Zeszyty Naukowe Towarzystwa Doktorantów UJ
Nauki Ścisłe, Nr 7 (2/2013)

PAWEŁ NOWAK, TOMASZ SEIDLER

(UNIWERSYTET JAGIELLOŃSKI)

SCHEMAT RÓŻNICOWY

1. STRESZCZENIE

Celem niniejszej pracy jest zaprezentowanie własności pewnego schematu iteracyjnego, zwanego dalej przez nas s c h e m a t e m r ó ż n i c o w y m. Działanie jego polega na odejmowaniu dwóch sąsiednich elementów ciągu i zwracaniu ich bezwzględnej różnicy w kolejnych krokach. Całą procedurę można dowolnie przedłużać i jednocześnie badać kolejne postacie generowanych ciągów, które tworzą pewną strukturę liczbową. Zgodnie z naszym założeniem, struktura ta może przyjmować formę dwuwymiarowych ugrupowań liczb (macierzy) lub postacie bardziej złożone.

Ewolucja schematu prowadzi do rozmaitych zachowań, wśród których wymienić należy pojawianie się charakterystycznych atraktorów, do których zmierzać mogą kolejne postacie generowanych ciągów. Mogą nimi być cykle graniczne, czyli oscylacje pojawiające się po przekroczeniu pewnej liczby iteracji, które albo są stałe i powtarzają się od pewnego momentu w nieskończoność, albo mogą ulegać tłumieniu. Innym atraktorem jest jednakowa i stała od pewnego momentu wartość wszystkich elementów ciągu, zwykle wartość zerowa. Interesujące jest, że to, czy kolejne postacie ciągów zmierzać będą do cyklu granicznego, czy do ujednolicenia elementów, zależeć może od liczby jego elementów oraz przyjętych warunków brzegowych. Jest to swoiste zjawisko, podobne do bifurkacji, zależne od parametrów strukturalnych samego schematu, pojawiające się bez względu na wartości liczbowe elementów tworzonych ciągów.

Podczas ewolucji schematu zaobserwowane zostały także oscylacje złożone, tzn. wykazujące różną częstotliwość. Przykładowo dla ciągów 5-elementowych

odmienna częstotliwość oscylacji ma tendencję do występowania w przypadku trzeciego elementu.

Została podjęta próba wizualizacji ewolucji schematu z wykorzystaniem *pakietu R*, dzięki czemu można było zaobserwować, że schemat generuje rozmaite struktury złożone, wykazujące pewien poziom uporządkowania. Niektóre zachowania są emergentne, możliwe do zaobserwowania po przekroczeniu pewnej złożoności układu. Charakterystycznymi obiektami są rozwidlenia dychotomiczne przypominające błyskawice, a także zachowania nazwane przez nas *ping-pong*.

Ostatnim aspektem pracy jest zaprezentowanie schematu różnicowego jako potencjalnego kandydata na funkcję jednokierunkową, algorytmu mogącego znaleźć zastosowanie w szyfrowaniu danych.

Opisane tutaj reguły prowadzenia iteracji na ciągach liczb znane są już od dawna pod hasłem jednowymiarowych automatów komórkowych (patrz punkt 13). Niniejszy artykuł został jednak w znacznej mierze napisany bez wiedzy autorów o ich istnieniu. Autorzy zaznajomili się z tematem dzięki życzliwym uwagom recenzentów niniejszej pracy.

2. ZASADA DZIAŁANIA

Mając dany dowolny ciąg liczbowy $\{a_i^n\} \in N$, tworzy się ciąg pomocniczy $\{b_i^n\} \in N$, którego elementy stanowią odległości między sąsiednimi elementami pierwszego ciągu mierzone na osi liczbowej, n numeruje kolejne iteracje: n = 0, 1, 2…, natomiast i numeruje kolejne elementy ciągu: i = 1, 2, 3…, K. Liczba elementów ciągu K wynika z przyjętego przez nas założenia. Tak więc dowolny element b_i^n ciągu pomocniczego wyraża się następująco:

$$b_i^n = |a_{i+1}^n - a_i^n| \quad (1)$$

Wynik ten określimy jako moduł „pochodnej" ciągu. Korzystając z pomocniczego ciągu, elementy ciągu głównego w $(n+1)$-szym kroku są zdefiniowane następująco:

$$a_{i+1}^{n+1} = |b_{i+1}^n - b_i^n| \quad (2)$$

Całość iteracji można również zapisać bezpośrednio:

$$a_{i+1}^{n+1} = \left||a_{i+2}^{n} - a_{i+1}^{n}| - |a_{i+1}^{n} - a_{i}^{n}|\right| \quad (3)$$

Jeden krok iteracji można zatem określić jako zmodyfikowane „różniczkowanie" ciągu[1]. Przykładowo:

a^{n+1}:			3			
b^{n}:		4		7		
a^{n}:	4		8		1	

Jak widać, każda kolejna iteracja skraca ciąg o dwa elementy. Można temu zapobiec, przyjmując pewne warunki brzegowe. Jedną z możliwości jest wprowadzenie dodatkowych elementów („zerowych" warunków brzegowych) $a_0 = 0, a_{K+1} = 0$. I tak, przyjmując powyższe założenia:

a^{n+3}:	0	0	0
a^{n+2}:	3	0	3
a^{n+1}:	0	3	6
a^{n}:	4	8	1

Innym możliwym wyborem mogą być cykliczne warunki brzegowe: $a_0 = a_K$, $a_{K+1} = a_1$.

Pierwszym wnioskiem, jaki możemy wyciągnąć, jest to, że schemat prowadzi do redukcji wartości liczbowych, kolejne ciągi (wiersze macierzy) wypełniane są coraz mniejszymi liczbami. W powyższym przykładzie liczby sprowa-

[1] P. Blanchard, R. L. Devaney, G. R. Hall, *Differential Equations*, London 2006.

dziły się do ciągu samych zer. Czy jest to jednak jedyna możliwa ścieżka ewolucji schematu? Okazuje się, że w tym przypadku, gdy tworzona macierz składa się z trzech kolumn (K = 3), niezależnie od początkowych wartości a^1 po przekroczeniu pewnej skończonej liczby iteracji p, elementy kolejnych ciągów przyjmują wartość 0 (a^{p+1} = 0). Zostanie to dokładniej omówione w dalszej części pracy. Teraz powiemy, w jakim rozumieniu w przedstawionym schemacie można zastosować pojęcie układu.

3. UKŁAD I PRZESTRZEŃ FAZOWA

W tym momencie zaprezentowana zostanie dodatkowa terminologia, dzięki której możliwy będzie opis badanych ewolucji schematu różnicowego. Przez u k ł a d rozumiemy strukturę złożoną z ciągów liczbowych K-elementowych zapisanych jedne nad drugimi wedle przyjętych w danym momencie zasad[2]. Układ jest K-wymiarowy, każda kolumna tworzonej struktury jest osobnym wymiarem. Tworzona jest więc p r z e s t r z e ń f a z o w a, w której reprezentacją danego ciągu $\{a_i^n\}$ jest p u n k t. Jego współrzędne w danym wymiarze zależą od wartości liczbowej danego elementu ciągu. Tak więc reprezentacją ciągu: $\{a_i^n\}$ =1, 2, 3 jest punkt w przestrzeni trójwymiarowej o współrzędnych: x = 1, y = 2, z = 3. Ewolucji układu towarzyszy ciągła zmiana położenia punktu w przestrzeni fazowej, toteż jej zobrazowaniem jest t r a j e k t o r i a u k ł a d u. Dalsze rozważania nad schematem skupione będą na analizie możliwych trajektorii, w tym poszukiwaniu specyficznych zachowań i atraktorów, do których zmierzać może ewolucja układu. Poniżej przedstawiamy wynik naszych analiz.

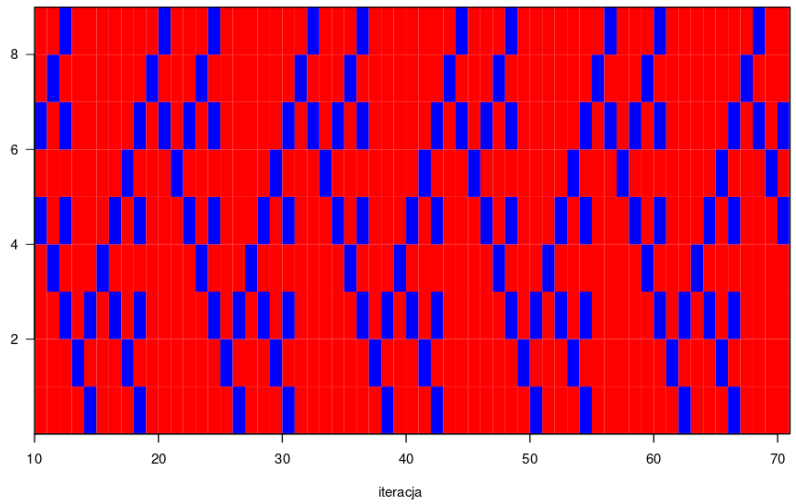
4. ATRAKTOR 1 – CYKL GRANICZNY

Okazuje się, że najczęstszym typem atraktora jest cykl graniczny. Oznacza to, że po przekroczeniu pewnej granicznej liczby iteracji, różnej dla różnych stanów układu, w tworzonej strukturze liczbowej wartości w poszczególnych kolumnach zaczynają powtarzać się cyklicznie. W przypadku liczb całkowitych najczęstsze są powtarzające się zera i jedynki. Gdy na wejściu schematu podamy nawet bardzo duże wartości liczbowe, to po przekroczeniu relatywnie małej liczby iteracji te olbrzymie wartości w wyniku wzajemnego odejmowania maleją, sprowadzają się do zer i jedynek, a te z kolei od pewnego momentu wchodzą

[2] P. Coveney, R. Highfield, *Granice złożoności. Poszukiwania porządku w chaotycznym świecie*, tłum. P. Amsterdamski, Warszawa 1997; J. D. Murray, *Wprowadzenie do biomatematyki*, tłum. U. Foryś, M. Bodnar, Warszawa 2007; H. Haken, *Synergetics. Introduction and Advanced Topics*, Springer 2004.

na zamkniętą trajektorię i zaczynają oscylować w nieskończoność (Ryc. 1). Osobną obserwacją jest, że wraz z ewolucją rośnie stopień uporządkowania tworzonej macierzy. W przeciwieństwie do układów fizycznych można stwierdzić, że entropia układu i ilość informacji maleje.

Ryc. 1. Oscylacje w układzie o K = 9 (wartości: czerwone: 0, niebieskie: 1)[3]

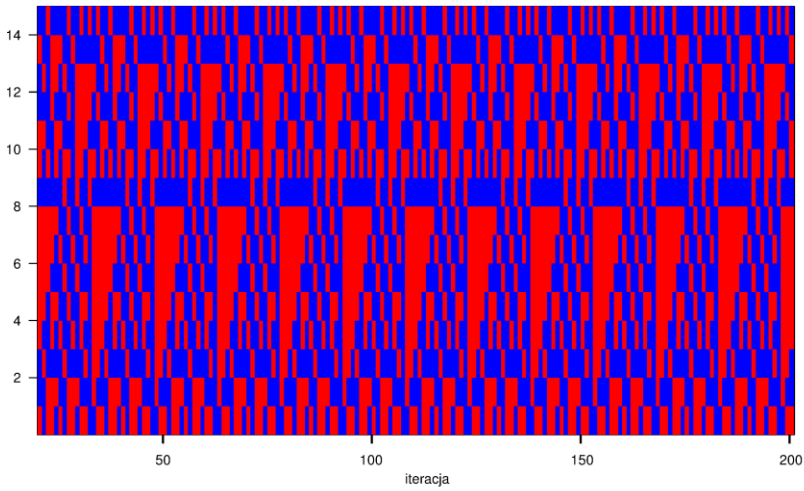


Źródło: Opracowanie własne

Pojawianie się cykli granicznych zaobserwowaliśmy również w schemacie działającym z cyklicznymi warunkami brzegowymi (Ryc. 2). Analogicznie do sytuacji rozważanych poprzednio, po przekroczeniu pewnej liczby iteracji w układzie pojawiają się oscylacje. Niezależnie od wyboru omawianych wcześniej warunków brzegowych graniczna liczba iteracji, po której układ wchodzi na trajektorię zamkniętą, jest różna, zależna od poszczególnych wartości liczbowych elementów ciągu, niemożliwa do przewidzenia *ad hoc*.

[3] W wersji kolorowej ryciny dostępne są online na stronie internetowej czasopisma, publikacja papierowa: barwa jasnoszara – 0, barwa ciemnoszara – 1; http://www.doktoranci.uj.edu.pl/zeszyty

Ryc. 2. Oscylacje w macierzach o cyklicznych warunkach brzegowych $K = 9$
(wartości: czerwone: 0, niebieskie: 1)

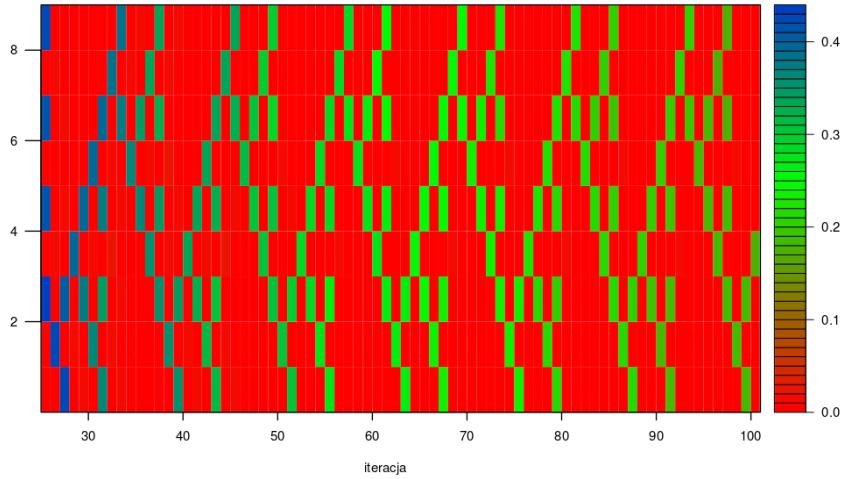


Źródło: Opracowanie własne

5. ATRAKTOR 2 – OSCYLACJE TŁUMIONE

Gdy algorytm operuje na liczbach naturalnych (jak w powyższych wzorach), najmniejszą różnicą pomiędzy nimi pojawiającą się w tworzonej strukturze jest wartość jeden. W przypadku liczb niecałkowitych różnice pomiędzy poszczególnymi elementami ciągu mogą być dowolnie małe. Konsekwencją tego są trajektorie układu, które często, choć nie zawsze okazują się być pseudocykliczne, tzn. wartości liczbowe oscylują z pewną określoną stałą częstotliwością, jednak ciągle maleją, zmierzając do zera. Są to więc oscylacje tłumione (Ryc. 3). Pamiętać jednak należy, że powyższe rozważania nie mogą być prowadzone drogą komputerowej analizy numerycznej w przypadku liczb zmiennoprzecinkowych, tzn. takich, których komputerowe odwzorowanie zależeć by mogło od przyjętej dokładności obliczeń. Doprowadziłoby to do sytuacji, w której końcowe wyniki mogłyby być różne dla tego samego stanu początkowego na skutek przyjęcia różnej skali dokładności (tzw. *roundoff error*).

Ryc. 3. Przykład oscylacji tłumionych dla liczb niecałkowitych,
których komputerową reprezentacją nie są liczby zmiennoprzecinkowe



Źródło: Opracowanie własne

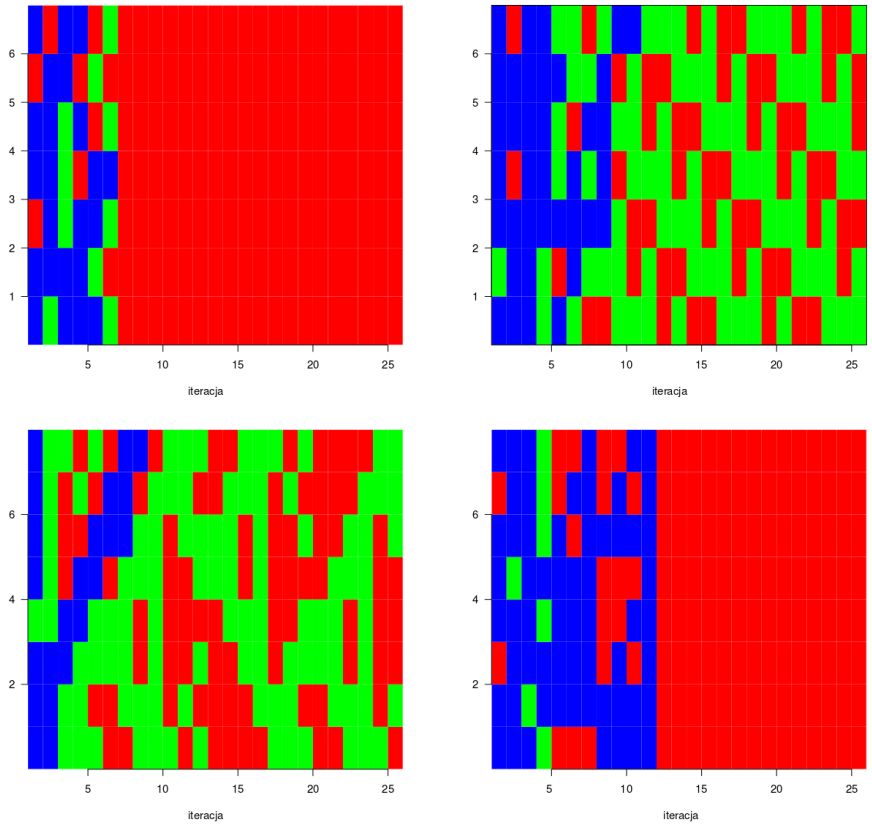
6. ATRAKTOR 3 – STAŁA

Czasami układ zamiast zmierzać do atraktora cyklicznego, zmierza do punktu przestrzeni fazowej (kolejne generowane postacie ciągów nie różnią się od siebie wartościami poszczególnych elementów). Prawie zawsze, poza pewnymi szczególnymi typami ciągów wejściowych, wszystkie elementy przyjmują wtedy wartość 0. Zaobserwowaliśmy pewne ogólne prawidłowości, kiedy układ zmierza do punktu (stałej), a kiedy nie. Prawidłowości te pojawiają się zawsze, gdy spełnione są poniższe warunki:

Atraktorem układu jest stała wartość elementów ciągów równa 0:

- dla ciągów z przyjętymi zerowymi warunkami brzegowymi – gdy liczba kolumn macierzy spełnia zależność: $K = 2^N - 1$, gdzie N – dowolna liczba naturalna;
- dla ciągów z cyklicznymi warunkami brzegowymi – gdy liczba kolumn macierzy spełnia zależność: $K = 2^N$, gdzie N – dowolna liczba naturalna.

Ryc. 4. Przykładowe zachowanie układów w zależności od wymiarowości K (górny wiersz 7, dolny 8) i typu warunków brzegowych (ciągi z zerowymi warunkami brzegowymi – lewa, z cyklicznymi warunkami brzegowymi – prawa). Zastosowano skalę kolorów: czerwony: 0, niebieski: 1, zielony: pozostałe [wersja kolorowa dostępna online]



Źródło: Opracowanie własne

7. PSEUDO-BIFURKACJE ZALEŻNE OD STRUKTURY

Bifurkacja – jakościowa zmiana własności modelu matematycznego przy drobnej zmianie jego parametrów, np. warunków początkowych.

Zgodnie z podaną powyżej definicją zaobserwowana przez nas zmiana własności schematu różnicowego, polegająca na podążaniu dwoma różnymi trajektoriami, nie może być określona jako rodzaj bifurkacji, gdyż wymiarowość nie

może zmieniać się w sposób ciągły, lecz dyskretny. Jest to więc zjawisko jedynie przypominające bifurkację.

Zmiana własności tego modelu polega na możliwości zadania różnej liczby elementów ciągu wejściowego, a także określenia dwóch różnych typów warunków brzegowych. I tak dla ciągu z cyklicznymi warunkami brzegowymi 7-elementowego trajektoria układu jest zdeterminowana, dąży do cyklicznych oscylacji, podczas gdy dla postaci 8-elementowej trajektoria dąży do punktu „0", zlokalizowanego w 8-wymiarowej przestrzeni fazowej. Natomiast dla 8-elementowego ciągu z zerowymi warunkami brzegowymi układ ponownie będzie dążył do cyklu granicznego, natomiast ciąg 7-elementowy wejdzie na trajektorię dążącą do stałej (Ryc. 4).

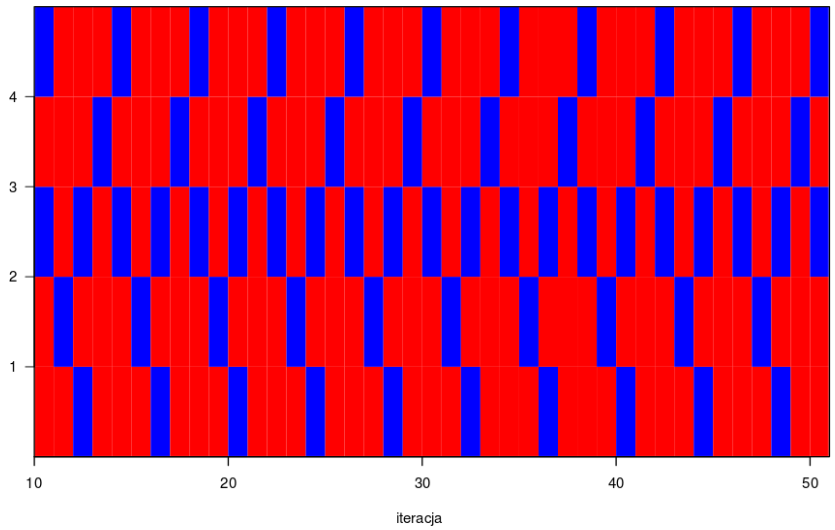
Opisywana pseudo-bifurkacja jest dość specyficzna. Po pierwsze, obserwujemy zmianę własności modelu nie tylko względem jednego warunku początkowego, ale względem dwóch warunków (wymiarowości i typu warunków brzegowych), które wzajemnie uzupełniają się we własnościach, jak to zostało pokazane w przypadku ciągów 7- i 8-elementowych. Jest to obserwowane dla par ciągów o długości spełniającej zależność 2^N i $2^N - 1$.

Po drugie, opisywane zjawisko jest niezależne od usytuowania punktu reprezentującego stan układu w przestrzeni fazowej, zależne zaś od samej natury tej przestrzeni. Jest to więc zjawisko zależne od struktury, własności przestrzeni, w której odbywa się ewolucja układu (patrz Ryc. 4).

8. OSCYLACJE ZŁOŻONE

W niektórych przypadkach pojawiające się w układzie oscylacje mogą być sumą oscylacji o krótszym okresie. Te pierwsze są więc oscylacjami złożonymi. Aby to łatwo przedstawić, warto wprowadzić parametr Σ, oznaczający sumę wszystkich elementów danego ciągu. Analizując zmianę tego parametru w czasie ewolucji schematu, obserwujemy, że jego wartości zmieniają się cyklicznie, gdy układ wchodzi na trajektorię zamkniętą. Czasem jednak okres tych cykli jest większy niż okres cyklicznych zmian wartości poszczególnych kolumn macierzy. Jednym z przykładów, gdzie obserwowane jest to zjawisko, jest ciąg otwarty 5-elementowy (Ryc. 5). Okazuje się, że zarówno wartości Σ, jak i wartości elementów w kolumnach 1, 2, 4, 5 oscylują z większym okresem niż wartości w kolumnie 3. Okres tych pierwszych oscylacji jest zwykle wielokrotnością oscylacji krótszych.

Ryc. 5. Oscylacje złożone algorytmu dla ciągu 5-elementowego
(wartości: czerwone: 0, niebieskie: 1)
[wersja kolorowa dostępna online]

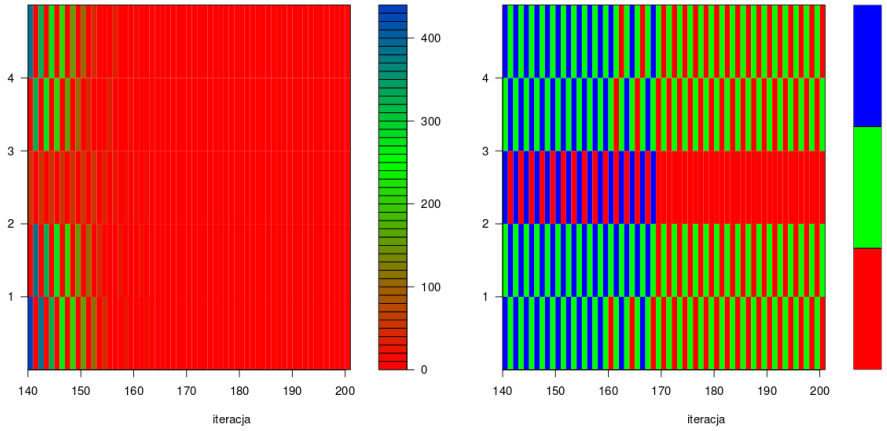


Źródło: Opracowanie własne

Powyższą własność ciągów 5-elementowych należy prawdopodobnie wytłumaczyć specyficznymi własnościami generowanej struktury liczbowej. Trzecia kolumna tworzonej macierzy ma centralne położenie względem pozostałych, jest więc pewną płaszczyzną symetrii całej struktury. Podobne zjawisko obserwowaliśmy dla innych ciągów otwartych, posiadających nieparzystą liczbą elementów, a oscylacje o najkrótszym okresie pojawiały się zawsze w centralnie położonej kolumnie.

W przypadku niektórych ciągów 5-elementowych obserwowaliśmy jeszcze inne zjawisko. Otóż wartości w kolumnach 1, 2, 4, 5 w ostateczności dążą do cykli granicznych, podczas gdy wartości w kolumnie 3. wydają się wchodzić na tor trajektorii zamkniętej dużo wcześniej, jednak jak się okazuje, gdy wartości w pozostałych kolumnach dostatecznie zmaleją, kolumna 3. ostatecznie zeruje się, czyli osiąga atraktor punktowy. To specyficzne zachowanie obserwowaliśmy przykładowo dla ciągu wejściowego: 22, 33, 4322, 55, 32 (Ryc. 6).

Ryc. 6. Wizualizacja zachowania schematu różnicowego przy danych początkowych: 22, 33, 4322, 55, 32. Po prawej zastosowano maskę ze skalą kolorów: czerwony: 0, zielony: 1, niebieski: pozostałe [wersja kolorowa dostępna online]



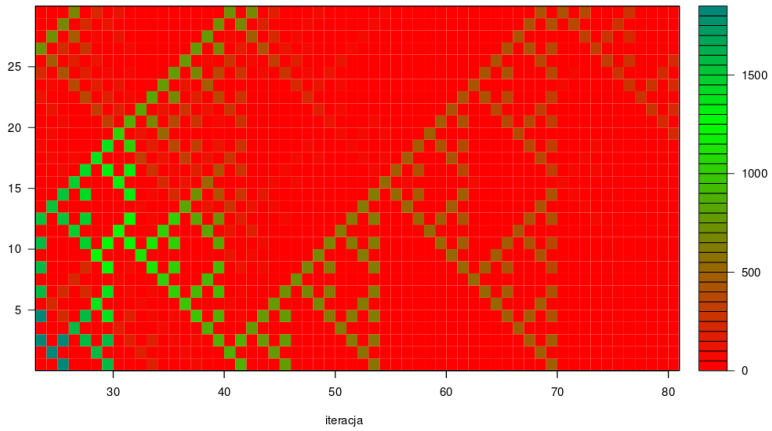
Źródło: Opracowanie własne

9. OBIEKTY EMERGENTNE

Wizualizując ewolucję schematu operującego na względnie dużej liczbie kolumn macierzy, a także stosunkowo dużych wartościach liczbowych, można zauważyć pojawianie się specyficznych zachowań układu. Są one widoczne, gdy spoglądamy na układ z pewnej odległości, tzn. gdy jesteśmy w stanie zaobserwować efekt co najmniej kilkudziesięciu iteracji. Zaobserwować można pojawianie się specyficznych obiektów, które należy nazwać obiektami emergentnymi. Zdecydowaliśmy się przedstawić dwa ich przykłady. Są nimi dychotomiczne rozwidlenia i obiekty ping-pong.

Rozwidlenia dychotomiczne to specyficzny rozkład zer i jedynek w macierzy, który niesie skojarzenia z rozwidlającą się na niebie błyskawicą (Ryc. 7 i 8). W tle tych rozwidleń reprezentowanych przykładowo przez wartości jeden znajdują się zera układające się również w specyficzne figury, np. piramidy.

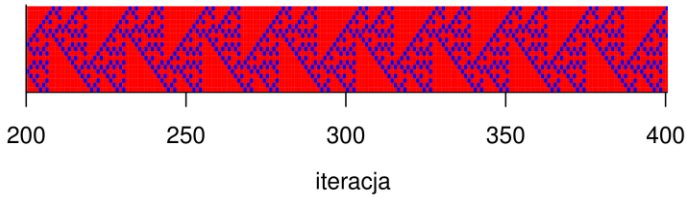
Ryc. 7. Wizualizacja rozwidleń dychotomicznych



Źródło: Opracowanie własne

Obiekty *ping-pong* to obrazowe „odbijanie" się trajektorii układu od „brzegów" (a_1, a_K), zachodzące cyklicznie, ze stałą częstotliwością. Oscylacje te w pewnym zakresie mogą pokrywać się z omówionymi wcześniej cyklami granicznymi, mogą je jednak w pewnym zakresie wyprzedzać, tzn. zachodzić, zanim jeszcze układ wejdzie na tor trajektorii zamkniętych. Obiekty te można również obrazowo opisać jako „zygzaki". Patrząc na nie z pewnej odległości, tak właśnie wyglądają (Ryc. 8).

Ryc. 8. Wizualizacja obiektu typu *ping-pong* oraz rozwidleń dychotomicznych (wartości: czerwone: 0, niebieskie: 1) [wersja kolorowa dostępna online]



Źródło: Opracowanie własne

10. INNE PODTYPY SCHEMATU RÓŻNICOWEGO

Na bazie opisanego schematu można tworzyć inne, bardziej bądź mniej złożone podtypy, wykorzystujące podobną zasadę pojedynczej iteracji. Jednym z przykładów jest nieco bardziej złożona postać schematu, który można nazwać sumowaniem piramid. Wejściem schematu jest również ciąg liczb, jego działanie jest analogiczne do opisanego wcześniej schematu macierzowego, z tą różnicą, że nie zakłada się żadnych warunków brzegowych – w kolejnych iteracjach korzysta się ze wzoru (1). Skutkuje to skracaniem się kolejnych ciągów i układaniem się liczb w formie trójkąta (piramidy), z jedną wartością liczbową zapisaną w wierzchołku. Przykładowo:

		1		
	0	1	1	
1	5	1	4	0

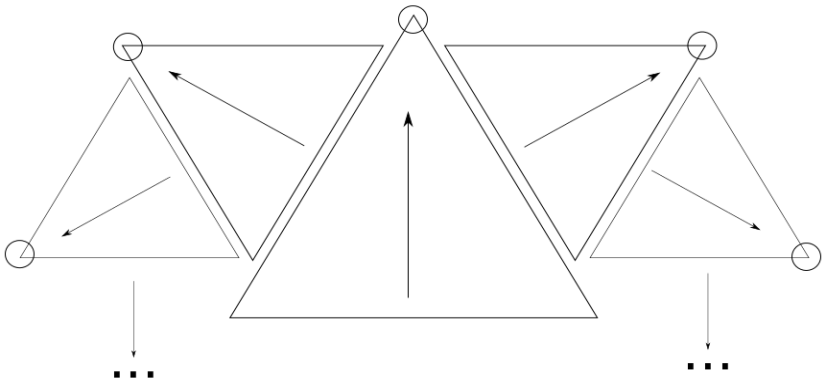
Natomiast gdy zapiszemy ten przykład w postaci szczegółowej, prezentując każde pojedyncze działanie:

			1					
		1		**0**				
	0		1		**1**			
4		4		3		**4**		
1	**5**		**1**		**4**		**0**	

Można zauważyć, że w wyniku podania na wejściu jednego ciągu (podstawa piramidy) generowane są dwa kolejne ciągi o tej samej liczbie elementów. Są to boki piramidy. Działanie algorytmu można więc przedłużać, tworzyć podobne struktury (kolejne piramidy) na bokach tej pierwszej, wyjściowej. W rezultacie można tworzyć bardzo złożoną strukturę, każda tworzona piramida tworzy dwa kolejne ciągi, które mogą stać się podstawami dwóch kolejnych piramid. Złożoność struktury rośnie więc w postępie geometrycznym 2^N.

Tak zapisany schemat już po stosunkowo niewielkiej liczbie iteracji staje się trudnym problemem obliczeniowym. Aby ograniczyć złożoność algorytmu, można zdecydować się na pewne upraszczające założenie: kontynuować „sumowanie" piramid, wybierając jedynie skrajnie położone boki, tzn. ciągle skrajnie lewe lub skrajnie prawe. W efekcie liczba piramid będzie rosnąć w postępie liniowym $2 \cdot N$. Przedstawia to Ryc. 9.

Ryc. 9. Schemat postępowania przy układzie piramidowym



Źródło: Opracowanie własne

Analiza tak powstałej złożonej struktury liczbowej może m.in. polegać na analizie wartości na wierzchołkach piramid (okręgi na Ryc. 9). Ewolucję schematu można przedstawić w postaci ciągu finalnego, którego elementami są kolejno pojawiające się wartości z wierzchołków w kolejno dodanych piramidach. Okazuje się, że w takim układzie również pojawiają się własności i obiekty opisywane poprzednio. Głównym atraktorem układu jest cykl graniczny, choć manipulując odpowiednio danymi wejściowymi, można wymusić dążenie układu do stałej. Jest to jednak problem trudny, według nas statystycznie zaniedbywalny. Pojawiające się oscylacje mają charakter złożony. Można je rozpatrywać i analizować zarówno na przykładzie wspomnianego ciągu prezentującego wierzchołki, jak i w samej strukturze liczbowej, w poszczególnych „kolumnach" powstałych piramid.

Okazuje się, że tutaj również liczba dodanych piramid konieczna do pojawienia się oscylacji może być bardzo różna. Co ciekawe, postać wygenerowanego ciągu finalnego złożonego z wartości w wierzchołkach może być niezgodna z pierwotną intuicją. Przykładem jest pojawiająca się wartość 3 w faktycznie otrzymanym ciągu finalnym:

1 1 1 3 1 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 … (1 0 0 0) – cykl graniczny

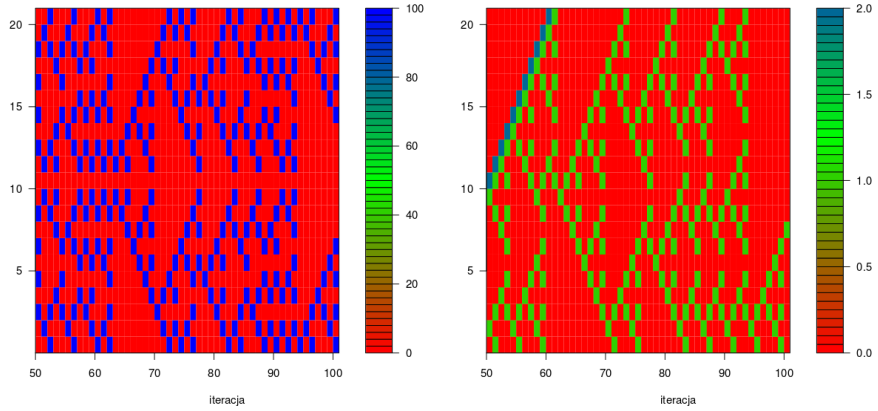
Innym możliwym wariantem schematu jest wprowadzenie modyfikacji w samej procedurze jego ewolucji. Można przykładowo założyć, że schemat oprócz liczenia różnicy bezwzględnej liczb może także obliczać ich sumę. Jak łatwo się domyślić, takie założenie powodować będzie zamiast spadku przyrost wartości liczbowych, zamiast wzrostu uporządkowania struktury – jej spadek. Można jednak liczenie sumy przeprowadzać jedynie wybiórczo, np. co pewną liczbę iteracji. Tym samym schemat stawałby się bardziej złożony, a jego obliczanie mniej trywialne. Szansę dla tej modyfikacji upatrywać można również w propozycji użycia schematu jako algorytmu do szyfrowania danych, o czym traktować będzie jeden z kolejnych punktów.

11. SCHEMAT A TEORIA CHAOSU

Innym wartym uwagi zagadnieniem jest zadanie sobie pytania, Czy zmiana wartości dowolnego elementu tworzonej struktury liczbowej wywiera taki sam efekt na dalszą ewolucję układu. Okazuje się, że nie. Niektóre elementy w tworzonej strukturze, zarówno bardzo złożonej, jak w przykładzie „sumowania" piramid, jak i w prostszych przypadkach macierzowych, wykazują bardzo duże znaczenie dla przebiegu dalszej ewolucji, inne zaś – mniejsze bądź wręcz żadne. Czasem bardzo mała zmiana wartości jednego elementu powoduje drastyczną zmianę na przykład atraktora, do którego zmierzać będzie układ. Często przypadkowa zamiana jedynki na zero lub odwrotnie powoduje zmianę okresu powstających oscylacji lub przebiegunowanie, tzn. zamianę miejscami zer i jedynek w powstałym cyklu granicznym. Analiza opisywanych tutaj struktur pod tym kątem jest bardzo interesująca, niesie skojarzenie z teorią chaosu. Należy jednak nadmienić, iż o ile pewne opisane wcześniej zjawiska, jak pojawiające się pseudo-bifurkacje, zależały od samej struktury algorytmu, o tyle różna wrażliwość ewolucji na dane elementy struktury zależy wprost od wartości liczbowych występujących w tej strukturze (Ryc. 10 i 11).

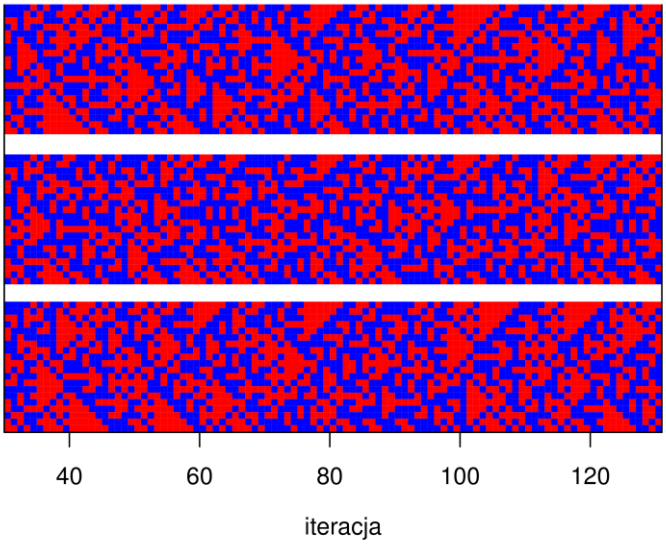
Analizując dogłębnie przebieg schematu i idąc dalej w swych rozważaniach, poszczególne liczby wydają się nam różnie „oddziaływać ze sobą", tzn. przekazywać większy bądź mniejszy potencjał wpływu na dalszą ewolucję układu. Jest to problem bardzo interesujący, ale także bardzo złożony, wykraczający poza ramy niniejszej pracy.

Ryc. 10. Ilustracja czułości układu na zaburzenia. Po lewej ewolucja ciągu postaci $(0)_{10}$ 100 $(0)_{10}$, po prawej $(0)_{10}$ 100 1 $(0)_9$, gdzie liczby w dolnym indeksie oznaczają wielokrotności danych elementów



Źródło: Opracowanie własne

Ryc. 11. Druga ilustracja czułości układu na zaburzenia w przypadku użycia liczb losowych. U góry rysunek uzyskany na podstawie oryginalnego ciągu, w środku w początkowym ciągu zmieniono pierwszy element o 1, na dole zmieniono drugi element o 1 (wartości: czerwone: 0, niebieskie: 1) [wersja kolorowa dostępna online]



Źródło: Opracowanie własne

11. SCHEMAT RÓŻNICOWY JAKO POTENCJALNA FUNKCJA JEDNOKIERUNKOWA

Funkcja jednokierunkowa – funkcja, która jest łatwa do wyliczenia (istnieje algorytm liczący jej wartości), natomiast niemożliwa do odwrócenia (nie istnieje algorytm pozwalający na otrzymanie elementu przeciwobrazu z prawdopodobieństwem większym niż zaniedbywalne[4].

Istnienie funkcji jednokierunkowych jest otwartym problemem w informatyce. W praktyce stosuje się funkcje słabo jednokierunkowe, tzn. umożliwiające odwrócenie funkcji (znalezienie przeciwobrazu), ale z jednoczesną koniecznością wykonania wielu obliczeń. Funkcje te znajdują zastosowanie w kryptografii, do szyfrowania danych. Obecnie wiele popularnych kryptosystemów opiera się na wykorzystaniu mnożenia dwóch dużych liczb pierwszych jako potencjalnej funkcji jednokierunkowej. Okazuje się, że wyliczenie iloczynu dwóch nawet bardzo dużych liczb jest bardzo proste, natomiast operacja odwrotna, czyli faktoryzacja, jest problemem bardzo złożonym. Zakłada się, że udane łamanie szyfrów opartych o faktoryzację będzie możliwe po skonstruowaniu komputera kwantowego.

Schemat różnicowy spełnia w pewnej mierze warunki stawiane potencjalnej funkcji jednokierunkowej. Dowolną informację można zapisać w postaci ciągu liczbowego, który może stać się wejściem schematu. W wyniku ewolucji generowane są kolejne ciągi liczb, aż do osiągnięcia danego atraktora, przykładowo cyklu granicznego. Znalezienie cyklu granicznego jest trywialne obliczeniowo, natomiast znalezienie przeciwobrazu, czyli ciągu wejściowego jest w gruncie rzeczy niemożliwe. Nie oznacza to jednakże, że schemat jest doskonałą funkcją jednokierunkową, albowiem do danego cyklu granicznego prowadzić może nieskończona liczba trajektorii. Znalezienie jednej konkretnej, która miałaby prowadzić do ciągu przedstawiającego informację poddaną szyfryzacji jest więc niewykonalne.

Być może jednak odpowiednio zmodyfikowana postać schematu połączona z utajoną procedurą szyfryzacji danych, pozwalającą na odzysk informacji zaszyfrowanej, mogłaby posłużyć jako alternatywa dla obecnych algorytmów kryptograficznych. Warta podkreślenia jest prostota całego schematu, a także możliwość wprowadzania różnych modyfikacji, jak liczenie różnicy bądź sumy liczb, różna geometria układu, a także możliwość podziału ciągów na mniejsze podjednostki.

[4] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, CRC Press 2007.

13. SCHEMAT RÓŻNICOWY JAKO AUTOMAT KOMÓRKOWY

Automat komórkowy to system składający się z pojedynczych komórek, znajdujących się obok siebie. Ich układ przypomina szachownicę lub planszę do gry. Każda z komórek może przyjąć jeden ze stanów, przy czym liczba stanów jest skończona, ale dowolnie duża. Stan komórki zmieniany jest synchronicznie, zgodnie z regułami mówiącymi, w jaki sposób nowy stan komórki zależy od jej obecnego stanu i stanu jej sąsiadów.

Zgodnie z powyższą definicją zaproponowany przez nas schemat różnicowy może być rozpatrywany jako jeden z przykładów automatu komórkowego[5]. Idea schematu różnicowego, a także generowane przez niego struktury i zachowania zostały zaobserwowane i opisane jeszcze bez wiedzy autorów o istnieniu automatów komórkowych. Okazuje się, że przedstawione przez autorów reguły prowadzenia iteracji i uzyskiwane wyniki były już wiele lat temu intensywnie badane i opisywane pod hasłem jednowymiarowych automatów komórkowych. Przykładowo tzw. *Rule 90* prezentuje schemat iteracyjny bardzo zbliżony do zaproponowanego przez autorów niniejszej pracy. Struktury opisywane tutaj jako rozwidlenia dychotomiczne zbieżne są z tzw. *stunted trees and triangular clearings*, strukturami generowanymi m.in. przez *Rule 90*. Ponadto klasyfikacja automatów komórkowych dokonana przez Wolframa[8] jest w pewien sposób zbliżona do zaproponowanej w tym artykule klasyfikacji atraktorów opisywanego układu. Kolejnym aspektem wartym podkreślenia jest postulowane użycia automatów komórkowych jako funkcji jednokierunkowych w celu szyfryzacji danych, co również zostało niezależnie zaproponowane przez autorów. Reasumując, autorzy pracy są wdzięczni recenzentom za zwrócenie ich uwagi i zainteresowanie tematem automatów komórkowych, bez czego niemożliwa byłaby rzetelna klasyfikacja omawianych tutaj struktur i zachowań**,** uwzględniając wcześniejsze dokonania.

14. REFLEKSJA FILOZOFICZNA

Czym jest otaczająca nas rzeczywistość? Czasami skłonni jesteśmy przyznać, że to, co odbieramy naszymi zmysłami, to niekończące się potoki informacji, zera i jedynki dopływające do naszych narządów zmysłów, które dopiero odpowiednio przetransformowane przez nasz mózg stwarzają wrażenie obrazów,

[5] A. Adamatzky, *Game of Life Cellular Automata*, Springer 2010; J. von Neumann, *The Theory of Self-reproducing Automata*, ed. A. Burks, Illinois 1966; S. Wolfram, *A New Kind of Science*, Wolfram Media 2002.

dźwięków, smaków i zapachów. Czyż więc nasza rzeczywistość jest swoistym *matriksem*?

Uderzającym argumentem jest to, jak łatwo obrazy i dźwięki przetłumaczyć na język bitów. Tak właśnie działają kamery, mikrofony, aparaty cyfrowe. Powstały zapis łatwo odtworzyć i uzyskać w zasadzie niemożliwe do odróżnienia obrazy i dźwięki uprzednio zakodowane. Skłonni jesteśmy przyznać, że naszą rzeczywistość można potraktować jako swoistą, niebywale skomplikowaną matrycę danych dopływających w sposób ciągły rozlicznymi strumieniami.

Gdy analizujemy przebieg schematu różnicowego, przychodzi nam na myśl pewna refleksja. Może istnieje analogiczna do naszego schematu ścieżka, którą podążając moglibyśmy zagłębić się w macierzy naszej rzeczywistości, przejść do najprostszych, „zero-jedynkowych" jakości, dostrzec ukryte z naszego punktu widzenia zjawiska i własności. Może taką właśnie własnością jest ukryta, immanentna cykliczność. Może te wszystkie ruchy oscylacyjne atomów i cząstek elementarnych, a także oscylacje wyższych stopni, jak cykle metaboliczne, komórkowe, fale akustyczne, stanowią coś na wzór atraktorów pojawiających się w ewolucji naszego algorytmu. Może tą ścieżką jest właśnie refleksja nad naszym światem, jego rozbiór na czynniki pierwsze, próba wydzielenia z tej skomplikowanej macierzy tego, co najbardziej pierwotne i najprostsze. Naszym zdaniem na najbardziej substancjalnym poziomie istnieją pewne pierwotne jakości, pierwotne ładunki, „+" i „–", to właśnie one, następując po sobie, wyznaczają pierwotny rytm, najbardziej substancjalne cykliczności, które następnie interferują, łączą się, wzmacniają lub wygaszają, przy okazji tworząc obiekty emergentne, analogiczne do rozwidleń dychotomicznych czy obiektów *ping-pong*. Może nimi właśnie są obiekty naszego świata i my sami...

Skrypt do programu symulującego działanie schematu różnicowego napisanego w języku R wraz z objaśnieniami jak z niego skorzystać jest dostępny pod adresem: www2.chemia.uj.edu.pl/~seidler/R.

THE DIFFERENTIAL PATTERN

The aim of this work is to present the prosperities of a certain iterative pattern, which we have called the „differential pattern". It operates through a subtraction of the two adjoining elements of the sequence and returning of their absolute difference, used subsequently in the next steps. The whole procedure can be prolonged, enabling the investigation of the generated sequences. The pattern generates two-dimensional matrixes and the numerical structures of a higher level.

The evolution of the pattern leads to various possible behaviours, among which characteristic attractors may be mentioned. They can be the limit cycles, i.e. oscillations appearing after the certain number of iterations, which may be constant or continuously silenced. Another type of a possible attractor is a constant number, which is usually zero. Interestingly enough, the type of attractor toward which the pattern leads may depend on the number of

elements in a single sequence, or the assumed edge conditions. It is a peculiar pseudo-bifurcation dependent on the parameters of generated structure, appearing regardless of the value of the elements filling the created numerical structure.

During the pattern evolution, complex oscillations have also been observed, i.e. those exerting a different frequency. For instance, in a 5-element sequence, a distinct frequency of oscillations tends to appear on the third position.

The visualisation of the pattern has been attempted with the use of R-packet, so it was possible to observe that the pattern generates more complex structures, exerting some level of order. Some behaviours are emerging only after reaching the specific level of complexity. These characteristic objects are dychotomic forks resembling the lightings, or other behaviours whoch we have called 'ping-pong objects'.

The last aspect of this work is the presentation of the differential pattern as a potential candidate for a one-way function, i.e. the procedure possible to be applied in data coding.

A distinct section of this article has also been devoted to discuss the pattern as a particular type of cellular automata, about which the authors did not know until the article's review.

BIBLIOGRAFIA

1. Adamatzky A., *Game of Life Cellular Automata*, Springer 2010.
2. Blanchard P., Devaney R. L., Hall R. G., *Differential Equations*, London 2006.
3. Coveney P., Highfield R., *Granice złożoności. Poszukiwania porządku w chaotycznym świecie*, tłum. P. Amsterdamski, Warszawa 1997.
4. Haken H., *Synergetics. Introduction and Advanced Topics*, Springer 2004.
5. http://en.wikipedia.org/wiki/Rule_90
6. Katz J., Lindell Y., *Introduction to Modern Cryptography*, CRC Press 2007.
7. Murray J. D., *Wprowadzenie do biomatematyki*, tłum. U. Foryś, M. Bodnar, Warszawa 2007.
8. von Neumann J., *The Theory of Self-reproducing Automata*, ed. A. Burks, Illinois 1966.
9. Wolfram S., *A New Kind of Science*, Wolfram Media 2002.