

Deterministický chaos jako generátor náhodných čísel v prostředí C a C++

Deterministic chaos as a generator of random numbers in the C and C++ environment

Radovan Fuchs

Bakalářská práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Radovan FUCHS**
Osobní číslo: **A09634**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační a řídicí technologie**

Téma práce: **Deterministický chaos jako generátor náhodných čísel v prostředí C a C++**

Zásady pro vypracování:

1. Vypracujte literární řešení na dané téma.
2. Vytvořte v programovacím prostředí C nebo C++ aplikace pro generování náhodných čísel pomocí zvolených chaotických systémů.
3. Proveďte statistické porovnání pro jednotlivé chaotické systémy a mezi jinými generátory náhodných čísel.
4. Diskutujte a navrhněte možnosti využití v praxi, např. pro kryptografické techniky či moderní metody softcomputingu.

Rozsah diplomové práce: \

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. PRATA, Stephen. Mistrovství v C++. Computer Press, 2007. 1120 s. ISBN 9788025117491.
2. VIRIUS, Miroslav. 1001 tipů a triků pro C++. Computer Press, 2011. 472 s. ISBN: 9788025129418.
3. GILMORE, R.; LEFRANC, M. The Topology of Chaos. Willey VCH, 2002. 518 s. ISBN 978-0-471-40816-1.
4. DOSTÁL, Radim. C, C++ Hotová řešení. . Computer Press, 2010. 376 s. ISBN: 9788025121900.
5. GLEICK, James. Chaos: vznik nové vědy. Ando Publishing, 1996. 350s. ISBN 80-86047-04-0.
6. HORÁK, Jiří. Deterministický chaos a jeho fyzikální aplikace. Academia, 2003. 437 s. ISBN 8020009108.

Vedoucí diplomové práce:

Ing. Roman Šenkeřík, Ph.D.

Ústav informatiky a umělé inteligence

Datum zadání diplomové práce:

24. února 2012

Termín odevzdání diplomové práce:

8. června 2012

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan



prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je vytvoření použitelné aplikace implementované v prostředí C++ pro využívání dynamických systémů, které vykazují známky chaotického chování, ke generování posloupností náhodných čísel. Následně je otestována použitelnost tohoto řešení. Teoretická část této práce obsahuje základní popis deterministického chaosu a generátorů náhodných čísel. V praktické části je pak popsána vytvořená aplikace a testy využitých chaotických systémů.

Klíčová slova: deterministický chaos, generátor náhodných čísel

ABSTRACT

The aim of this thesis is to create a usable application implemented in C++ environment to use dynamic systems that show signs of chaotic behavior to generate random number sequences. Subsequently the applicability of this solution is tested. The theoretical part of this thesis provides a basic description of deterministic chaos and random number generators. In the practical part there is described the created application and utilized tests of chaotic systems.

Keywords: Deterministic chaos, Random number generator

Chtěl bych poděkovat vedoucímu práce Ing. Romanu Šenkeříkovi, Ph.D. za poskytnuté rady při tvorbě této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	9
I TEORETICKÁ ČÁST	10
1 DETERMINISTICKÝ CHAOS	11
1.1 HISTORICKÝ VÝVOJ	11
1.2 ZÁKLADNÍ POHLED	12
1.3 BIFURKAČNÍ DIAGRAM	13
1.4 LOGISTICKÁ ROVNICE.....	14
1.5 LORENZŮV MODEL	16
1.6 DISIPATIVNÍ SYSTÉMY	18
1.7 LJAPUNOVŮV EXPONENT	18
1.8 PŘEHLED VYBRANÝCH CHAOTICKÝCH SYSTÉMŮ	20
1.9 HÉNONOVA MAPA	22
2 GENERÁTOR NÁHODNÝCH ČÍSEL	24
2.1 SKUTEČNĚ NÁHODNÉ A PSEUDONÁHODNÉ SEKVENCE GENEROVANÝCH ČÍSEL	25
2.2 DEFINICE GENERÁTORU.....	26
2.3 GENERÁTOR NÁHODNÝCH ČÍSEL S ROVNOMĚRNÝM ROZDĚLENÍM.....	26
2.4 GENERÁTORY NÁHODNÝCH ČÍSEL ZALOŽENÉ NA CHAOTICKÝCH SYSTÉMECH.....	27
II PRAKTICKÁ ČÁST	28
3 POPIS PROGRAMU	29
3.1 POPIS IMPLEMENTACE	31
3.1.1 Vstupy	31
3.1.2 Chaotické systémy	31
3.1.3 Generování výstupních hodnot	32
4 SROVNÁNÍ CHAOTICKÝCH SYSTÉMŮ	34
4.1 NASTAVENÍ PARAMETRŮ	34
4.2 LOZI	34
4.3 SINAI.....	36
4.4 ARNOLD CAT MAP	36
4.5 IKEDA.....	37
4.6 HÉNONOVA MAP.....	38
4.7 HOLMES CUBIC MAP	39
4.8 BURGERS MAP	40
4.9 CHIRIKOV	41
4.10 DISIPATIVNÍ SYSTÉM	42
4.11 POROVNÁNÍ SYSTÉMŮ	43
5 MOŽNOSTI REÁLNÉHO VYUŽITÍ	44
ZÁVĚR	45
ZÁVĚR V ANGLIČTINĚ	46
SEZNAM POUŽITÉ LITERATURY	47
SEZNAM OBRÁZKŮ	49

SEZNAM TABULEK.....	50
SEZNAM PŘÍLOH.....	51

ÚVOD

V posledních několika letech se vyvinul velice zajímavý vztah mezi chaosem a kryptografií. Výsledkem této kombinace bylo rozvinutí několika šifrovacích systémů založených na teorii chaosu. Jednou z vlastností, kterou by měly tyto dnešní počítačové systémy poskytovat je schopnost generovat náhodná čísla. Toto je hlavní nutností zvláště v různých vědních disciplínách, kde se ukazuje nutnost používání dobrých generátorů. Během let bylo vytvořeno mnoho generátorů náhodných čísel, ale většina z nich generuje výstupy, které nebývají zcela náhodné.

Cílem této práce je vytvořit aplikaci, která by byla použitelná pro využívání dynamických systémů vykazujících známky chaosu ke generování pseudonáhodných hodnot srovnatelných s výstupem běžně používaných generátorů náhodných čísel.

I. TEORETICKÁ ČÁST

1 DETERMINISTICKÝ CHAOS

1.1 Historický vývoj

Téměř ve všech soustavách, které se pokoušely vysvětlit podstatu a vznik vesmíru, hrála důležitou roli idea chaosu. Ve starověkém Řecku byl chaos považován za prázdnotu mezi nebem a zemí, z níž se zrodil svět. Ve středověku pak převládala myšlenka stálosti a neměnnosti, která byla podle newtonské fyziky založena na neměnnosti matematických přírodních zákonů shrnutých společně s dalšími aspekty v zákonu o zachování energie a hmoty. Základy k novému chápání světa, umožňujícímu odklon od stávající teorie pořádku, položil Galileo Galilei.[1]

V 19. Století se stále věřilo tomu, že žádné neurčitosti neexistují. Až s příchodem kvantové mechaniky byl znovu objeven indeterminismus v přírodě. Za jednu z nejznámějších stop vedoucích z tohoto období je považován objev E. N. Lorenze. Ten se intenzivně zabýval modelováním nepředvídatelnosti a neperiodičnosti chování počasí a následně objevil tzv. „motýlí efekt“. Tento objev prezentoval v 60. letech. Motýlí efekt ukazuje nemožnost dlouhodobé předpovědi počasí a tím jeho chaotičnost. Lorenzův atraktor je dnes symbolem chaosu.

V 70. letech Lorenz objevil deterministický chaos při zkoumání jednoho modelu počasí, kdy při nastavení přibližně stejných počátečních podmínek docházel po určitém čase k různým výsledkům. Poukázal tím na citlivost mnoha systémů na počáteční podmínky a díky tomu jejich schopnost generovat výsledky, které můžeme označit za chaotické.[1]

Základem současné vědy o chaosu, aplikované stále častěji k řešení konkrétních problémů je uvažování o reálném světě jako o nelineárním a nespojitém systému. Tyto systémy nejsou oproti tradiční vědě považovány za výjimky, ale jsou označeny za normu. O chaotickém chování takového systému lze hovořit, pokud vzdálenost jeho sousedních stavů exponenciálně roste.[2]

1.2 Základní pohled

Základním principem deterministického chaosu je soustava diferenciálních rovnic, která je charakterizována svým chaotickým chováním. Výzkum chaosu je v dnešní době slibný vědecký směr s možností praktického uplatnění (využití v kryptografii, při přenosu informací). [1]

Existuje mnoho definicí chaotického chování. Ve většině z nich jsou za chaotický proces považována řešení diferenciálních nebo diferenčních rovnic, která jsou charakterizována lokální nestabilitou a globálním omezením. Znamená to, že řešení, která mají nepatrně odlišné počáteční podmínky, mohou po určité době divergovat k nekonečné vzdálenosti. [3]

Chaotické chování na první pohled vypadá pro běžného pozorovatele jako naprosto náhodný systém, na který působí vnější náhodný šum. Případně může tento systém být také ovlivněn složitostí systému při mnoha stupních volnosti. Bylo dokázáno, že ke generování chaotického chování nejsou potřeba složité systémy, ale stačí i velmi jednoduché systémy téměř neobsahující šum.

Různé náhle a nepředvídatelné změny v systémech mohou způsobit vznik chaotického chování. Chaotický systém je obecně definován pomocí:

- a) Časově závislé rovnice
- b) Hodnoty parametrů popisující systém
- c) Počáteční podmínky

Systém lze nazvat deterministickým, pokud jsme schopni při znalosti všech 3 výše uvedených bodů určit následující (a případně i minulé) stavy systému. Důležitou roli v těchto systémech hraje nelinearita systému, způsobující odezvu systému. Systém můžeme nazvat nelineárním, pokud v něm provedeme určitou změnu, ale nedocílíme očekávané odezvy. [3]

Chaotické systémy můžeme rozdělit na spojité a diskrétní systémy. Vzhledem k problematice náhodných čísel budou dále zkoumány převážně systémy diskrétní.

Systém se znaky deterministického chaosu je možné definovat pomocí 3 základních podmínek:

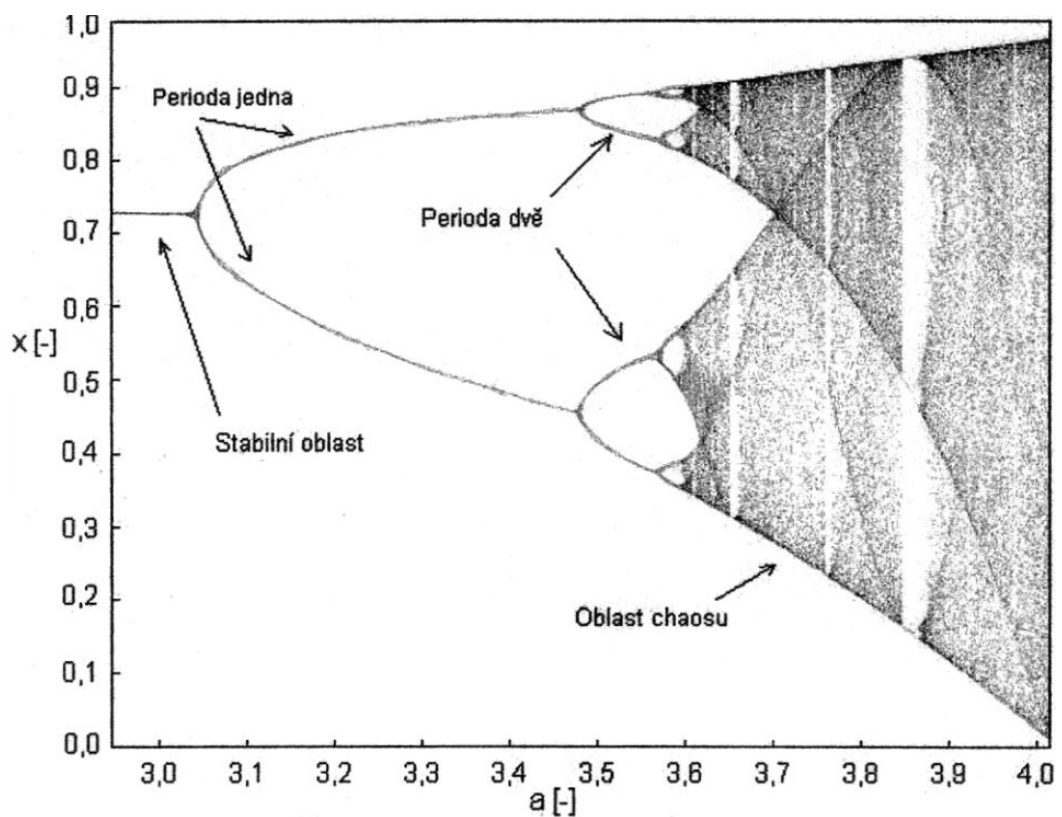
- a) Veliká citlivost na počátečních podmínkách
- b) Hustá množina periodických bodů
- c) Tranzitivita

Jedním z důvodů, proč se v dnešní době tolik vědců z různých vědních oborů zajímá o chaos je, že chaotické chování se ukazuje jako velmi univerzální. Znamky tohoto chování můžeme nalézt v různých vědních disciplínách jako např. v elektronice (nežádoucí rušení), chemii a mnoha dalších.[3]

1.3 Bifurkační diagram

Pro zobrazování chaotického chování se používá bifurkačních diagramů. Jde o graf zobrazující závislost chování systému na řídicím parametru. Ukázkou bifurkačního diagramu nalezneme na obr. 1. Při pohledu na bifurkační diagram vidíme v částech grafu plné křivky, které znázorňují ustálený stav systému. [4]

Naopak široké skvrny plné rozptýlených bodů označují, že systém v této části vykazuje chaotické chování. Samotným pojmem bifurkace označujeme jev, kdy dochází ke změně vnitřního stavu systému při nepatrných změnách jednoho ze vstupních parametrů, zatímco ostatní zůstávají zachovány. Na obrázku 1 je uveden příklad bifurkačního diagramu, kde x je výstupní proměnnou a a je kontrolním parametrem.[1]



Obrázek 1 Příklad bifurkačního diagramu

1.4 Logistická rovnice

Logistická rovnice je jedním z velice jednoduchých modelů deterministického chaosu a je možné tento model označit za spojité v čase. Běžně používané jsou však také logistické mapy, což jsou modifikované logistické rovnice. Rovnice vznikla pro potřeby simulace biologických procesů jako například chování různých živočišných druhů v jejich přirozeném prostředí. Příkladem takového procesu může být soužití 2 druhů v uzavřeném prostředí, kdy jeden druh slouží jako potrava druhého. Následkem bude to, že konzumovaný druh bude decimován. Ale Jakmile bude jedinců tohoto druhu nedostatek, bude naopak vymírat hlady opačný druh, díky čemuž opět dojde ke zvýšení počtu jedinců prvního druhu. Z popisu je zřejmé, že populace obou druhů budou periodicky oscilovat, nebo se ustálí na konstantní hodnotě. Na základě simulací bylo dokázáno, že takový systém může vykazovat velmi složité chaotické chování. [4]

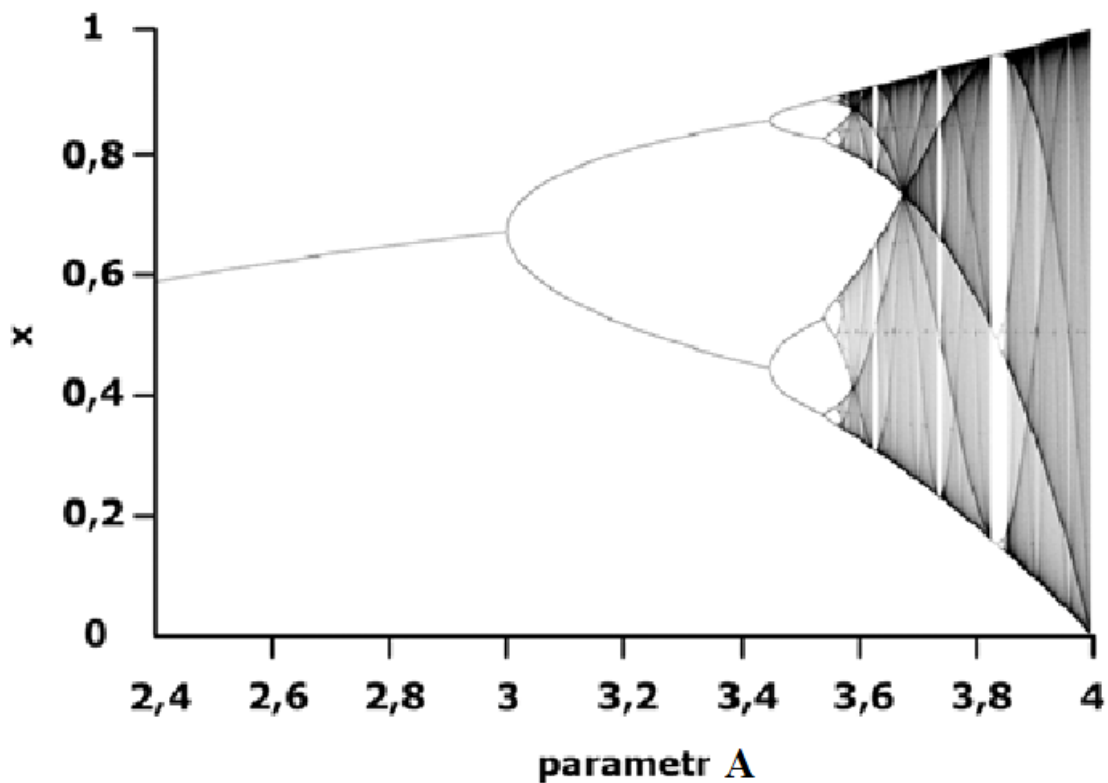
$$x_{n+1} = Ax_n(1 - x_n) \equiv f_a(x_n) \quad (1)$$

V tomto matematickém zápisu logistické rovnice je pomocí hodnoty x_n vyjádřena populace v n -tém roce. Tuto funkci je možné označit za iterační, protože k dosažení použitelných výsledků je potřeba provést určitý počet iterací. Pokud pomocí iterace vygenerujeme sekvenci hodnot x , dostáváme trajektorii (orbit). Počátky trajektorií obvykle závisí na zvolené počáteční hodnotě x . Další průběhy trajektorií jsou však stejné pro téměř libovolně zvolené počáteční hodnoty x v intervalu $[0,1]$. Některé z těchto počátečních hodnot x se však od ostatních odlišují. Příkladem může být, pokud nastavíme počáteční hodnotu na 0. Hodnota funkce pak bude 0 a na této hodnotě vzhledem k definici rovnice zůstane i v následujících iteracích. Tyto hodnoty x , které po dosazení do iterační funkce generují stejný výsledek jako je jejich hodnota, jsou nazývány fixními body. Ty lze definovat následujícím vztahem. [3]

$$x_A = f_A(x_A) \quad (2)$$

Pokud se všechny trajektorie pro určité počáteční hodnoty s rostoucím počtem iterací přibližují danému bodu, pak je tento bod nazván atraktorem. Obecně je atraktorem definován jako množina bodů, ke které jsou trajektorie přitahovány v souvislosti s počtem iterací, blížícím se k nekonečnu. Domény přitažlivosti pak obsahují počáteční body, které dávají vznik trajektoriím, jež se přibližují atraktoru. Princip atraktoru spočívá v tom, že

jsou veškeré údaje o systému zredukovány do jednoho bodu, který je po každé změně systému posunut. U chaotických systémů, jejichž chování je nepředvídatelné, nemůžeme krátkodobě říct, ve které oblasti fázového prostoru se objeví další bod popisující stav systému v následujícím okamžiku. Zajímavá je však skutečnost, že z dlouhodobého hlediska představují toto možné chování pouze body nacházející se na atraktoru. Na obr. 2 je vykreslen bifurkační diagram logistické rovnice. Vidíme, že pro hodnoty $A < 1$ je atraktorem $x=0$. Pro $1 < A < 3$ je atraktorem fixní bod $x=1 - \frac{1}{A}$. Pro A blíží se 4 pozorujeme chaotické chování systému.[3]



Obrázek 2 Bifurkační diagram Logistické rovnice

1.5 Lorenzův model

Tento model byl prezentován roku 1963 meteorologem Edwardem Lorenzem a jde o zjednodušený model cirkulace kapaliny v malé idealizované nádobě. Lorenzův model popisuje atmosféru jako vrstvu, která je zesponu ohřívána a z horní části chlazena. Dolní část atmosféry má teplotu označovanou T_w , která je vyšší než teplota horního okraje označovaná T_C . U modelu se předpokládá, že rozdíl teplot $\delta T \equiv T_w - T_C$ je udržován na konstantní hodnotě. [5]

Dokud není rozdíl teplot příliš velký, je teplo odváděno nahoru a předáváno okolnímu médium. Díky tomu lineárně klesá teplota z hodnoty T_w na hodnotu T_C . Jakmile dosáhne rozdíl teplot požadované hodnoty, dostane se teplá kapalina až na vrchol, kde zchladne. Následkem toho poklesne dolů, kde se opět začíná ohřívát a kapalina bude takto opakovaně cirkulovat. Při ještě vyšším rozdílu teplot se začnou cirkulační proudy a výsledné teplotní rozdíly $T_w - T_C$ měnit v závislosti na čase. To je typickým příkladem nelineárního chování. I přesto, že je prostředí v čase stabilní, systém spontánně vykazuje časově závislé chování. Tento systém je popsán následujícími rovnicemi. [6]

$$\frac{dx}{dt} = \sigma(y - x) \quad (3)$$

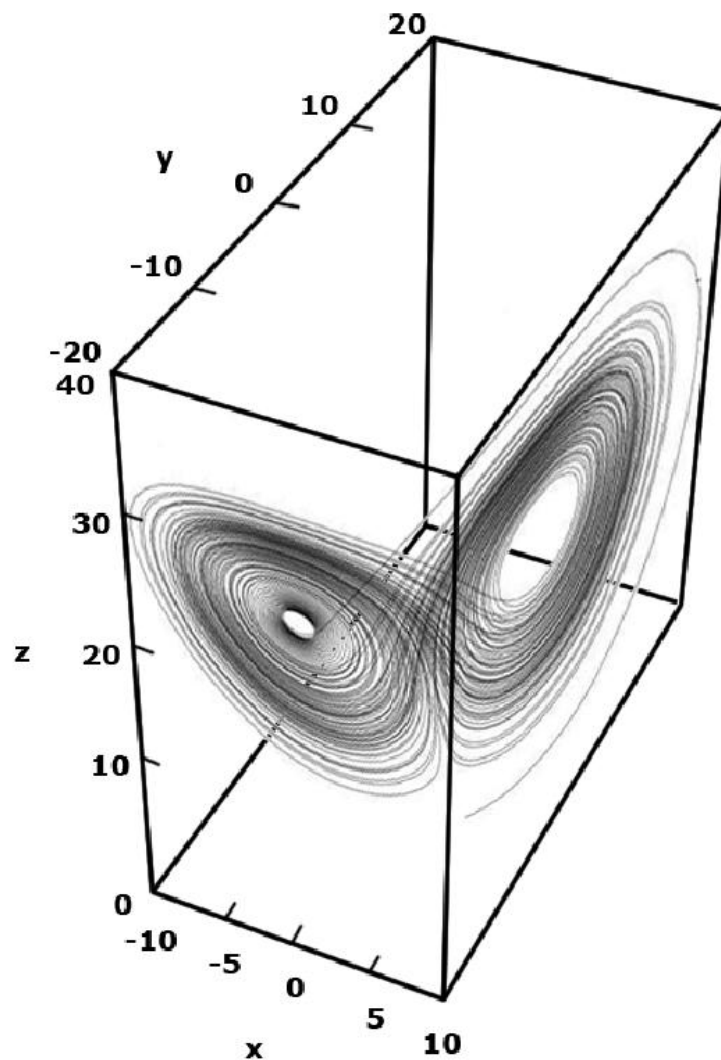
$$\frac{dy}{dt} = x(r - z) - y \quad (4)$$

$$\frac{dz}{dt} = xy - \beta z \quad (5)$$

kde σ je Prandtovo číslo, jehož hodnota je závislá na vlastnostech kapaliny a r je Rayleighovo číslo, pro které platí, že aby docházelo k cirkulaci kapaliny musí být větší než 1. [6]

Atraktor příslušející tomuto systému je zobrazen na obrázku níže a je prvním z tzv. „podivných atraktorů“.

Lorenzův atraktor



Obrázek 3 *Lorenzův atraktor*

1.6 Disipativní systémy

Zvláštní pozornost si zaslouží tzv. disipativní systémy, tj. systémy, které mají tu vlastnost, že ať se počáteční stav nachází kdekoli (v určité oblasti, tzv. oblasti přitažlivosti) ve fázovém prostoru, s rostoucím časem se trajektorie stahují do určité části tohoto prostoru s nulovým objemem. Jsou těmito oblastmi, zvanými atraktory, přitahovány. Atraktory souvisí s limitním chováním se systémů po odeznění přechodových jevů v čase $t \rightarrow \infty$. Charakter tohoto limitního chování může podstatně záviset na hodnotách řídicích parametrů. Při jejich změně dochází při určitých kritických hodnotách k náhlé kvalitativní změně v typu atraktoru a druhu pohybu. Takovému jevu se říká bifurkace.[1]

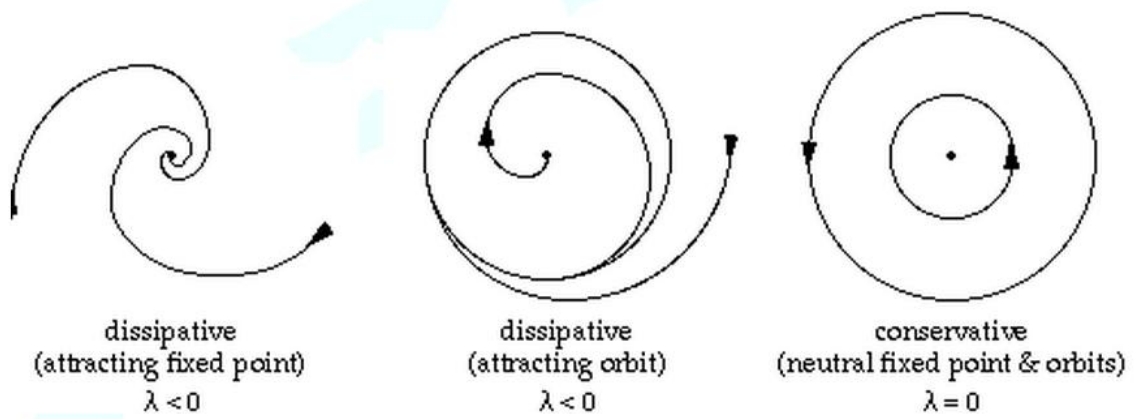
Nejjednodušším atraktorem je bod, který odpovídá stavu klidu. Hodnoty veličin $X_i(t)$ se přibližují jistým hodnotám a v čase poté se již nemění. Příkladem může být pohyb kyvadla, které se v důsledku tření a znehodnocování mechanické energie třením na teplo (tj. disipací) posléze zastaví. Poloha ani rychlost se pak již nemění. Jiným příkladem možného atraktoru je uzavřená orbita (tzv. limitní cyklus), podél níž systém trvale obíhá. Ilustrací je kyvadlo hodin, kterému je trvale dodávána energie zvenčí poklesem závaží či z elektrické baterie. Takový systém je disipativní, znehodnocuje energii, ta je však trvale doplňována. Systém je ovšem otevřený, je v kontaktu s okolím.[1]

1.7 Ljapunovův exponent

Ljapunovův exponent je měřítkem divergence blízkých trajektorií a je označován symbolem λ . Jedná se tedy o kvantitativní měřítko chaotičnosti a s jeho pomocí je možné rozlišit chaotičnost od šumu. Tento exponent je možné využít jak pro diskrétní, tak i pro spojité systémy. Ljapunovův exponent je definován pomocí vzorce:[4]

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \log_2 \frac{dx_{n+1}}{dx_n} \quad (6)$$

Pro záporné hodnoty tohoto exponentu je trajektorie přitahována do jednoho bodu. Tyto hodnoty jsou také známkou disipativních systémů. Takovéto systémy vykazují asymptotickou stabilitu, která roste se snižujícím se exponentem. Nulovou hodnota Ljapunovova exponentu vykazují konzervativní systémy v klidovém stavu, nacházející se ve stavu Ljapunovské stability. Pokud je exponent kladný jedná se o chaotický a nestabilní systém, jehož trajektorie bez ohledu na svou vzdálenost budou divergovat. Toto je zobrazeno na obrázku 4.[4]



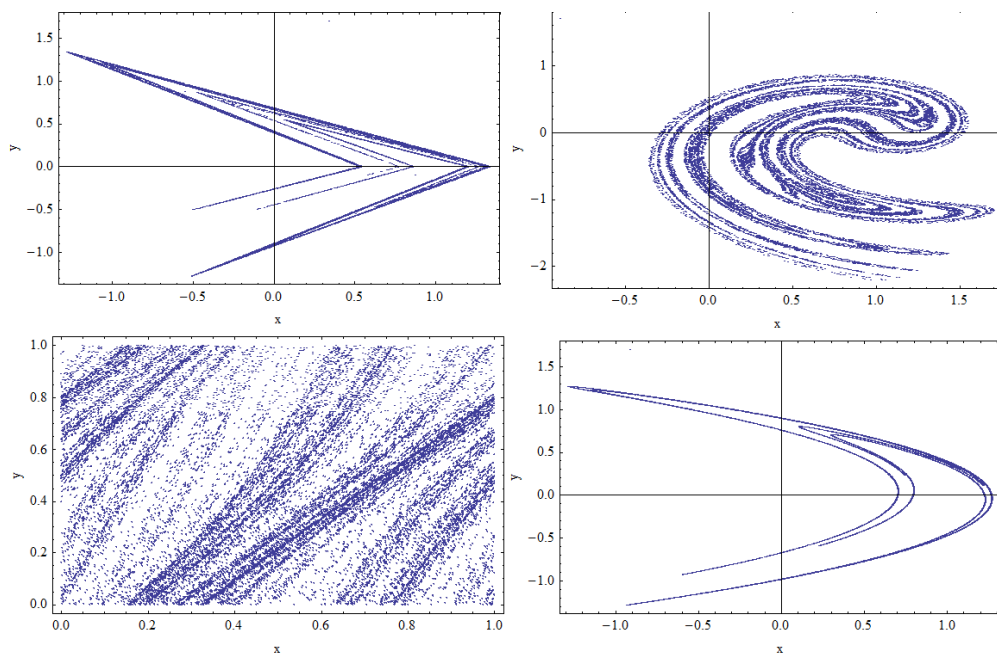
Obrázek 4 Trajektorie s hodnotami Ljapunovského exponentu[4]

1.8 Přehled vybraných chaotických systémů

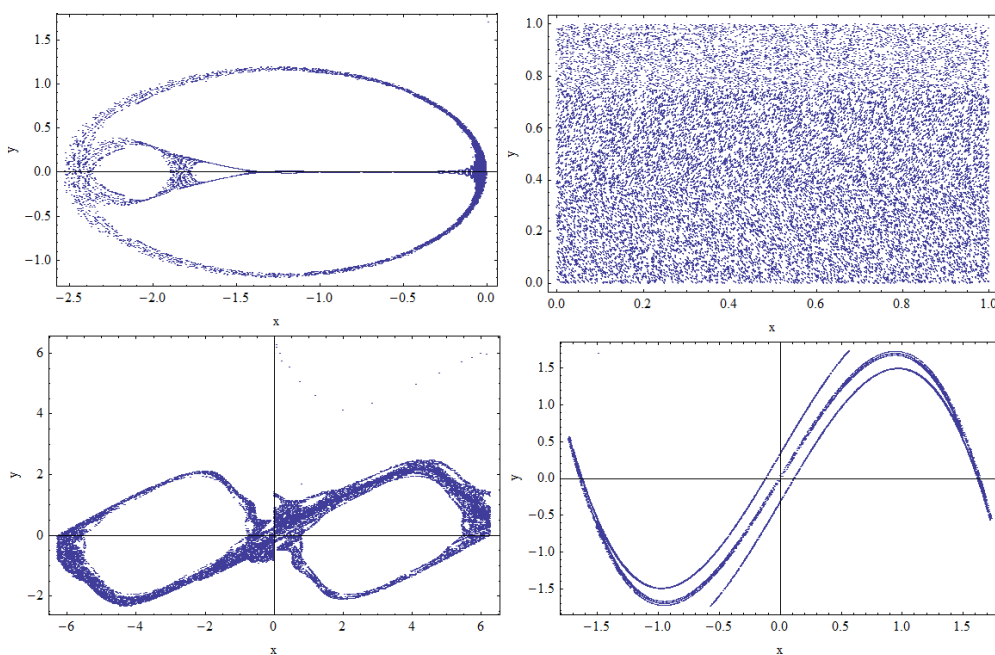
V následující tabulce jsou uvedeny definující matematické zápisy chaotických systémů, nejčastější hodnoty vstupních parametrů a počátečních podmínek, kdy tyto systémy vykazují chaotické chování. [7] Na obrázcích 5, 6 a 7 jsou zobrazeny atraktory těchto systémů.

Tabulka 1 Přehled vybraných chaotických systémů

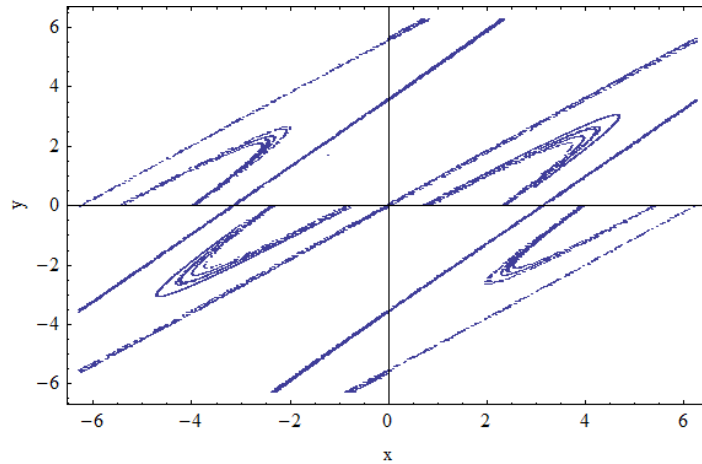
Systém	Matematický zápis	Parametry	Poč. podmínky
Lozi	$X_{n+1} = 1 + a X_n + bY_n$ $Y_{n+1} = X_n$	$a = 1,7 ; b = 0,5$	$X_0 = -0,1$ $Y_0 = 0,1$
Ikeda	$X_{n+1} = \gamma + \mu(X_n \cos \Phi - Y_n \sin \Phi)$ $Y_{n+1} = \mu(X_n \sin \Phi + Y_n \cos \Phi)$ $\Phi = \beta - \frac{\alpha}{1 + X_n^2 + Y_n^2}$	$\alpha = 6 ; \beta = 0,4$ $\gamma = 1 ; \mu = 0,9$	$X_0 = 0$ $Y_0 = 0$
Sinai	$X_{n+1} = X_n + Y_n + \delta \cos 2\pi Y_n (\text{mod } 1)$ $Y_{n+1} = X_n + 2Y_n (\text{mod } 1)$	$\delta = 0,1$	$X_0 = 0,5$ $Y_0 = 0,5$
Hénon map	$X_{n+1} = 1 - aX_n^2 + bY_n$ $Y_{n+1} = X_n$	$a = 1,4 ; b = 0,3$	$X_0 = 0$ $Y_0 = 0,9$
Burgers map	$X_{n+1} = aX_n - Y_n^2$ $Y_{n+1} = bY_n + X_n Y_n$	$a = 0,75 ;$ $b = 1,75$	$X_0 = -0,1$ $Y_0 = 0,1$
Holmes cubic map	$X_{n+1} = Y_n$ $Y_{n+1} = -bX_n + dY_n - Y_n^3$	$b = 0,2 ; d = 2,77$	$X_0 = 1,6$ $Y_0 = 0$
Disipative	$X_{n+1} = X_n + Y_{n+1} (\text{mod } 2\pi)$ $Y_{n+1} = bY_n + k \sin X_n (\text{mod } 2\pi)$	$b = 0,1 ; k = 8,8$	$X_0 = 0,1$ $Y_0 = 0,1$
Arnold cat	$X_{n+1} = X_n + Y_n (\text{mod } 1)$ $Y_{n+1} = X_n + kY_n (\text{mod } 1)$	$k = 2$	$X_0 = 0$ $Y_0 = \frac{1}{\sqrt{2}}$
Chirikov	$X_{n+1} = X_n + Y_{n+1} (\text{mod } 2\pi)$ $Y_{n+1} = Y_n + k \sin X_n (\text{mod } 2\pi)$	$k = 1$	$X_0 = 0$ $Y_0 = 6$



Obrázek 5 Atraktory systémů. Zleva doprava a shora dolů: Lozi, Ikeda, Sinai a Henon map



Obrázek 6 Atraktory systémů. Zleva doprava a shora dolů: Burgers map, Arnold cat map, Chirikov a Holmes cubic map



Obrázek 7 Atraktor disipativního systému

1.9 Hénonova mapa

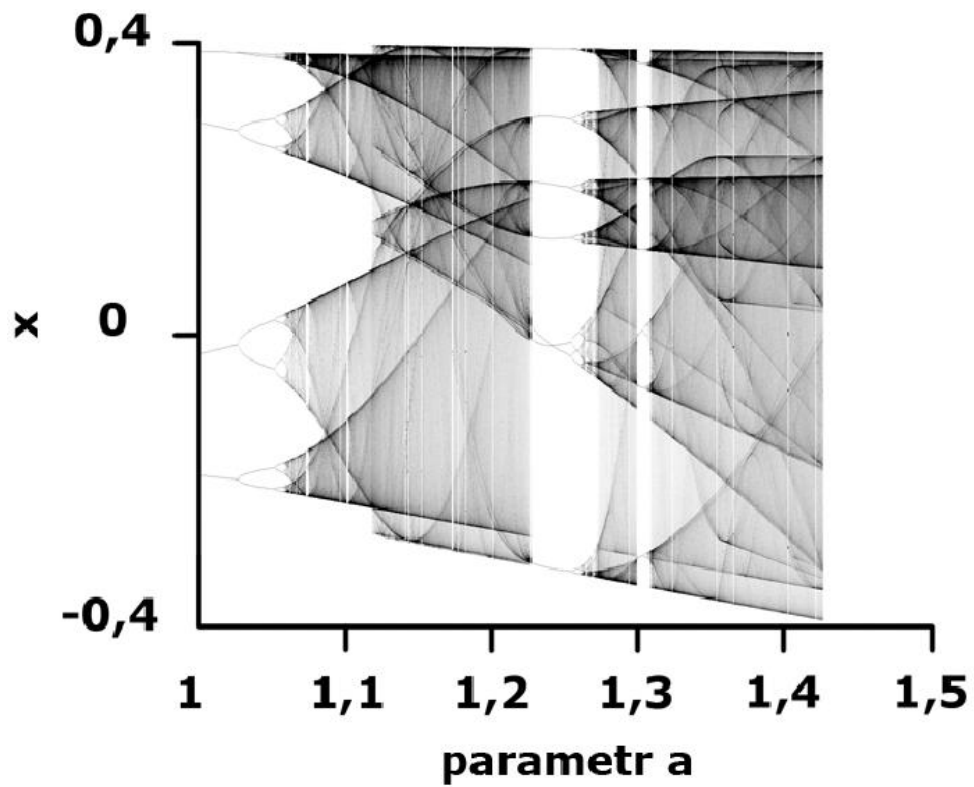
Hénonova mapa je jedním z příkladů diskrétního dynamického systému, vytvořených jako matematický model pro vyšetřování chaosu. Jedná se o jeden z nejstudovanějších modelů dynamického systému. Tento systém lze označit za dvourozměrné vyjádření jednorozměrné kvadratické mapy. Hénonovu mapu popisuje následující matematické vyjádření.

$$x_{n+1} = 1 + by_n - ax_n^2 \quad (7)$$

$$y_{n+1} = x_n \quad (8)$$

Mapa závisí na hodnotách dvou parametrů a a b , které pro kanonickou Hénonovu mapu mají hodnoty $a = 1,4$ a $b = 0,3$. Pro tyto kanonické hodnoty parametrů Hénonova mapa vykazuje chaotické chování. Pro ostatní hodnoty a a b může být chování chaotické, přerušované, nebo může konvergovat k pravidelné dráze. [5]

Hénonova mapa bývá označována jako další ze skupiny tzv. „podivných traktorů“. Jak lze vypořádat z grafu níže, na svislé ose grafu je opět vynesena parametr x a na vodorovné ose parametr a . Tento graf představuje bifurkační diagram Hénonovy mapy.



Obrázek 8 Bifurkační diagram Hénonovy mapy

2 GENERÁTOR NÁHODNÝCH ČÍSEL

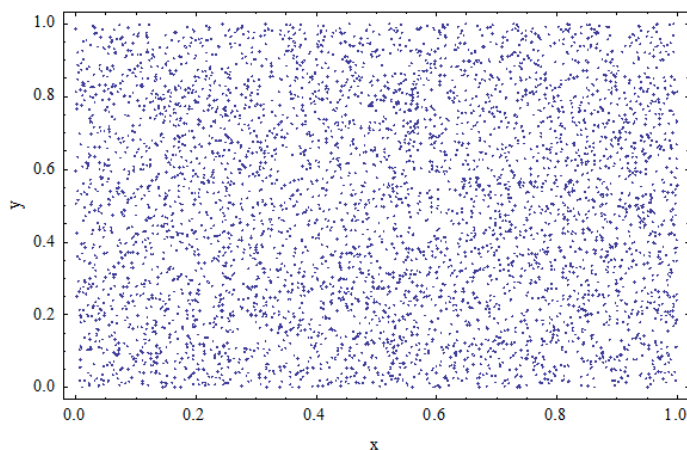
Náhodný generátor je zařízení nebo algoritmus, který produkuje sekvenci statisticky nezávislých dat. Ten ale není možné algoritmicky sestavit, proto se používá pseudonáhodný generátor, což je algoritmus, implementovaný na konečném automatu. Ten využívá náhodnou sekvenci čísel délky k , nazývanou semínkem generátoru (anglicky seed), ze které je schopen generovat pole čísel délky $l \gg k$, které vypadají z mnoha pohledů naprosto náhodně. Je důležité poznamenat, že pseudonáhodný generátor pracuje deterministicky, tedy tento algoritmus sám o sobě nefunguje náhodně - na základě stejných inicializačních hodnot produkuje jednoznačné výstupy.[9]

Kvalitní náhodná data jsou v kryptografii velmi užitečná, poskytují plné využití např. pro praxi generování klíčů nebo pro náhodnou inicializaci určitých proměnných v kryptografických protokolech.[9]

Samotné vytvoření a existence opravdu dokonale náhodného generátoru je nemožná. Je možné se k výsledkům náhodných generátorů pouze více či méně přiblížit na základě určitých postupů a ověřením statistických výsledků výstupních dat generátorů. Cílem je nejčastěji produkce výstupu s rovnoměrným rozložením.[10]

Volba generátoru pro použití v různých aplikacích do velké míry závisí na požadavcích těmito aplikacemi danými. Pokud je nutná schopnost generátoru vytvořit vícekrát po sobě stejnou sekvenci (například pro ladění různých aplikací) nebo požadavky na náhodnost nejsou velice přísné, pak je běžnější použití generátorů pseudonáhodných. Ty, i když jsou nutně periodické, tak jejich perioda může být velká a tyto generátory projdou většinou statistických testů. Takovéto generátory mohou být jednoduše sestaveny pomocí rychlých a jednoduchých softwarových operací. Ale pro potřeby šifrovacích aplikací jsou tyto generátory velice nevhodné. Pokud jsou totiž klíče těchto algoritmů generovány pseudonáhodně, pak bezpečnost celého algoritmu je rovna bezpečnosti, se kterou je schopen tento generátor pracovat.[10]

Ideální generátor náhodných čísel by měl být diskrétní bezeztrátový informační zdroj generující symboly se stejnou pravděpodobností. Účinný generátor náhodných čísel se chová jako informační zdroj s pamětí generující znaky s různou pravděpodobností.



*Obrázek 9 Graf rozložení čísel rovnoměrného
generátoru náhodných čísel*

2.1 Skutečně náhodné a pseudonáhodné sekvence generovaných čísel

V loteriích jsou vítězná čísla obvykle skutečně náhodná čísla, stanovená například vytažením míčku z nějakého druhu nádoby. Toto ovšem není moc praktické pro počítačové simulace, jelikož je zde nutnost velkého množství náhodných čísel. Na moderních počítačích jsou proto generována tzv. pseudonáhodná čísla pomocí deterministických algoritmů. Samozřejmě chceme, aby tato čísla pro náhodného pozorovatele, který nezná strukturu algoritmu, vypadala naprosto náhodně. Tedy aby nebyl schopen rozpoznat tato čísla od čísel skutečně náhodných v reálním časovém intervalu, určených například z pokusu házení mincí. V praxi je ovšem většina generátorů náhodných čísel takovéto vlastnosti nemá. Jsou zde ovšem aplikace, pro které je většina dnešních generátorů neúčinná, protože takovéto vlastnosti vyžadují. Například v kryptologii je většina dostupných generátorů nebezpečná, protože existují účinné způsoby jak předpovídat další generované hodnoty.[11]

2.2 Definice generátoru

Generátor je uspořádaná pětice:

$$Q = \{S, s_0, T, U, G\}, \quad (9)$$

kde S je konečný vektor stavů, $s_0 \in S$ je počáteční stav (seed), $T: S \rightarrow S$ je přenosová funkce, U je konečný vektor výstupních symbolů a $G: S \rightarrow U$ je výstupní funkce.

Generátor začíná z počátečního stavu a $u_0 = G(s_0)$, Pak pro kroky $i=1,2,\dots$ bude

$s_i = T(s_{i-1})$ a $u_i = G(s_i)$. Předpokládáme, že pro výpočet hodnot funkcí T a G jsou použity efektivní algoritmy. Pro pseudonáhodný generátor je možné říct, že se sekvence $\{u_i\}$ bude zvenčí jevit jako hodnoty náhodných proměnných rovnoměrně rozložených na U . U je obvykle konečný vektor celých čísel, nebo konečný vektor hodnot mezi 0 a 1 k přibližné simulaci rovnoměrného rozložení $U(0,1)$. [11]

2.3 Generátor náhodných čísel s rovnoměrným rozdělením

Náhodná čísla mohou být generována pomocí různých fyzikálních mechanismů, jako je načasování následných událostí v atomovém rozpadu, tepelného šumu v polovodičích a podobných. Klíčovým problémem při tvorbě generátoru náhodných čísel založeného na fyzickém zařízení je, že náhodný nebo chaotický výstup není dostačující. Čísla na výstupu generátoru musí splňovat základní podmínku, tedy musí být alespoň dobrou aproximací realizace nezávislých a rovnoměrně rozložených náhodných proměnných. Pokud zařízení generuje řadu bitů, což bývá velice běžné, pak by pravděpodobnost, že každý bit bude obsahovat 0 nebo 1 měla být stejná a současně by měly hodnoty těchto bitů být nezávislé na hodnotách bitů okolních. Obecně platí, že tuto podmínku není možné prokázat, proto je nutné spoléhat na výsledky empirického testování, kde se dá ověřit, zda mají výstupní hodnoty požadované statistické chování. Pro výpočetní statistiky mají tato zařízení několik nevýhod oproti algoritmům napsaným na několika řádcích kódu:

- a) Jsou mnohem obtížněji instalovatelné a spustitelné
- b) Jsou dražší
- c) Jsou mnohem pomalejší
- d) Nejsou schopny vygenerovat dvakrát po sobě stejnou sekvenci

Položka d je důležitá v několika situacích, jako je ověřování a ladění programu, stejně jako srovnávání podobných systémů simulací s běžnými náhodnými čísly pro snížení rozptylu. [9]

Nicméně tyto fyzické generátory mohou být využity pro výběr semínka algoritmických generátorů zejména při aplikaci v kryptologii a různých automatech. Zde je velice důležité při častém novém nastavování počátečního semínka využití externího zdroje entropie. Dobrý generátor náhodných čísel, jehož semínko bývá zvoleno náhodně lze považovat za rozšíření náhodnosti krátkých náhodných řad čísel do dlouhých sekvencí pseudonáhodných čísel.

2.4 Generátory náhodných čísel založené na chaotických systémech

Jelikož chaotické systémy se chovají nepravidelně a mají zdánlivě nepředvídatelné chování, je zde mnoho aspektů spojujících generátory náhodných čísel a chaotické systémy.[12]

Základní myšlenkou konstrukce chaotického generátoru je využití citlivosti trajektorií na počáteční podmínky. Generovaným hodnotám jsou pak přiřazována určitá chování trajektorií.

Vzhledem k chaotickým vlastnostem systému, mohou jakékoliv 2 počáteční podmínky, bez ohledu na to jak jsou si blízké, vést na naprosto odlišné sekvence čísel. Tato vlastnost je velice užitečná v různých aplikacích. Ke splnění různých statistických testů musí mít generátor jisté vlastnosti. Ty jsou ale již zajištěny teorií dynamických systémů.[12]

II. PRAKTICKÁ ČÁST

3 POPIS PROGRAMU

Program je ovládán přes příkazovou řádku pomocí vybírání položek z menu (Ukázka menu na obrázcích 10 a 11). Po spuštění programu je uživatel vyzván k volbě použitého chaotického systému podle tabulky 1 a následně po jeho výběru k nastavení parametrů a počátečních podmínek nutných k vygenerování posloupnosti čísel. Tyto hodnoty je nutné zadat pomocí čísel 0-9 s desetinnou tečkou. Při chybně zadané hodnotě je uživatel vyzván k opakování zadání. Po úspěšném nastavení systému je vygenerována posloupnost čísel, ze které je možné :

- a) Vypisovat po jednom vygenerovaná čísla
- b) Vypsat čísla do souboru, který je možné následně zpracovat a převést do grafické podoby (histogram, atraktor)
- c) Vytvořit posloupnost hodnot pro bifurkační diagram se změnou vybraného parametru

Nebo je možné změnit generovaný systém. Na obrázku 12 a 13 jsou ukázky generovaných výstupů uložených do souboru.

```
Zvolte chaoticky system:
1: Lozi
2: Ikeda
3: Sinai
4: Disipative
5: Arnold Cat map
6: Henon map
7: Burgers map
8: Holmes cubic map
9: Chirikov
-
```

Obrázek 10 Ukázka prvního menu

```
Zvoleny system: Ikeda
1: generovat nahodne cislo
2: zmenit system
3: vypis hodnot do souboru
4: vypis hodnot pro bifurkacni diagram
5: konec
-
```

Obrázek 11 Ukázka druhého menu

i	x	y	i	x
1	0.900000	0.5	1	0.955618
2	0.300000	0.9	2	0.86652
3	0.280733	0.100001	3	0.658547
4	0.461654	0.480734	4	0.317141
5	0.843139	0.423123	5	0.121135
6	0.177765	0.689384	6	0.0349194
7	0.829773	0.556533	7	0.983557
8	0.292487	0.942839	8	0.914851
9	0.328840	0.178166	9	0.764375
10	0.550675	0.685172	10	0.455231
11	0.196031	0.921018	11	0.190614
12	0.204846	0.0380671	12	0.0742577
13	0.340069	0.28098	13	0.0294977
14	0.601794	0.902029	14	0.0140671
15	0.585301	0.405852	15	0.0126853
16	0.908217	0.397005	16	0.0239754
17	0.225517	0.702227	17	0.0591505
18	0.897962	0.629971	18	0.152126
19	0.459319	0.157904	19	0.375128
20	0.671955	0.775126	20	0.710852
21	0.462559	0.222207	21	0.892225
22	0.702210	0.906973	22	0.973302
23	0.692421	0.516155	23	0.0268816
24	0.109074	0.72473	24	0.107429
25	0.817765	0.558534	25	0.287442
26	0.282921	0.934832	26	0.622386
27	0.309368	0.152585	27	0.846897
28	0.519449	0.614538	28	0.940407
29	0.058655	0.748524	29	0.975035
30	0.806014	0.555704	30	0.984089
31	0.267719	0.917421	31	0.97654
32	0.271834	0.102562	32	0.944904
33	0.454360	0.476957	33	0.858586
34	0.832385	0.408274	34	0.648262
35	0.156883	0.648933	35	0.310396
36	0.746331	0.454749	36	0.120551

Obrázek 12 Ukázka částí vyexportovaných výstupních hodnot aplikace vlevo neupravených a vpravo v intervalu (0,1)

parametr	x
-5	0.5
-5	0.999994
-5	0.499987
-5	-0.499993
-5	0.999974
-5	0.499921
-5	-0.500154
-5	0.999509
-5	0.498642
-5	-0.502749
-5	0.988697
-5	0.456366
-5	-0.433482
-5	0.577158
-5	0.185625
-5	-0.265757
-5	0.51223
-5	-0.432591
-5	0.871089
-5	0.00148247
-5	-0.101478
-5	0.651817
-5	0.928482
-5	-0.644952
-5	-0.0484677
-5	0.658126
-5	0.0761483
-5	0.788195
-5	0.944794
-5	-0.537351
-5	-0.230459
-5	-0.0721658
-5	0.131263
-5	-0.369457
-5	-0.685244
-5	-0.987381

Obrázek 13 Ukázka části vyexportovaných dat pro bifurkační diagram

3.1 Popis implementace

Celá aplikace je implementovaná pomocí jediné třídy generator a několika globálních funkcí. Třída obsahuje metody pro obsluhu použitých chaotických systémů, metody pro libovolný výpis a pro revaluaci. Tato metoda slouží k prodloužení vektoru generovaných hodnot nastavením počátečních podmínek z konce intervalu a novým spuštěním aktuálně používaného systému. Toho lze využít ke generování teoreticky nekonečně dlouhého vektoru hodnot. K přiměřené regulaci paměťových nároků jsou tyto hodnoty pro generování běžného výstupu omezeny na 20000 ale pro hodnoty k vykreslení bifurkačního diagramu až 150000.

3.1.1 Vstupy

Jako vstupní hodnoty jsou brána pouze čísla. Při kombinaci s písmeny, nebo při zadání jakéhokoliv chybného znaku je uživatel vyzván k opakování zadání. Tohoto je docíleno zadáváním čísel ve smyčce a kontrolou validity zadaných znaků po ukončení zadávání (konec řádku).

3.1.2 Chaotické systémy

Po zkontrolování správnosti zadání položky z menu je uživatel vyzván k zadání počátečních hodnot pro vybraný systém a následně parametrů tohoto systému. Vlastní implementace různých chaotických systémů je představována jednoduchou smyčkou for omezenou maximální zadanou hodnotou nejvyššího indexu generovaného pole bez využití revaluace. Tím jsou vygenerovány prvky posloupnosti, se kterou je možné provádět další operace.

```
FOR i = 1 to POCET_VYPISOVANÝCH
  Vypocitej uhel
  Vypocitej nasledujici hodnotu poley
  Vypocitej nasledujici hodnotu poley
ENDFOR
```

Obrázek 14 Ukázka výpočtu dat chaotického systému Ikeda
v pseudokódu

3.1.3 Generování výstupních hodnot

Pro generování hodnot z aktuální posloupnosti je sestaveno jednoduché menu. Při výběru první položky z tohoto menu je generována jedna hodnota, tedy je vypsána jedna hodnota z vygenerované posloupnosti. Index této hodnoty se zvyšuje s počtem vypsanych čísel. Při výběru druhé možnosti, kterou je volba systému, jsou resetovány hodnoty indexů využívané k vypisování různých hodnot a následně je znovu spuštěn výběr systému.

Při třetí možnosti (výpis hodnot do souboru) je nejprve otevřen soubor. Pokud je toto úspěšně provedeno, jsou do souboru pomocí cyklu for vypsány vygenerované hodnoty. V případě, že je požadovaný počet vypsanych hodnot vyšší než počet hodnot vygenerovaných, je spuštěna pomocná metoda pro revaluaci popsána výše.

```
Vytvoř a otevři soubor vystup.txt
IF soubor neotevřen
  Vypiš: nelze otevřít soubor
  KONEC
ENDIF
Vypiš hlavičku dat do soubor.txt
FOR i = 1 to počet generovaných
  IF i = počet vygenerovaných THEN
    Nastav index na 0
    Vygeneruj nové hodnoty posloupnosti
  ENDIF
  Inkrementuj index vypisovaného prvku
  Vypiš hodnotu pplex a poley do souboru vystup.txt
ENDFOR
Uzavři soubor
Vypiš: Data úspěšně uložena do souboru
KONEC
```

Obrázek 15 Ukázka výpisu dat do souboru v pseudokódu

Poslední možností výpisu je vytvoření hodnot pro bifurkační diagram. Zde je opět vytvořen a otevřen soubor, do kterého jsou postupně zapisovány hodnoty generovány pro různě nastavenou hodnotu parametru (zvolen před výpisem). Toto je provedeno pomocí 2 vnořených cyklů. Hodnota, která je inkrementována ve vnějším cyklu, současně představuje hodnotu měněného parametru. Inkrementovaná hodnota z vnitřního cyklu pak představuje index vypisované hodnoty, začínající na 900. hodnotě.

Při volbě poslední položky menu, tedy konce, je program ukončen.

```
Vytvoř a otevři soubor vystupbif.txt
IF soubor neotevřen
  Vypiš: Nelze otevřít soubor
  KONEC
DO
{
  Vypiš: Vyber parametr
  Načtení hodnoty parametru ze vstupu
  SWITCH (parametr)
  1:
    FOR i=0.47 TO 1.75
      Vypočítej hodnoty posloupnosti vybraného chaotického systému
      FOR j=900 TO 1000
        Vypiš hodnoty parametru a vygenerované hodnoty polest do souboru
      ENDFOR
    ENDFOR
  2:
    FOR i=0.47 TO 1.75
      Vypočítej hodnoty posloupnosti vybraného chaotického systému
      FOR j=900 TO 1000
        Vypiš hodnoty parametru a vygenerované hodnoty polest do souboru
      ENDFOR
    ENDFOR
}WHILE (nesprávně zvolená položka)
Uzavři soubor
KONEC
```

Obrázek 16 *Ukázka výpisu dat pro bifurkační diagram
do souboru v pseudokódu*

4 SROVNÁNÍ CHAOTICKÝCH SYSTÉMŮ

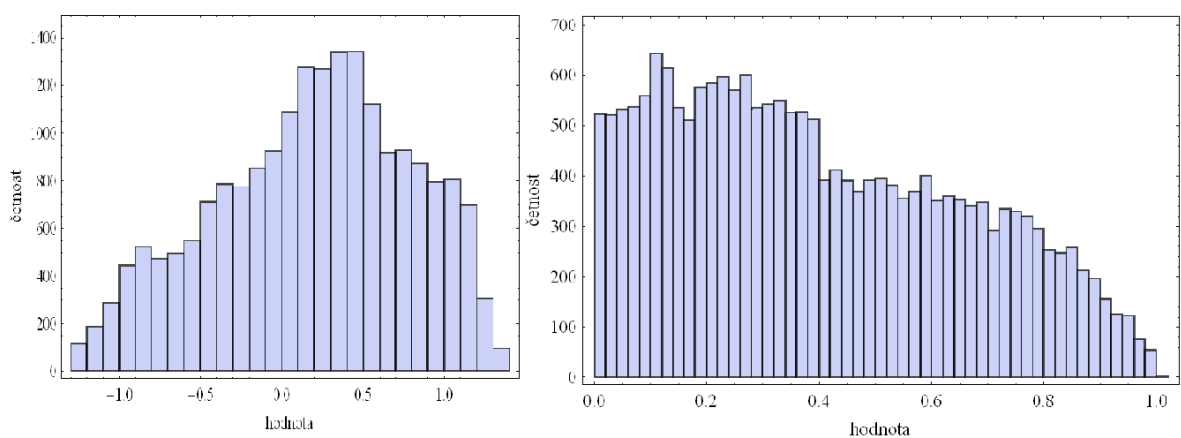
V této kapitole bude provedena nejprve analýza použitých chaotických systémů. Následně bude provedeno srovnání chaotických systémů uvedených v tabulce 1 s běžným generátorem náhodných čísel, vytvářejícím posloupnost náhodných čísel s rovnoměrně rozložených na intervalu $\langle 0,1 \rangle$. Pro lepší srovnání použitých systému s tímto běžným generátorem byl u každého systému kromě histogramu rozložení hodnot na celém intervalu vytvořen také histogram hodnot upravených do intervalu $\langle 0,1 \rangle$. To bylo provedeno pouze v případě, že tyto hodnoty nejsou obsaženy již v prvním histogramu. Dále jsou pro každý systém vykresleny bifurkační diagramy pro všechny použité parametry ke zjištění oblasti chaotického chování systému.

4.1 Nastavení parametrů

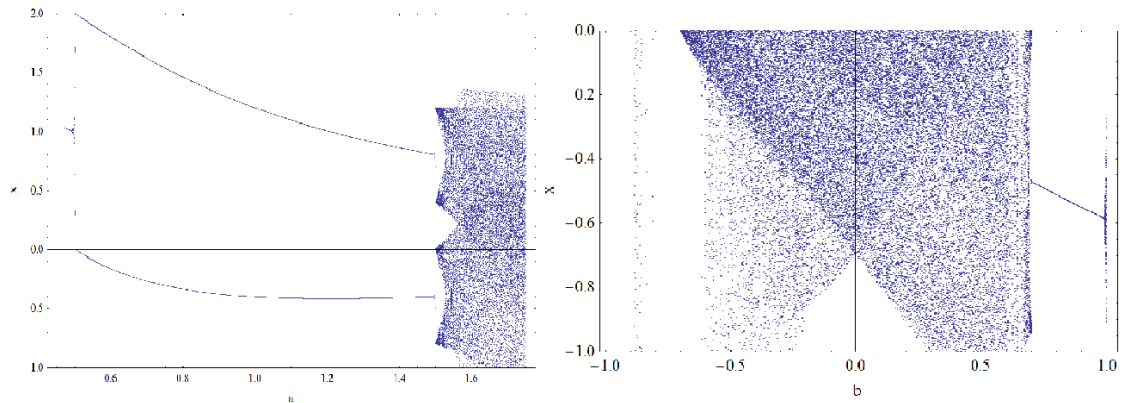
Pro chaotické systémy byly nejprve nastaveny hodnoty vstupních parametrů dle tabulky 1, při kterých by systémy měly generovat chaotická výstupní data. Následně byly testovány převážně kombinace vstupních podmínek. Změna parametrů je již viditelná na bifurkačních diagramech.

4.2 Lozi

Pro tento chaotický systém lze z histogramů zobrazených na obrázku 17 vidět, že tento systém generuje při nastavení počátečních podmínek podle tabulky 1 posloupnost čísel s binomickým rozdělením se středem přibližně v hodnotě 0.45. Při úpravě histogramu do intervalu $\langle 0,1 \rangle$ je většina hodnot rozložena spíše v levé části intervalu.



Obrázek 17 Neupravený (vlevo) a upravený histogram systému Lozi

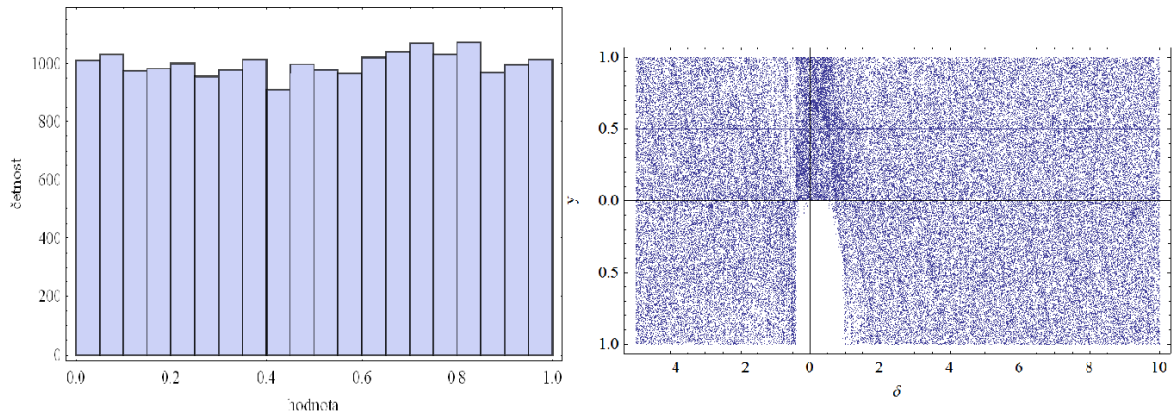


Obrázek 18 Bifurkační diagramy systému Lozi, vlevo pro parametr a , vpravo b

Pro libovolně nastavené počáteční podmínky z intervalu $\langle -1.5, 1.5 \rangle$ zůstává histogram nezměněn. Při nastavení libovolné z těchto hodnot mimo tento interval posloupnost diverguje k nekonečnu. Reakce systému na změnu parametru je vidět na bifurkačních diagramech na obrázku výše, tedy pro parametr a vykazuje systém chaotické chování při hodnotách vyšších než 1.5. Pro parametr b lze pozorovat chaotické chování v intervalu $\langle -0.7, 0.7 \rangle$.

4.3 Sinai

Chaotický systém Sinai je, vzhledem k použití modulární operace v definici, možné použít téměř s libovolně zadanými počátečními podmínkami k vygenerování odlišné posloupnosti čísel. Výjimku tvoří nulové počáteční podmínky. Dochází pouze ke změně tvaru atraktoru, ale rozložení čísel zůstává přibližně rovnoměrné, jak lze vidět na obrázku níže, v intervalu $(0,1)$.

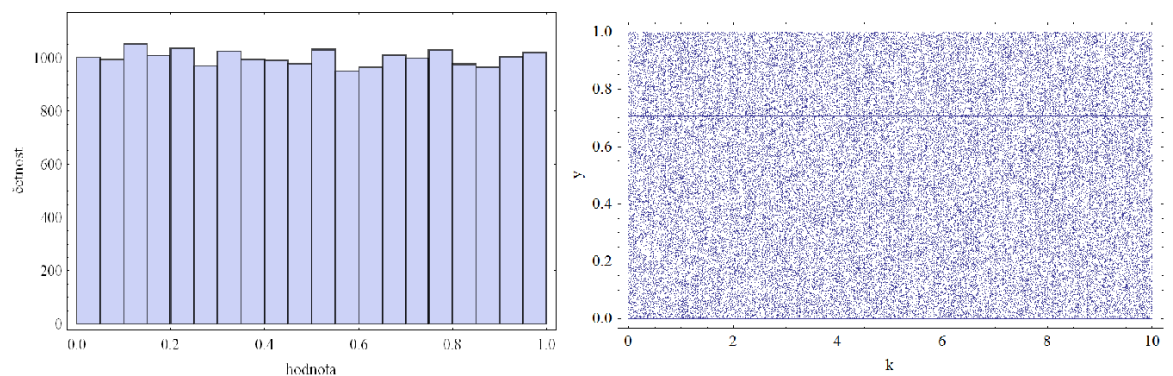


Obrázek 19 Histogram a bifurkační diagram pro chaotický systém Sinai

Z bifurkačního diagramu tohoto systému je vidět chaotické chování na celém intervalu hodnot parametru α .

4.4 Arnold cat map

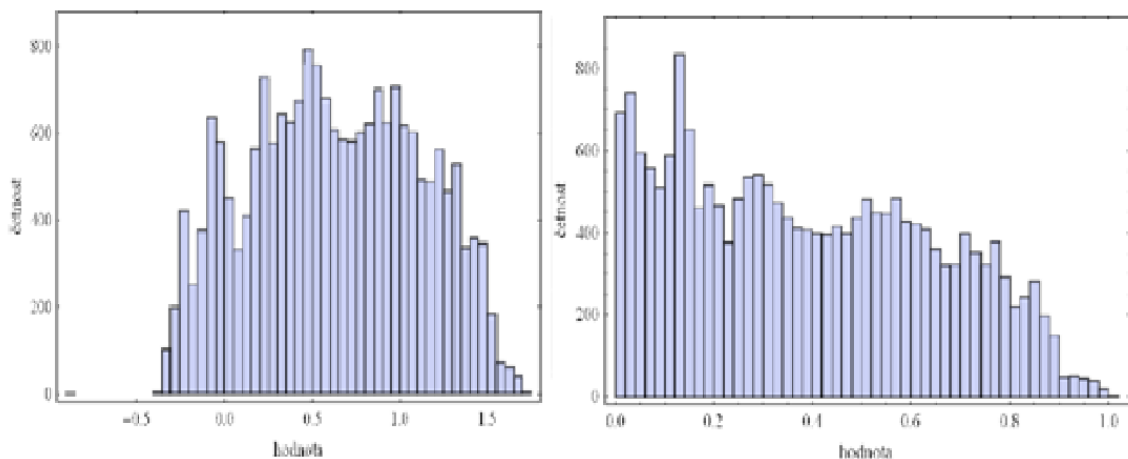
Pro chaotický systém Arnold cat map lze říct to samé jako u předchozího systému Sinai s rozdílem u atraktoru, který zde zůstává nezměněn. Další změna je vidět u bifurkačního diagramu, kde u tohoto systému je pokrytý celý interval.



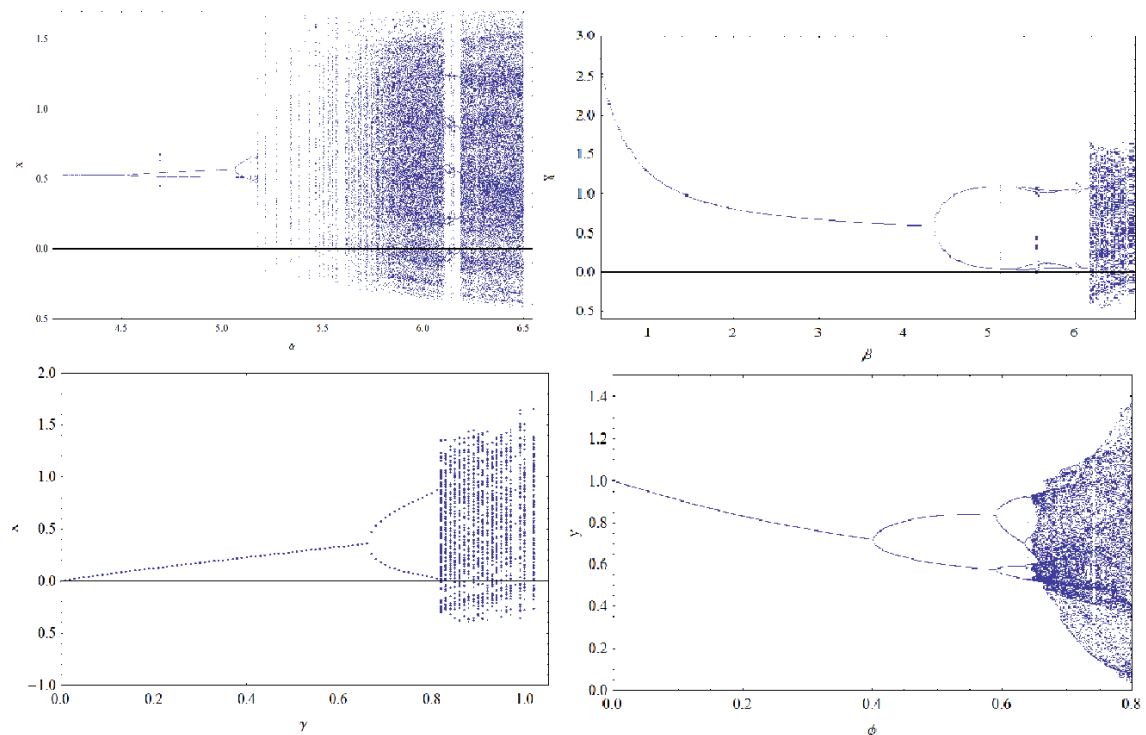
Obrázek 20 Histogram a bifurkační diagram chaotického systému Arnold cat map

4.5 Ikeda

Pro graf rozložení tohoto systému na obrázku 21 platí, že vzhledem k použití goniometrických funkcí v definici systému jsou generovány pouze hodnoty v omezeném intervalu. Tato vlastnost se ztrácí při změně počátečních podmínek bez změny parametrů, po které se vytrácí z řady náhodnost a po určité době se hodnoty ustálí. Toto je vidět na bifurkačních diagramech, kde pro každý z parametrů je pouze úzká oblast chaotického chování. Pouze u parametru β se diagram periodicky opakuje.



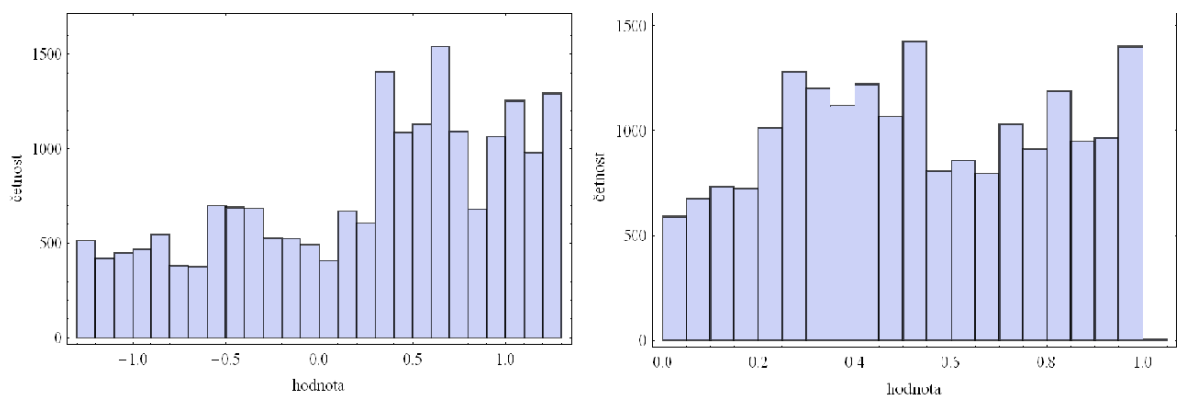
Obrázek 21 Neupravený (vlevo) a upravený histogram systému Ikeda



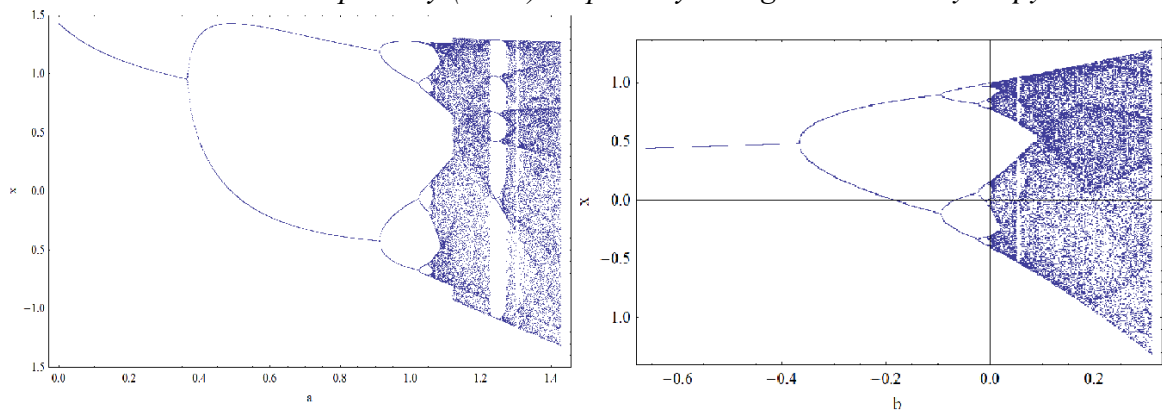
Obrázek 22 Bifurkační diagramy systému Ikeda, pro změny parametrů α, β, γ a ϕ (zleva doprava a shora dolů)

4.6 Hénonova map

U tohoto systému jsou generované hodnoty rozprostřeny v intervalu $\langle -1.5, 1.5 \rangle$ s téměř dvojnásobnou četností v kladných hodnotách. Na upraveném histogramu je vidět nejvyšší hustota okolo hodnot 0.5 a 1, která se směrem doleva snižuje. Při změně vstupních podmínek dochází k opakování několika desítek hodnot. Při větších změnách vstupních parametrů posloupnost diverguje. Podle bifurkačního diagramu pro první parametr systém vykazuje chaotické chování při hodnotách parametru a a přibližně v intervalu $(1, 1.4)$. U druhého parametru je chaotické chování viditelné pro hodnoty vyšší než 0.



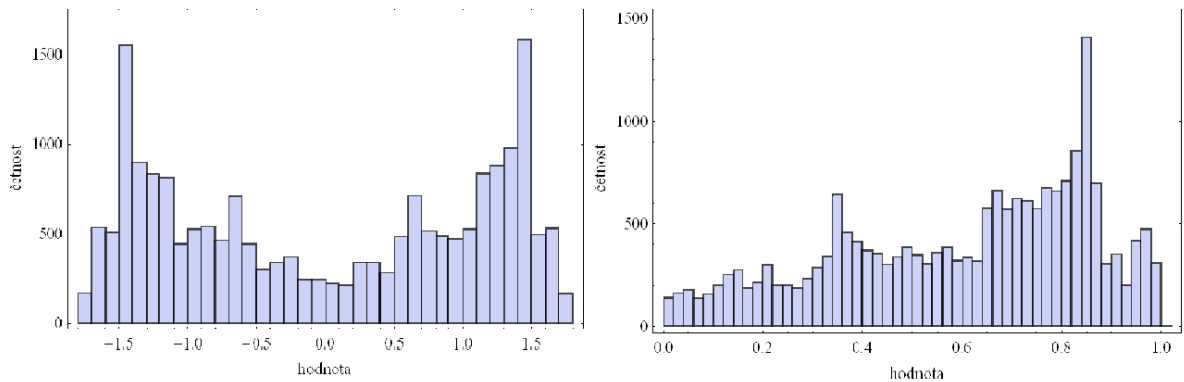
Obrázek 23 Neupravený (vlevo) a upravený histogram Hénonovy mapy



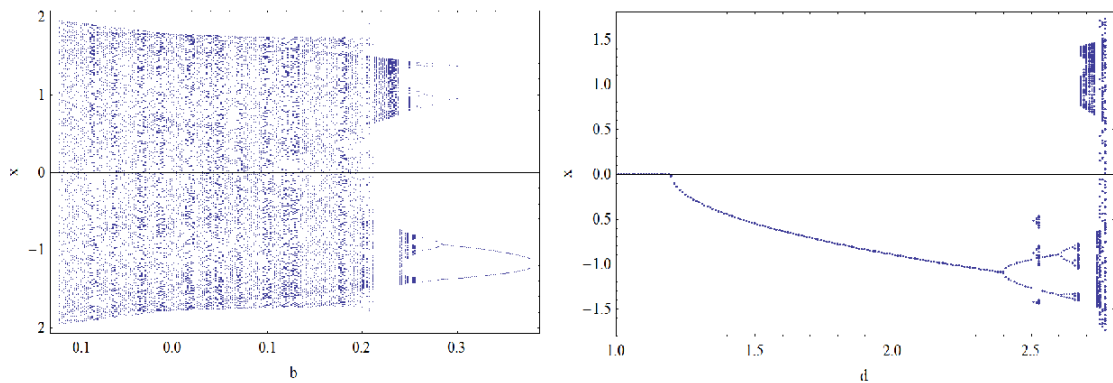
Obrázek 24 Bifurkační diagramy pro Hénonovu map, měněným parametrem je vlevo a , vpravo b

4.7 Holmes cubic map

Z histogramu systému Holmes zobrazeného níže je vidět, že je možné rozložení hodnot označit za binomické rozdělení se středem okolo bodu 1.5. Graf tohoto rozdělení je také symetrický podle osy y . Podle bifurkačního diagramu pro první parametr lze pozorovat chaotické chování pro jeho hodnoty menší než 0.25. Pro druhý parametr je oblastí chaotického chování přibližně interval $\langle 2.6, 2.8 \rangle$.



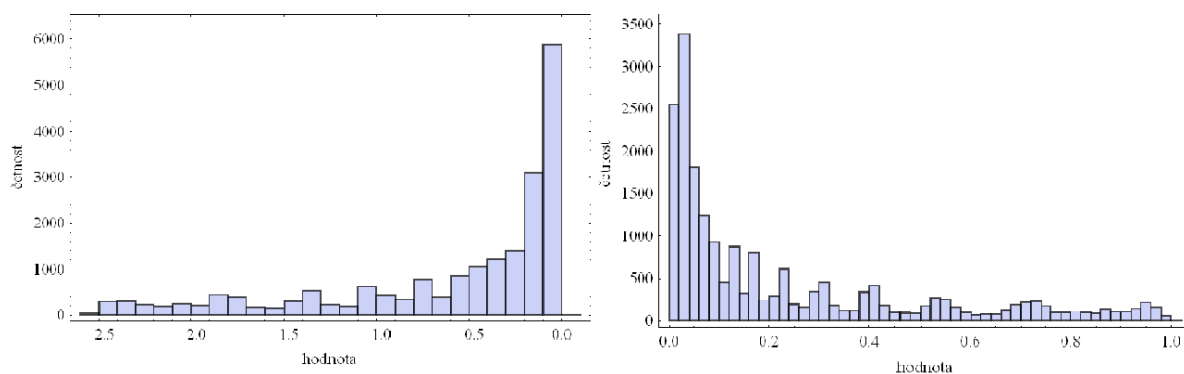
Obrázek 25 Neupravený (vlevo) a upravený histogram systému Holmes cubic map



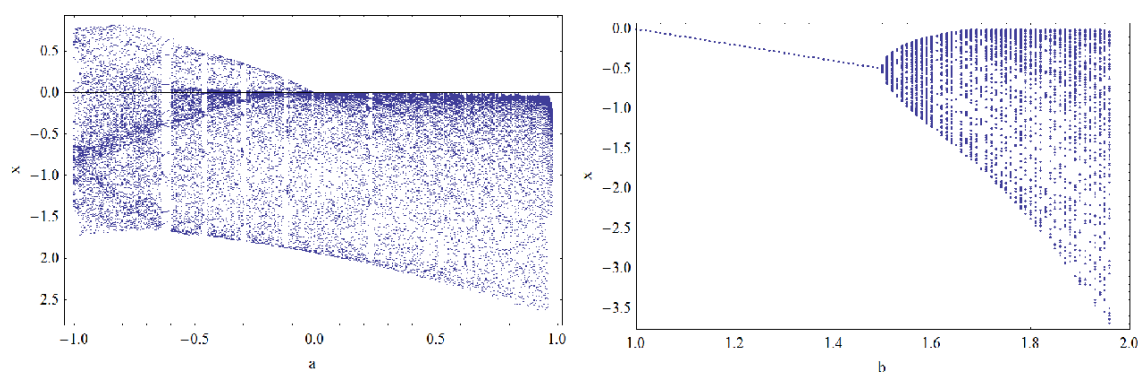
Obrázek 26 Bifurkační diagramy pro Holmes cubic map, měněným parametrem vlevo b , vpravo d

4.8 Burgers map

Histogram tohoto systému připomíná exponenciální rozložení s maximem v hodnotě 0. Toto lze vidět i v upraveném histogramu. Z bifurkačního diagramu pro první parametr je vidět chaotické chování na celém vykresleném intervalu. Pro druhý parametr systém vykazuje chaotické chování pro hodnoty z intervalu $\langle 1.5, 2 \rangle$.



Obrázek 27 Neupravený (vlevo) a upravený histogram systému Burgers map

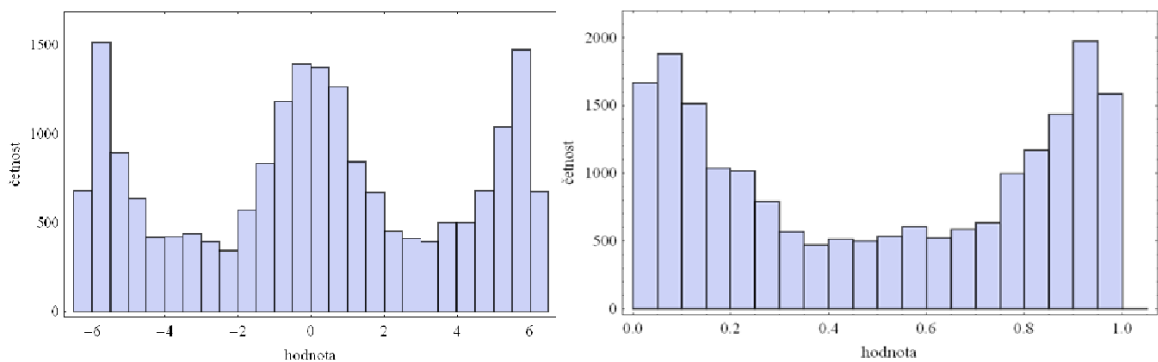


Obrázek 28 Bifurkační diagramy pro Burgers map, měněným

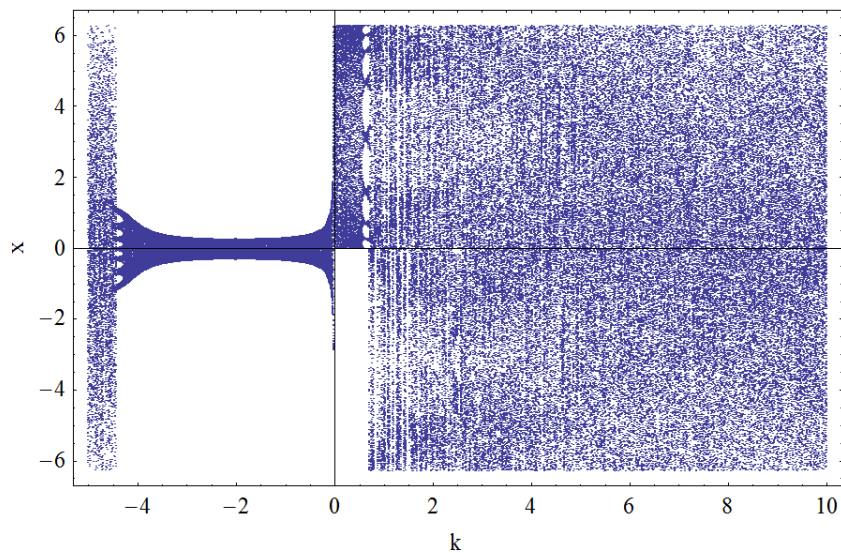
Parametrem je vlevo a , vpravo b

4.9 Chirikov

Stejně jako u systémů Arnol cat a Sinai je díky použití modulárních operací možné volit téměř libovolné hodnoty vstupních parametrů s výjimkou 0. Z obou histogramů je vidět, že hodnoty jsou rozloženy spíše na krajích intervalu než v jeho středu, což je možné pozorovat hlavně v upraveném histogramu. Při různých změnách, jsou hodnoty čísel více či méně rozprostřeny okolo hodnoty 0. Z bifurkačního diagramu je vidět, že systém při kladných hodnotách parametru k generuje hodnoty ve větším intervalu než při hodnotách záporných.



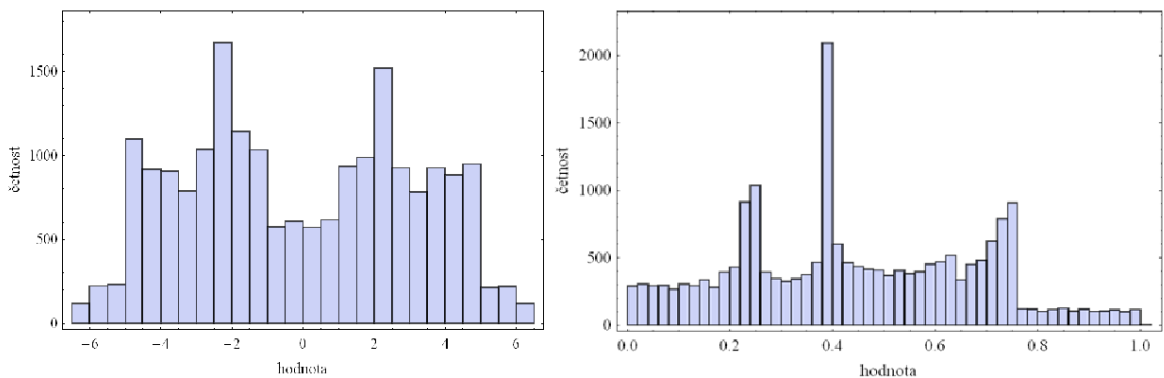
Obrázek 29 Neupravený (vlevo) a upravený histogram systému Chirikov



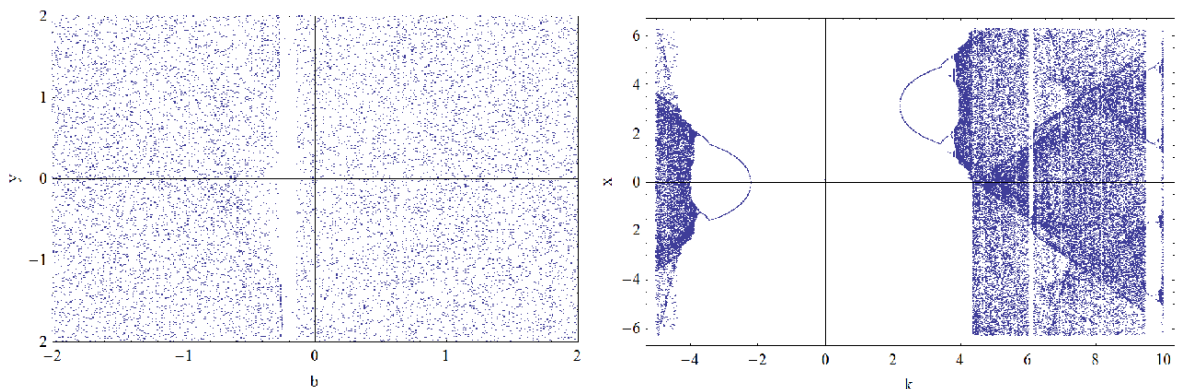
Obrázek 30 Bifurkační diagram pro systém Chirikov

4.10 Disipativní systém

Při počátečních parametrech systému nastavených podle tabulky 1. vytváří disipativní systém rozdělení hodnot, zobrazené na obrázku níže, připomínající normální rozdělení se středem v hodnotě 2 symetrické pro kladné a záporní hodnoty. Toto je lépe vidět v upraveném histogramu, kde je vidět nejvyšší výskyt hodnot okolo hodnoty 0.4. Při úpravách parametrů jsou tyto hodnoty rozprostřeny více či méně okolí hodnoty 0. Podle bifurkačního diagramu pro první parametr systém vykazuje chaotické chování téměř pro libovolné hodnoty tohoto parametru. Pro druhý parametr lze pozorovat chaotické chování pro hodnoty menší než -4 a větší než 4 s drobnými výjimkami.



Obrázek 31 Neupravený (vlevo) a upravený histogram disipativního systému



Obrázek 32 Bifurkační diagramy pro disipativní systém, měněným parametrem vlevo b , vpravo k

4.11 Porovnání systémů

Z pohledu reálné použitelnosti pro generování různých čísel s rozdílnými parametry jsou mnohem lépe využitelné systémy s modulárními operacemi, kdy jsou při libovolných nastaveních hodnoty stále udržovány v určeném intervalu. Při srovnání s běžně používanými generátory náhodných čísel jsou právě tyto systémy těmto výsledkům nejbližší.

5 MOŽNOSTI REÁLNÉHO VYUŽITÍ

Tyto generátory náhodných čísel je možné využívat v různých odvětvích kryptografie jako například generování různých klíčů nebo hesel. Toho lze využít pouze za předpokladu externího náhodného zdroje k nastavení počátečních podmínek a parametrů. Při známých počátečních hodnotách je totiž velice jednoduché určit hodnoty generované posloupnosti. Nejlépe využitelné k těmto účelům by byly systémy Arnold cat map a Sinai, generující výstupy pokrývající rovnoměrně oblast dat stejně jako běžné generátory. Oblast použitelnosti ostatních systémů je obvykle o hodně menší vzhledem k úzkému intervalu chaotického chování. Klíčovým prvkem v takovýchto systémech je také výběr čísel z vygenerované posloupnosti, což by pro zajištění nejlepšího zabezpečení těchto aplikací bylo ideální realizovat s využitím externího zdroje, např. uživatelské zadání nebo jiný generátor.

ZÁVĚR

Účelem bakalářské práce bylo vytvoření aplikace využívající dynamických systémů, které vykazují známky chaotické chování, jako generátory pseudonáhodných čísel a srovnání jejich výstupů s běžně používaným generátorem náhodných čísel. Na základě výsledků testů provedených na každém z použitých systémů, jako různé nastavování parametrů a vykreslování různých typů grafů pro tyto nastavení lze říct, že tyto systémy mohou být při splnění určitých podmínek velice užitečné. Jednou z těchto podmínek by měl být velice přesný výběr systému, protože v chování různých z použitých systémů při různých záměnách parametrů vznikaly občas propastné rozdíly.

Výstupem této práce je aplikace napsaná v programovacím jazyku C++ a k vizualizaci dat je přiložen zdrojový soubor programu Wolfram Mathematica.

ZÁVĚR V ANGLIČTINĚ

The purpose of this thesis was to create an application using dynamic systems that show signs of chaotic behavior as a pseudo-random number generators and straightening of these outputs to the commonly used random number generator. Based on the results of tests performed on each of the systems used, as different parameter settings and rendering various types of graphs for these settings. It can be said that this system may be subject to certain conditions, very helpful. One of these conditions should be very precise selection system, because the behavior of various systems used in various parameter substitutions arose occasionally divides.

The outcome of this thesis is an application written in C++ and to visualize data, there is attached source file program Wolfram Mathematica.

SEZNAM POUŽITÉ LITERATURY

- [1]. KRATOCHVÍL, C. a P. HERIBAN. Dynamické systémy a chaos. Brno: Vysoké učení technické v Brně, 2010, 229 s. ISBN 978-80-214-4152- 1
- [2]. HORÁK, Jiří. Deterministický chaos a jeho fyzikální aplikace. Academia, 2003. 437 s. ISBN 8020009108.
- [3]. HILBORN, Robert C. Chaos and nonlinear dynamics : an introduction for scientists and engineers. New York : Oxford University Press, Inc., 1994. 672 s. ISBN 0-19-508816-8.
- [4]. ELERT, Glenn. *The Chaos Hypertextbook* [online]. 1995-2007 [cit. 2011-02-27]. Lyapunov Exponent. Dostupné z WWW: <http://hypertextbook.com/chaos/43.shtml>
- [5]. ŠENKEŘÍK, Roman. Optimal Control of Deterministic Chaos. Zlín, 2008. 316 s. Dizertační práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky. ISBN 978-80-7318-783-5.
- [6]. CROSS, Michael. The Lorenz Model. [online]. 1999-12-16 [cit. 2012-05-29]. Dostupné z: http://www.cmp.caltech.edu/~mcc/Chaos_Course/Lesson1/Lorenz.pdf
- [7]. SPROTT, Julien C. Chaos and time-series analysis. Oxford : Oxford University Press, 2003. 528 s. ISBN 0198508395
- [8]. VINOD, Patidar a K.K. SUD. A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing [online]. Rajasthan, India: Sir Padampat Singhania University, 2009, s. 327-344 [cit. 2012-05-27]. Dostupné z <http://www.ejtp.com/articles/ejtpv6i20p327.pdf>
- [9]. L'ECUYER, Pierre. Random Number Generation Montreal: D'épartement d'Informatique et de Recherche Op'erationnelle, 2008 [cit. 2012-05-27].
- [10]. STOJANOVSKI, Toni a Ljup'co KOCAREV. Chaos-Based Random Number Generators—Part I: Analysis. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: FUNDAMENTAL THEORY AND APPLICATIONS, [online]. 2001, č. 48, s. 281-287 [cit. 2012-05-27].
- [11]. L'ECUYER, Pierre. UNIFORM RANDOM NUMBER GENERATION [online]. Universite de Montreal, 1993 [cit. 2012-05-27]. Dostupné z: <http://webcache.googleusercontent.com/search?q=cache:wayIBHTB0fcJ:www.iro.umontreal.ca/~lecuyer/myftp/papers/tutaor.ps+&cd=3&hl=cs&ct=clnk&gl=cz>

- [12]. SZCZEPAŃSKI, Janusz a Zbigniew KOTULSKI. Pseudorandom Number Generators Based on Chaotic Dynamical Systems [online]. Netherlands: Kluwer Academic Publishers, 2001,s.137-146[cit.2012-05-27].Dostupné z http://www.ippt.gov.pl/~tlipnia/docs/js_Random_Number_Generator_Open.pdf
- [13]. GLEICK, James. Chaos: vznik nové vědy. Ando Publishing, 1996. 350s. ISBN 80-86047-04-0.

SEZNAM OBRÁZKŮ

<i>Obrázek 1 Příklad bifurkačního diagramu</i>	13
<i>Obrázek 2 Bifurkační diagram Logistické rovnice</i>	15
<i>Obrázek 3 Lorenzův atraktor</i>	17
<i>Obrázek 4 Trajektorie s hodnotami Ljapunovského exponentu[4]</i>	19
<i>Obrázek 5 Atraktory systémů. Zleva doprava a shora dolů: Lozi, Ikeda,</i>	21
<i>Obrázek 6 Atraktory systémů. Zleva doprava a shora dolů: Burgers map,</i>	21
<i>Obrázek 7 Atraktor disipativního systému</i>	22
<i>Obrázek 8 Bifurkační diagram Hénonovy mapy</i>	23
<i>Obrázek 9 Graf rozložení čísel rovnoměrného</i>	25
<i>Obrázek 10 Ukázka prvního menu</i>	29
<i>Obrázek 11 Ukázka druhého menu</i>	29
<i>Obrázek 12 Ukázka částí vyexportovaných výstupních hodnot</i>	30
<i>Obrázek 13 Ukázka částí vyexportovaných dat</i>	30
<i>Obrázek 14 Ukázka výpočtu dat chaotického systému Ikeda</i>	31
<i>Obrázek 15 Ukázka výpisu dat do souboru v pseudokódu</i>	32
<i>Obrázek 16 Ukázka výpisu dat pro bifurkační diagram</i>	33
<i>Obrázek 17 Neupravený (vlevo) a upravený histogram systému Lozi</i>	34
<i>Obrázek 18 Bifurkační diagramy systému Lozi, vlevo pro parametr a, vpravo b</i>	35
<i>Obrázek 19 Histogram a bifurkační diagram pro chaotický systém Sinai</i>	36
<i>Obrázek 20 Histogram a bifurkační diagram chaotického systému Arnold cat map</i>	36
<i>Obrázek 21 Neupravený (vlevo) a upravený histogram systému Ikeda</i>	37
<i>Obrázek 22 Bifurkační diagramy systému Ikeda, pro změny</i>	37
<i>Obrázek 23 Neupravený (vlevo) a upravený histogram Hénonovy mapy</i>	38
<i>Obrázek 24 Bifurkační diagramy pro Hénonovu map, měněným</i>	38
<i>Obrázek 25 Neupravený (vlevo) a upravený histogram systému Holmes cubic map</i>	39
<i>Obrázek 26 Bifurkační diagramy pro Holmes cubic map, měněným</i>	39
<i>Obrázek 27 Neupravený (vlevo) a upravený histogram systému Burgers map</i>	40
<i>Obrázek 28 Bifurkační diagramy pro Burgers map, měněným</i>	40
<i>Obrázek 29 Neupravený (vlevo) a upravený histogram systému Chirikov</i>	41
<i>Obrázek 30 Bifurkační diagram pro systém Chirikov</i>	41
<i>Obrázek 31 Neupravený (vlevo) a upravený histogram disipativního systému</i>	42
<i>Obrázek 32 Bifurkační diagramy pro disipativní</i>	42

SEZNAM TABULEK

Tabulka 1 Přehled vybraných chaotických systémů.....	20
--	----

SEZNAM PŘÍLOH

PI CD s textem práce a zdrojovými kódy