Obliczenia inspirowane Naturą

Wykład 03 – Zastosowania automatów komórkowych (uzupełnienie Wykładu 02)

Jarosław Miszczak

IITiS PAN Gliwice

31/03/2016

Model Lotki-Voltery

Dynamika populacji

Równania Lotki-Voltery opisują model drapieżnik-ofiara.

- 1910, Alfred J. Lotka – zastosowanie do teorii reakcji chemicznych;
- 1926, Vito Volterra, Umberto D'Ancona – model wyjaśniający dynamikę populacji ryb w Adriatyku;
- 1965, Richard Goodwin – zastosowanie w ekonomii.

Model Lotki-Voltery

Dynamika populacji

$$\frac{dx(t)}{dt} = \alpha x(t) - \beta y(t)x(t), \quad \frac{dy(t)}{dt} = \delta x(t)y(t) - \gamma y(t)$$

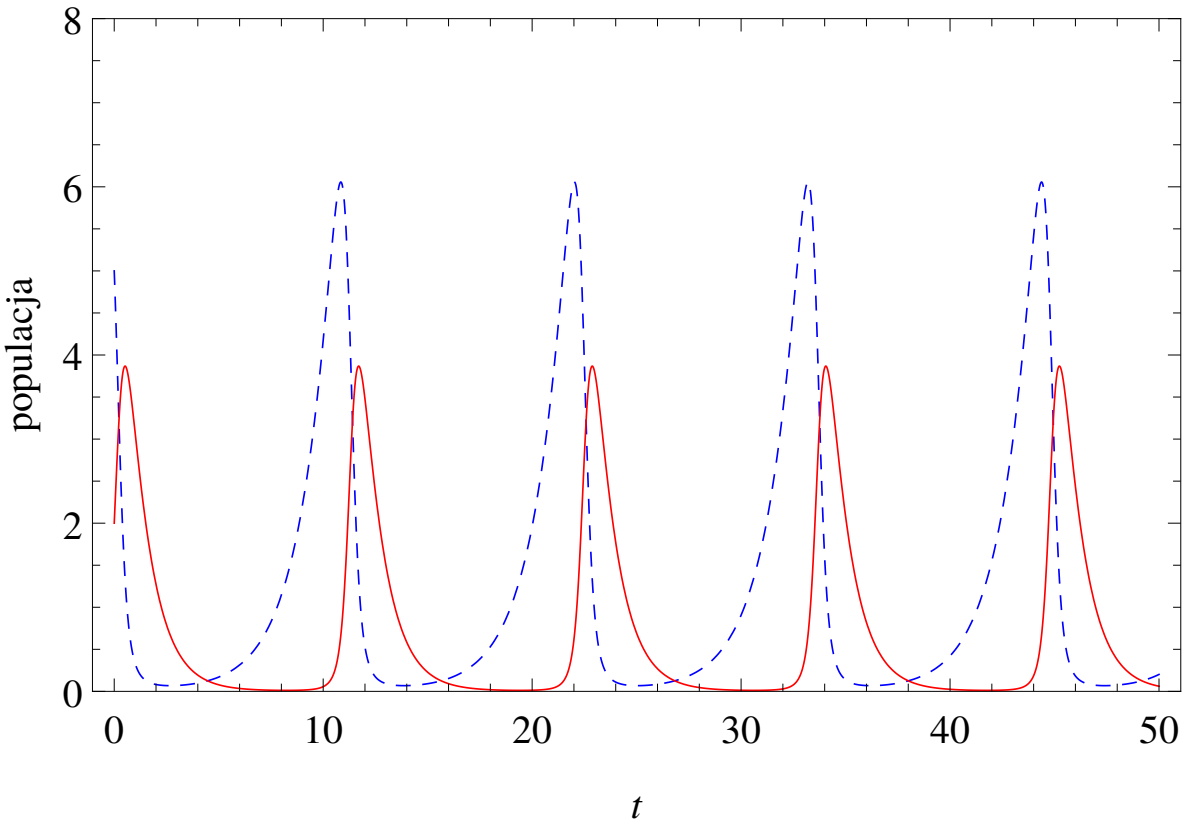
- $x(t)$ – populacja ofiar (np. królików)
- $y(t)$ – populacja drapieżników (np. lisów)
- $\alpha, \beta, \delta, \gamma$ – paramenty opisujące oddziaływanie między populacjami.

Model Lotki-Voltery

Dynamika populacji

Przykład rozwiązania

Dla $x(0) = 5$, $y(0) = 2$ oraz $\alpha = \frac{2}{3}$, $\beta = 1$, $\delta = \frac{3}{4}$, $\gamma = 1$.



Model Lotki-Voltery

Dynamika populacji

Problem

- populacje mogą osiągnąć wartości bardzo bliskie zeru, a pomimo tego odrodzić się – tzw. problem atto-lisów (ang. *atto-fox problem*), czyli ilości 10^{-18} lisów.

Model Lotki-Voltery

Dynamika populacji – automat komórkowy

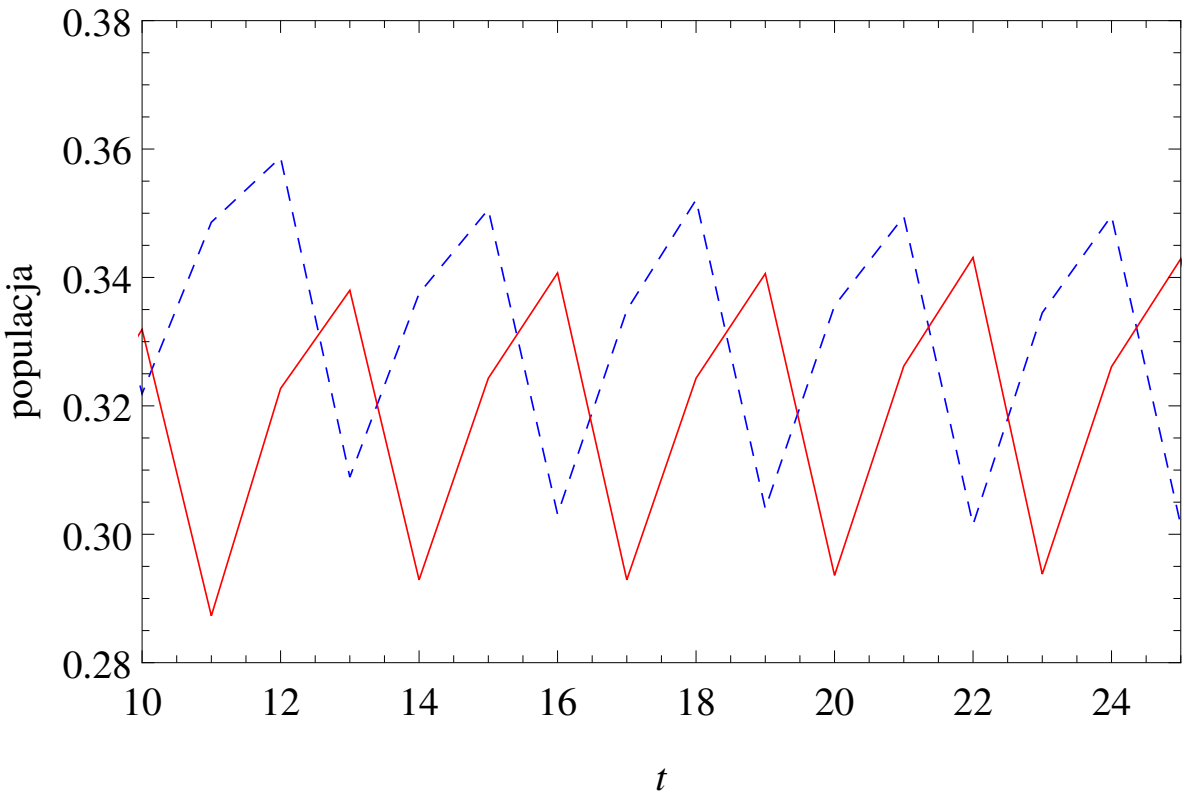
- opis podobnej dynami uzyskujemy za pomocą automatu z następującymi regułami:
  $F + R \mapsto 2F$ (lis zjada zająca i pojawia się nowy lis)
  $G + F \mapsto 2G$ (lis nie je trawy i umiera)
  $R + G \mapsto 2R$ (zając zjada trawę i pojawia się nowy zając)

Model Lotki-Voltery

Dynamika populacji – automat komórkowy

Przykład

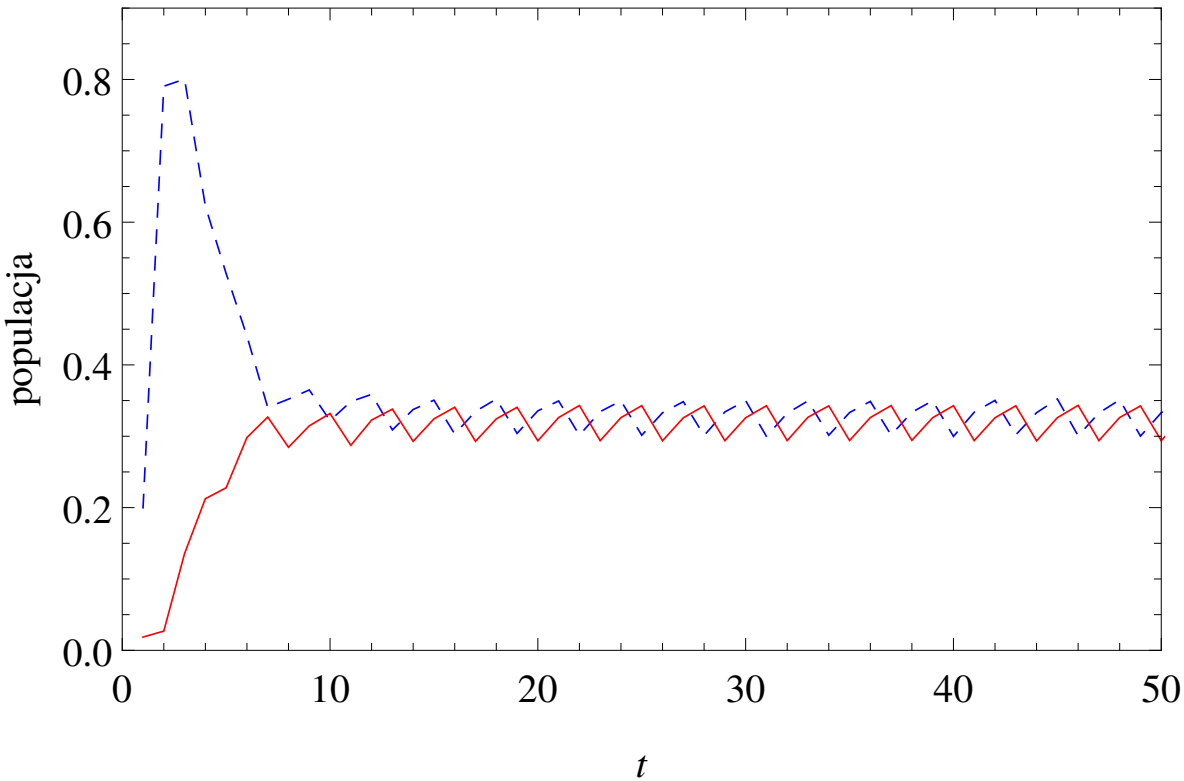
Prawdopodobieństwo zasiedlenia: $\frac{78}{100}$ (G), $\frac{20}{100}$ (R) i $\frac{2}{100}$ (F).



Model Lotki-Voltery

Dynamika populacji – automat komórkowy

Populacje dążą od początkowej koncentracji do stanu równowagi.



Model Isinga
Zastosowania w fizyce

- 1920, Wilhelm Lenz, Ernst Ising – zastosowane do fizyki ferromagnetyków;
- 1982, John Joseph Hopfield – zastosowanie do modelowania sieci neuronowych;

Model Isinga

Zastosowania w fizyce – model

Model Isinga jest zbudowany bardzo podobnie do automatu komórkowego:

- dana jest sieć spinów (które mogą przyjmować wartość ± 1)
- spin atomu może być dodatni lub ujemny, ale jego wartość bezwzględna jest stała;
- energia układu, określona poprzez oddziaływanie spinów,

$$E = -\sum_{ij} J_{ij} s_i s_j - h \sum_i s_i$$

zależy od wzajemnej orientacji spinów, gdzie J jest sprzężeniem, zwykle stałym dla sieci.

Jeżeli $J > 0$ to układ jest nazywany ferromagnetykiem, jeżeli $J < 0$ – antyferromagnetykiem.

Model Isinga
Zastosowania w fizyce

Cel

Obliczenie namagnesowania układu w zależności od temperatury i zewnętrznego pola.

- Ścisłe wyliczenia są możliwe tylko w szczególnych przypadkach.
- Metody Monte Carlo wymagają generatorów liczb pseudolosowych.

Model Isinga
Reguły automatu

Reguła automatu

Podstawową regułą jest minimalizacja energii:
$s_i(t+1) = \text{sign}\left(\sum_j J_{ij} s_j + h\right)$

- Temperatura układu $T = 0$.
- Taka reguła jest deterministyczna.
- Tak określona dynamika prowadzi do automatów typu I lub II (czyli jest nieciekawa).

Model Isinga

Zastosowania w fizyce – algorytm Metropolisa

Algorytm Metropolisa pozwala na symulację modelu Isinga dla $T > 0$.

- Wybieramy losową komórkę;
- Odwracamy jej spin i obliczamy zmianę ΔE.
- Jeżeli $\Delta E < 0$, akceptujemy zmianę.
- Jeżeli $\Delta E > 0$, to losujemy liczbę r z $[0, 1]$ i
  - jeżeli $r < \exp(\frac{\Delta E}{T})$, to akceptujemy zmianę;
  - jeżeli $r > \exp(\frac{\Delta E}{T})$, to odwracamy spin.

Model Isinga

Zastosowania w fizyce – kąpiel cieplna

Inny sposób modelowanie sytuacji $T > 0$ to tzw. kąpiel cieplna.

- Dla każdej komórki obliczamy $r_i(t) = \left[1 + \exp\left(-\frac{2}{T}\sum_j J_{ij} s_j(t)\right)\right]^{-1}$.
- Losujemy liczbę r z $[0, 1]$.
- Jeżeli $r > r_i(t)$, to $s_i(t+1) = -1$.
- W przeciwnym wypadku $s_i(t+1) = 1$.

Kryptografia
Liczby pseudolosowe

- Reguła 30 jest wykorzystywana do generowania liczb pseudolosowych.
- *Mathematica* dostarcza opartej na niej metody – parametr $\mathrm{Method} \rightarrow \text{"}\mathrm{Rule30CA}\text{"}$ dla funkcji $\mathrm{SeedRandom}$
- Generator ten posiada bardzo dobre właściwości.
- Więcej na http://mathworld.wolfram.com/Rule30.html

S.Wolfram, *Random sequence generation by cellular automata*, Advances in Applied Mathematics, Vol. 7 (2), pp. 123-169 (1986).

Kryptografia
Funkcje mieszające

- określamy funkcję na ciągach binarnych jako

$$g(x)_i = x_{i-1} \oplus (x_i \vee x_{i+1})$$

- dla dwóch liczb naturalnych $c < d$ budujemy

$$f_0(x) = b_c(x), b_{c+1}(x), \ldots, b_d(x)$$

gdzie $b_k(x)$ to k-ty bit wyniku działania g na ciągu x

- wartość funkcji mieszające powinna zależeć od wszystkich elementów ciągu wejściowego, czyli musimy mieć $c = 1$;

Zalety to bardzo wydajna i tania implementacja.

I.B. Damgård, *A Design Principle for Hash Functions*, Advances in Cryptology – Proceedings of CRYPTO' 89, LNCS, Vol. 435, pp. 416-427 (2001)