11-30-2010

2D Spatial Distributions for Measures of Random Sequences Using Conjugate Maps

Qingping Li
Yunnan University, China

Jeffrey Zhi J. Zheng

DOI: 10.4225/75/57a83351aa0e2
11th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia,30th November - 2nd December 2010

2D Spatial Distributions for Measures of Random Sequences Using Conjugate Maps

Qingping Li, Jeffrey Zhi J. Zheng
School of Software
Yunnan University, China
visualizationmodel@gmail.com

Abstract
Advanced visual tools are useful to provide additional information for modern information warfare. 2D spatial distributions of random sequences play an important role to understand properties of complex sequences. This paper proposes time-sequences from a given logical function of 1D Cellular Automata in both Poincare map and conjugate map. Multiple measure sequences of Markov chains can be used to display spatial distributions using conjugate maps. Measure sequences recursively produced by different logical functions generating maps. Possible complementary feature exits between pair functions, Conjugate symmetry relationships between a pair of logical functions in conjugate maps can be observed.

Keywords
Time sequence, random property, cellular automata, spatial distribution, conjugate symmetry.

INTRODUCTION

Random sequences are widely used in many security based applications such as security communication, cryptology coding and information security systems (Key, 1976). To make proper analysis, Markov chain methodologies and technologies provide a series of important methods and tools to help analysers decoding process (James & Michael, 1972; Haccoun, 1980; Sheynin, 1989). In modern information warfare, it is essential for analysers to detect and decrypt the opponent's communications using information acquisition toolkits from real coding sequences (Widnall & Fogelman, 1997).

Information Warfare describes terms of 'actions' executed to achieve a sought outcome - denial, exploitation, corruption and destruction of an opponent's 'information' and related functions, and prevention of such 'actions' executed by an opponent (Borden, 1999).

The battle between the obscurers and those who sought to break the codes has been a continual one, but it reached a new level of stature and importance during World War II with its decryption of Germany's Enigma messages. Historic events are approved that statistical and probability tools are extremely important in Information Warfare applications. This battle of wits fought by British mathematicians and statisticians shortened World War II and ushered in the age of information warfare (Budiansky & Stephen, 2000).

Prerequisite of executing these attack actions is thorough understood the mechanism of information encryption that opponent uses (Carlo & Bruce, 2002). In information warfare, secured-communications among opposite parts may use public networks. It is feasible to capture relevant information for further analysis. Different quantitative tools and methods are useful to provide additional information in decoding process. Variant features play an important role for measurement and analysis of random sequences (Denning, 1999).

Because of the implicated expression of functions that generate random sequences, it is hard to get the characteristic of random sequences from the function and coding sequences themselves (Li & Tian, 2006). Traditionally, time sequence Map and Poincare Map are two most popular methods to take the measure features of a random sequence in 2 dimensions (Graeme & Matthew, 2009). From a visual viewpoint, current Markov chain schemes do not provide efficient visual mechanism to display multiple measurement sequences from the spatial characteristic of complex random sequences.

To extract further information from random sequences, this paper establishes a visual system to illustrate multi-parameter measurement sequences of Markov chains as conjugate maps. For a given set of measurement sequences, the conjugate map proposed in this paper can provide refined information of distributed structure than present map technologies (Li & Zheng, 2010).

In the second section, respective characteristics of traditional methods and conjugate method are discussed. The measurement mechanism of logical function's spatial characteristics: disposal model, measuring model, and visualizing model are described in the third section. The results of maps and analysis of the results are discussed in the fourth and fifth sections, and then, conclusion remarks are provided in the last section.

TRADITIONAL METHODS AND CONJUGATE METHOD

In this section, two typically traditional methods: Time Sequence Map and Poincare Map are discussed for comparison.

Time Sequence Map generates a 2D coordinate, X axis is determined by the time scale t and Y axis is determined by the value of measured parameter $f(t)$, as shown in Figure 1(a).

The measure sequence $\{f(t)\}_{t=0}^{T-1}$ with length of T can form Poincare Map according to the matching pattern considering data correlation. Poincare method maps one group of measures of time sequence to a 2D map. It detects spatial distribution of sequence through the distribution of point cluster. In Poincare Map, X axis is determined by the value of $f(t)$ while Y is $f(t+l)$. It's vicinity related patterns map when $l=1$, as shown in Figure 1(b).

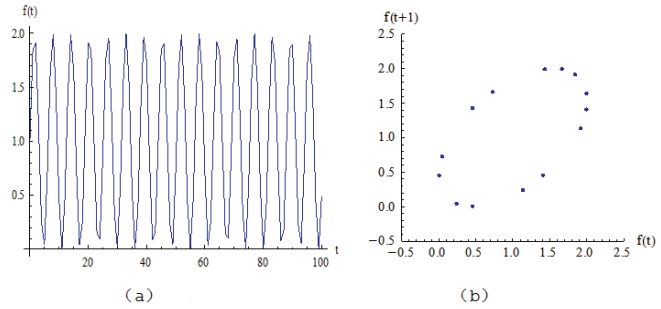

Figure 1: Simple Time-Sequence Map and Poincare Map; (a) Time Sequence Map, (b) Poincare Map.

Different from Poincare method based on one group of measures, new map proposed in this paper chooses 2 groups of measures from relevant parallel measures sequences. As two different groups of measures are acted simultaneously, the value of each axis is determined by these two groups of measurements. It is convenient to name new map as Conjugate Map to present this kind of multiple parameter measurement map.

GENERATE AND MEASURE MECHANISM OF TIME SEQUENCE

In this section, the CA (Cellular Automata) method is applied to generate time sequence and then to make concomitant measurement sequence. First, the initial sequence inputted, and the output sequence is generated by a given logical function using 1D cellular automata; Using this data sequence, measurements are formed by probability measurement according to pairs of Input and Output sequences; Finally, the generated measure sequences can be used to construct a 2D conjugate map showing 2D spatial distribution of the time sequence. The processing flow of the mechanism is shown in Figure 2.

Figure 2: Flow Sheet of the Produce and Detect Mechanism of Time-Sequences

Disposal Model

Consider a logical function f as a function of CA. The function generates equal-length output sequence $\{Y_i\}_{i=0}^{N-1}$ for any initial input sequence $\{X_i\}_{i=0}^{N-1}$ with N-length bits. The I/O pattern is shown in Table 1.

A total of 2^N states of N-length initial input sequence are exhaustively generated and the corresponding sequence under the logical function $f: X \to Y$ can be generated. The input and the output sequences are in the same group corresponded to each other; there are 2^N groups of corresponding relationship (Wolfram, 1986). Exhaustion of all the initial input sequences is shown in Table 2.

Measure Model

The basic model of measurement can be confirmed to establish the transformation relation between the input sequence $\{X_i\}_{i=0}^{N-1}$ and the output sequence $\{Y_i\}_{i=0}^{N-1}$ for each group.

In the transformation of $f: X_i \to Y_i, 0 \le i < N$, there are a total of 4 types of transformations, each type determines a number, and corresponding relationships are shown in Table 3. This type of measurement structure has a directly corresponding relationship to the Markov chain mechanism (Sheynin, 1989).

Consider $j \in \{0,1,2,\ldots,2^N-1\}$ as the serial number of different initial input sequence. There are 4 measurements that can be identified by the measurement parameters above shown in Table 4 with Markov chain properties respectively.

Table 1: I/O Pattern of Disposal Model

Function f	**Input sequence**	$X_0, X_1, \ldots, X_i, \ldots X_{N-1}, X_i \in \{0,1\}$
	Output sequence	$Y_0, Y_1, \ldots, Y_i, \ldots Y_{N-1}, Y_i \in \{0,1\}$

Table 2: Exhaustion of Initial Input Sequences

Serial number	Input sequences
0	0 0 0……0 0 0
1	0 0 0……0 0 1
…	……
2^N-2	1 1 1……1 1 0
2^N-1	1 1 1……1 1 1

Table 3: Measure Parameters

Transform type	Number of type	Number of 0、1 in input sequence	Total number
$0 \to 0$	N_{00}	$N_0 = N_{00} + N_{01}$	$N = N_0 + N_1 = N_{00} + N_{01} + N_{10} + N_{11}$
$0 \to 1$	N_{01}		
$1 \to 0$	N_{10}	$N_1 = N_{10} + N_{11}$	
$1 \to 1$	N_{11}		

Table 4: Probability Measure

Measure parameters	Value of parameter
$P_{00}(j)$	$N_{00}(j)/N_0(j)$
$P_{01}(j)$	$N_{01}(j)/N_0(j)$
$P_{10}(j)$	$N_{10}(j)/N_1(j)$
$P_{11}(j)$	$N_{11}(j)/N_1(j)$

For different initial input sequences, there can be generated 4 groups of measurements on the corresponding I/O sequences: $\{P_{00}(j)\}_{j=0}^{2^N-1}$, $\{P_{01}(j)\}_{j=0}^{2^N-1}$, $\{P_{10}(j)\}_{j=0}^{2^N-1}$ and $\{P_{11}(j)\}_{j=0}^{2^N-1}$.

Visualization Model

Based on the probability measurements presented above, two measurements are chosen to construct 2D map. As two different groups of measurements are used simultaneously, to name this kind of map conjugate map, of which the value of each axis is determined by these two groups of measurements.

According to the construction pattern introduced above, there are $C_4^2 = 6$ kinds of different combinations as below: $\{P_{00}(j), P_{01}(j)\}$, $\{P_{00}(j), P_{10}(j)\}$, $\{P_{00}(j), P_{11}(j)\}$, $\{P_{10}(j), P_{11}(j)\}$, $\{P_{01}(j), P_{11}(j)\}$, $\{P_{01}(j), P_{10}(j)\}$.

On the same group of sequences, construct 2D conjugate maps respectively by using the combinations above as shown in Figure 3.

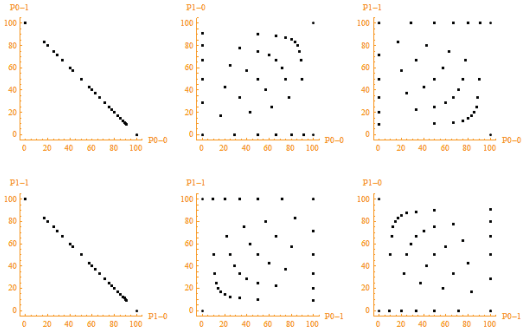

Figure 3: 2D Conjugate Maps Constructed By Separate 6 Pairs Of Measures of No.6 Function; N=13.

This paper chooses the typical combination $\{P_{01}(j), P_{10}(j)\}$ constructing 2D conjugate map to detect the special distribution of time sequences for N=13 condition.

VISUALIZATION RESULT

Because of the restriction of the structural complexity of the logical function, 16 functions of 2 variables are used to describe them in the way of exhaustion (Wan & Zheng, 2010). Output sequences are generated by different initial input sequences under the given logical function and then obtaining various measure data from the corresponding I/O sequence based on probability method. Then the map is constructed using these measurement data.

This paper choose No. 1, 5, 6 and 13 functions which are typical functions as an example, observing the characteristic of three kinds of maps which are given in Figure 4.

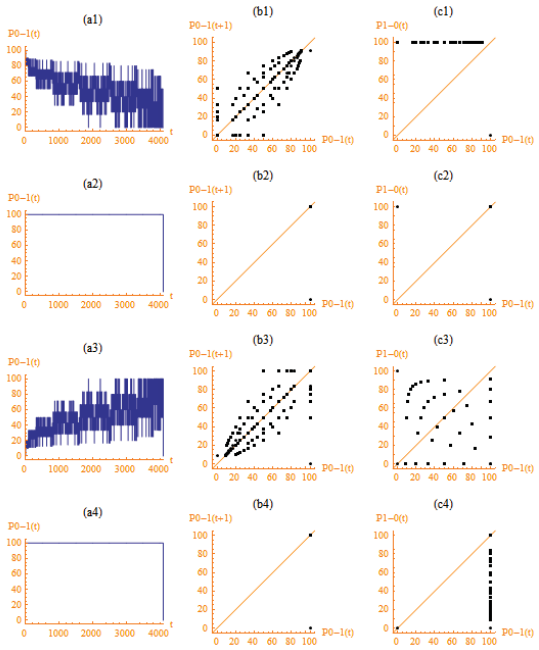

Figure 4: Time-Sequence Maps, Poincare Maps and 2D Conjugate Maps. (a) Time Sequence Map; (b) Poincare Map; (c) 2D Conjugate Map.

In (a) group of time sequence maps, only one measurement sequence transform with time.
In (b) group of Poincare maps, different function forms different points cluster.
In (c) group of Conjugate maps the distribution of the points cluster has clear polarized properties.

According to the variable-value logic theory, 3 kinds of encoding model can be distinguished: W, F and C (Zheng & Zheng, 2010).

The visualization information that can be acquired from a single function's map is rather limited. In order to compare the spatial property of different logical function, an 4×4 array is constructed using the maps that are generated from 16 logical functions in different encoding pattern as shown in Figure 5.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

W

0	2	1	3
4	6	5	7
8	10	9	11
12	14	13	15

F

0	4	1	5
2	6	3	7
8	12	9	13
10	14	11	15

C

Figure 5: Assemble Pattern of Maps in W-code, F-code and C-code

By assemble maps of total 16 logical functions under the models, the entire structure information among logical functions themselves can be observed.

To compare conveniently, combinations of 16 recursive images which generated from 16 functions are given in this paper under different codes. Recursive images in W-code, F-code and C-code from a given initial sequence are shown in Figure 6—Figure 8 respectively.

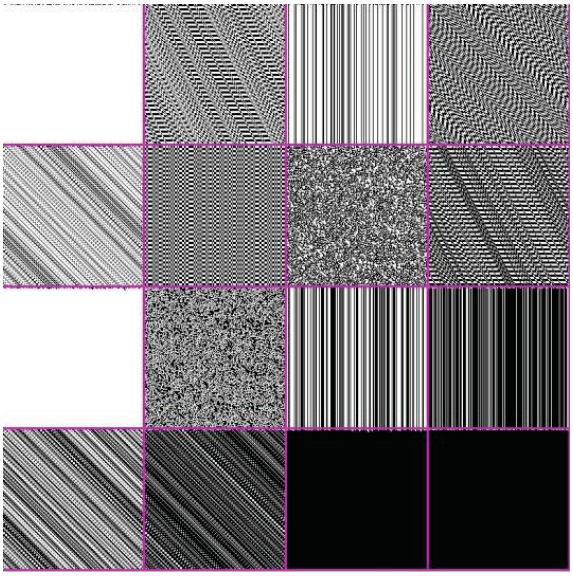

Figure 6: Recursive Images in W-Code

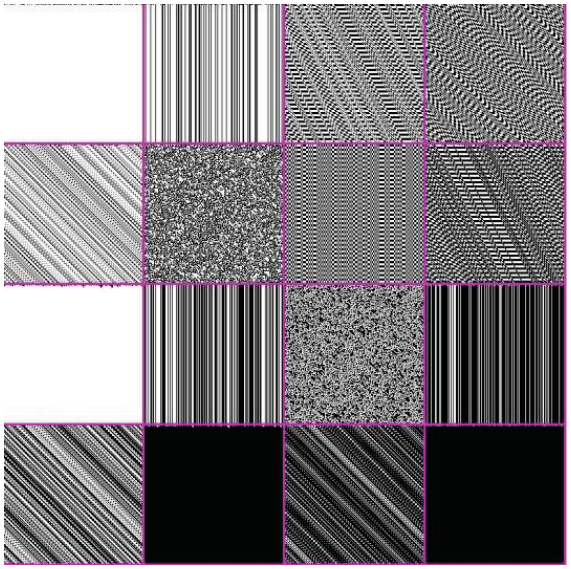

Figure 7: Recursive Images in F-Code

The combination of time sequence map is shown in Figure 9. The figure shows that different function has different distribution property, and also reveals the trend of single measurement's transforming with time.

The combination of Poincare map in W-code is shown in Figure 10. Different distribution properties of functions can be observed from the figure. It is clear that there are four groups of configurations appeared in the figure: {0,8,2,10}, {1,3,9,11}, {4,6,12,14}, {5,7,13,15}.

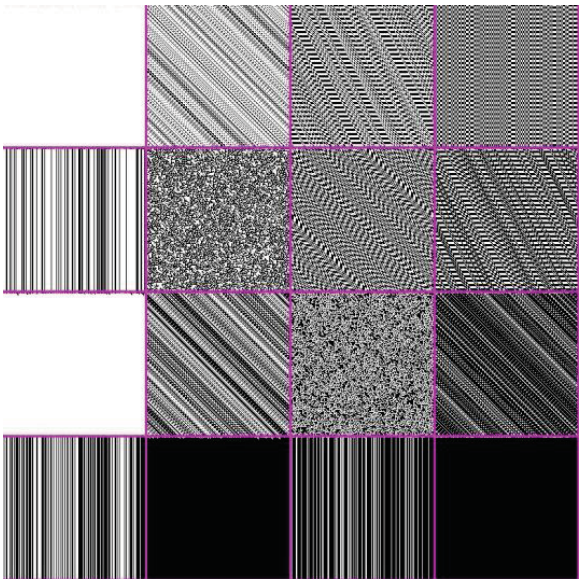

Figure 8: Recursive Images in C-Code

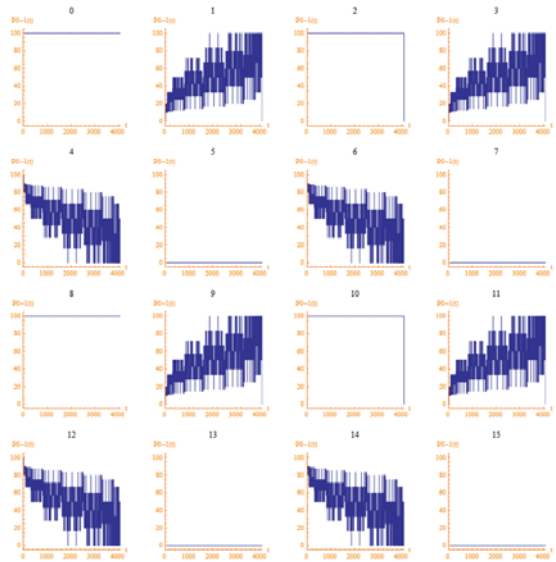

Figure 9: Time-sequence maps of 16 functions constructed by $\{t, P_{0-1}(t)\}$ sequences

For W-code, Poincare maps are shown in Figure 10 and corresponding 2D conjugate maps are shown in Figure 11. Conjugate maps have polarized properties and their function pairs of 0:15, 1:7, 2:11, 4:13 and 8:14 have conjugate symmetry. In general, 16 conjugate maps are different from relevant maps generated by Poincare maps.

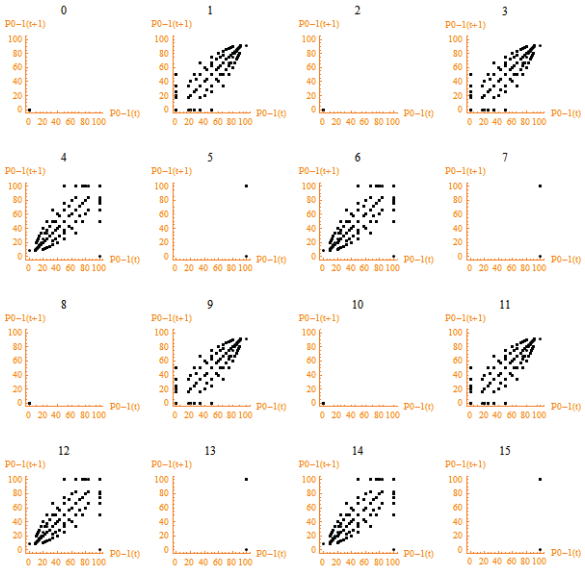

Figure 10: Poincare Maps in W-Code

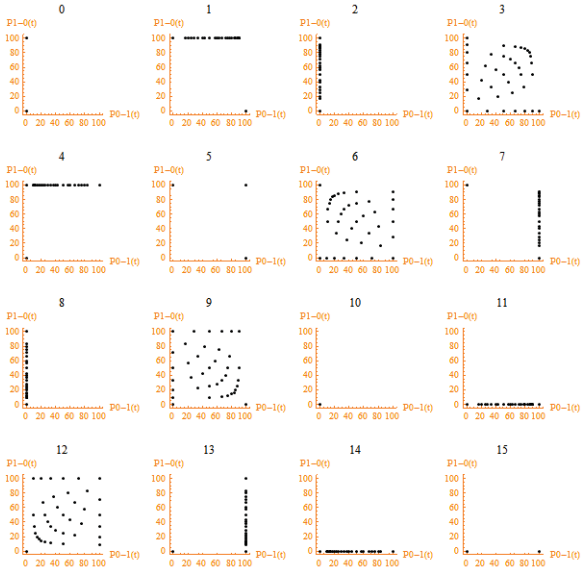

Figure 11: Conjugate Maps in W-Code

To arrange 16 Poincare maps and conjugate maps by F-Code structure, F-code maps are shown in Figures 12 & 13 respectively.

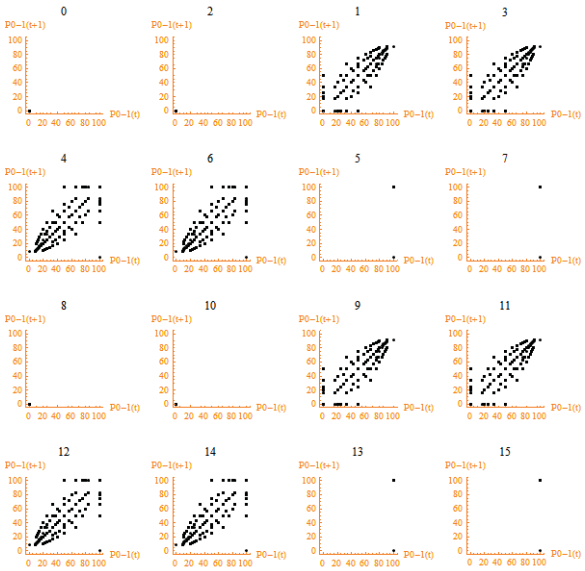

Figure 12: Poincare Maps in F-Code

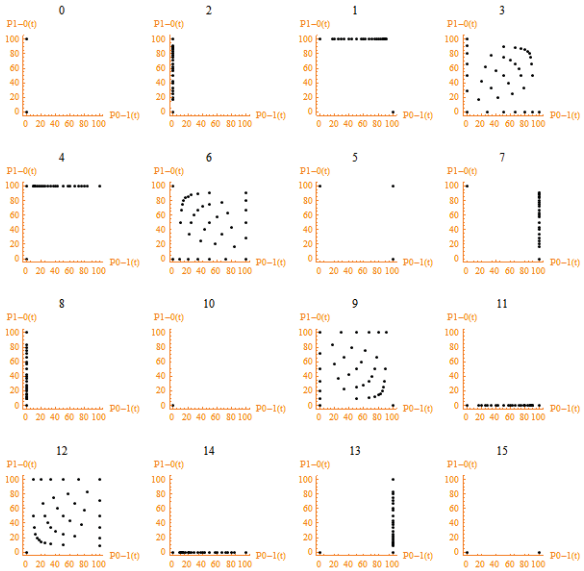

Figure 13: Conjugate Maps in F-Code

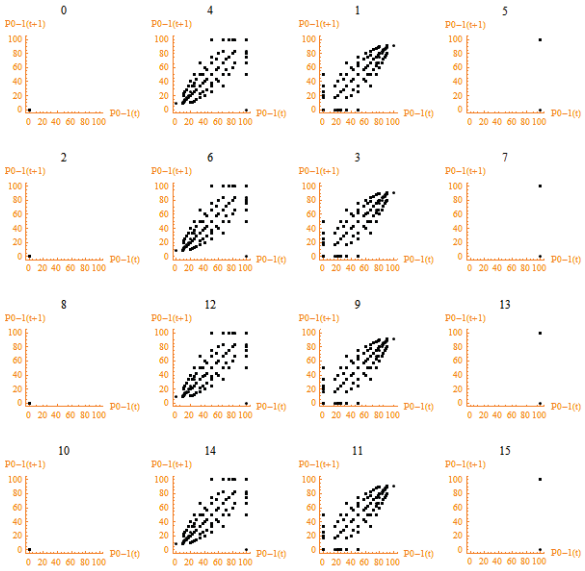

Figure 14: Poincare Maps in F-Code

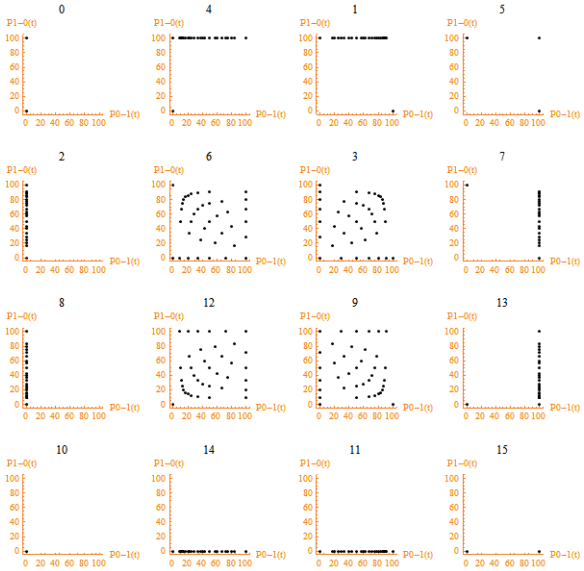

Figure 15: Conjugate Maps in C-Code

Under C-Code structure, Poincare maps and conjugate maps are shown in Figure 14 and Figure 15.

In the above maps, 2D conjugate maps not only show spatial distributions of different logical functions, but also have special holistic symmetries under the F and C code conditions.

ANALYZE

Through three types of different maps, three different coding schemes can be observed.

Time sequence map can show the simple trend of single measurement series with time variations, but it has difficult for the scheme to describe spatial distributions of time sequence.

Poincare map can apply a single measurement sequence, although the map can be generated under different length in a correlation, information of distribution is naturally limited by the selected measurement sequence.

A 2D conjugate map uses 2 groups of independent measurements simultaneously; this scheme can show differences and connections between spatial distributions of logical functions, furthermore, through different coding model, it can illustrate holistic relationships among different functions. i.e. function pairs of 0:15, 1:7, 2:11, 4:13 and 8:14 have clear conjugated symmetry in conjugate maps. In addition, for C code condition, the points of 4 functions on each edge of maps are located on the same side of edge. For example, points clusters of (0, 4, 1, 5), (0, 2, 8, 10), (10, 14, 11, 15) and (5, 7, 13, 15) functions are separately located on four side of the 2D map space.

CONCLUSION

Refined property of various time sequences can be identified from 2D conjugate maps to illustrate multiple measurement sequences under Markov chain mechanism. Spatial property of time sequence plays an important role in the study of dynamic sequence's behaviour. The stable distribution under visualization method can help people understand relevant issues.

In compared with Poincare maps and conjugate maps, there are additional properties in the complex dynamic sequences. Conjugate map method uses multiple parameters of Markov chains to make independent measurements simultaneously.

Proposed technology can provide further structural information among multiple measurements, refined relationship via spatial distributions can be established. It is possible for the scheme to use statistical and probability methodologies to enhance visual tools of Markov chain mechanisms to resolve real problems and requirements for modern information warfare and information security applications in near future.

ACKNOWLEDGEMENT

Thanks Mr. Jie Wan for him to generate data for this study and the special fund of Information Security (No. 2010KS06), Software School of Yunnan University to fund the project.

REFERENCES

Borden, A. (1999) "What is Information Warfare?". Aerospace Power Chronicles, United States, Air Force, Air University, Maxwell AFB, Contributor's Corner: http://www.airpower.maxwell.af.mil/ airchronicles/cc/borden. html.

Budiansky & Stephen. (2000) "Battle of Wits: The Complete Story of Codebreaking in World War II". New York: Free Press.

Carlo Kopp & Bruce Mills. (2002) "Information Warfare and Evolution". Proceedings of the 3 rd Australian Information Warfare & Security Conference, ECU.

Denning, D. E. (1999) "Information Warfare and Security". Massachusetts: Addison Wesley.

Graeme Pye & Matthew Warren. (2009) "Appraising Critical Infrastructure Systems with Visualisation". In 10th Australian Information Warfare and Security Conference, 5-12.

Haccoun D. (1980) "A Markov chain analysis of the sequential decoding metric". *Information Theory*, IEEE Transactions, Volume 26, Issue 1, 109-113.

James L. Massey & Michael K. Sain. (1972) "Certain infinite Markov chains and sequential decoding". *Discrete Mathematics*, Volume 3, Issues 1-3, 163-175.

J. Wan & J. Z.J. Zheng. (2010) "Showing exhaustive number sequences of two logic variables for variant logic functional space". Proceedings of Asia-Pacific Youth Conference on Communication., 69-73

J. Z.J. Zheng & C. Zheng. (2010) "A framework to express variant and invariant functional spaces for binary logic". *Front. Electr. Election. Eng. China*, 5(2): 163-172, Higher Education Press & Springer Press.

Key E.L. (1976) "An analysis of the structure and complexity of nonlinear binary sequence generators". *Information Theory*, IEEE Transactions. Vol. IT-22, No.6, 732-736.

Q. Li & J. Z.J. Zheng. (2010) "Spacial Distributions for Measures of Random Sequences Using 2D Conjugate Maps". Proceedings of Asia-Pacific Youth Conference on Communication, 64-68.

S. Li & X. Tian. (2006) "Nonlinear study and complexity study". Harbin Institute of Technology Press.

S. Wolfram. (1986) "Theory and Applications of Cellular Automata". World Scientific Press.

Sheynin O.B. (1989) "Markov's work on Probability". *Artch. History Exact Sci.*, 39(3): 337-377.

Widnall, S. E. & Fogelman, R. R. (1997) "Cornerstones of Information Warfare". *Doctrine/Policy Document,* United States Air Force.