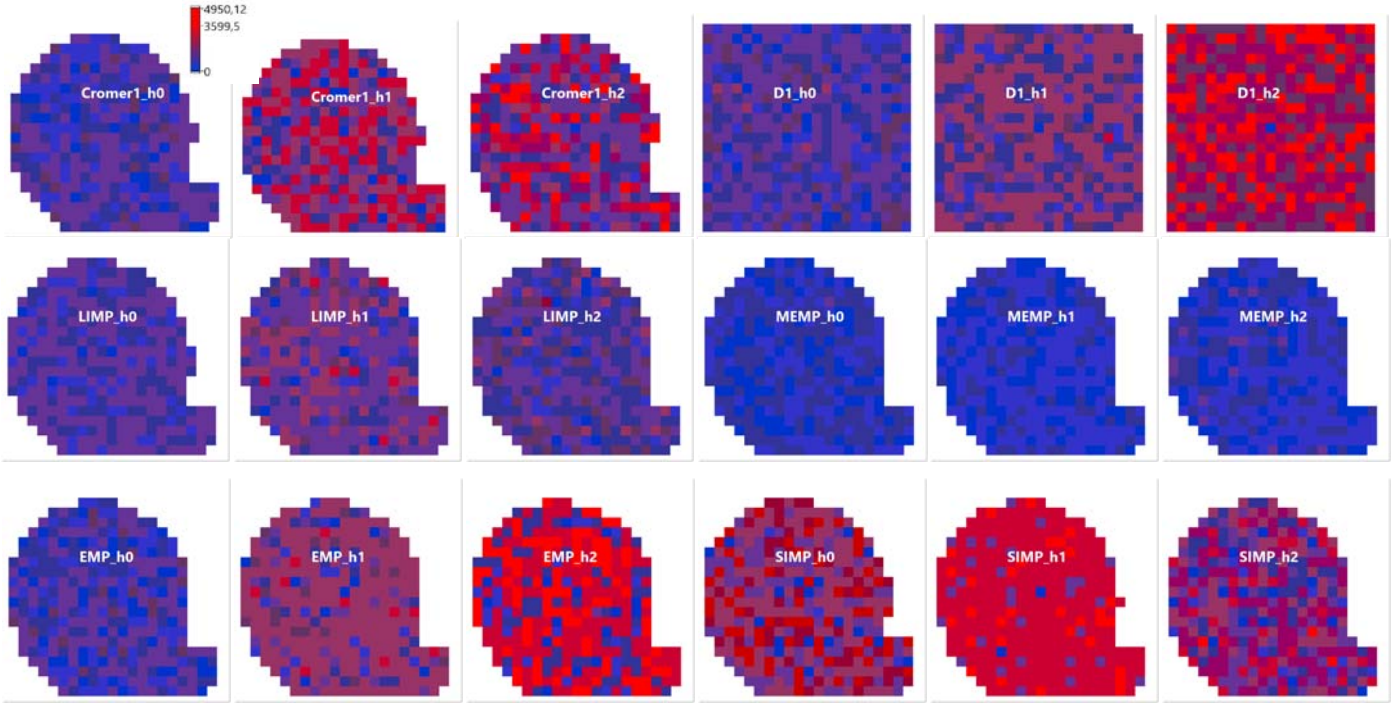

Fig.4. The dependency of generator quality *Q* to the initial conditions for four different numerical methods and three step sizes

IV. Quasi-chaotic mode prevention

The main idea of proposed quasi-chaos prevention algorithm is to introduce a periodical disturbance into the numerical solution. One way to do it is to change system parameters slightly for every N_d-th iteration, called a disturbance period. According to the chaos sensitivity, this will push the solution trajectory from slipping into the fixed-point "bin" and thus will extend the true chaotic waveform generation as well as quasi-chaotic period. Let us formulate the quasi-chaotic mode prevention algorithm as following:

1. If step index $n \bmod N_d = 0$, then add small values $\Delta_a, \Delta_b, \Delta_c$ (1-2 LSB) to system parameters *a*, *b*, *c*, else use common parameters.

2. Perform the next integration step with new parameters.

3. If the system parameters were changed, recall original ones.

The possible development of this idea is to use a finite array of Δ_x values. We tested the arrays of length 1, 2 and 3; some results are shown in Fig. 5. The 200 000 sec simulation was performed with *Euler-Cromer* method.

It is also extremely important to properly select the disturbance period. A simulation shows that we can extend chaotic oscillation period theoretically up to infinity combining proper disturbance period and Δ_x values array.

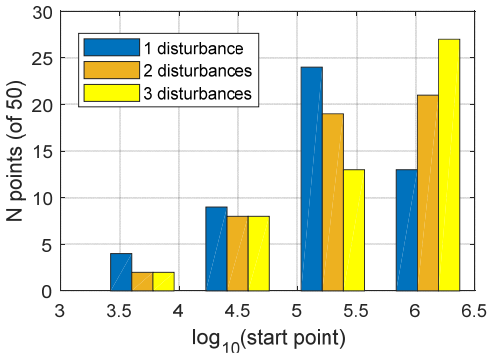

Fig. 5. Extension of chaotic mode length depending of disturbances quantity

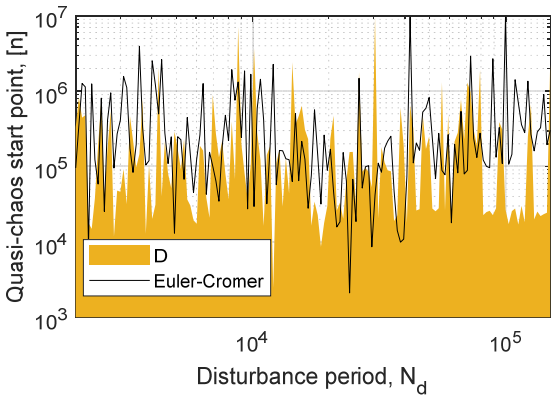

Fig. 6. Dependency of chaotic mode length from N_d and chosen method

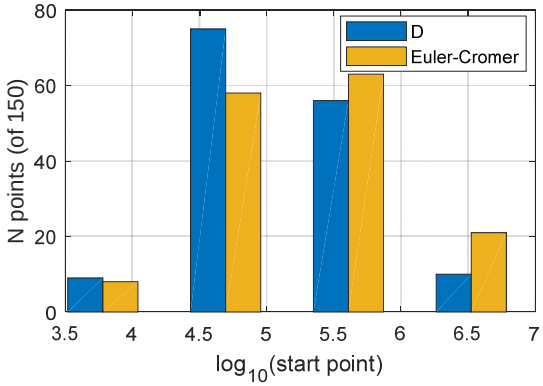

Fig. 7. Quasi-chaotic mode period length depending from method

Fig. 6 shows that several points of *Euler-Cromer* solution reached limit of 10 million of solution points equal to simulated waveform length. In this series, no chaotic behavior was detected. The comparison of points distribution shows that *Euler-Cromer* method delivers longer chaotic behavior in average (see Fig. 7).

V. Conclusion and Discussion

We investigated the quasi-chaotic mode appearance in various finite-difference models of Rössler system implemented with 16-bit fixed-point data type. The influence of a numerical method on quasi-chaotic mode start time and period was demonstrated in a series of computational experiments. The absence of trivial dependency of the start time and period from integration step size was shown. The complex characteristic Q was introduced to estimate the quality of chaos generator. The excellence of semi-implicit methods like *D* or *Euler-Cromer* algorithm was experimentally shown.

Finally, we proposed an algorithm of quasi-chaotic mode prevention based on a small periodical disturbance introduced into nonlinearity parameters. This approach allowed generating significantly longer chaotic waveforms without changing the data representation of finite-difference models.

Acknowledgement

The reported study was partially supported by RFBR, research project No. 17-07-00862.

References

[1] Falcioni M., Palatella L., Pigolotti S., Vulpiani A. Properties making a chaotic system a good pseudo random number generator. Physical Review E. vol. 1, i. 72, 2005. 016220 p. DOI: 10.1103/PhysRevE.72.016220

[2] Skiadas C.H., Skiadas C. Handbook of applications of chaos theory. CRC Press. 2016

[3] Tutueva A.V., Butusov D.N., Pesterev D.O., Belkin D.A., Ryzhov N.G. Novel normalization technique for chaotic Pseudo-random number generators based on semi-implicit ODE solvers. Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2017 International Conference IEEE. pp. 292–295. DOI: 10.1109/ITMQIS.2017.8085814

[4] Baptista M.S. Cryptography with chaos. Physics Letters A. vol. 1–2. i. 240. 1998. pp. 50–54. DOI: 10.1016/S0375-9601(98)00086-3

[5] Persohn K.J., Povinelli R.J. Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. Chaos, Solitons & Fractals. vol. 3. i. 45. 2012. pp. 238-245. DOI: https://doi.org/10.1016/j.chaos.2011.12.006

[6] Nepomuceno E.G., Mendes E.M.A.M. On the analysis of pseudo-orbits of continuous chaotic nonlinear systems simulated using discretization schemes in a digital computer. Chaos, Soltions and Fractals. vol. 95. 2017. pp. 21–32. DOI: https://doi.org/10.1016/j.chaos.2016.12.002

[7] Rössler O.E. An equation of continious chaos. Physical letters. vol. 57, i. 5. 1976. pp. 397–398. DOI: https://doi.org/10.1016/0375-9601(76)90101-8

[8] Butusov D.N., Tutueva A.V., Homitskaya E.S. Extrapolation Semi-implicit ODE solvers with adaptive timestep. Soft Computing and Measurements (SCM), 2016 XIX IEEE International Conference on. IEEE, 2016. pp. 137–140. DOI: 10.1109/SCM.2016.7519708