OBSERVABILITY AND SINGULARITY IN THE CONTEXT OF RÖSSLER MAP

Madalin FRUNZETE[1], Adrian LUCA[2], Adriana VLAD[3], Jean-Pierre BARBOT[4]

Conceptele de observabilitate şi singularitate descriu structural un sistem dinamic multi-dimensional şi reprezintă elemente foarte importante în dezvoltarea unui observator în multe aplicaţii bazate pe haos. Lucrarea discută cele două concepte în contextul sistemului Rössler discret. Scopul este de a decide care variabilă de stare este cea mai potrivită pentru a fi aleasă criptogramă într-o metoda de cifrare de tip incluziune, bazată pe sistemul Rössler. Rezultatele experimentale obţinute sunt sustinute şi de coeficientul de observabilitate calculat pentru sistemul Rössler discret prin adaptarea unui algoritm cunoscut în literatura pentru sisteme dinamice continue.

The concepts of observability and observability singularity describe structurally a multi-dimensional dynamical system and they represent very important elements for developing an observer for many applications, as for example: observer based diagnostic, control of induction motor without mechanical sensor or again as it is emphasized in this paper cryptographic application (of type inclusion method). Here, the two concepts are discussed and evaluated in the context of Rössler map, coming up in the end with a strong argument in order to know which state variable of the system will be chosen as cryptogram.

Keywords: chaotic map, observability, singularity manifold, Rössler map

[1]Faculty of Electronics, Telecommunications and Information Technology, Politehnica University of Bucharest, Romania; Electronique et Commande des Systmes Laboratoire, EA 3649 (ECS-Lab/ENSEA) ENSEA, Cergy-Pontoise, France, e-mail: `madalin.frunzete@upb.ro`

[2]Faculty of Electronics, Telecommunications and Information Technology, Politehnica University of Bucharest, Romania, e-mail: `adrian.luca@upb.ro`

[3]Faculty of Electronics, Telecommunications and Information Technology, Politehnica University of Bucharest, Romania; The Research Institute for Artificial Intelligence, Romanian Academy, Bucharest, Romania, e-mail: `avlad@racai.ro`

[4]Electronique et Commande des Systèmes Laboratoire, EA 3649 (ECS-Lab/ENSEA) ENSEA, Cergy-Pontoise, France; EPI Non-A INRIA, France, e-mail: `barbot@ensea.fr`

1. Introduction

Since Shannon's work in 1949 [1], cryptography has experienced different development directions including the approach between the chaotic systems and cryptography. Thus, the approach of different concepts such as statistics, cryptography and dynamical systems theory have led to numerous studies in the field of chaos based cryptography (*e.g.* [2], [3], [4], [5]). In general, the applicability of dynamical systems in cryptography is based on ergodicity, the property of mixing and the sensitivity to initial conditions. Besides these properties, the notions of observability and singularity are basic elements in the development of cryptographic applications of type inclusion method (see [2], [4]).

Thus, from the perspective of applications in cryptography, this paper makes a detailed analysis of Rössler map in terms of the two concepts, namely observability and singularity. The interest in Rössler map is derived from previous studies [6, 7] which showed good statistical properties and thus its suitability for applications in cryptography.

Roughly speaking, observability in the context of a n-dimensional chaotic system means that having involved a sequence of values generated by one of the n state variables of the system, the phase space of the system can be reconstructed. Note that the concept of observability is discussed in the hypothesis that the system parameters are known.

A complete point of view and the definition of the locally weakly observable is given by R. Hermann and A. Krener in [8]. An algebraic point of view, given by S. Diop and M. Fliess, may be also found in [9].

Singularity manifold of a chaotic system (noted by $S_{\bar{O}}$) is the space where the system loses its observability property from the perspective of the considered state variable. In terms of use in cryptography is ideal if the system has no singularity manifold, $S_{\bar{O}} = \emptyset$. In other words, the system is 100% observable from the point of view of the considered state variable. A detailed example on the interpretation of the singularity manifolds of Rössler continuous system [10] is found in [11].

Section 2 presents theoretical interpretation of the notions of observability and singularity in the context of three-dimensional discrete time chaotic systems. Section 3 exemplifies in theory and evaluates experimentally the two concepts in the context of Rössler map. The results support the usage of Rössler map in cryptographic applications of type inclusion method and help the experimenter in choosing state variable to serve as a cryptogram.

2. **Theoretical background**

Let us consider a nonlinear discrete system described (1) in the three-dimensional space $\mathbb{R}^3$, *i.e.* $(x_1, x_2, x_3)^T$, where $x_i \in \mathbb{R}$ are the state variables.

$$x_i^+ = f_i(x_1, x_2, x_3), \quad i = 1, 2, 3, \tag{1}$$

$x = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ represents the state vector evaluated at k iteration (*i.e.* $x(k)$), so $x^+ = x(k+1)$. Assume that an observable s is obtained using the measurement function $h : \mathbb{R}^3(x) \to \mathbb{R}(s)$. It is thus possible to reconstruct the phase space from the time series $\{x_i(k)\}$ using for instance consecutive iterations $(X = s, Y = s^+, Z = s^{++})$. The coordinate transformation between the original phase space $\mathbb{R}^3(x_1, x_2 x_3)$ and the iterative embedding $\mathbb{R}^3$, *i.e.* $(X, Y, Z)^T$, is defined by:

$$\Phi_i \begin{cases} X = s = x_i \\ Y = s^+ = x_i^+ \\ Z = s^{++} = x_i^{++} \end{cases} \tag{2}$$

Variables X, Y and Z correspond to the current k iteration, next iteration $k+1$ and to the $k+2$ iteration, respectively. The observability matrix O_i of a nonlinear system of type (1) observed using the i^{th} state variable is the Jacobian matrix of map Φ_i, [12]. The same idea has been shown for continuous systems (Lorenz, Rössler systems) by Letellier *et al.* in [13].

$$O_i = \begin{pmatrix} \frac{\partial X}{\partial x_1} & \frac{\partial X}{\partial x_2} & \frac{\partial X}{\partial x_3} \\ \frac{\partial Y}{\partial x_1} & \frac{\partial Y}{\partial x_2} & \frac{\partial Y}{\partial x_3} \\ \frac{\partial Z}{\partial x_1} & \frac{\partial Z}{\partial x_2} & \frac{\partial Z}{\partial x_3} \end{pmatrix} \tag{3}$$

The system is thus fully observable when the determinant $det(O_i)$ never vanishes, that is when map Φ_i defines a global diffeomorphism (Φ_i must also be injective, a property observed in most of the cases). When $det(O_i)$ never vanishes, the map Φ_i can be inverted everywhere and the system can always be rewritten under a reiterative form:

$$\begin{cases} X^+ = Y \\ Y^+ = Z \\ Z^+ = F_i(X, Y, Z) \end{cases} \tag{4}$$

where the model function $F_i(X, Y, Z)$ is free of singularities and subscript i designates the measured state variable. Otherwise, a system such (4) might be obtained, but with singularities. This situation occurs when $det(O_i) = 0$ over some space in the original space: the system is said to be not fully observable.

The subspace mentioned in the previous paragraph can be Ø or many points. The different states in such a subspace, in the original phase space, cannot be distinguished in the reconstructed space using the observable. It is then said that the original system cannot be fully observed from the recorded state variable. From a practical point of view, even two different states that are close to the aforementioned subspace are very hard to distinguish in the reconstructed space.

The singularity manifold $S_{\bar{O}}$ is the subspace where the map Φ_i cannot be inverted and the system cannot be rewritten under a form as (4). A mathematical interpretation of the singularity manifold is given in (5):

$$S_{\bar{O},i} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid det(O_i) = 0\} \tag{5}$$

where subscript i designates for which state variable was computed $S_{\bar{O}}$. Therefore the quality of the observable depends on the existence of a singularity subset, its dimension and its location with respect to the attractor of the system.

3. **Case study: Rössler map**

In this section the way to obtain the singularity manifold in the context of Rössler map (6) will be presented; the parameter vector was considered for the experiments: $(a_1, a_2, b_1, b_2, b_3, b_4, c_1, c_2)^T = (3.78, 0.2, 0.1, 2, 0.35, 1.9, 3.8, 0.05)^T$. The analytic exemplification is done in the case when selected observable is the first state variable x_1. Also some experimental results are given for the other two state variables.

$$\begin{cases} x_1^+ = a_1x_1(1 - x_1) + a_2x_2 \\ x_2^+ = b_1[(1 - b_2x_1)(x_2 + b_3) - 1](1 - b_4x_3) \\ x_3^+ = c_1x_3(1 - x_3) - c_2(1 - b_2x_1)(x_2 + b_3) \end{cases} \tag{6}$$

By the form (6) considering as observable the first state variable $s = x_1$, the coordinate transformation between the original phase space **3**, *i.e.* $(x_1, x_2, x_3)^T$, and the iterative embedding $\mathbb{R}^3$, *i.e.* $(X, Y, Z)^T$, of type (2) is obtained:

$$\Phi_1 \begin{cases} X = s = x_1 \\ Y = s^+ = x_i^+ \\ Z = s^{++} = x_1^{++} \end{cases} \Rightarrow \begin{cases} x_1 \\ a_1x_1(1 - x_1) + a_2x_2 \\ a_1x_1^+(1 - x_1^+) + a_2x_2^+ \end{cases} \tag{7}$$

The observability matrix O_1 of Rössler map (6) obtained using the first state variable x_1 is the Jacobian matrix of map Φ_1 (see (3) and (7)):

$$O_1 = \begin{pmatrix} 1 & 0 & 0 \\ e_1 & a_2 & 0 \\ e_2 & e_3 & a_2b_1b_4[(1 - b_2x_1)(x_2 + b_3) - 1] \end{pmatrix} \tag{8}$$

where:

$$e_1 = a_1 - 2a_1x_1$$

$$e_2 = a_1^2 - a_1^2(a_1^2 - 2)x_1 + a_1^2(a_1^2 + 2a_2)x_1^2 - 2a_1^2a_2x_1^3 - a_1^3a_2x_2 + \\ + 2a_1a_2^2x_1x_2 - a_2b_1b_2(x_2 + b_3)(1 - b_4x_3)$$

$$e_3 = -2a_1^3a_2x_1(1 + x_1) - 2a_1^2a_2^2x_2 + a_1a_2 + a_2b_1(1 - b_2x_1)(1 - b_4x_3)$$

The determinant of observability matrix O_1 from (8):

$$det(O_1) \overset{not}{=} \Delta_{x_1} = a_2^2b_1b_4[(1 - b_2x_1)(x_2 + b_3) - 1] \tag{9}$$

From (5) and (9) the singularity manifold $S_{\bar{O},1}$ is:

$$\begin{aligned} S_{\bar{O},1} &= \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid \Delta_{x_1} = 0\} \\ &= \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid (1 - b_2x_1)(x_2 + b_3) - 1 = 0\} \end{aligned} \tag{10}$$

The graphical representation of the singularity manifold and the attractor of the Rössler map is presented in Fig. 1.

The system attractor was computed for 10^6 iterations starting from the initial condition $x(0) = (x_1(0), x_2(0), x_3(0))^T = (0.224, 0.054, 0.741)^T$. By computing the determinant of the observability matrix for each point of this attractor in all three cases it can be concluded which of the state variables has a better observability. For interpreting the results the experimental distribution law of each Δ_{x_i} is given in the Figs. 2, 3 and 4.

So, in each of the three Figs. 2, 3 and 4 is given a distribution $p(\Delta_{x_i})$ of the values for each determinant. The intersection with the singularity manifold is represented by the points situated on 0.

Selecting the observable as first state variable $s = x_1$ of (6) it can be observed that there are no values around the critical point 0. By performing a comparative analysis, Figs. 1 and 2, it is confirmed that there are no intersections between the Rössler attractor and singularity manifold $S_{\bar{O},1}$ because the determinant of the observability matrix Δ_{x_1} is always different than 0. So, there are no points of the attractor on the singularity manifold and the system is fully observable when x_1 is selected as observable.

An interpretation in terms of the distribution of the computed values for Δ_{x_2} and Δ_{x_3} was given only for the state variables x_2 and x_3. A graphic interpretation of the type given in Fig. 1 for x_1 was not comprehensive for x_2 or x_3. This is because the complexity of singularity manifolds for these state variables does not allow a clear view.

Analyzing the distribution of values of Δ_{x_2} for the same 10^6 points of the system attractor it can be observed that all the values of the determinant can be

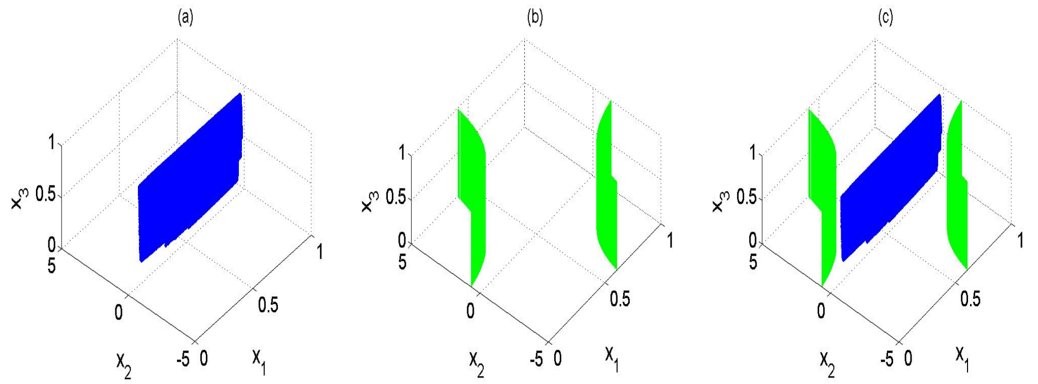

FIG. 1. Rössler attractor (a), singularity manifold $S_{\bar{O},1}$ (b) and combined Rössler attractor and singularity manifold $S_{\bar{O},1}$ (c)

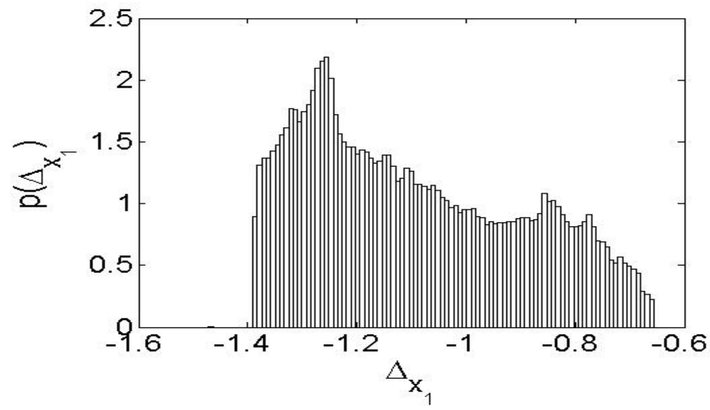

FIG. 2. Determinant of the observability matrix for x_1

found in the vicinity of the critical value 0 determined with an approximation of 10^{-1}.

The corresponding Fig. 4 for the state variable x_3 is obtained in the same manner as for the observable $s = x_2$. It can be observed that most of the values are in the vicinity of 0 too.

An interval of range $\epsilon = 10^{-4}$ around the critical point 0 was set in order to compute an average probability to reach this singularity region. The probability that Δ_{x_i} to belong to this interval was computed as a ratio between the occurrences of $\Delta_{x_i} \in \epsilon$ and 10^6 (total number of the points for the experimental attractor). For the state variable x_2 the values of the determinant represented in Fig. 3 found

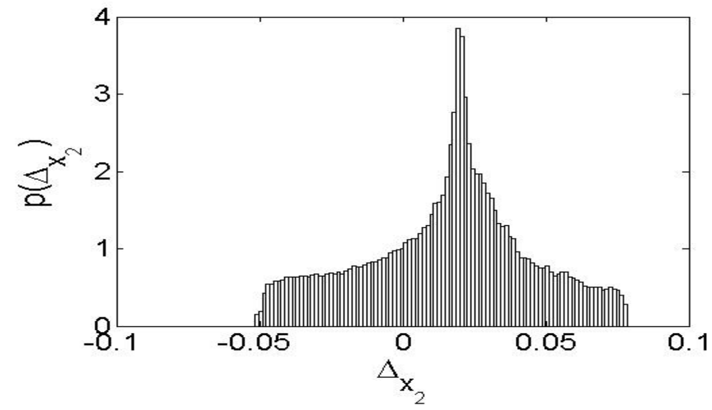

FIG. 3. Determinant of the observability matrix for x_2

in the interval ϵ are 0.0803% from the ensamble of 10^6. For the state varable x_3, 3.18% values of the determinant from the ensamble of 10^6 belong to the ϵ interval.

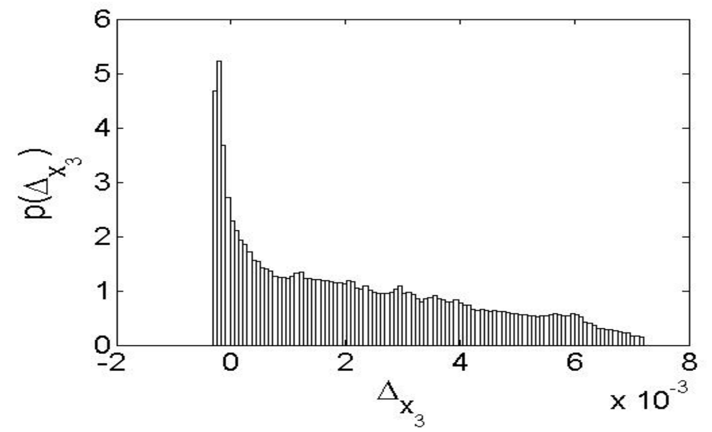

FIG. 4. Determinant of the observability matrix for x_3

The results, obtained in this section, are in line with the observability coefficients computed for Rössler map in the Appendix. The algorithm implemented represents the interpretation for the discrete case for an existing algorithm [14].

4. Conclusions

Analyzing the experimental results for this new approach it can be said that the choice of the state variables x_1 to act as a cryptogram in an application of type inclusion method [4] is well done. In terms of the principle of bi-univocal cryptography concepts, this paper makes a contribution in terms of respecting it; namely for x_1 as cryptogram there is no loss of observability, then there is no loss of information.

Also, concepts for a multi-dimensional discrete systems by adjusting analysis for continuous systems were presented.

Acknowledgement. The authors are very grateful to *Professor Christophe Letellier* for his advice and encouragement during all this research.

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family and Social Protection through the Financial Agreement POSDRU/6/1.5/S/19.

Also, the paper has been partially supported by PEPS-A2SDC (Automatique et Analyse de Système à Dynamiques Chaotiques).

REFERENCES

[1] *C. E. Shannon.* Communication Theory of Secrecy Systems. *Bell Systems Technical Journal*, 28:656–715, 1949.

[2] *F. Anstett, G. Millerioux and G. Bloch.* Message-Embedded Cryptosystems: Cryptanalysis and Identifiability. In *Proc. and 2005 European Control Conf. Decision and Control CDC-ECC '05. 44th IEEE Conf*, pages 2548–2553, 2005.

[3] *M. S. Baptista.* Cryptography with chaos. *Physics Letters A*, 240(1-2):50 – 54, 1998.

[4] *I. Belmouhoub, M. Djemai and J.-P. Barbot.* Cryptography by discrete-time hyperchaotic systems. In *Proc. 42nd IEEE Conf. Decision and Control*, volume 2, pages 1902–1907, 2003.

[5] *A. Vlad, A. Luca and M. Frunzete.* Computational Measurements of the Transient Time and of the Sampling Distance That Enables Statistical Independence in the Logistic Map. In O. Gervasi, D. Taniar, B. Murgante, A. Lagan, Y. Mun, and M. Gavrilova, editors, *Computational Science and Its Applications ICCSA 2009*, volume 5593 of *Lecture Notes in Computer Science*, pages 703–718. Springer Berlin / Heidelberg, 2009.

[6] *M. Frunzete, A. Luca and A. Vlad.* On the Statistical Independence in the Context of the Rössler Map. In *3rd Chaotic modeling and Simulation International Conference (CHAOS2010), Chania, Greece*, 2010 http://cmsim.net/sitebuildercontent/sitebuilderfiles/.

[7] *M. Frunzete, A. Luca, A. Vlad and J-P. Barbot.* Statistical Behaviour of Discrete-Time Rössler System with Time Varying Delay. In Beniamino Murgante, Osvaldo Gervasi, Andrs Iglesias, David Taniar, and Bernady Apduhan, editors, *Computational Science and Its Applications - ICCSA 2011*, volume 6782 of *Lecture Notes in Computer Science*, pages 706–720. Springer Berlin / Heidelberg, 2011.

[8] *R. Hermann and A. Krener.* Nonlinear controllability and observability. *IEEE Transactions on Automatic Control*, 22(5):728–740, 1977.

[9] *S. Diop and M. Fliess.* Nonlinear observability, identifiability, and persistent trajectories. In *Proc. 30th IEEE Conf. Decision and Control*, pages 714–719, 1991.

[10] *O. E. Rössler.* An equation for hyperchaos. *Physics Letters A*, 71(2-3):155 – 157, 1979.

[11] *C. Letellier and L. A. Aguirre.* Graphical interpretation of observability in terms of feedback circuits. *Phys. Rev. E*, 72(5):056202, Nov 2005.
[12] *W. Perruquetti and J-P. Barbot. Chaos in automatic control.* CRC Press, Taylor & Francis Group, 2006.
[13] *C. Letellier, L. A. Aguirre and J. Maquet.* Relation between observability and differential embeddings for nonlinear dynamics. *Phys. Rev. E*, 71(6):066213, Jun 2005.
[14] *C. Letellier and L. A. Aguirre.* Interplay between synchronization, observability, and dynamics. *Phys. Rev. E*, 82(1):016204, Jul 2010.

Appendix

Observability coefficient in discrete case is computed by adapting the algorithm proposed in [14].

(1) Write the so-called fluency matrix by replacing each (non)linear element of the Rössler map (6) with ($\bar{1}$) 1, and zero otherwise. This corresponds to (non)linear term in the vector field. The elements from the first line corresponding to the first equation ($x_1^+ = a_1x_1(1-x_1) + a_2x_2$) are: $F_{11} = \bar{1}$ because there exists a nonlinear dependence on x_1, $F_{12} = 1$ means that it is a linear dependence on x_2 and $F_{13} = 0$ as there is no dependence on x_3.

$$F_{ij} = \begin{bmatrix} \bar{1} & 1 & 0 \\ \bar{1} & \bar{1} & \bar{1} \\ \bar{1} & \bar{1} & \bar{1} \end{bmatrix} \tag{11}$$

(2) Choose a variable to "reconstruct" the dynamics. Define a column vector $C_{1,i}$ when 1 corresponds to the "measured" state variable x_i and 0 otherwise. Then replace the diagonal element of the fluency matrix F corresponding to this variable by a dot and multiply each row of it by the corresponding element in $C_{1,i}$. The matrix $H_{1,i}$ is thus obtained:

$$C_{1,1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \qquad C_{1,2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \qquad C_{1,3} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$H_{1,1} = \begin{bmatrix} \bullet & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad H_{1,2} = \begin{bmatrix} 0 & 0 & 0 \\ \bar{1} & \bullet & \bar{1} \\ 0 & 0 & 0 \end{bmatrix} \qquad H_{1,3} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \bar{1} & \bar{1} & \bullet \end{bmatrix}$$

(3) Count the number $p_{1,i}$ of the linear elements and the number $q_{1,i}$ of nonlinear elements in $H_{1,i}$ for each state variable x_i, $i \in \{1, 2, 3\}$.

$$p_{1,1} = 1 \qquad p_{1,2} = 0 \qquad p_{1,3} = 0$$
$$q_{1,1} = 0 \qquad q_{1,2} = 2 \qquad q_{1,3} = 2$$

(4) Replace the dot in $H_{1,i}$ by 0, 1 or $\bar{1}$ acording to the fluency matrix F_{ij}, and transpose $H_{1,i}$.

$$H_{1,1}^T = \begin{bmatrix} \bar{1} & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad H_{1,2}^T = \begin{bmatrix} 0 & \bar{1} & 0 \\ 0 & \bar{1} & 0 \\ 0 & \bar{1} & 0 \end{bmatrix} \qquad H_{1,3}^T = \begin{bmatrix} 0 & 0 & \bar{1} \\ 0 & 0 & \bar{1} \\ 0 & 0 & \bar{1} \end{bmatrix}$$

(5) Count the sum ot the elements of each row, both 1 and $\bar{1}$ should be counted as 1. This defines the new column vector $C_{2,i}$.

$$C_{2,1} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \qquad C_{2,2} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \qquad C_{2,3} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

(6) $H_{2,i}$ is obtained by replacing each non zero element of $H_{1,i}^T$ by a dot and replacing each remaining element by its corresponding element in the fluency matrix multiplied by the corresponding element of the column vector $C_{2,i}$.

$$H_{2,1} = \begin{bmatrix} \bullet & 1 & 0 \\ \bullet & \bar{1} & \bar{1} \\ 0 & 0 & 0 \end{bmatrix} \qquad H_{2,2} = \begin{bmatrix} \bar{1} & \bullet & 0 \\ \bar{1} & \bullet & \bar{1} \\ \bar{1} & \bullet & \bar{1} \end{bmatrix} \qquad H_{2,3} = \begin{bmatrix} \bar{1} & 1 & \bullet \\ \bar{1} & \bar{1} & \bullet \\ \bar{1} & \bar{1} & \bullet \end{bmatrix}$$

(7) Count the number $p_{2,i}$ of 1 and the number $q_{2,i}$ of $\bar{1}$.

$$\begin{array}{lll} p_{2,1} = 1 & p_{2,2} = 0 & p_{2,3} = 1 \\ q_{2,1} = 2 & q_{2,2} = 5 & q_{2,3} = 5 \end{array}$$

(8) By the notation $p_1 = p_{1,i}$, $p_2 = p_{2,i}$, $q_1 = q_{1,i}$, $q_2 = q_{2,i}$ with $i \in \{1, 2, 3\}$. The observability coefficient is given by:

$$\eta_i = \frac{1}{2}\left[\frac{p_1}{p_1 + q_1} + \frac{q_1}{(p_1 + q_1)^3} + \frac{p_2}{p_2 + q_2} + \frac{q_2}{(p_2 + q_2)^2}\right]$$

where $p_k + q_k$ is replaced with $1 + q_k$, if $p_k = 0$.

$$\begin{array}{ccc} x_1 & x_2 & x_3 \\ \eta_1 = 0.7778 & \eta_2 = 0.1065 & \eta_3 = 0.1898 \end{array}$$

The results of the observability coefficient computed for Rössler map are in line with the experimental results from section 3.