Chaos and Source Coding

K.W. Wong

Department of Electronic Engineering

City University of Hong Kong

Content

- *Background*
- *Coding by Continuous-time Chaotic Systems*
- *Coding by Discrete-time Chaotic Maps*
- *Simultaneous Compression and Encryption using Chaotic Maps*
- *Conclusions*

Content

- *Background*
- *Coding by Continuous-time Chaotic Systems*
- *Coding by Discrete-time Chaotic Maps*
- *Simultaneous Compression and Encryption using Chaotic Maps*
- *Conclusions*

Chaos

- Dictionary definition of chaos: "a state of complete disorder and confusion" (Longman Active Study English-Chinese Dictionary)
- Chaos: output highly sensitive to initial condition and system parameters

Source Coding

- Represent the signal or message sequence in another form or domain
- Goal: to eliminate or reduce redundancy so as to minimize the amount of information to be stored or transmitted.
- Final length < original length → Compression
- Reconstruction: can be lossless or lossy

This talk

- Describe some approaches of using a chaotic signal to represent a sequence of source symbols.
- Chaotic signal: can be the output of a continuous-time chaotic system or a discrete-time chaotic map
- Lossless reconstruction
- Propose a scheme for simultaneous compression (arithmetic coding) and encryption using chaotic maps

Content

- *Background*
- *Coding by Continuous-time Chaotic Systems*
- *Coding by Discrete-time Chaotic Maps*
- *Simultaneous Compression and Encryption using Chaotic Maps*
- *Conclusions*

Continuous-time Chaotic System

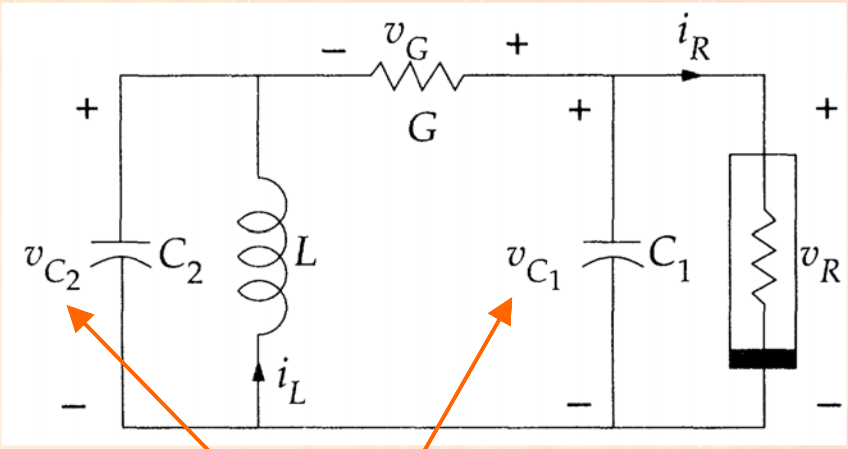
- The output of a chaotic system can be controlled by small perturbations

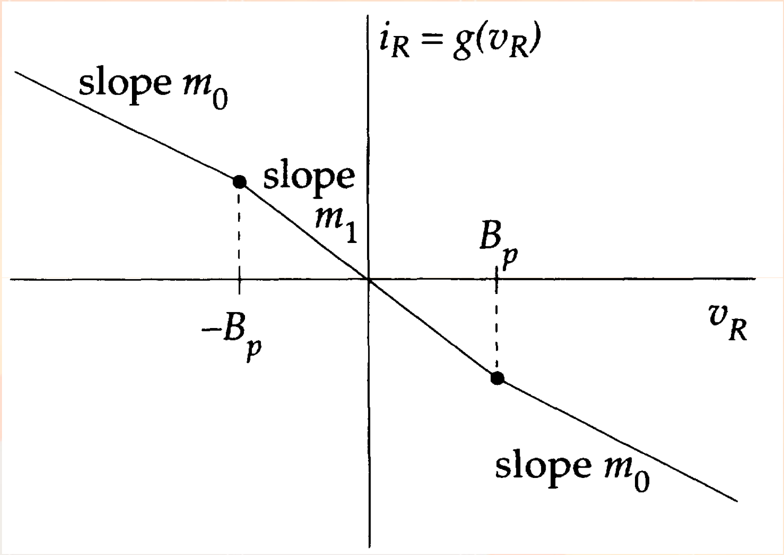
- Chaotic systems can be guided to produce a signal bearing desired (digital) information

- Coding: make the symbolic dynamics of the output of a chaotic system follow a prescribed symbol sequence

Double Scroll Circuit

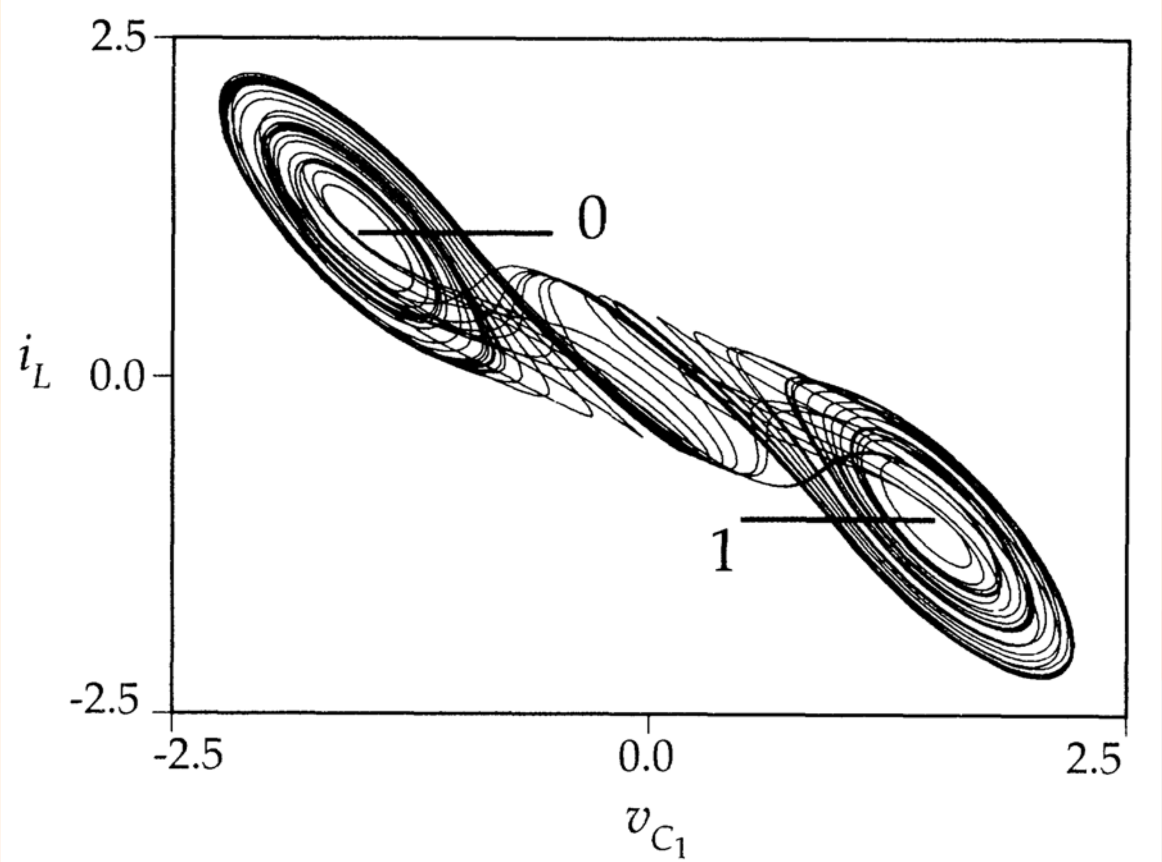
S. Hayes, C. Grebogi, E. Ott, "Communicating with Chaos," *Physical Review Letters*, vol. 70, no. 20, pp.3031-3034, 1993.



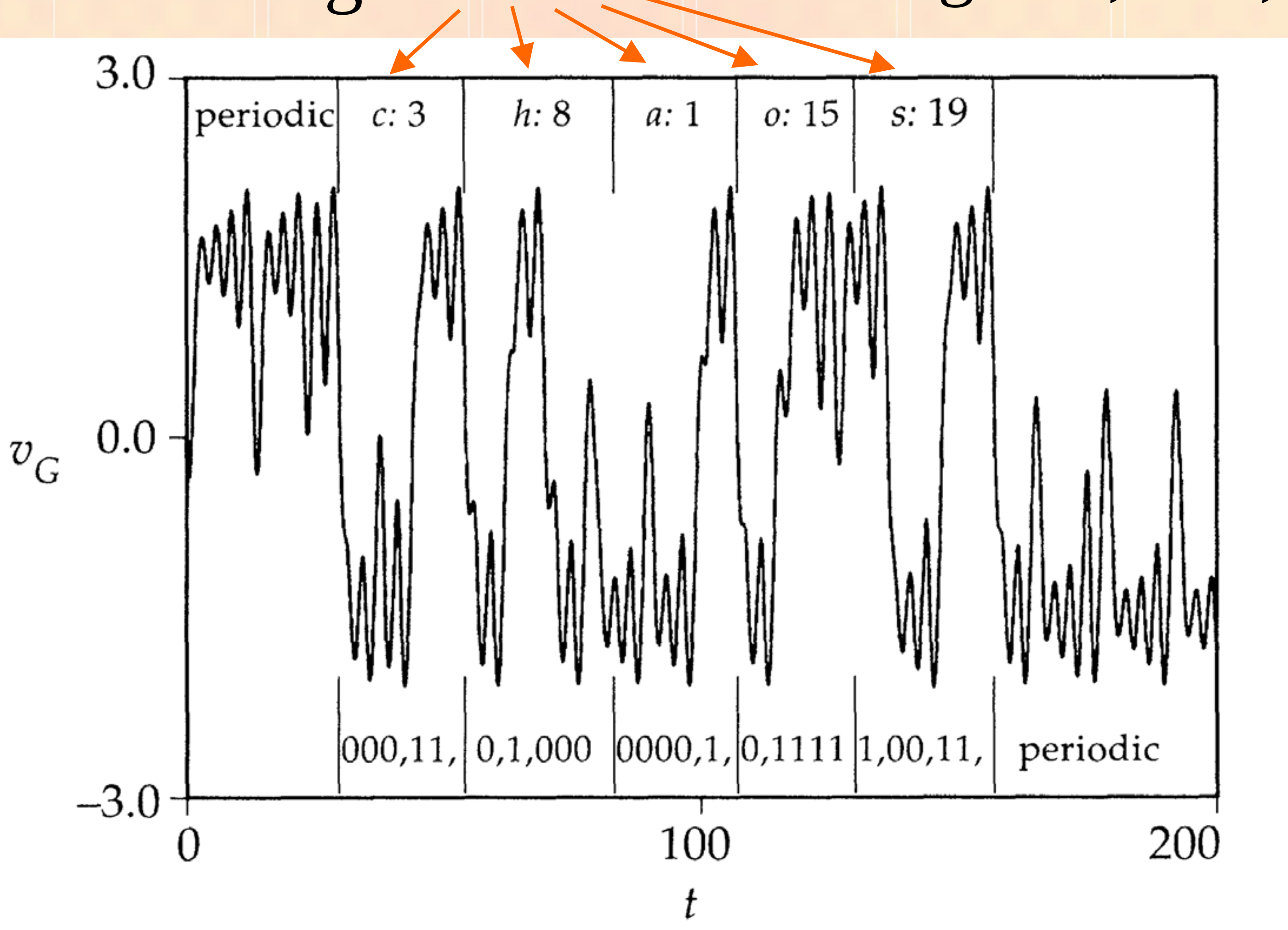


Small correcting voltage perturbation $\delta v_{C1}, \delta v_{C2}$

Double-scroll oscillator state-space trajectory

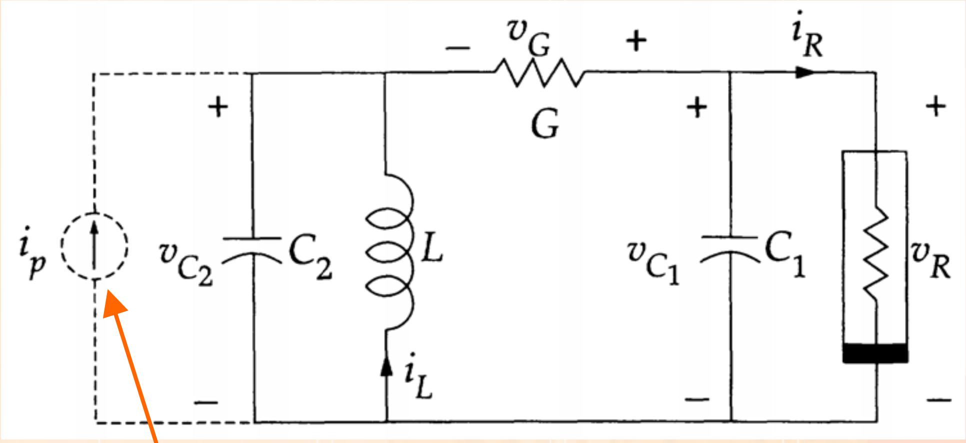


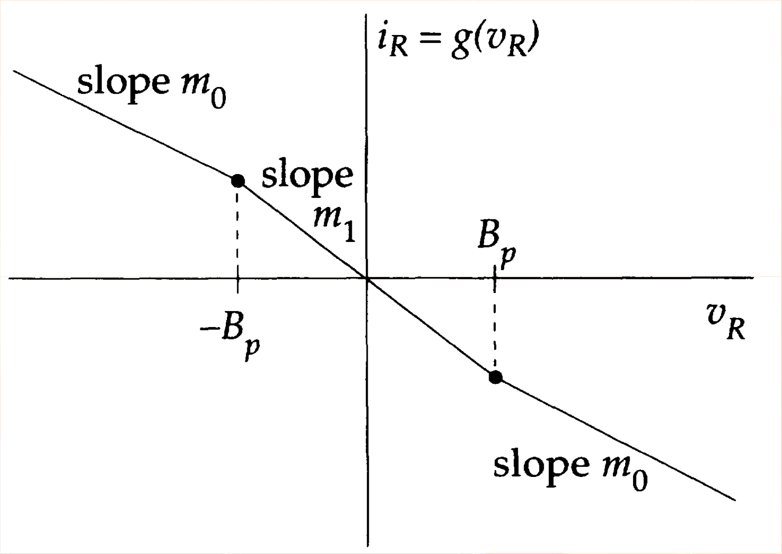
Message: *chaos* Coding rule, a=1, b=2,… z=26



Another attractor

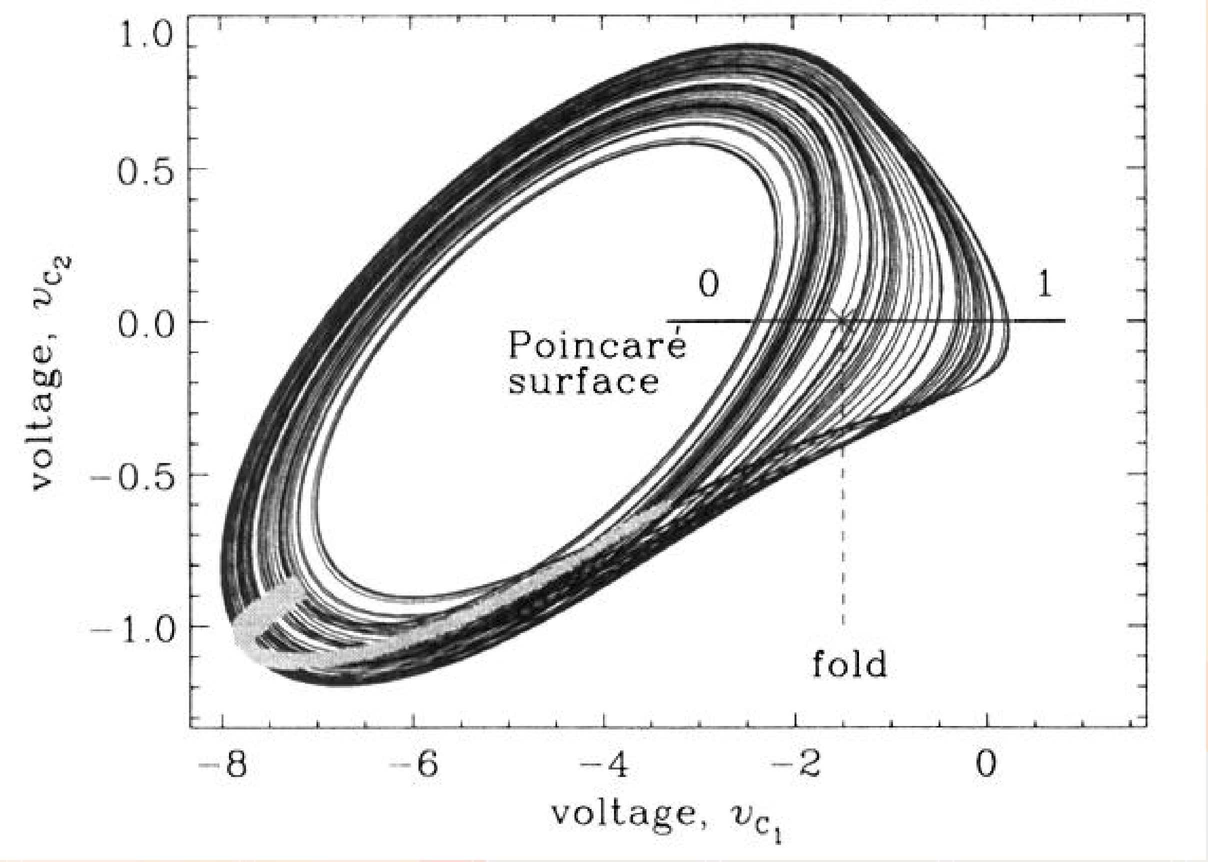
S. Hayes, C. Grebogi, E. Ott, and A. Mark, “Experimental Control of Chaos for Communication,” *Physical Review Letters*, vol. 73, no. 13, pp.1781-1784, 1994.





Small current pulse generator for perturbation

Another attractor



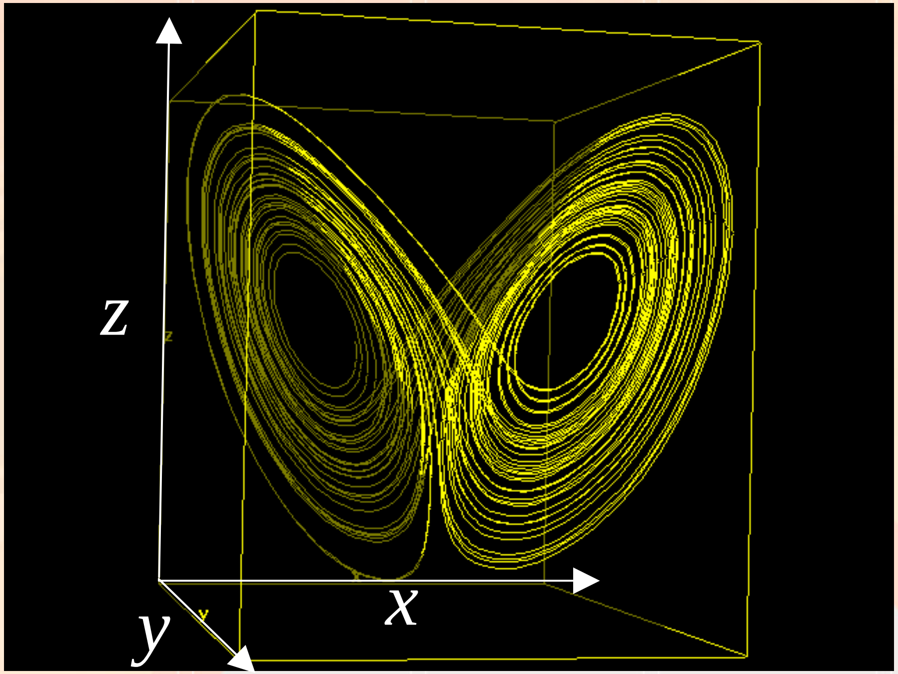
Lorenz System

E. Bollt, Y.C. Lai, and C. Grebogi, “Coding, Channel Capacity, and Noise Resistance in Communicating with Chaos,” *Physical Review Letters*, vol. 79, no. 19, pp.3787-3790, 1997.

$$\frac{dx}{dt} = 10(y - x)$$

$$\frac{dy}{dt} = x(28 - z) - y$$

$$\frac{dz}{dt} = xy - \frac{8}{3}z$$



http://hypertextbook.com/chaos/21.shtml

Lorenz System

- Let z_n be the maximum of the state variable $z(t)$.
- Successive maxima can be described by a 1-D single maximum, non-differentiable map

$$z_{n+1} = f(z_n)$$

- Natural partition: at the critical point z_c where $f(z_c)$ is maximum.
- A trajectory point with $z < z_c$, symbol 0
- Otherwise, it represents symbol 1.

Content

- *Background*
- *Coding by Continuous-time Chaotic Systems*
- *Coding by Discrete-time Chaotic Maps*
- *Simultaneous Compression and Encryption using Chaotic Maps*
- *Conclusions*

Coding using Transient Chaos

- Ying-Cheng Lai, “Encoding Digital Information using Transient Chaos,” *International Journal of Bifurcation and Chaos*, vol. 10, no. 4, pp. 787-795, 2000.
- Symbolic representations of controlled chaotic orbits can be utilized for encoding digital information.
- From the standpoint of channel capacity, it is more advantageous to use transient chaos naturally arising in wide parameter regimes of nonlinear systems as information sources.

- Channel capacity: the amount of information the channel or device can encode.

- Topological entropy h_T: the rate at which information is generated by the system.

- A sequence of N random binary symbols

$$b_1 \, b_2 \ldots b_{N\text{-}1} \, b_N$$

$$h_T = \lim_{N \to \infty} \frac{\ln 2^N}{N} = \ln 2$$

- 1-D logistic map:

$$x_{n+1} = f(x_n) = r\,x_n(1 - x_n)$$

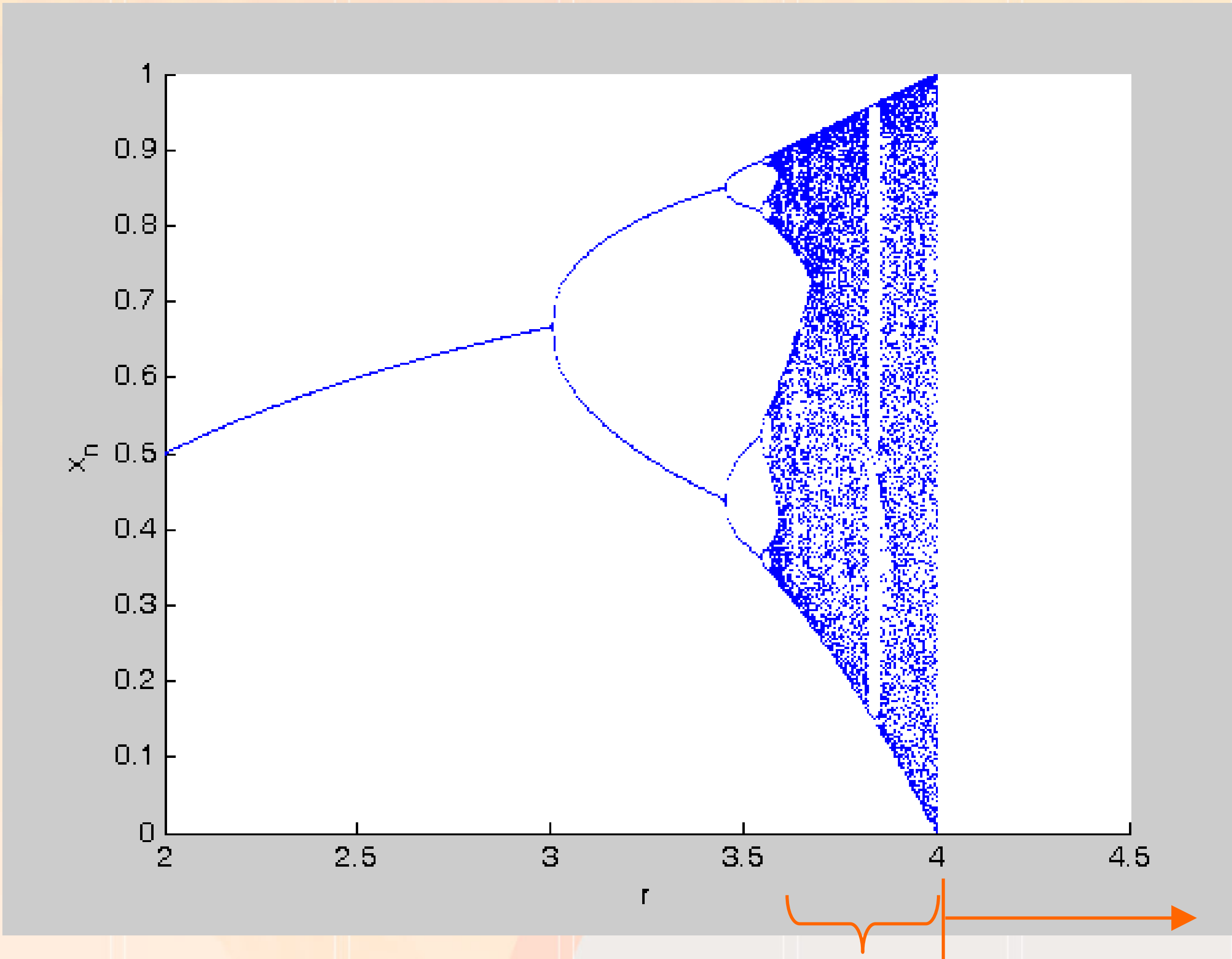
r : control parameter

$r_F \cong 3.58$ Feigenbaum point, transition to chaos

$r_F < r \le r_C = 4$ Chaotic attractors and stable periodic attractors

$r > r_C$ Transient chaos

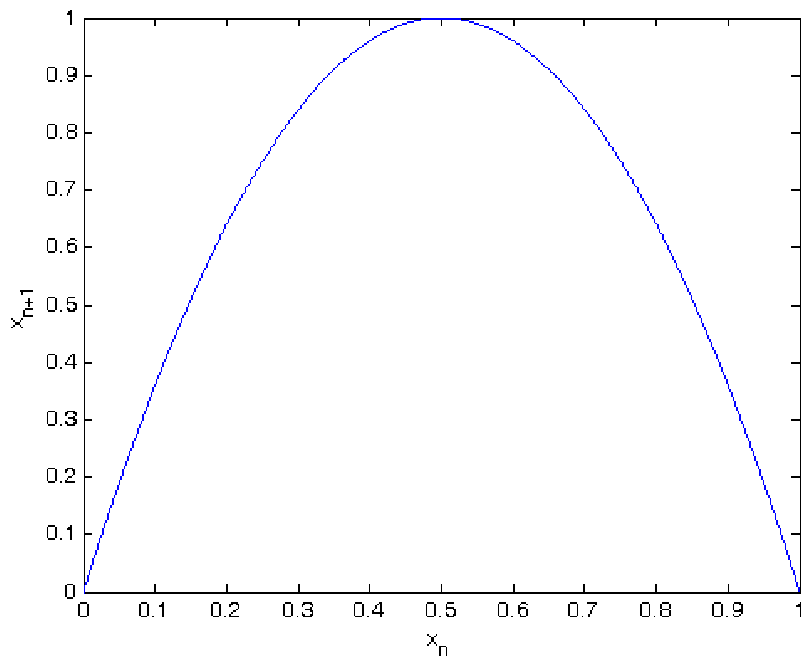
Logistic Map (Bifurcation Diagram)



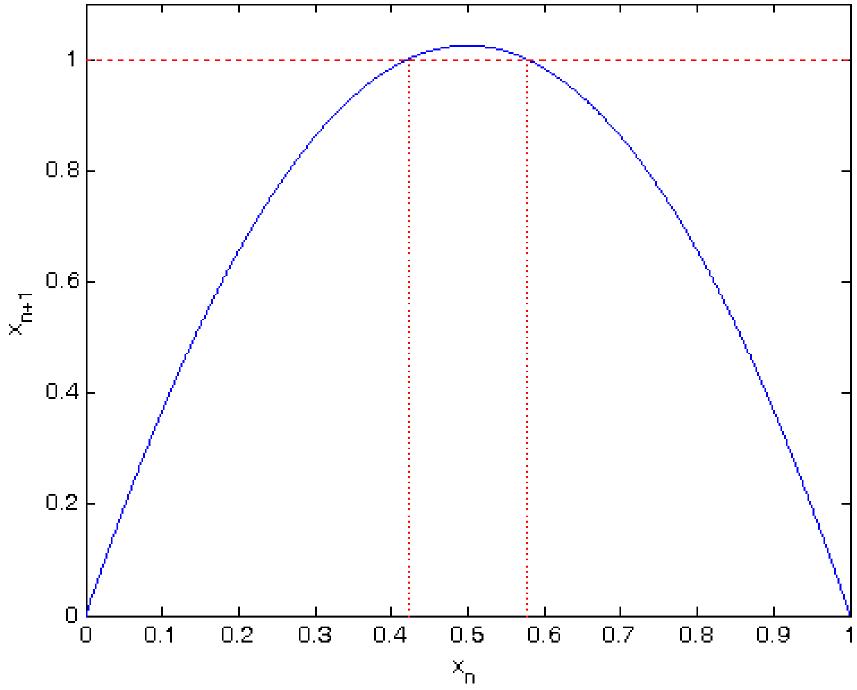
chaotic region *transient chaos*

$$x_{n+1} = r\, x_n (1 - x_n)$$

$r = 4$



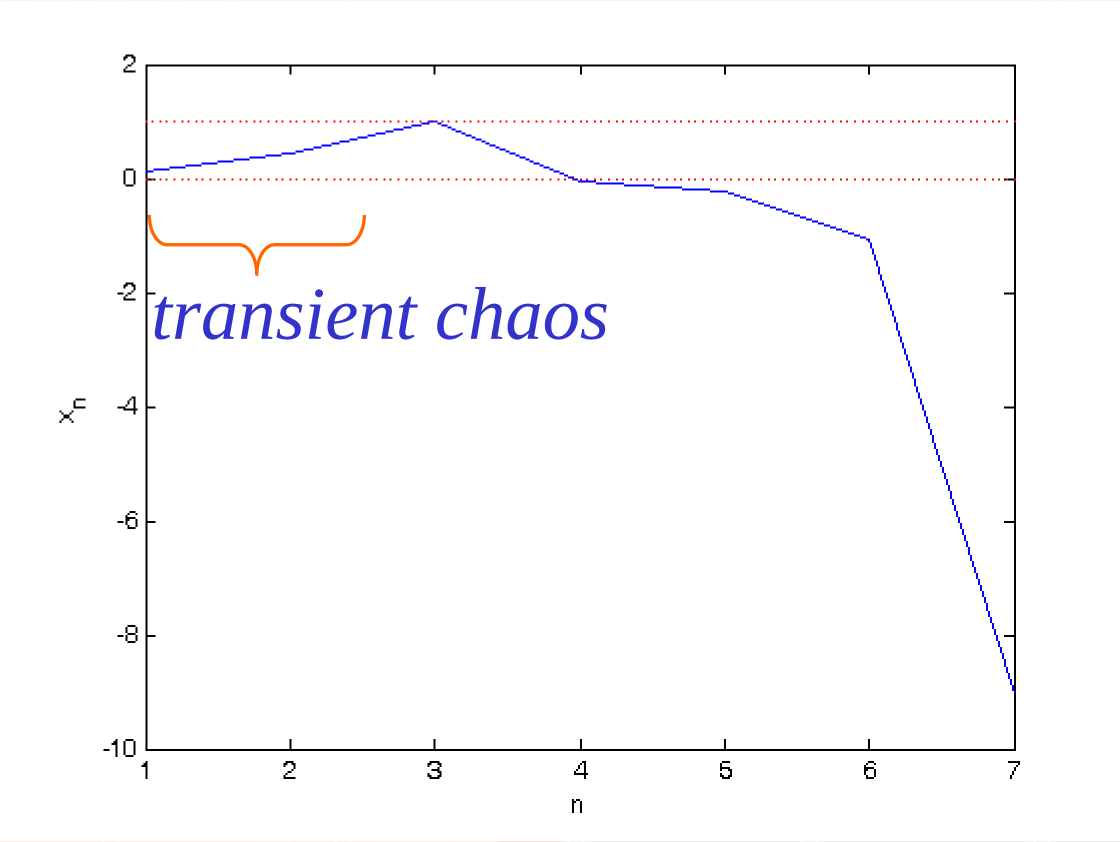
$r = 4.1$



Logistic map output (r = 4.1, x_0= 0.123456) :

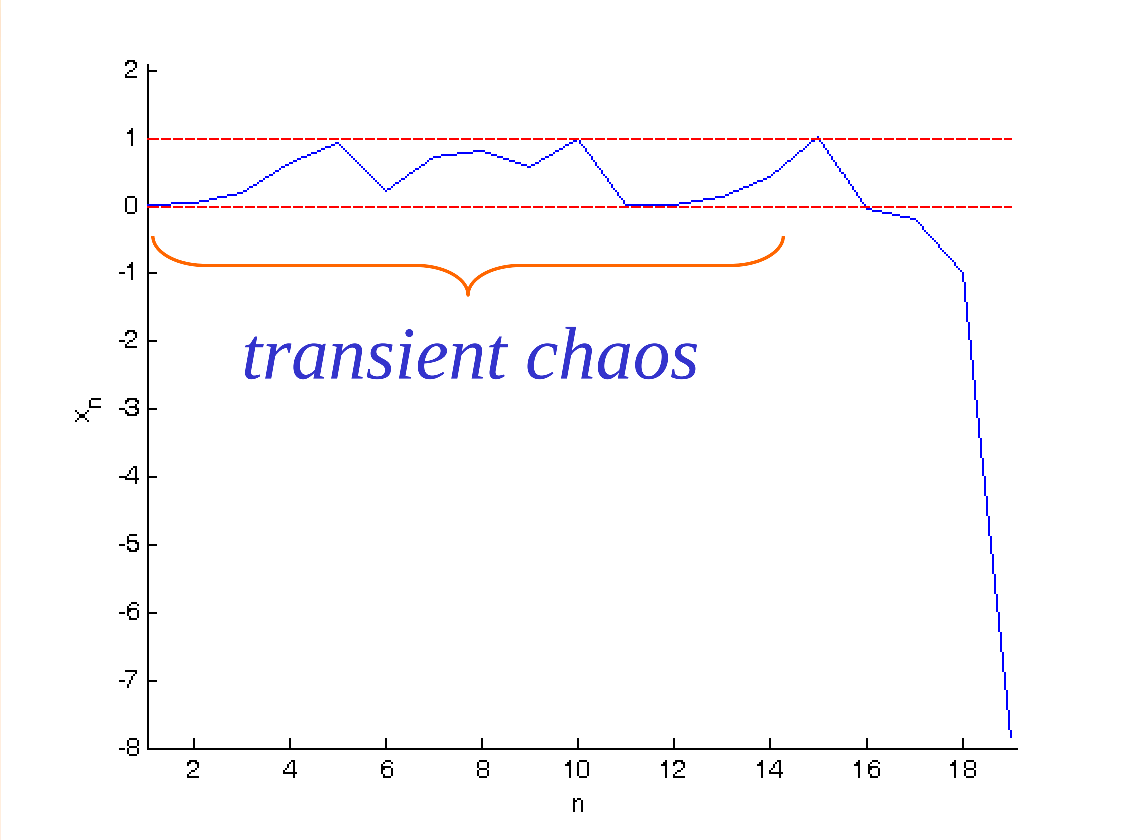
0.1235 0.4437 1.0120 -0.0498 -0.2142 -1.0664 -9.0347 -371.7106

-5.68×10^5 -1.32×10^{12}



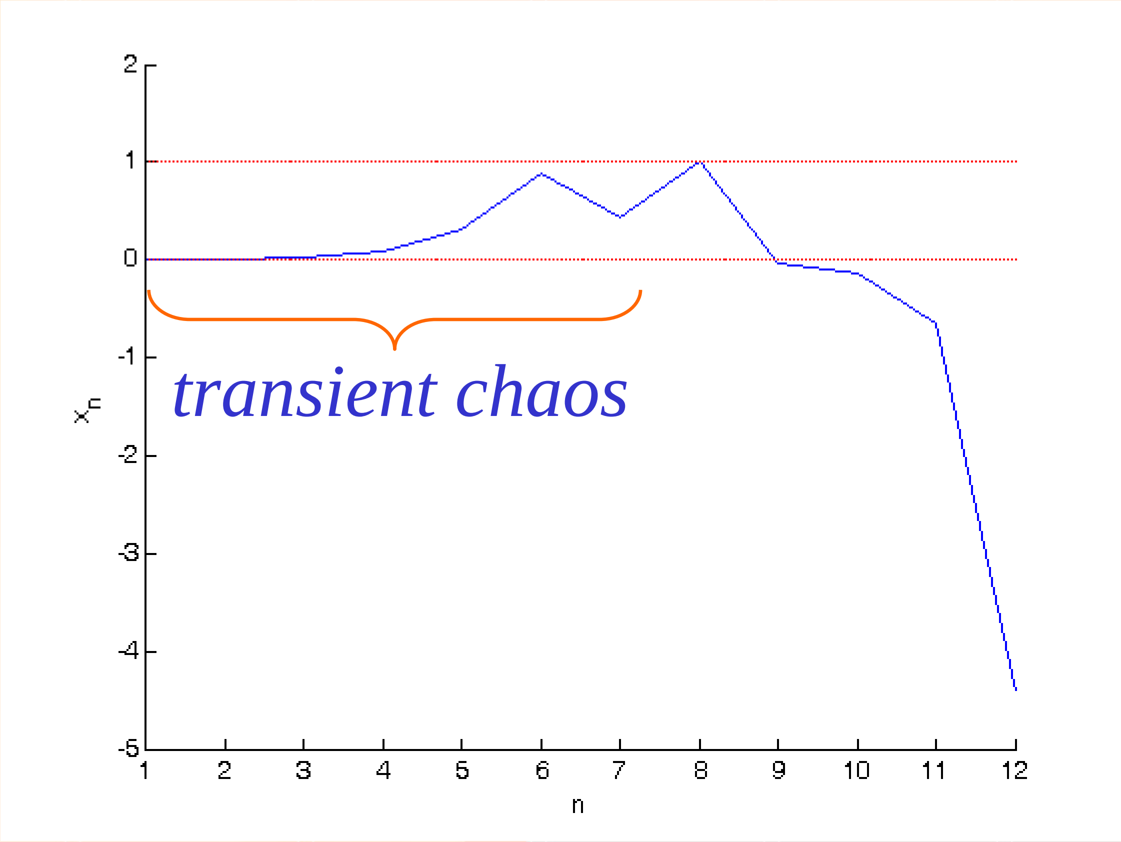
Logistic map output (r = 4.1, x_0= 0.0123456) :

0.0123	0.0500	0.1947	0.6429	0.9413	0.2266	0.7186	0.8291	0.5809	0.9981
0.0076	0.0309	0.1229	0.4419	1.0111	-0.0462	-0.1981	-0.9729	-7.8700	



Logistic map output (r = 4.1, x_0= 0.00123456) :

0.0012 0.0051 0.0206 0.0828 0.3114 0.8792 0.4356 1.0080 -0.0330
-0.1396 -0.6521 -4.4174 -98.1158 -3.99×10^4 -6.52×10^9

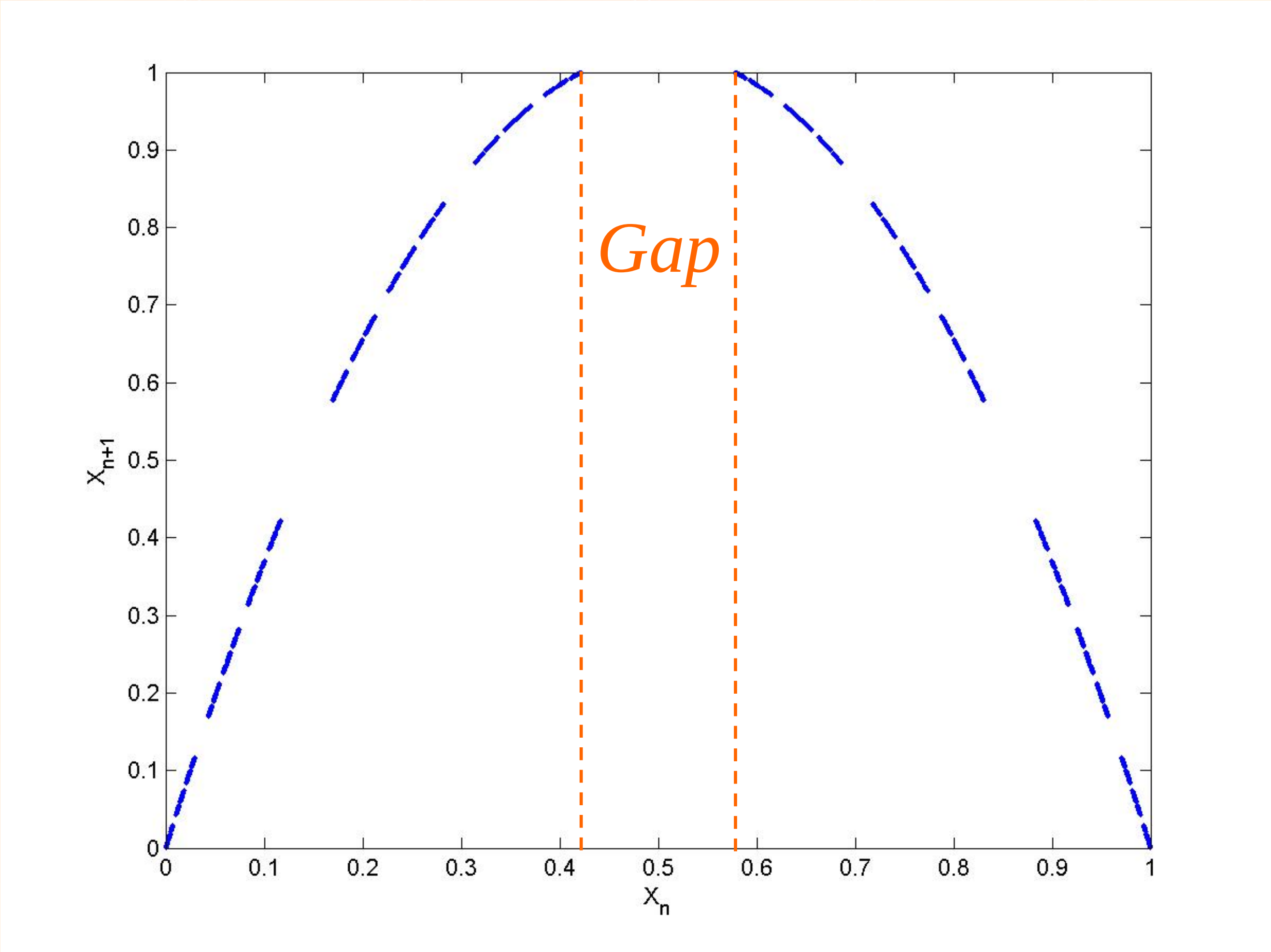


Transient Chaos in 1-D Logistic Map

- $r > 4$: transient chaos, the trajectory behaves chaotically for a period of time and then asymptotes to $x = -\infty$.
- A chaotic repeller, i.e., a fractal Cantor set in the unit interval.
- A primary gap of size

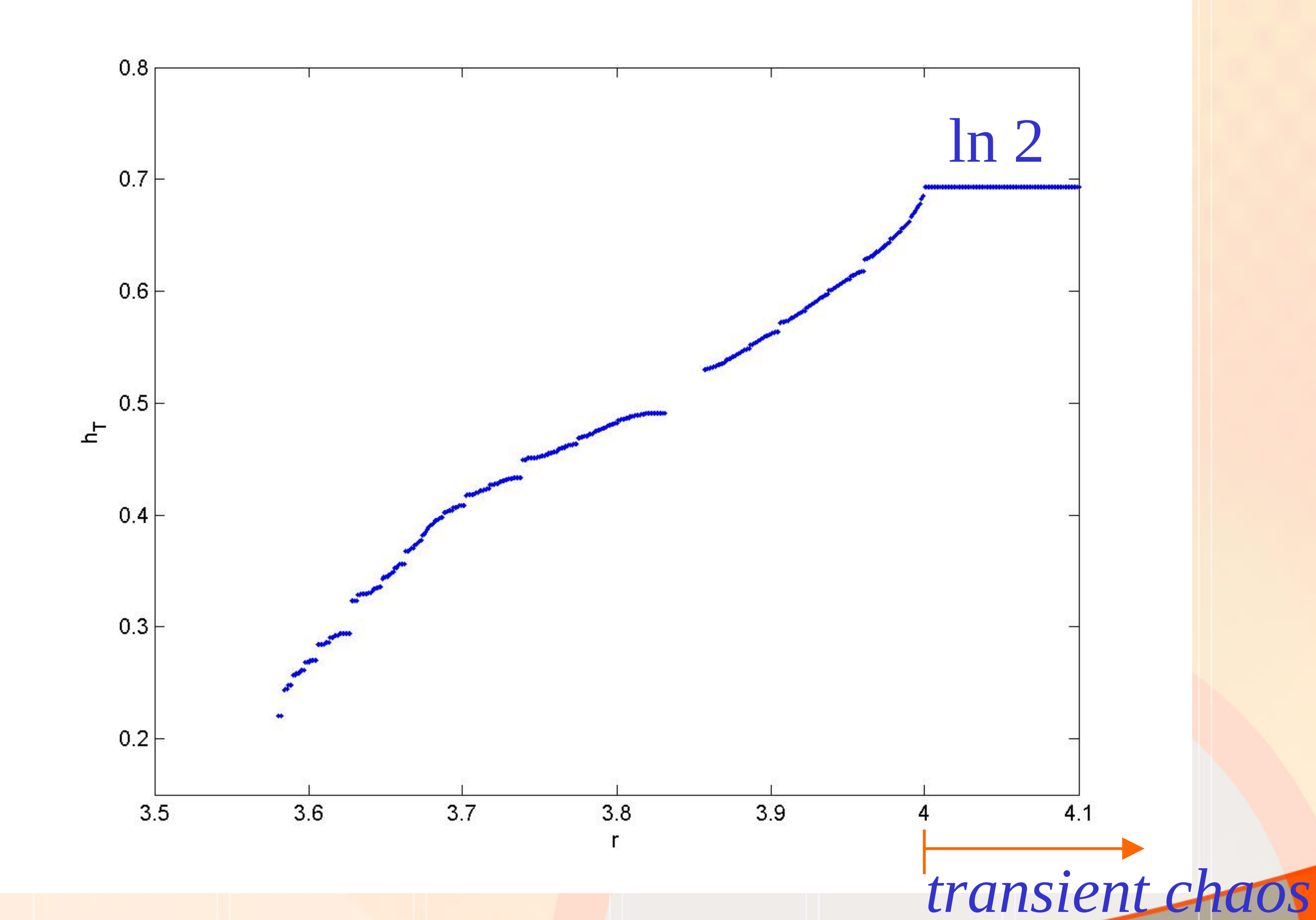
$$\sqrt{\frac{s}{1+s}} \quad where\ s = \frac{r}{4} - 1$$

Chaotic Repeller

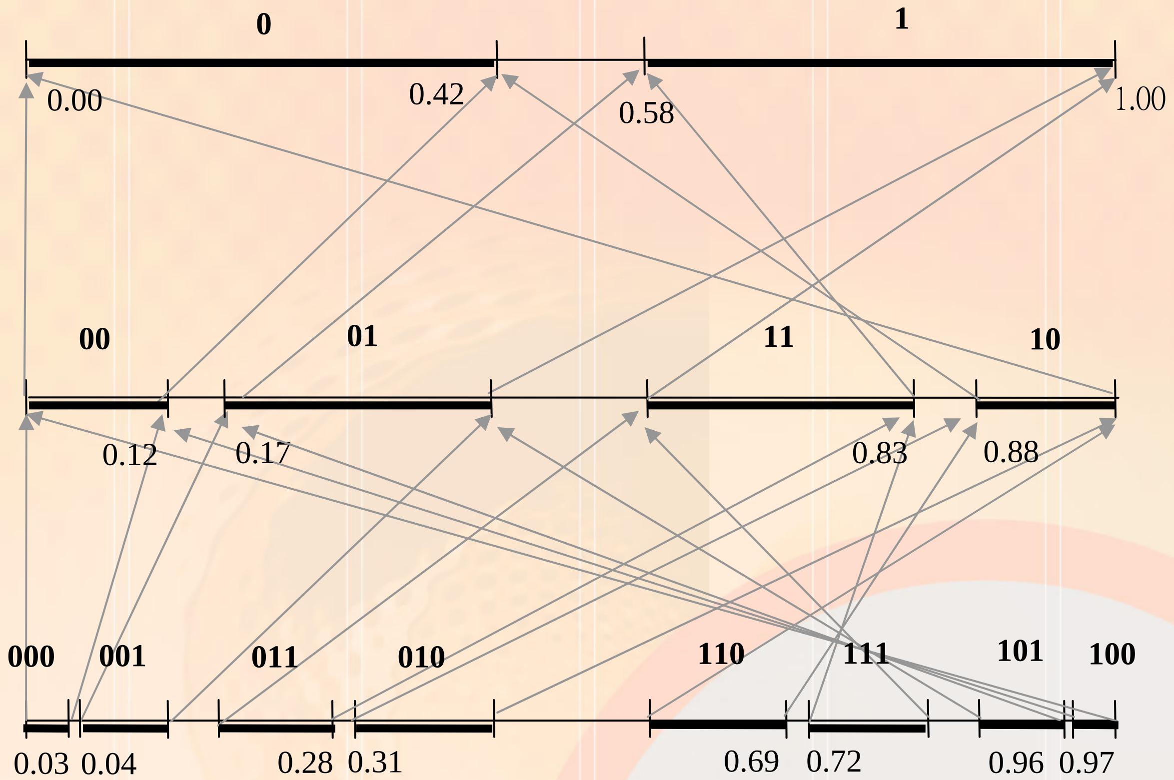


100,000 points

Topological Entropy



Mapping between Codeword and Interval



Gray Code

How to Encode?

- Represent each symbol in ASCII code. A symbol sequence is converted to a (longer) binary sequence, $b_1 b_2 b_3 \ldots$
- Choose an initial condition x_0 randomly.
- Iterate the logistic map for m times and determine the binary value a_i of the m points.
- If $a_m = b_1$ → matched. No action.
- Otherwise, apply a small perturbation Δx to x <u>now</u> so as to make $a_m = b_1$ <u>after m iterations</u>.

How to Encode?

- Output difference $\Delta R = (a_m - b_1) / 2^m$
- Pre-calculate the required perturbation Δx for different ΔR. Apply the smallest Δx as the perturbation. Then advance to the next bit.

Δx ↓

$x_1 \; x_2 \; x_3 \ldots \; x_{m-1} \; x_m$

$a_1 \; a_2 \; a_3 \ldots a_{m-1} \; a_m$

0 / 1

1

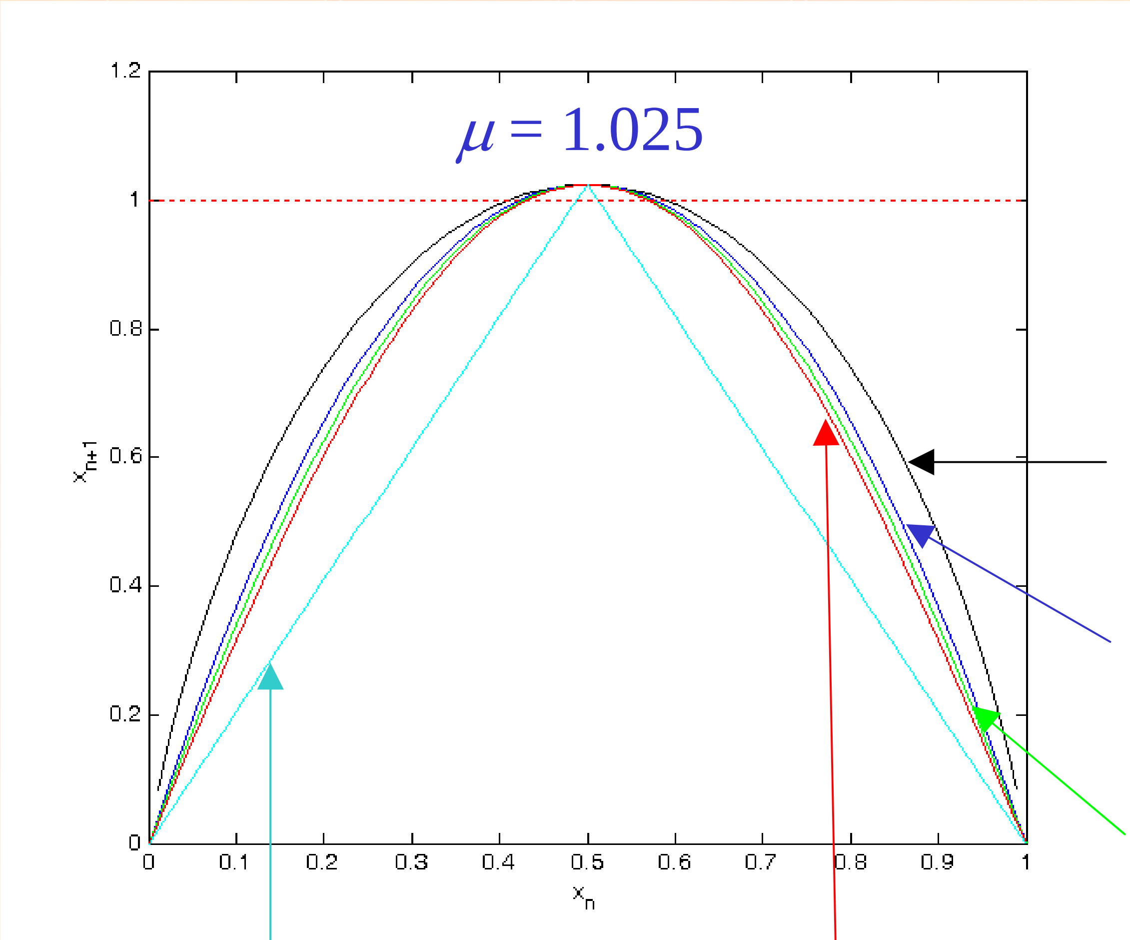
Message : $b_1 \; b_2 \; b_3 \ldots$

Not equal / Matched

$x \in [0, 1]$

$a_i \; b_i$: *binary*

Other Chaotic Maps



$$x_{n+1} = \mu \, f(x_n) \qquad \mu > 1$$

$$f : [0,1] \to [0,1]$$

$$f(0) = 0, \qquad f(1) = 0$$

$$f(0.5) = 1, \qquad f(x) = f(1-x)$$

Entropy map:

$$f_e(x) = -x \log_2 x - (1-x)\log_2(1-x)$$

Logistic map:

$$f_l(x) = 4x(1-x)$$

Bell map:

$$f_b(x) = \frac{e^{-(x-0.5)^2} - e^{-0.25}}{1 - e^{-0.25}}$$

Tent map:

$$f_t(x) = 1 - 2|x - 0.5|$$

Sine map:

$$f_s(x) = \sin(\pi x)$$

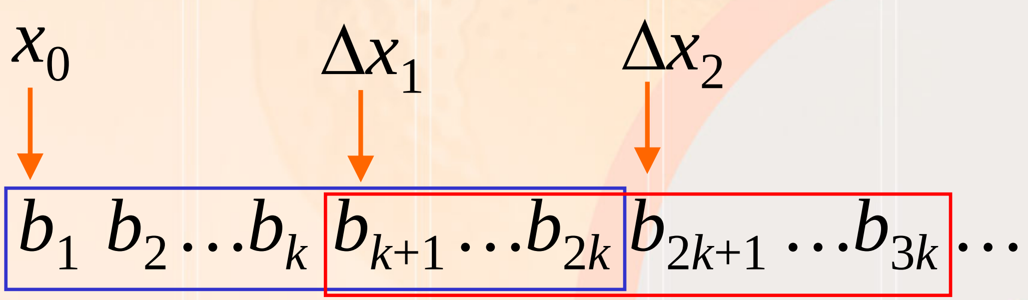
Problem:

- Irregular perturbation: some bits need perturbation, some bits do not need this.
- A better approach: apply perturbation <u>regularly</u>

Y. Hardy, and D. Sabatta, “Encoding, symbolic dynamics, cryptography and C++ implementation,” *Physics Letters A*, vol. 366, pp. 575-584, 2007.

Regular Perturbation

- $2k$ bits as a block.
- By reverse interval mapping, find the best initial condition x_0 to generate the <u>first</u> $2k$ bits correctly.
- Iterate k times. At the $(k+1)$ bit, find the best initial condition to generate the <u>next</u> $2k$ bits correctly.
- Calculate and apply the necessary perturbation.
- Shift the window k bits and continue.



Using Piecewise Linear Chaotic Map

- Not utilizing transient chaos
- Based on iterating a piecewise linear chaotic map
- Equivalent to arithmetic coding

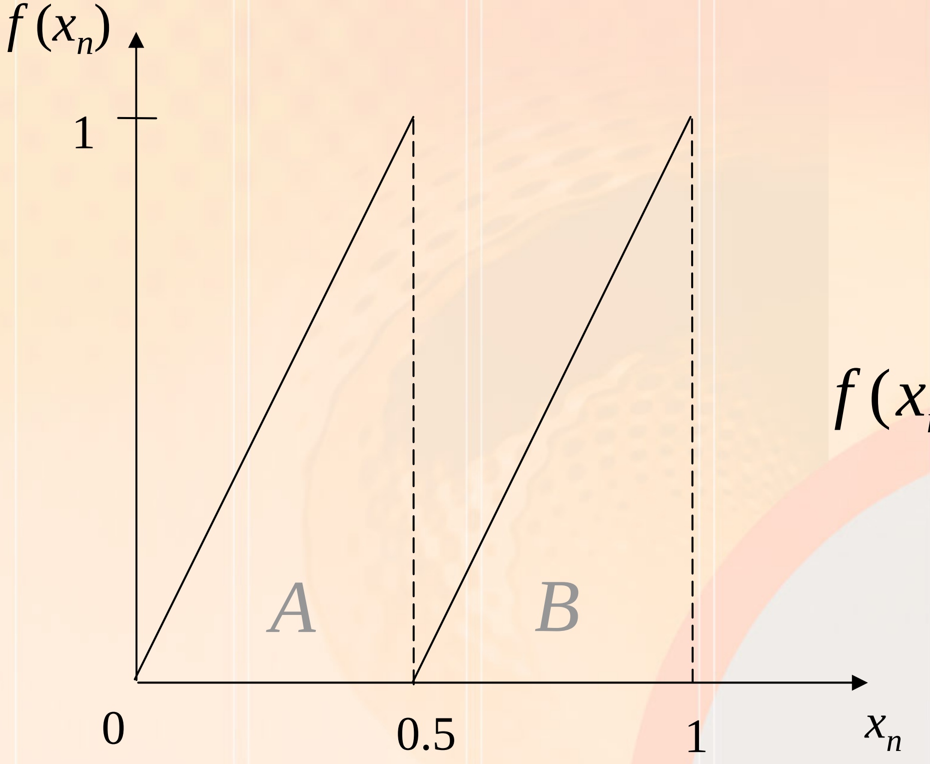
- M.B. Luca, A. Serbanescu, S. Azou, and G. Burel, “A new compression method using a chaotic symbolic approach,” *Proceedings of IEEE Communications Conference 2004*, Bucharest, Romania, June 3-5, 2004.
- N. Nagaraj, P.G. Vaidya, K.G. Bhat, “Arithmetic coding as a non-linear dynamical system,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, pp. 1013-1020, 2009.

Bernoulli Shift Map

2 Equiprobable Symbols *A* & *B*

$$P(A) = 0.5$$

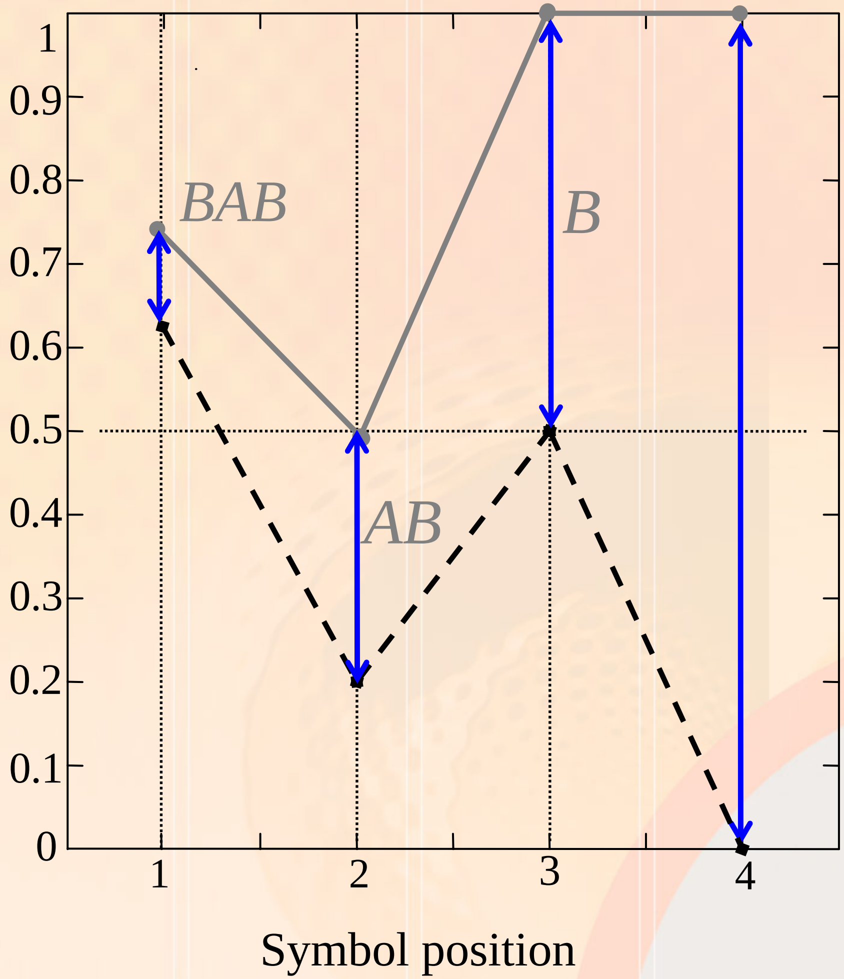
$$P(B) = 0.5$$

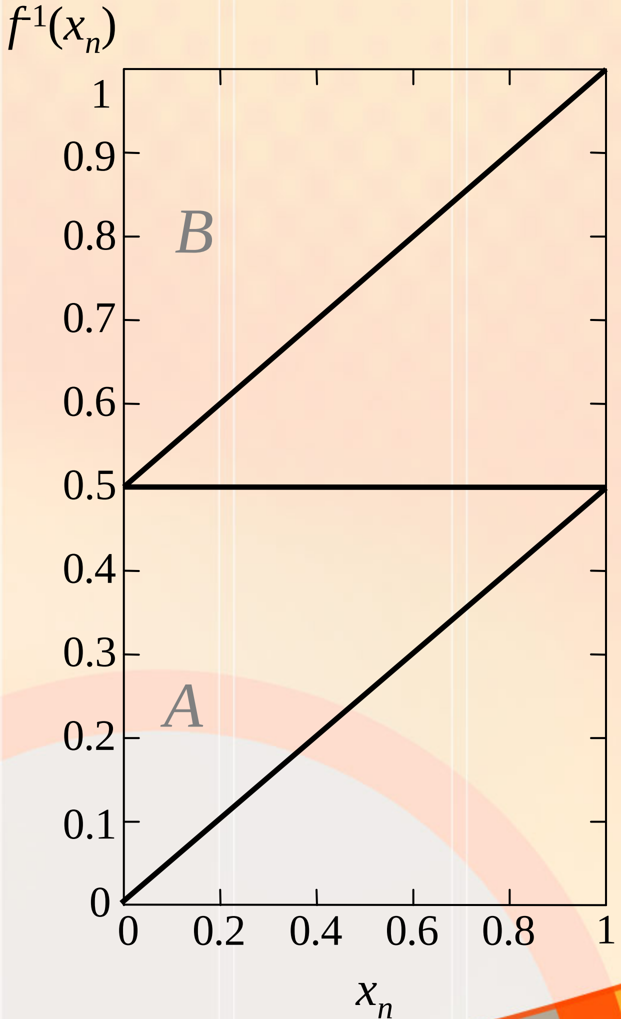


$$f(x_n) = \begin{cases} 2x_n & 0 \le x_n \le 0.5 \\ 2x_n - 1 & 0.5 < x_n \le 1 \end{cases}$$

Reverse Interval Mapping

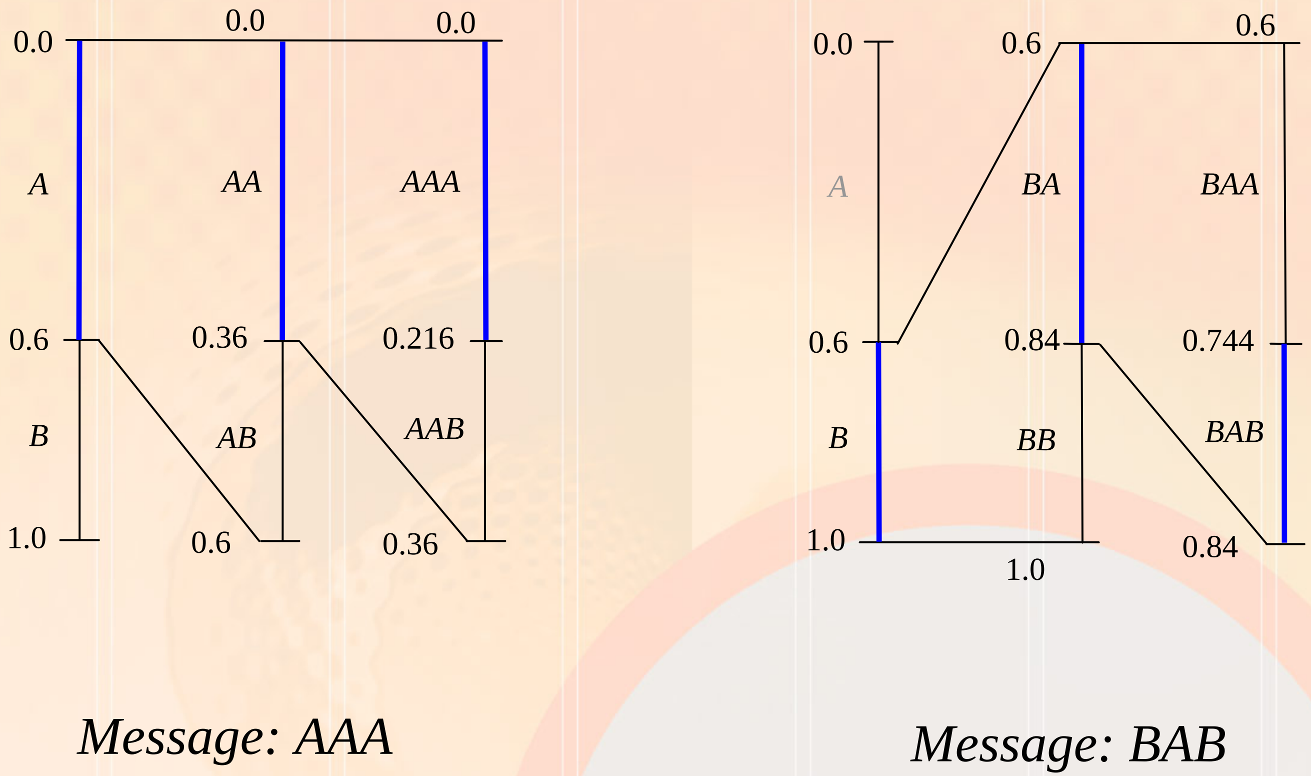
Message : *BAB*



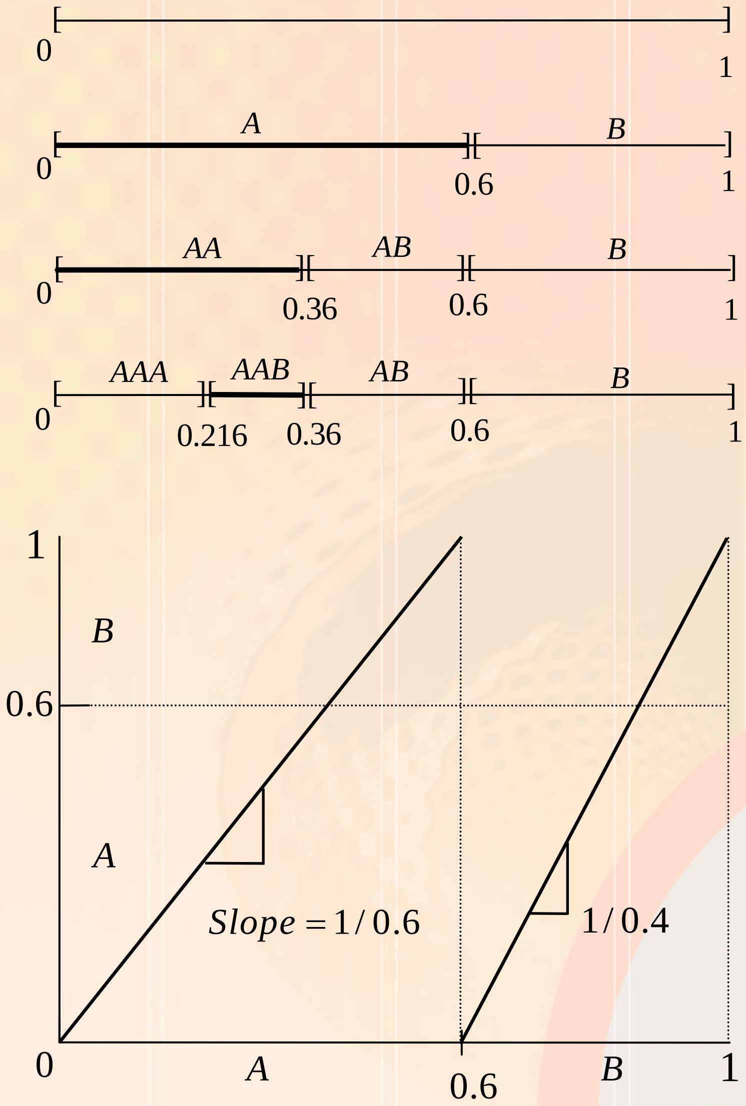


Arithmetic Coding

$P(A)=0.6 \qquad P(B)=0.4$



Arithmetic Coding and Chaotic Map



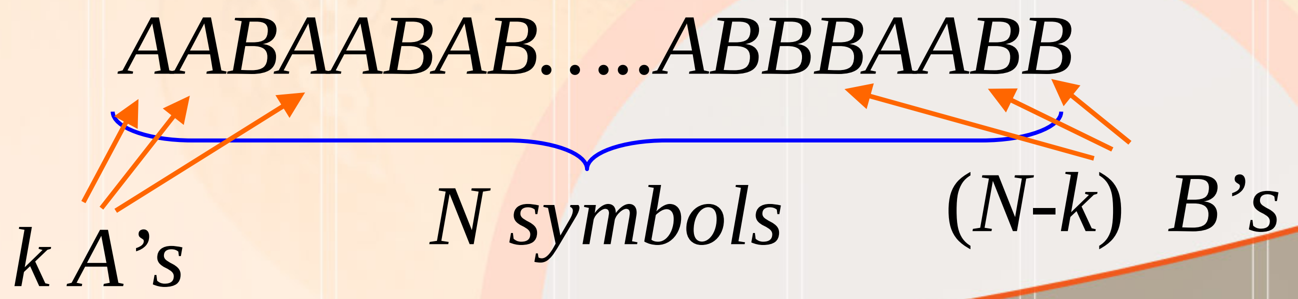
Arithmetic Coding

Equivalent

Iterating a piecewise linear chaotic map

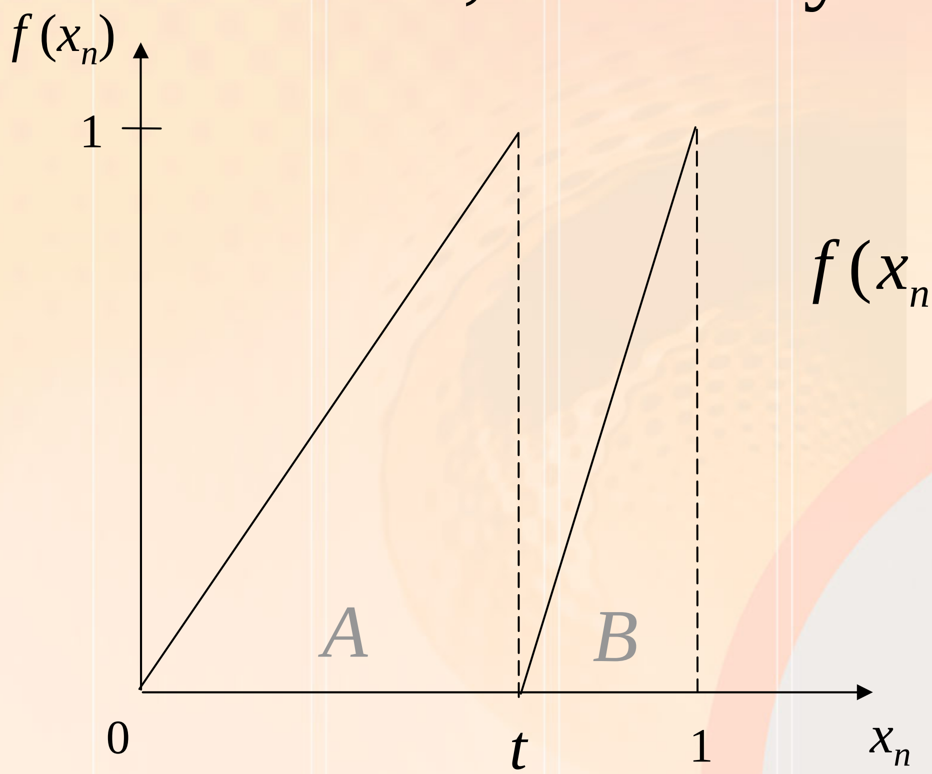
Proof of Optimality

- Binary *i.i.d* source, 2 symbols (*A* & *B*)
- $P(A)=p, \quad P(B)=1-p$
- Shannon entropy $H = -p \log p - (1-p) \log(1-p)$ bits/symbol
- An arbitrary binary message of finite length *N* from this source.
- *k* symbols are *A* while (*N*-*k*) symbols are *B*.



Proof of Optimality

- Reverse interval mapping: start from [0,1].
- If the symbol is *A*, shrink by a factor of *k*/*N*.
- Otherwise, shrink by the factor (1-*k*/*N*).



$$f(x_n) = \begin{cases} x_n / t & 0 \le x_n \le t \\ (x_n - t)/(1-t) & t < x_n \le 1 \end{cases}$$

$$t = k/N$$

Proof of Optimality

- After N iterations, the final interval $[x_{lower}, x_{upper}]$ has a length $(x_{upper} - x_{lower}) = \left(\frac{k}{N}\right)^k \left(1-\frac{k}{N}\right)^{N-k}$
- To represent the initial condition x_0 in this interval, it needs

$$\left\lceil -\log_2(x_{upper} - x_{lower}) \right\rceil \; bits$$

$$\left\lceil -\log_2(x_{upper} - x_{lower}) \right\rceil = \left\lceil -\log_2\left(\left(\frac{k}{N}\right)^k \left(1-\frac{k}{N}\right)^{N-k}\right) \right\rceil$$

$$= \left\lceil -k\log_2\frac{k}{N} - (N-k)\log_2\left(1-\frac{k}{N}\right) \right\rceil$$

$$\leq -k\log_2\frac{k}{N} - (N-k)\log_2\left(1-\frac{k}{N}\right) + 1$$

Proof of Optimality

Number of bits per symbol

$$\left(\frac{1}{N}\right)\left\lceil -\log_2(x_{upper} - x_{lower})\right\rceil \le -\frac{k}{N}\log_2\frac{k}{N} - \frac{N-k}{N}\log_2\left(1-\frac{k}{N}\right) + \frac{1}{N}$$

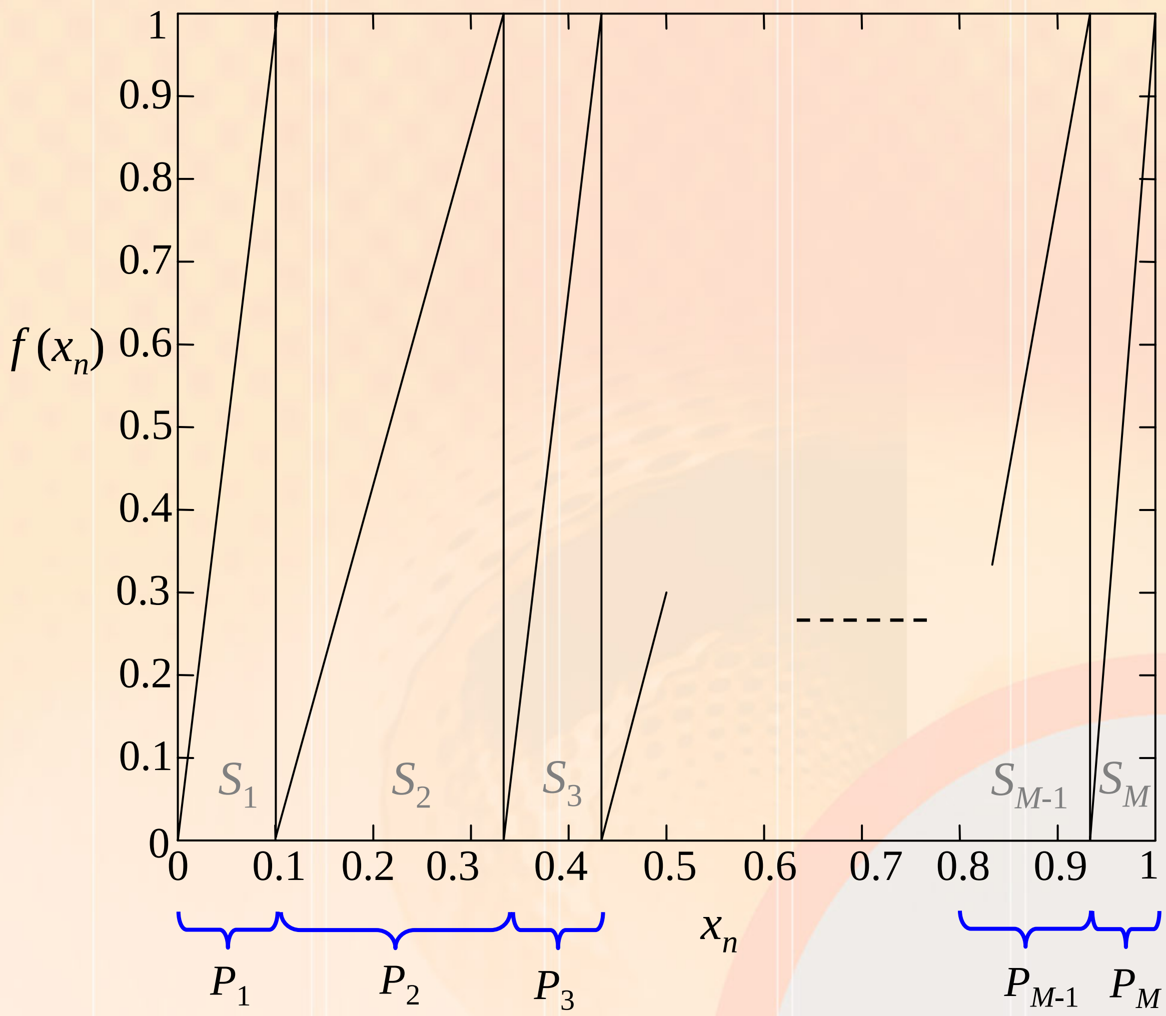
$$= -p\log_2 p - (1-p)\log_2(1-p) + \frac{1}{N}$$

$$= H + \frac{1}{N}$$

$$\to H \quad as \quad N \to \infty$$

⇒ approach Shannon's entropy bound

Piecewise Linear Map for M Symbols



M source symbols

S_1 S_2 … S_M

P_i : probability of occurrence of symbol S_i

Coding Example

- 4 source symbols *A*, *B*, *C*, *D*
- Need an "end" symbol "#" to indicate the end of the message sequence, so as to stop the chaotic map iteration.
- Message: "*AABACAADCBABD#*" (14 symbols)

Symbol	*Probability*	*Range*
A	6/14	0 – 0.4286
B	3/14	0.4286 – 0.6429
C	2/14	0.6429 – 0.7857
D	2/14	0.7857 – 0.9286
#	1/14	0.9286 - 1

Coding Example

- Entropy H = 2.074 bits /symbol
- Message Length N = 14
- Bits required = $H * N$ = 29.0383 bits.
- By reverse interval mapping, find boundaries:

$$x_{upper} = 0.089953692\underline{893821}$$

$$x_{lower} = 0.089953691\underline{079982}$$

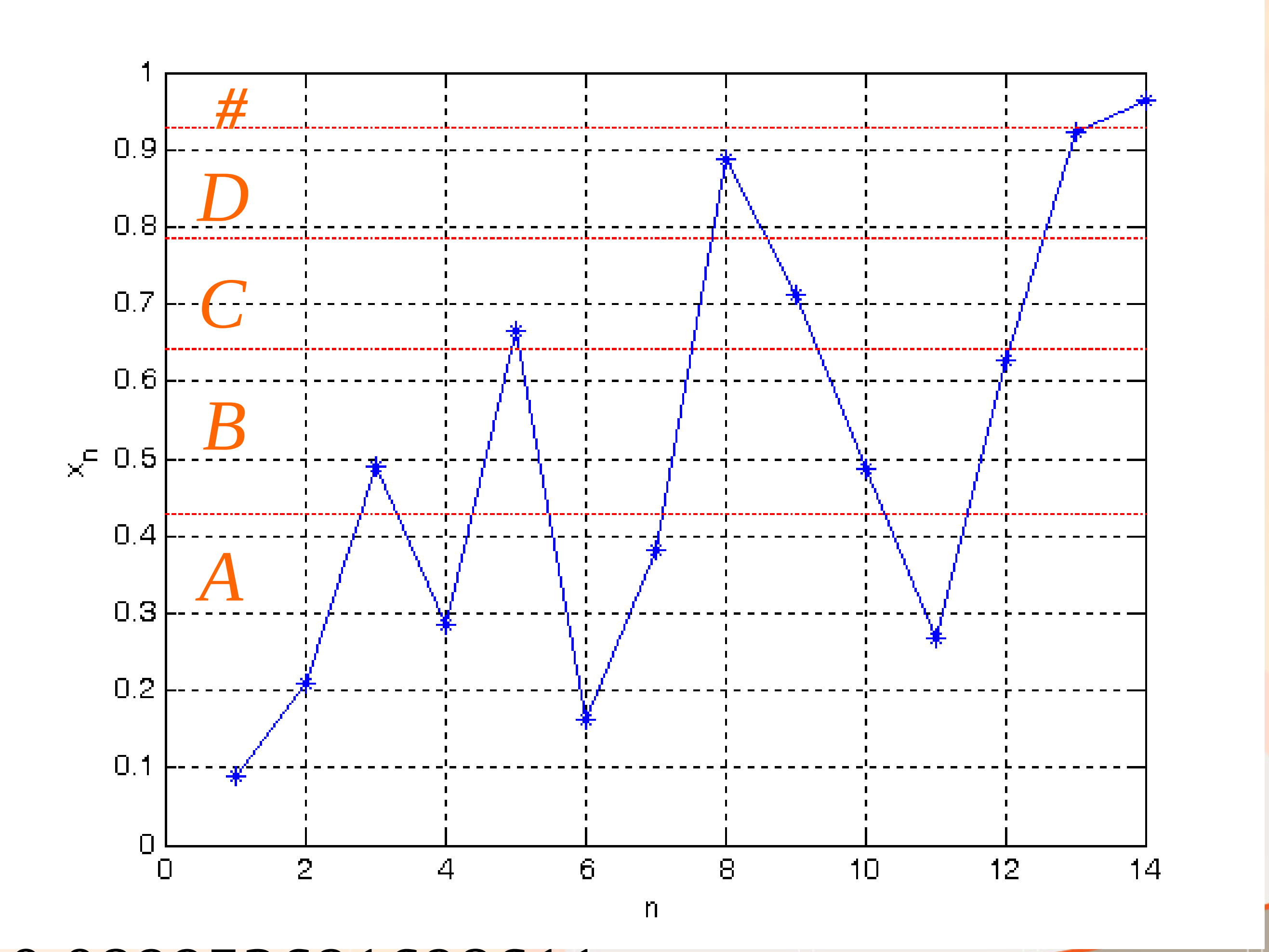
- $x_0 = (x_{upper} + x_{lower})/2 = 0.089953691\underline{986901}$
- 30-bit binary representation after decimal point

0 0 0 1 0 1 1 1 0 0 0 0 0 1 1 1
0 0 1 1 0 1 0 0 1 0 0 0 0 1

equivalent to $0.089953691\underline{698611}$

Decoded Sequence

Original Message: "*AABACAADCBABD#*"



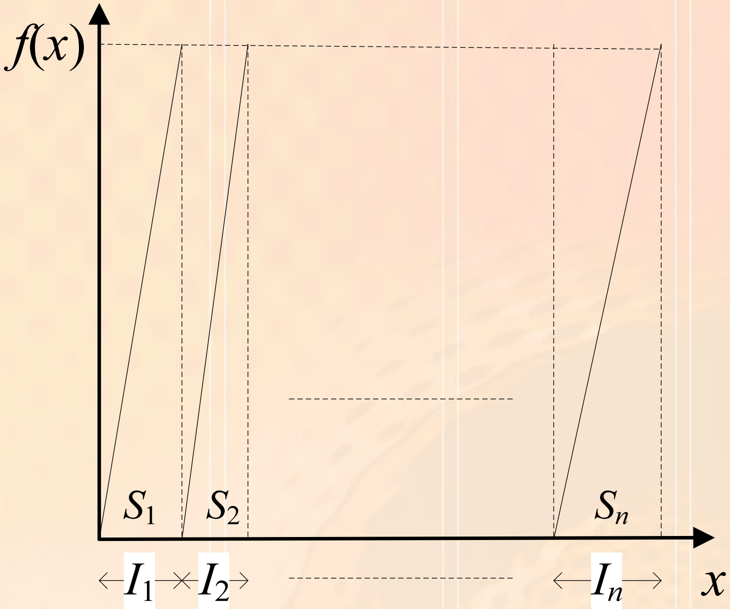
$x_0 = 0.089953691\underline{698611}$

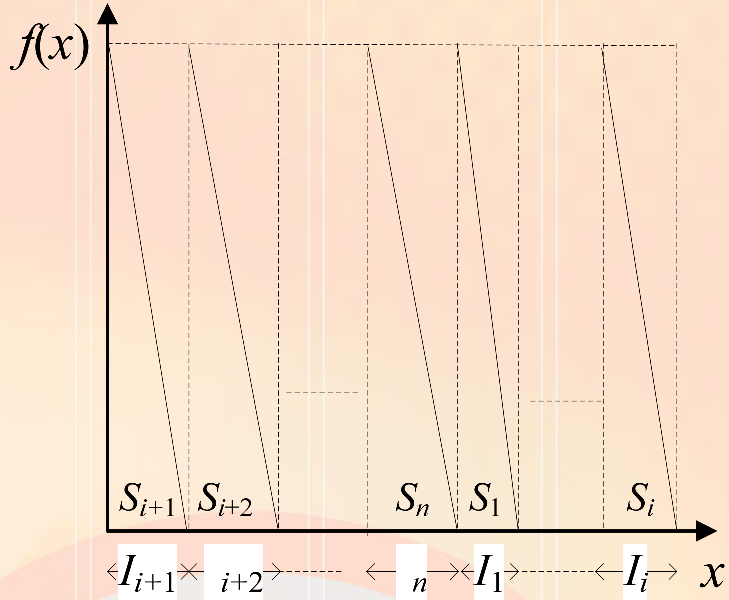
Content

- *Background*
- *Coding by Continuous-time Chaotic Systems*
- *Coding by Discrete-time Chaotic Maps*
- *Simultaneous Compression and Encryption using Chaotic Maps*
- *Conclusions*

Simultaneous Compression and Encryption

Use a secret key to control the form of the piecewise linear chaotic map used for arithmetic coding





Public Mode
(fixed)

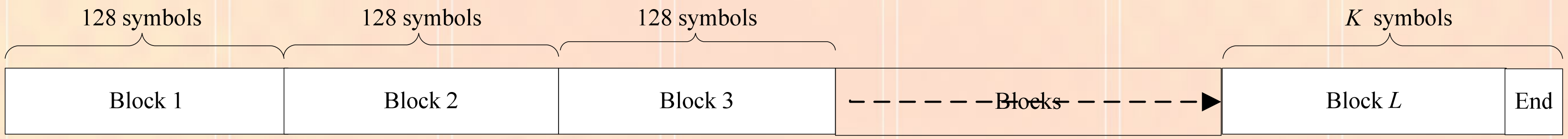
Secret Mode

Cyclic Shift Key = *i*

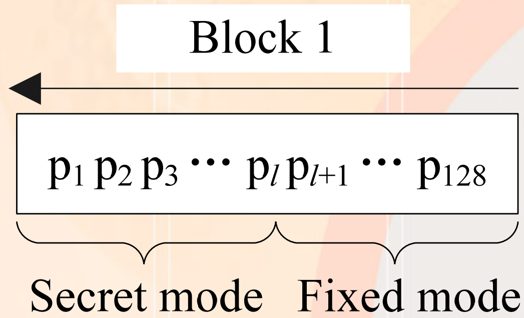
Slope Key =1

Simultaneous Compression and Encryption

1. Message sequence: divided into a number of blocks, each has 128 symbols.

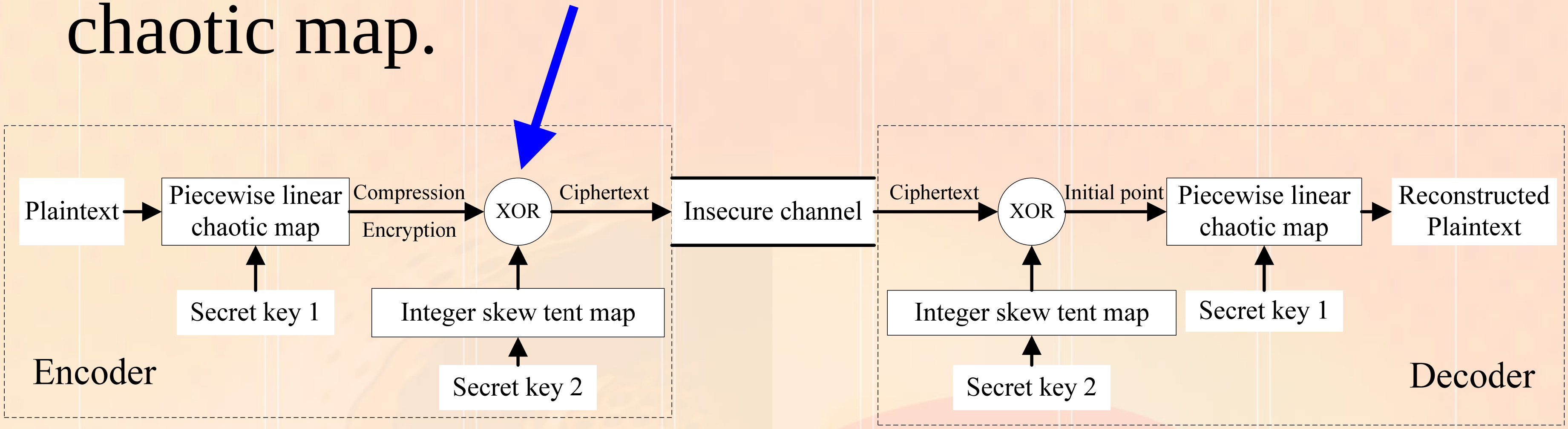


2. In each block, the first group of symbols are encoded by the secret mode of the piecewise linear chaotic map while the remaining symbols are encoded by the fixed public mode.



Simultaneous Compression and Encryption

3. Further protection: mask the arithmetic code with a pseudo-random sequence generated by another chaotic map.



Simultaneous Compression and Encryption

Tested using 18 standard files from the Calgary Corpus

- Compression ratio: slightly worse than the best ratio (Shannon's entropy) by 0.16% to 4.69%.
- Compression speed: 1.2 MB/s - 3.4 MB/s
- Decompression speed: 0.72 MB/s - 2.3 MB/s.

File	Size (Byte)	Best Compression Ratio (Entropy)	Our Compression Ratio	Compress Time (s)	Decompress Time (s)
obj2	246,814	78.25%	79.66%	0.1592	0.2621
news	377,109	64.87%	65.99%	0.2215	0.3526
pic	513,216	15.13%	16.18%	0.1435	0.2153
book2	610,856	59.91%	61.10%	0.3353	0.5367
book1	768,771	56.59%	57.63%	0.4149	0.6442

Simultaneous Compression and Encryption

- Key length: 512 bits
- Key sensitivity: 46.13% - 49.96%,
- Plaintext sensitivity: 49.27% - 50.11%,
- Both are very close to the ideal value (50%).

Content

- *Background*
- *Coding by Continuous-time Chaotic Systems*
- *Coding by Discrete-time Chaotic Maps*
- *Simultaneous Compression and Encryption using Chaotic Maps*
- *Conclusions*

Conclusions

- A message sequence can be encoded by the symbolic representation of the output of a continuous-time chaotic system or a discrete-time chaotic map.
- Iterating a piecewise linear chaotic map from an appropriate initial value is equivalent to arithmetic coding.
- By using a secret key to control the form of the piecewise linear chaotic map, simultaneous arithmetic coding and encryption is achieved.

Thank You!

Q & A