

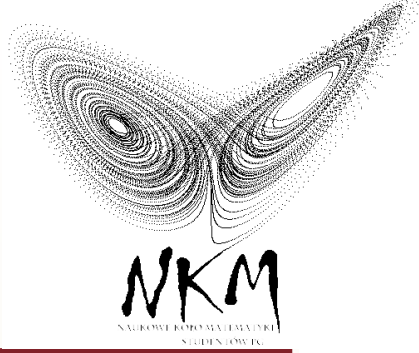
Chaotyczne generatory liczb pseudolosowych

Michał Krzemiński

michalkrzeminski@wp.pl

Politechnika Gdańska

Wydział Fizyki Technicznej i Matematyki Stosowanej



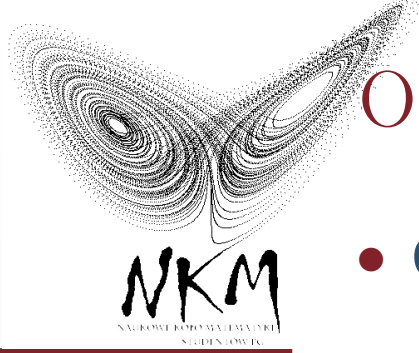
Wstęp

- ❖ Outline
- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne'
PRBGs

Bibliografia

Wstęp



Outline

- Ciągi liczb losowych i pseudolosowych

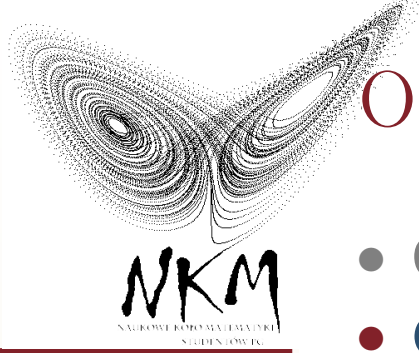
Wstęp

❖ Outline

- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne'
PRBGs

Bibliografia



Outline

- Ciągi liczb losowych i pseudolosowych
- Generatory ciągów liczb losowych

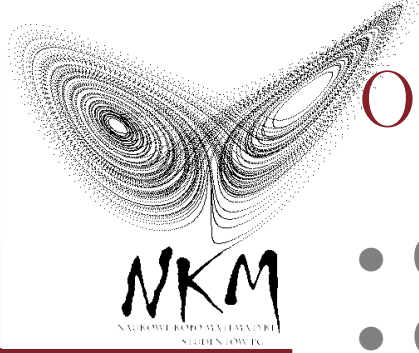
Wstęp

❖ Outline

- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne'
PRBGs

Bibliografia



Outline

- Ciągi liczb losowych i pseudolosowych
- Generatory ciągów liczb losowych
- Test następnego bitu, czyli ocena jakości generatora

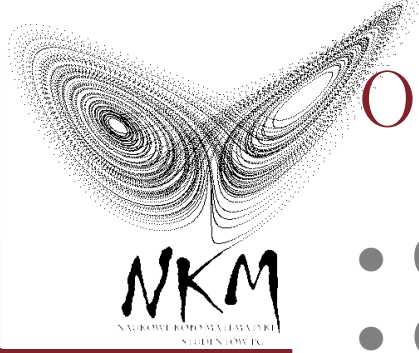
Wstęp

❖ Outline

- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne'
PRBGs

Bibliografia



Outline

- Ciągi liczb losowych i pseudolosowych
- Generatory ciągów liczb losowych
- Test następnego bitu, czyli ocena jakości generatora
- PRBGs

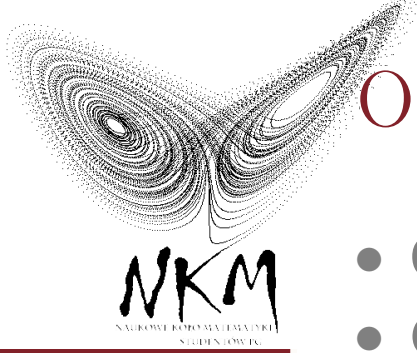
Wstęp

❖ Outline

- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne'
PRBGs

Bibliografia



Outline

- Ciągi liczb losowych i pseudolosowych
- Generatory ciągów liczb losowych
- Test następnego bitu, czyli ocena jakości generatora
- PRBGs
- Rozwiązywalne i konstruowalne układy dynamiczne

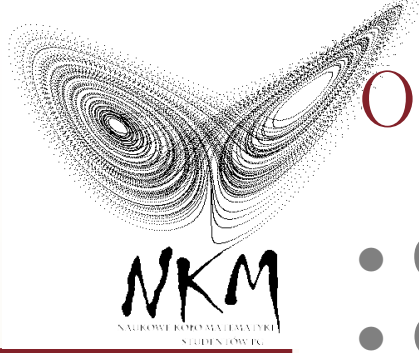
Wstęp

❖ Outline

- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne'
PRBGs

Bibliografia



Outline

- Ciągi liczb losowych i pseudolosowych
- Generatory ciągów liczb losowych
- Test następnego bitu, czyli ocena jakości generatora
- PRBGs
- Rozwiązywalne i konstruowalne układy dynamiczne
- Bibliografia

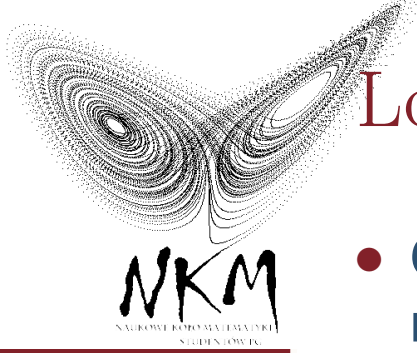
Wstęp

❖ Outline

- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne'
PRBGs

Bibliografia



Losowe i pseudolosowe ciągi liczbowe

- **Ciągiem losowym** (albo losowym ciągiem znaków) nazwiemy taki ciąg, którego nie możemy zapisać w postaci pewnej formuły czy algorytmu, krótszego od samego ciągu.

Wstęp

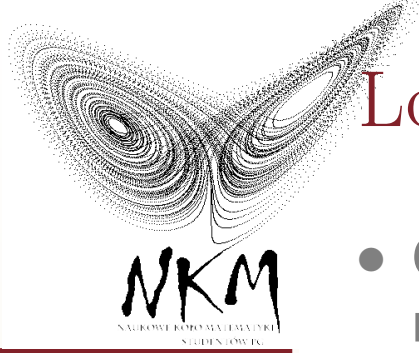
❖ Outline

❖ Losowe i pseudolosowe ciągi liczbowe

❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia



Losowe i pseudolosowe ciągi liczbowe

- **Ciągiem losowym** (albo losowym ciągiem znaków) nazwiemy taki ciąg, którego nie możemy zapisać w postaci pewnej formuły czy algorytmu, krótszego od samego ciągu.
- **Ciągiem pseudolosowych** nazwiemy takie ciągi, które powstały według pewnej formuły, stosunkowo krótkiej, jednak nasza niewiedza czy niemoc obliczeniowa nie pozwala nam na jej identyfikację.

Wstęp

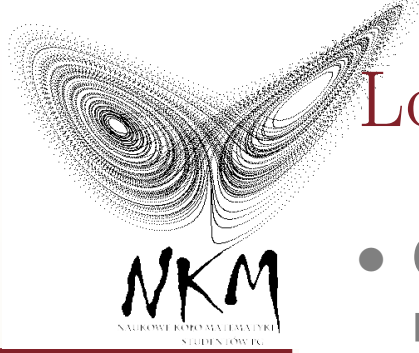
❖ Outline

❖ Losowe i pseudolosowe ciągi liczbowe

❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia



Losowe i pseudolosowe ciągi liczbowe

- **Ciągiem losowym** (albo losowym ciągiem znaków) nazwiemy taki ciąg, którego nie możemy zapisać w postaci pewnej formuły czy algorytmu, krótszego od samego ciągu.
- **Ciągiem pseudolosowych** nazwiemy takie ciągi, które powstały według pewnej formuły, stosunkowo krótkiej, jednak nasza niewiedza czy niemoc obliczeniowa nie pozwala nam na jej identyfikację.

Wstęp

❖ Outline

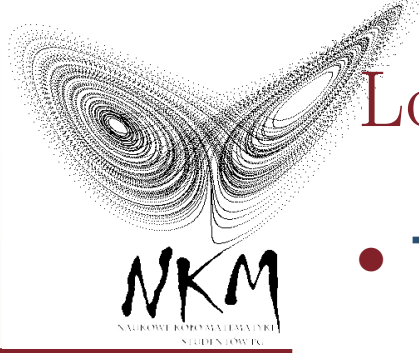
❖ Losowe i pseudolosowe ciągi liczbowe

❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia

- Dla ustalenia uwagi będziemy mówić o ciągach liczbowych, a później ciągach bitów tzn. '0' i '1'.



Losowe i pseudolosowe ciągi liczbowe

- **Tablice liczb losowych.**

Wstęp

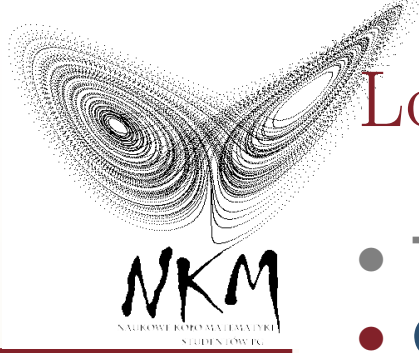
❖ Outline

❖ Losowe i pseudolosowe ciągi liczbowe

❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia



Losowe i pseudolosowe ciągi liczbowe

- Tablice liczb losowych.
- **Generatory ciągów liczb losowych:**
 - ◆ generatory fizyczne (liczb losowych): mechaniczne i oparte na procesach fizycznych
 - ◆ generatory matematyczne (liczb pseudolosowych)

Wstęp

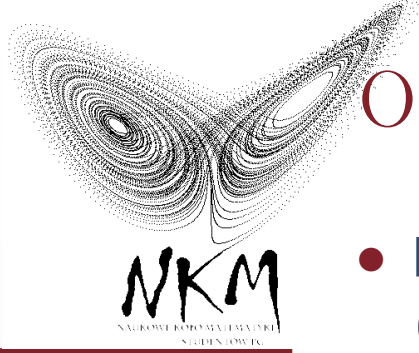
❖ Outline

❖ Losowe i pseudolosowe ciągi liczbowe

❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia



Ocena jakości generatora - test następnego bitu

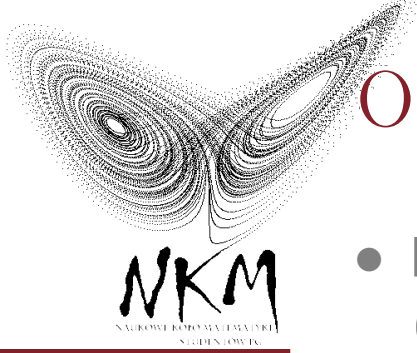
- Dany jest generator, wytwarzający ciąg n bitów (b_1, b_2, \dots, b_n) ,

Wstęp

- ❖ Outline
- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia



Ocena jakości generatora - test następnego bitu

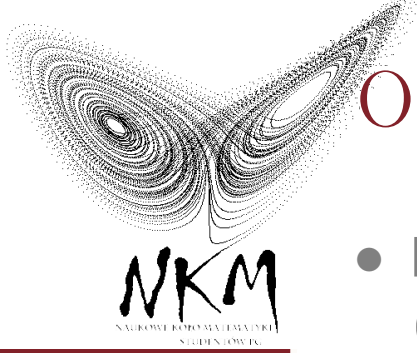
- Dany jest generator, wytwarzający ciąg n bitów (b_1, b_2, \dots, b_n) ,
- dana jest statystyka $\bar{B}(\cdot)$, która na podstawie znajomości m pierwszych bitów, pozwala przewidzieć bit b_{m+1} .

Wstęp

- ❖ Outline
- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia



Ocena jakości generatora - test następnego bitu

- Dany jest generator, wytwarzający ciąg n bitów (b_1, b_2, \dots, b_n) ,
- dana jest statystyka $\bar{B}(\cdot)$, która na podstawie znajomości m pierwszych bitów, pozwala przewidzieć bit b_{m+1} .
- Powiemy, że generator bitów spełnia test następnego bitu, gdy dla dostatecznie dużych n oraz dla wszystkich wielomianów $w(n)$ i dla wszystkich liczb całkowitych $m \in [1, n]$ zachodzi nierówność:

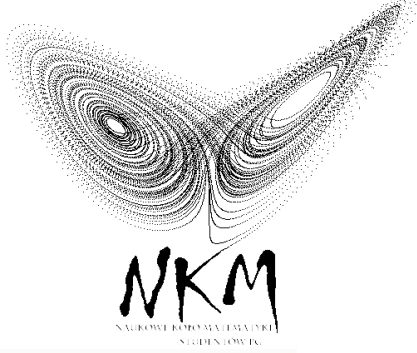
$$\left| P(\bar{B}(b_1, b_2, \dots, b_m) = b_{m+1}) - \frac{1}{2} \right| < \frac{1}{w(n)}.$$

Wstęp

- ❖ Outline
- ❖ Losowe i pseudolosowe ciągi liczbowe
- ❖ Ocena jakości generatora - test następnego bitu

'Chaotyczne' PRBGs

Bibliografia



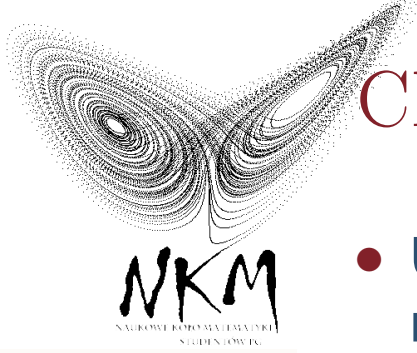
Wstęp

'Chaotyczne' PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia

'Chaotyczne' PRBGs



Chaotyczny układ dynamiczny

- **Układem dynamicznym** (dyskretnym albo i nie) będziemy nazywać parę **(F,S)**, gdzie S będzie oznaczać przestrzeń stanów, a $F: S \rightarrow S$, będzie odwzorowaniem mierzalnym będącym generatorem półgrupy iteracji.

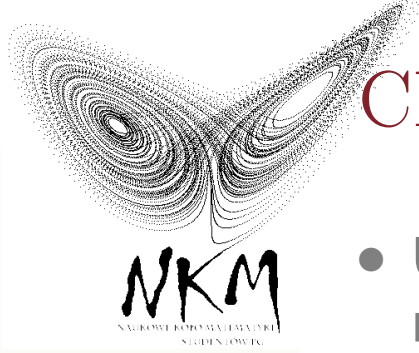
Wstęp

'Chaotyczne'
PRBGs

❖ Chaotyczny układ
dynamiczny

- ❖ Kilka twierdzeń
bez dowodów :P
- ❖ Rozwiązywalne
układy
dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- **Układem dynamicznym** (dyskretnym albo i nie) będziemy nazywać parę (F, S) , gdzie S będzie oznaczać przestrzeń stanów, a $F: S \rightarrow S$, będzie odwzorowaniem mierzalnym będącym generatorem półgrupy iteracji.
- **Trajektorią** startującą ze stanu początkowego s_0 nazwiemy ciąg $\{s_n\}_{n=0}^{\infty} \subset S$ uzyskany poprzez kolejne iteracje:

$$s_{n+1} = F(s_n), \text{ gdzie } n = 0, 1, \dots$$

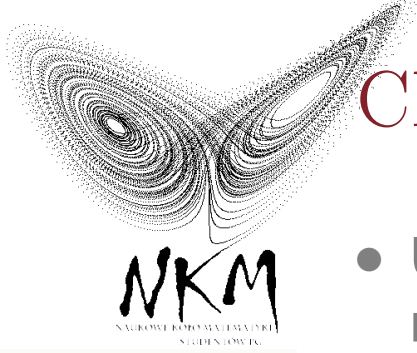
Wstęp

'Chaotyczne'
PRBGs

❖ Chaotyczny układ
dynamiczny

- ❖ Kilka twierdzeń
bez dowodów :P
- ❖ Rozwiązywalne
układy
dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- **Układem dynamicznym** (dyskretnym albo i nie) będziemy nazywać parę **(F,S)**, gdzie S będzie oznaczać przestrzeń stanów, a $F: S \rightarrow S$, będzie odwzorowaniem mierzalnym będącym generatorem półgrupy iteracji.
- **Trajektorią** startującą ze stanu początkowego s_0 nazwiemy ciąg $\{s_n\}_{n=0}^{\infty} \subset S$ uzyskany poprzez kolejne iteracje:

$$s_{n+1} = F(s_n), \text{ gdzie } n = 0, 1, \dots$$

- **Chaos**

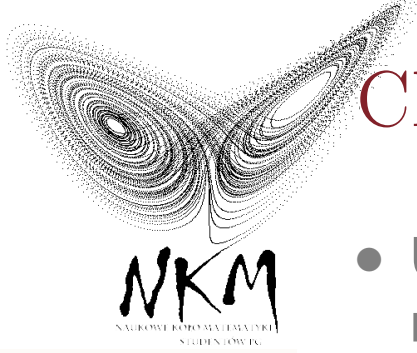
Wstęp

'Chaotyczne'
PRBGs

❖ Chaotyczny układ
dynamiczny

- ❖ Kilka twierdzeń
bez dowodów :P
- ❖ Rozwiązywalne
układy
dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- **Układem dynamicznym** (dyskretnym albo i nie) będziemy nazywać parę (F, S) , gdzie S będzie oznaczać przestrzeń stanów, a $F: S \rightarrow S$, będzie odwzorowaniem mierzalnym będącym generatorem półgrupy iteracji.
- **Trajektorią** startującą ze stanu początkowego s_0 nazwiemy ciąg $\{s_n\}_{n=0}^{\infty} \subset S$ uzyskany poprzez kolejne iteracje:

$$s_{n+1} = F(s_n), \text{ gdzie } n = 0, 1, \dots$$

- **Chaos**
- **Def. Wykładnikiem Lapunowa** nazywamy liczbę:

$$\lambda_{s,v} = \lim_{n \rightarrow \infty} \frac{1}{n} \|DF^n(s)(v)\|,$$

gdzie $\|\cdot\|$ jest normą w przestrzeni stycznej w punkcie $s \in S$, $DF^n(s)(v)$ jest pochodną Frecheta n -tej iteracji F w punkcie s w kierunku v .

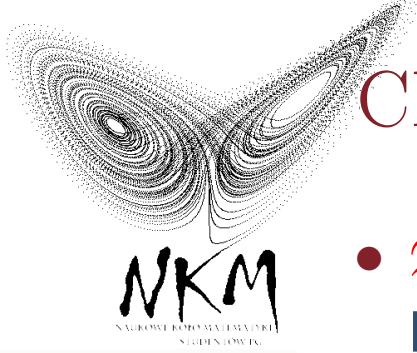
Wstęp

'Chaotyczne'
PRBGs

❖ Chaotyczny układ
dynamiczny

- ❖ Kilka twierdzeń
bez dowodów :P
- ❖ Rozwiązywalne
układy
dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- **Def.** Powiemy, że układ dynamiczny jest **chaotyczny** w pewnym obszarze, gdy dla μ prawie wszystkich punktów tego obszaru ma on co najmniej jeden dodatni wykładnik Lapunowa.

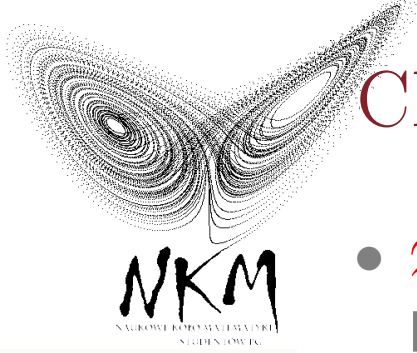
Wstęp

'Chaotyczne'
PRBGs

❖ Chaotyczny układ
dynamiczny

- ❖ Kilka twierdzeń
bez dowodów :P
- ❖ Rozwiązywalne
układy
dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- **Def.** Powiemy, że układ dynamiczny jest **chaotyczny** w pewnym obszarze, gdy dla μ prawie wszystkich punktów tego obszaru ma on co najmniej jeden dodatni wykładnik Lapunowa.
- miara niezmiennicza μ skończona na $\sigma(S)$,

$$\forall A \in \sigma(S) \mu(A) = \mu(F^{-1}(A)),$$

dla której istnieje dodatnia ograniczona mierzalna funkcja $f: S \rightarrow \mathbb{R}$ taka, że

$$\forall A \in \sigma(S) \mu(A) = \int_A f(s) ds.$$

Wstęp

'Chaotyczne'
PRBGs

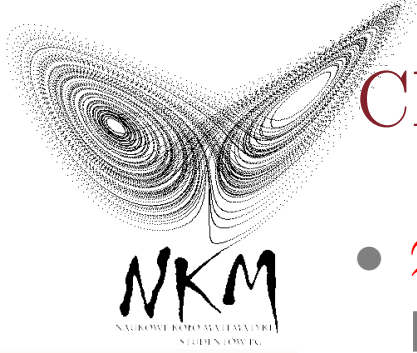
❖ Chaotyczny układ
dynamiczny

❖ Kilka twierdzeń
bez dowodów :P

❖ Rozwiązywalne
układy
dynamiczne

❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- **Def.** Powiemy, że układ dynamiczny jest **chaotyczny** w pewnym obszarze, gdy dla μ prawie wszystkich punktów tego obszaru ma on co najmniej jeden dodatni wykładnik Lapunowa.

- miara niezmiennicza μ skończona na $\sigma(S)$,

$$\forall A \in \sigma(S) \mu(A) = \mu(F^{-1}(A)),$$

dla której istnieje dodatnia ograniczona mierzalna funkcja $f: S \rightarrow \mathbb{R}$ taka, że

$$\forall A \in \sigma(S) \mu(A) = \int_A f(s) ds.$$

- **Def.** Powiemy, że układ dynamiczny jest **mieszający**, gdy

$$\forall A, B \in \sigma(S) \lim_{n \rightarrow \infty} \mu(F^{-n}(A) \cap B) = \mu(A)\mu(B).$$

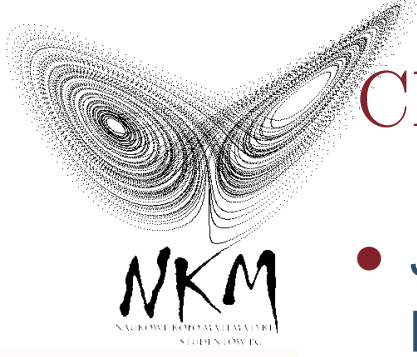
Wstęp

'Chaotyczne'
PRBGs

❖ Chaotyczny układ
dynamiczny

- ❖ Kilka twierdzeń
bez dowodów :P
- ❖ Rozwiązywalne
układy
dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- Jeżeli dodatkowo założymy, że nasza miara stacjonarna jest **probabilistyczna**, wtedy otrzymamy:

$$\lim_{n \rightarrow \infty} \frac{\mu(F^{-n}(A) \cap B)}{\mu(B)} = \frac{\mu(A)}{\mu(S)}$$

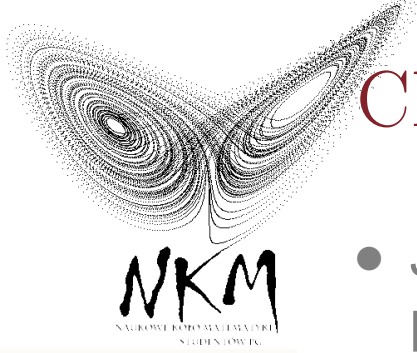
Wstęp

'Chaotyczne'
PRBGs

❖ Chaotyczny układ
dynamiczny

- ❖ Kilka twierdzeń
bez dowodów :P
- ❖ Rozwiązywalne
układy
dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- Jeżeli dodatkowo założymy, że nasza miara stacjonarna jest **probabilistyczna**, wtedy otrzymamy:

$$\lim_{n \rightarrow \infty} \frac{\mu(F^{-n}(A) \cap B)}{\mu(B)} = \frac{\mu(A)}{\mu(S)}$$

- Niech $S = S_0 \cup S_1$, gdzie $S_0 \cap S_1 = \emptyset$, $\mu(S_0) = \mu(S_1) = \frac{1}{2}$. Niech \hat{S} będzie zbiorem dopuszczalnych warunków początkowych, niech $\hat{s}_0 \in \hat{S}$.

$$s_n = \begin{cases} 0 & , \text{gdy } F^n(\hat{s}_0) \in S_0 \\ 1 & , \text{gdy } F^n(\hat{s}_0) \in S_1 \end{cases} , \text{ dla } n = 0, 1, 2, \dots$$

Wstęp

'Chaotyczne'
PRBGs

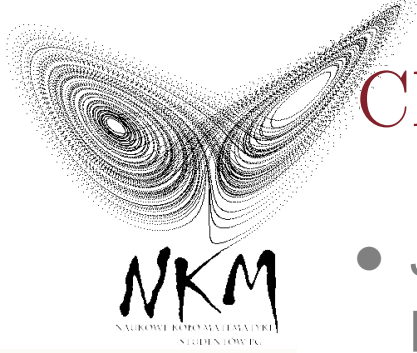
❖ Chaotyczny układ
dynamiczny

❖ Kilka twierdzeń
bez dowodów :P

❖ Rozwiązywalne
układy
dynamiczne

❖ KoAsDeLoUkDy

Bibliografia



Chaotyczny układ dynamiczny

- Jeżeli dodatkowo założymy, że nasza miara stacjonarna jest **probabilistyczna**, wtedy otrzymamy:

$$\lim_{n \rightarrow \infty} \frac{\mu(F^{-n}(A) \cap B)}{\mu(B)} = \frac{\mu(A)}{\mu(S)}$$

- Niech $S = S_0 \cup S_1$, gdzie $S_0 \cap S_1 = \emptyset$, $\mu(S_0) = \mu(S_1) = \frac{1}{2}$. Niech \hat{S} będzie zbiorem dopuszczalnych warunków początkowych, niech $\hat{s}_0 \in \hat{S}$.

$$s_n = \begin{cases} 0 & , \text{gdy } F^n(\hat{s}_0) \in S_0 \\ 1 & , \text{gdy } F^n(\hat{s}_0) \in S_1 \end{cases} , \text{ dla } n = 0, 1, 2, \dots$$

- Stąd otrzymamy nieskończony ciąg bitów $O(\hat{s}) = \{\hat{s}_0, \hat{s}_1, \hat{s}_2, \dots\} = \{\hat{s}_i\}_{i=0}^{\infty}$.

Wstęp

'Chaotyczne'
PRBGs

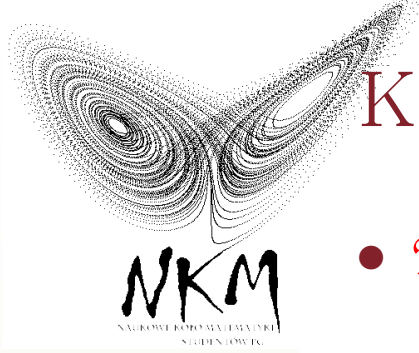
❖ Chaotyczny układ
dynamiczny

❖ Kilka twierdzeń
bez dowodów :P

❖ Rozwiązywalne
układy
dynamiczne

❖ KoAsDeLoUkDy

Bibliografia



Kilka twierdzeń bez dowodów :P

- Σ .

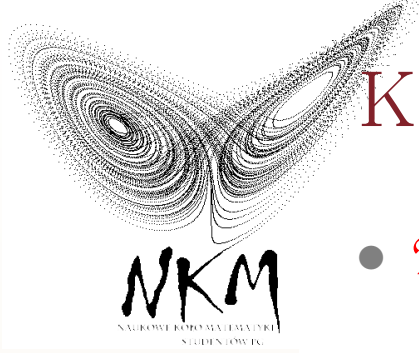
$$\forall s \in S \mu(O^{-1}(\{\hat{s}_i\}_{i=0}^{\infty})) = 0$$

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Kilka twierdzeń bez dowodów :P

• Tw.

$$\forall s \in S \mu(O^{-1}(\{\hat{s}_i\}_{i=0}^{\infty})) = 0$$

• Tw.

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \mathbf{1}_{S_0}(F^n(s)) = \int_S \mathbf{1}_{S_0} d\mu = \mu(S_0).$$

Wstęp

'Chaotyczne'
PRBGs

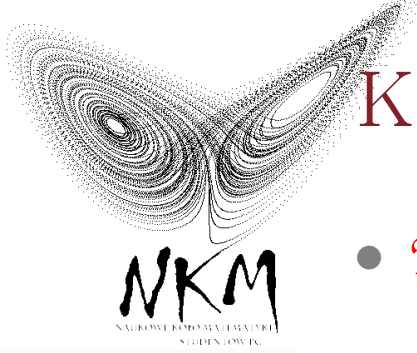
❖ Chaotyczny układ
dynamiczny

❖ Kilka twierdzeń
bez dowodów :P

❖ Rozwiązywalne
układy
dynamiczne

❖ KoAsDeLoUkDy

Bibliografia



Kilka twierdzeń bez dowodów :P

- **Tw.**

$$\forall s \in S \mu(O^{-1}(\{\hat{s}_i\}_{i=0}^{\infty})) = 0$$

- **Tw.**

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \mathbf{1}_{S_0}(F^n(s)) = \int_S \mathbf{1}_{S_0} d\mu = \mu(S_0).$$

- **Tw.** Jeżeli układ dynamiczny, jest mieszający, to istnieje takie $k \in \mathbb{N}$, że dla każdego $\hat{s} \in \hat{S}$ bity \hat{s}_i oraz \hat{s}_{i+k} są dla $k \rightarrow \infty$ niezależne dla $i = 1, 2, \dots$

Wstęp

'Chaotyczne'
PRBGs

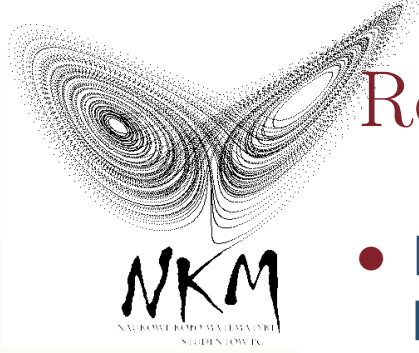
❖ Chaotyczny układ
dynamiczny

❖ Kilka twierdzeń
bez dowodów :P

❖ Rozwiązywalne
układy
dynamiczne

❖ KoAsDeLoUkDy

Bibliografia



Rozwiązywalne układy dynamiczne

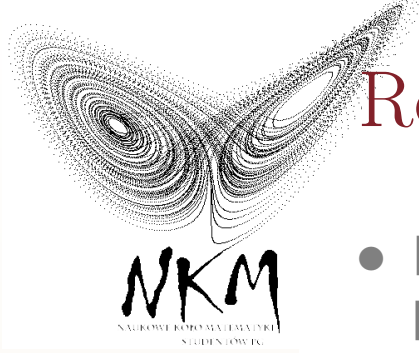
- Rozwiązywalnymi układami dynamicznymi nazywamy takie, których rozwiązanie może być przedstawione w postaci jawnej.

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Rozwiązywalne układy dynamiczne

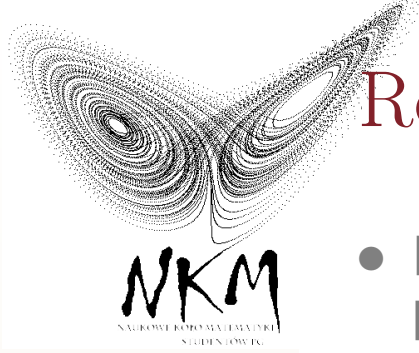
- Rozwiązywalnymi układami dynamicznymi nazywamy takie, których rozwiązanie może być przedstawione w postaci jawnej.
- Rozważmy równanie $x_n = p(\theta T z^n)$, gdzie $p(\cdot)$ jest funkcją okresową, T jest jej okresem, $z \in \mathbb{N}$, a θ definiuje warunek początkowy.

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Rozwiązywalne układy dynamiczne

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia

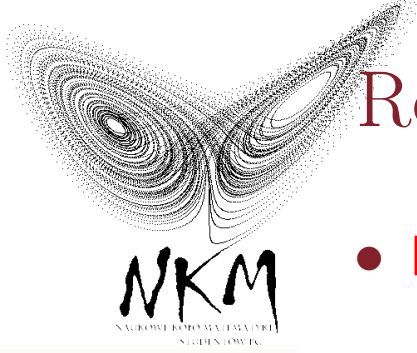
- Rozwiązywalnymi układami dynamicznymi nazywamy takie, których rozwiązanie może być przedstawione w postaci jawnej.
- Rozważmy równanie $x_n = p(\theta T z^n)$, gdzie $p(\cdot)$ jest funkcją okresową, T jest jej okresem, $z \in \mathbb{N}$, a θ definiuje warunek początkowy.
- **Przykład 1**
Weźmy rozwiązywalny układ dynamiczny, którego odwzorowanie generujące ma postać:

$$X_{n+1} = \sin^2(z \arcsin \sqrt{X_n})$$

Rozwiązanie tego równania jest postaci

$$X_n = \sin^2(\pi \theta z^n)$$

Wykładnik Lapunowa ma wartość $\lambda = \ln z$, więc układ jest chaotyczny dla $z > 1$.



Rozwiązywalne układy dynamiczne

- Przykład 2

$$(\star) x_n = \sin^2(\pi\theta z^n)$$

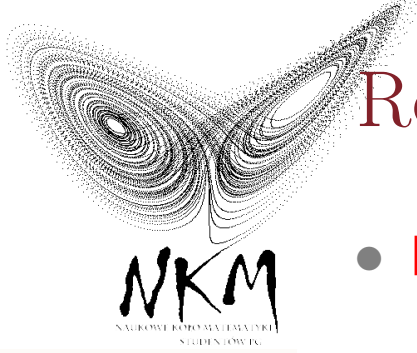
Niech $\theta = \theta_0 + q^m k$, $z = \frac{p}{q} > 1$ takie, że $NWD\{p, q\} = 1$,
 $k, m \in \mathbb{Z}$.

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Rozwiązywalne układy dynamiczne

- Przykład 2

$$(\star) x_n = \sin^2(\pi\theta z^n)$$

Niech $\theta = \theta_0 + q^m k$, $z = \frac{p}{q} > 1$ takie, że $NWD\{p, q\} = 1$, $k, m \in \mathbb{Z}$.

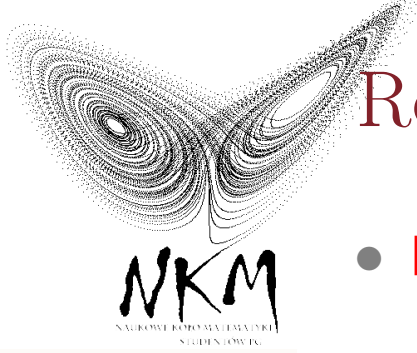
- Weźmy ciąg x_0, x_1, \dots, x_m dany formułą (\star) . Kolejna liczba x_{m+1} może przyjmować q możliwych wartości. Zjawisko to nazywamy "*multi-value correspondence*".

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Rozwiązywalne układy dynamiczne

• Przykład 2

$$(\star) x_n = \sin^2(\pi\theta z^n)$$

Niech $\theta = \theta_0 + q^m k$, $z = \frac{p}{q} > 1$ takie, że $NWD\{p, q\} = 1$, $k, m \in \mathbb{Z}$.

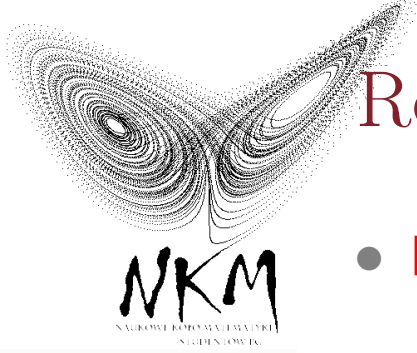
- Weźmy ciąg x_0, x_1, \dots, x_m dany formułą (\star) . Kolejna liczba x_{m+1} może przyjmować q możliwych wartości. Zjawisko to nazywamy "*multi-value correspondence*".
- Zatem otrzymujemy nieprzewidywalny ciąg dla krótkich serii.
Deterministyczna losowość.

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



Rozwiązywalne układy dynamiczne

• Przykład 2

$$(\star) x_n = \sin^2(\pi\theta z^n)$$

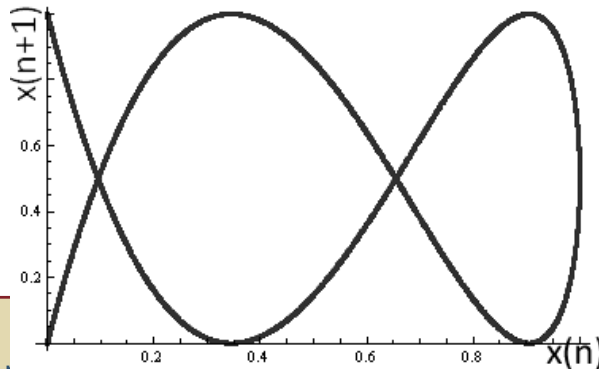
Niech $\theta = \theta_0 + q^m k$, $z = \frac{p}{q} > 1$ takie, że $NWD\{p, q\} = 1$, $k, m \in \mathbb{Z}$.

- Weźmy ciąg x_0, x_1, \dots, x_m dany formułą (\star) . Kolejna liczba x_{m+1} może przyjmować q możliwych wartości. Zjawisko to nazywamy "*multi-value correspondence*".
- Zatem otrzymujemy nieprzewidywalny ciąg dla krótkich serii. *Deterministyczna losowość*.

$p = 5; q = 2; \theta = 2;$

$$x[n_1] = \left(\text{Sin}\left[\pi\theta\left(\frac{p}{q}\right)^n\right] \right)^2;$$

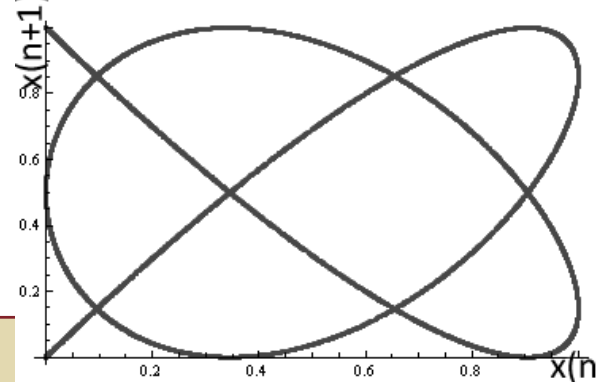
`ListPlot[Table[{x[n], x[n+1]}, {n, 9000}]]`

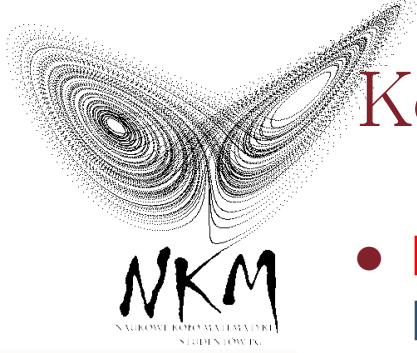


$m = 3; p = 5; q = 4; \theta = 2;$

$$x[n_1] = \left(\text{Sin}\left[\pi\theta\left(\frac{p}{q}\right)^n\right] \right)^2;$$

`ListPlot[Table[{x[n], x[n+1]}, {n, 10000}]]`





- **Przykład 3**

Rozważmy dwa przedziałami liniowe odwzorowania:

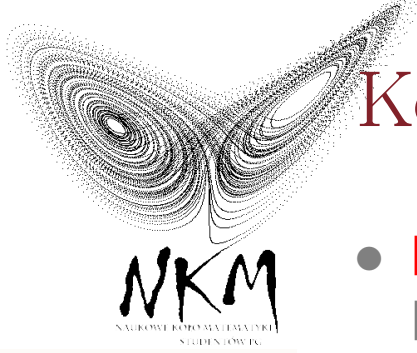
$$h(a, t) = \text{mod}(at, 1), \quad g(a, t) = \begin{cases} \text{mod}(at, 1) & \text{mod}(\lfloor at \rfloor, 2) = 0 \\ -\text{mod}(at, 1) + 1 & \text{mod}(\lfloor at \rfloor, 2) = 1 \end{cases}$$

Wstęp

'Chaotyczne'
PRBGs

- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

Bibliografia



- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

- **Przykład 3**

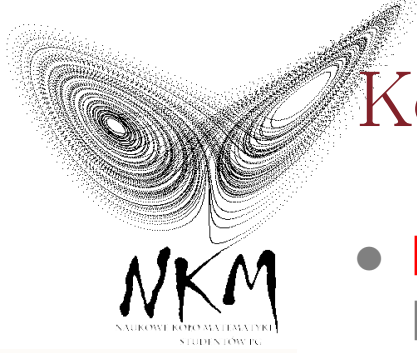
Rozważmy dwa przedziałami liniowe odwzorowania:

$$h(a, t) = \text{mod}(at, 1), \quad g(a, t) = \begin{cases} \text{mod}(at, 1) & \text{mod}(\lfloor at \rfloor, 2) = 0 \\ -\text{mod}(at, 1) + 1 & \text{mod}(\lfloor at \rfloor, 2) = 1 \end{cases}$$

- Dla $a = \frac{p}{q} > 2$ rozważmy dwie nieodwracalne, nieliniowe transformacje:

$$(\circ) x_{n+1} = h(a, x_n), y_n = h(b, x_n)$$

$$(\diamond) x_{n+1} = g(a, x_n), y_n = g(b, x_n)$$



- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy

● Przykład 3

Rozważmy dwa przedziałami liniowe odwzorowania:

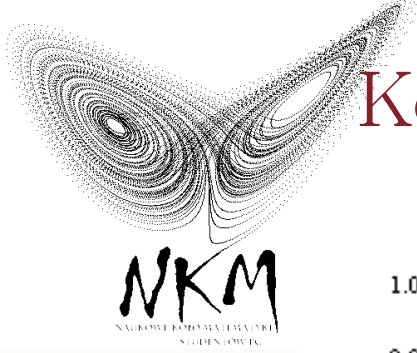
$$h(a, t) = \text{mod}(at, 1), \quad g(a, t) = \begin{cases} \text{mod}(at, 1) & \text{mod}(\lfloor at \rfloor, 2) = 0 \\ -\text{mod}(at, 1) + 1 & \text{mod}(\lfloor at \rfloor, 2) = 1 \end{cases}$$

- Dla $a = \frac{p}{q} > 2$ rozważmy dwie nieodwracalne, nieliniowe transformacje:

$$(\circ) x_{n+1} = h(a, x_n), y_n = h(b, x_n)$$

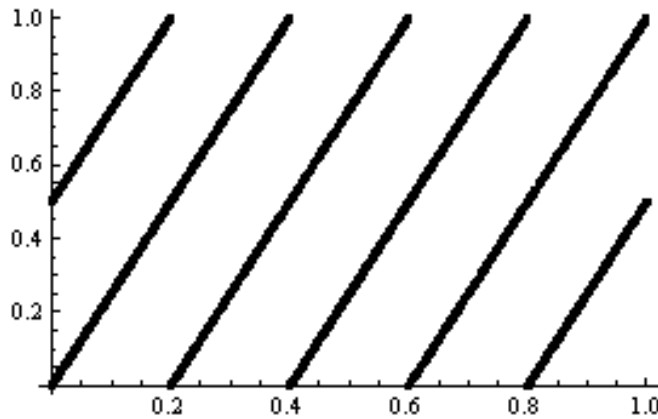
$$(\diamond) x_{n+1} = g(a, x_n), y_n = g(b, x_n)$$

- **Tw.** Jeżeli $b = q^N$, to y_n oraz y_{n+m} dla $m = 1, 2, \dots, N$ mają 'perfect multi-value correspondence' z $p^m : q^m$.



'Chaotyczne' PRBGs

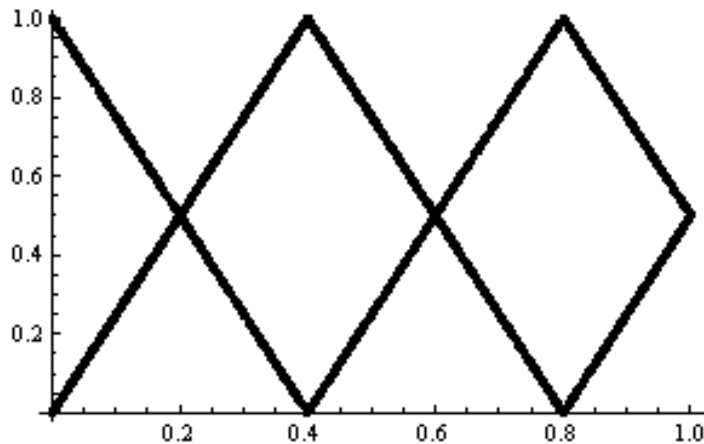
- ❖ Chaotyczny układ dynamiczny
- ❖ Kilka twierdzeń bez dowodów :P
- ❖ Rozwiązywalne układy dynamiczne
- ❖ KoAsDeLoUkDy



$$x_{n+1} = h(a, x_n), \quad y_n = h(b, x_n)$$

$$a = \frac{5}{2}, \quad b = 8$$

$$y_{n+1}(y_n)$$

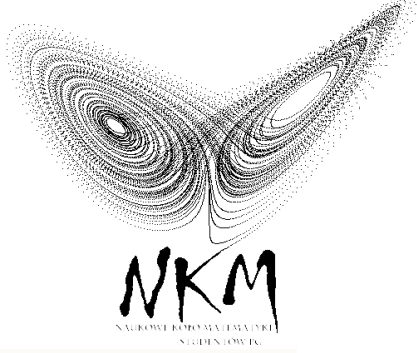


$$x_{n+1} = g(a, x_n), \quad y_n = g(b, x_n)$$

$$a = \frac{5}{2}, \quad b = 8$$

$$y_{n+1}(y_n)$$

Figure 1: zależność w jednym kroku kolejnych wyrazów ciągu $\{y_n\}$



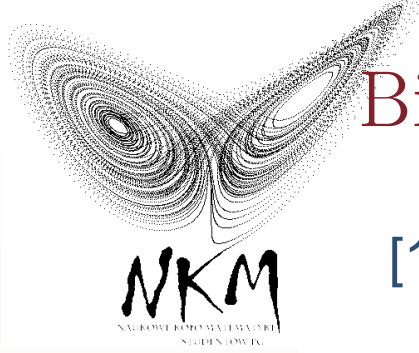
Wstęp

'Chaotyczne'
PRBGs

Bibliografia

❖ Bibliografia

Bibliografia



Bibliografia

Wstęp

'Chaotyczne'
PRBGs

Bibliografia
❖ Bibliografia

- [1] K. Wang, W. Pei, H. Xia, Y. Cheung *Pseudo-random number generators based on asymptotic deterministic randomness*
- [2] Z. Kotulski *Budowanie szyfrów blokowych*
- [3] Kai Wang, Wenjiang Pei, Liuhua Zou, Yiu-ming Cheung and Zhenya He *The asymptotic deterministic randomness*, Physics Letters A, Volume 368, Issues 1-2, 13 August 2007, Pages 38-47.
- [4] Z. Kotulski, J. Szczepański *Discrete chaotic cryptography (DCC).*, Ann. Physic 6 (1997), 381-394.