۸

بررسی رفتار دنباله‌های تولید شده توسط نگاشتهای آشوبی

محمد دخیل علیان — دانشگاه صنعتی اصفهان — دانشکدهٔ برق و کامپیوتر — تلفن: ۸۹۱۲۴۵۰(۰۳۱) — Md-alian@iut.cc.ac.ir

محمدرضا عارف — دانشگاه صنعتی شریف — دانشکدهٔ برق — تلفن:۸۹۱۲۱۱۴(۰۳۱) — Aref@awww.dci.co.ir

بابک صادقیان — دانشگاه صنعتی امیر کبیر — دانشکدهٔ کامپیوتر — تلفن:۶۱۳۹۴۳۳(۰۲۱) — Basadegh@ce.aku.ac.ar

چکیده: سیستمهای آشوبی از آنجا که دارای رفتاری نامنظم و تصادف‌گون هستند در بسیاری از کاربردها می‌توانند مورد استفاده قرار گیرند.در این مقاله با توجه خواص قابل توجه این سیستمها سعی شده است رفتار نامنظم دنباله‌های تولید شده توسط برخی نگاشتهای آشوبی به منظور استفاده جهت تولید دنباله‌های شبه تصادفی مورد بررسی قرار گیرد.

کلمات کلیدی: آشوب، دنباله‌های شبه‌تصادفی، سیستمهای رمز پی‌درپی، متغیرهای تصادفی.

۱- مقدمه

آشوب یکی از رفتارهای جالب توجه است که بسیاری از پدیده‌های فیزیکی، شیمیایی، جوی و... قابل مشاهده می‌باشد[۲] غیرخطی بودن از جمله عوامل مهم برای بروز رفتار آشوبی در سیستمهای دینامیکی و پدیده‌های طبیعی است. سیستمهای آشوبی از آنجا که دارای ساختاری معین[1] بوده و در عین حال دارای رفتاری تصادفی هستند، در سالهای اخیر توجه بسیاری از محققین را به خود معطوف داشته است.

سیستمهای رمز پی‌درپی از آنجا که برای رمز کردن اطلاعات از یک دنبالهٔ تصادفی باید استفاده نمایند زمینهٔ مساعدی را جهت استفاده از دنباله‌های تولید شده توسط سیستمهای آشوبی(دنباله‌های آشوبی) فراهم می‌کند. به همین خاطر در این مقاله توجه خود را به بررسی رفتار این نگاشتها معطوف نموده‌ایم. در این مقاله ابتدا سیستمهای با دینامیک یک بعدی[2] را به اجمال بیان خواهیم نمود. بر همین اساس چهار نگاشت ارگادیک متداول که دارای رفتار آشوبی هستند معرفی خواهند شد. پارامترهای نمای لیاپانف و تابع خودهمبستگی دنباله‌های تولید شده توسط این نگاشتها و علاوه بر آن تابع‌چگالی پایا[3](*idf*) از جمله مواردی است که به آن پرداخته خواهد شد. متعاقب آن با توجه به ارتباط تنگاتنگ رفتار تصادفی دنباله‌های آشوبی با متغیرهای تصادفی که با تابع‌چگالی پایا(*idf*) ارتباط مستقیم دارد، متغیرهای تصادفی را با دیدگاهی خاص مورد بررسی قرار داده و قضایایی را در این ارتباط مطرح خواهیم نمود. نتایج این بخش کمک موثری در توجیه رفتار دنباله‌های آشوبی می‌نماید. در ادامه رفتار نگاشتهای آشوبی را در عمل مورد بررسی قرار داده و اثر محدودیت محاسبات یا گردکردن اعداد را بر دنباله‌های آشوبی خصوصاً در مورد دوره تناوب آنها مورد توجه قرار می‌دهیم.

۲-نگاشتهای یک بعدی

آشوب در سیستمهای با معادلات غیرخطی در حالتهای یک بعدی و چندبعدی بروز می‌کند و غیرخطی بودن یک شرط لازم برای ظهور این

1- Deterministic

2 -One dimentional

3 - Invariant Density Function.

رفتار در سیستمها می‌باشد [۲]. از آنجا که هدف ما نهایتاً بکارگیری این سیستمها برای تولید دنباله‌های شبه‌تصادفی است، لذا سیستمهایی با معادلات دیفرنس[1] که توسط نگاشتهایی به صورت (۱) قابل بیان هستند، مورد بررسی قرار می‌گیرند:

$$x_{n+1} = g(x_n) \qquad (۱)$$

$g(.)$ یک نگاشت غیرخطی است و x_n نیز در حالت کلی می‌تواند یک بردار باشد. از آنجا که پیاده‌سازی نگاشتهای یک بعدی ساده بوده و ثانیاً رفتار آنها به قدر کافی پیچیده می‌باشد، بدین جهت این نگاشتها برای هدف مورد نظر انتخاب گردیدند. نگاشتهایی که در این مقاله مورد بررسی قرار می‌گیرند، نگاشتهایی هستند که روی یک ناحیه پیوسته محدود از اعدادحقیقی دارای رفتار آشوبی می‌باشد.

فرض کنید دنبالهٔ اعداد $x_0, x_1, x_2, \cdots, x_n$ توسط نگاشت(۱) بدست آمده باشد که در این دنباله x_i برابر(۲) می‌باشد:

$$x_i = g(g(\cdots g(x_0)\cdots)) \qquad (۲)$$

تحت شرایط خاصی رفتار دنبالهٔ مورد نظر نامنظم واصطلاحاً آشوبی خواهد شد. از جملهٔ این شرایط حساسیت نسبت به حالت اولیه، "تراگذار توپولوژیکی[2]"بودن و چگال[3] بودن نقاط تناوبی درناحیهٔ تعریف[۲]می‌باشد. البته‌آشوب در شاخه‌های مختلف علوم تعاریف و تعابیر مختلفی پیدا کرده است وتعریف واحدی برای آن ذکر نشده است، با این وجود حساسیت نسبت به حالت اولیه از مهمترین این ویژگیها به شمار می‌رود[۳].

تحت نگاشت آشوبی g دو نقطه کنار هم از یکدیگر دور خواهند شد. میزان دور شدن نقاط از یکدیگر معیاری برای رفتار آشوبی نگاشت می‌باشد. نمای لیاپانف($\lambda(x_0)$)پارامتری است که به همین منظور تعریف شده است.

$$\lambda(x_0) = \lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N-1} \log\left|g'(x_i)\right| \qquad (۳)$$

برای آشوبی بودن نگاشت، باید λ مثبت باشد. این پارامتر جهت مقایسه کمی نگاشتها مورد استفاده قرار می‌گیرد.

یکی از ویژگیهای دنباله‌های تولید شده توسط نگاشتهای آشوبی(دنباله‌های آشوبی) رفتار نامنظم و تصادفی آنها می‌باشد. به منظور توصیف این رفتار برای دنباله‌های آشوبی "تابع چگالی پایا" *(idf)* تعریف شده است. تابع چگالی پایا درست نظیر تابع چگالی احتمال بوده و تمامی خواص آن را دارا می‌باشد. تابع چگالی پایا برای نگاشت $g(.)$ که روی فاصلهٔ واحد[4] به صورت(۴) بیان شده است :

$$x_{n+1} = g(x_n) \quad x_n \in [0,1] \qquad n = 0,1,2,\cdots \qquad (۴)$$

اینچنین تعریف می‌گردد :

$$f(x) = \lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N} \delta\left[x - g^{i}(x_0)\right] \qquad (۵)$$

اگر تابع چگالی پایا به x_0 وابسته نباشد، نگاشت مورد نظر را ارگادیک گویند[۴]. برای یک نگاشت آشوبی ارگادیک با تابع چگالی‌پایای $f(x)$، نمای لیاپانف از رابطهٔ انتگرالی(۵-۶) بدست می‌آید:

$$\lambda = \int f(x) \log\left|g'(x)\right| dx \qquad (۶)$$

با استفاده از تابع چگالی پایا تابع همبستگی[5] دنباله‌ها نیز به‌صورت (۷) محاسبه می‌شود[۴]:

$$c(m) = \lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N-1} \overline{x}_{i+m} \cdot \overline{x}_i \qquad ; \overline{x}_i = f^{i}(x_0) - \overline{x} \qquad \text{و} \qquad \overline{x} = \lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N-1} f^{i}(x_0) \qquad (۷)$$

که در عبارت فوق $\overline{x}$ برابر میانگین اعداد حاصل از تکرارهای مختلف در دنباله می‌باشد.

اگر تابع چگالی پایا برای نگاشت ارگادیک مورد نظر برابر $f(x)$ باشد، در این صورت تابع خودهمبستگی به‌صورت زیر محاسبه می‌شود[۴]:

---

1 -Difference

2 -Topologically trnsitive.

3 - Dense.

4 -Unit interval

5 -Correlation function.

$$c(m) = \int x g^{m}(x) f(x)\,dx - \left[\int x f(x)\,dx\right]^2 \quad (۸)$$

نگاشت لجستیک: نگاشت لجستیک به صورت(۹)تعریف می‌شود. رفتار این نگاشت به ازای تغییرات پارامتر μ دقیقاً مورد بررسی قرار گرفته است[۲].

$$g(x) = \mu x(1-x) \qquad x \in [0,1] \quad (۹)$$

این بررسیها نشان می‌دهد، حوالی $\mu = 4$ رفتار نگاشت روی فاصلهٔ واحد آشوبی می‌گردد. هنگامی که μ از مقدار خاصی حوالی ...۳/۸۳ بزرگتر شود نمای لیاپانف مثبت شده، و از این نقطه به بعد است که رفتار آشوبی نمایان می‌گردد. به ازای، $\mu = 4$ نگاشت لجستیک دارای ویژگیهای خاص یک نگاشت آشوبی بوده و نگاشت مذکور دارای هیچ سیکل جاذبی[1] روی ناحیه واحد نخواهد بود[۲]. این نگاشت یک نگاشت ارگادیک می‌باشد که تابع چگالی پایا برای آن به صورت(۱۰) محاسبه شده است[۴]:

$$f(x) = \frac{1}{\pi\sqrt{x(1-x)}} \qquad x \in [0,1] \quad (۱۰)$$

باتوجه به تابع چگالی پایا، نمای لیاپانف برای این نگاشت برابر $Ln2$ بدست آمده است[۴].

علاوه بر این تابع خودهمبستگی نگاشت $g(x) = 4x(1-x)$ به صورت زیر بدست می‌آید[۱]

$$c(m) = \frac{\delta(m)}{8} \qquad m = 0,1,2,\cdots \quad (۱۱)$$

رابطهٔ(۱۱) نشان می‌دهد که نتایج حاصل شده از تکرارهای نگاشت لجستیک ناهمبسته هستند.

نگاشت مثلثی: نگاشت مثلثی در حالت کلی به صورت (۱۲) تعریف می‌شود:

$$g(x) = \begin{cases} cx & 0 < x \le 0.5 \\ c(1-x) & 0.5 < x \le 1 \end{cases} \qquad 1 < c \le 2 \quad (۱۲)$$

تابع چگالی پایا برای این نگاشت(به ازای $c=۲$)به صورت یکنواخت می‌باشد[۵]. یعنی:

$$f(x) = 1 \qquad 0 \le x \le 1 \quad (۱۳)$$

بر همین اساس به سادگی می‌توان دید که نمای لیاپانف این نگاشت برابر $Ln(c)$ می‌گردد[۵].

با توجه به یکنواخت بودن تابع‌چگالی، تابع همبستگی نگاشت مثلثی به‌صورت زیر محاسبه شده است[۴] :

$$c(m) = \frac{\delta(m)}{12} \qquad m = 0,1,2,\cdots \quad (۱۴)$$

رابطهٔ(۱۴) نشان می‌دهد که نتایج حاصل شده از تکرارهای نگاشت مثلثی نیز همچون نگاشت لجستیک ناهمبسته می‌باشد.

نگاشت بکر : نگاشت بکر به‌صورت زیر تعریف می‌شود :

$$g(x) = \begin{cases} \frac{x}{c} & 0 \le x < c \\ \frac{x-c}{1-c} & c \le x \le 1 \end{cases} \qquad 0 < c < 1 \quad (۱۵)$$

تابع چگالی پایا و نمای لیاپانف این نگاشت نظیر نگاشت مثلثی بوده ولی تابع همبستگی این نگاشت کاملاً متفاوت می‌باشد. تابع همبستگی نگاشت بکر به ازای $c = 0.5$ برابر(۱۶) می‌گردد[۵]:

$$c(m) = \frac{1}{3 \times 2^{m+2}} \qquad m = 0,1,2 \quad (۱۶)$$

همانطور که ملاحظه می‌شود نتایج حاصل از تکرار نگاشت بکر همبسته بوده و میزان همبستگی با افزایش m به‌صورت نمایی کاهش می‌یابد.

نگاشت چبی‌چف: نگاشتهای چبی‌چف به‌صورت زیر تعریف می‌شود:

$$g_k(x) = \cos(t\cos^{-1}x) \qquad -1 \le x \le 1 \qquad ,t = 2,3,\cdots \quad (۱۷)$$

نگاشت چبی‌چف به ازای مقادیر مختلف t دارای تابع چگالی پایایی برابر $\frac{1}{\pi\sqrt{1-x^2}}$ می‌باشد[۶] و نمای لیاپانف و تابع همبستگی برای این نگاشت به‌صورت زیر محاسبه شده است [۱]:

1-Attracting periodic orbit.

$$\lambda = ln(t) \tag{۱۸}$$

$$c(m) = \frac{\delta(m)}{2} \qquad m = 0,1,2,\cdots \tag{۱۹}$$

با توجه به رابطهٔ(۱۹) مقادیر حاصل شده از تکرارهای نگاشت چبی‌چف نیز ناهمبسته می‌باشند.

۳- برخی ویژگیهای متغیرهای تصادفی

همانطور که بیان گردید، نگاشتهای آشوبی ارگادیک، دنباله‌هایی تولید خواهند نمود که رفتاری نامنظم و تصادف‌گونه داشته- که رفتار تصادفی آنها مستقل از حالت اولیهٔ نگاشت، توسط تابع‌چگالی پایا توصیف می‌گردد. تابع‌چگالی پایا نظیر تابع چگالی احتمال برای متغیرهای تصادفی می‌باشد. بنابراین مشابهت دنباله‌های آشوبی با نمونه‌های یک متغیر تصادفی کمک مؤثری در توجیه رفتار دنباله‌های آشوبی خواهد نمود. برای این منظور متغیرهای تصادفی پیوسته‌ای که روی فاصلهٔ[۰،۱] تعریف شده‌اند را مورد بررسی قرار می‌دهیم.

فرض کنید X یک متغیر تصادفی پیوسته باشد که نمونه‌های آن را به صورت اعداد اعشاری و با دقت نامحدود نمایش می‌دهیم. قبل از مطرح کردن قضیه‌ای در این خصوص، توضیح این نکته ضروری است که مقدار یک عدد اعشاری در پیمانه یک برابر مقدار اعشار آن عدد تعریف می‌شود[۷]

قضیه ۱: فرض کنید X یک متغیر تصادفی پیوسته با تابع چگالی احتمال $f_X(x)$ باشد که روی ناحیه [۰،۱] تعریف شده است. اگر $f_X(x)$ تابعی پیوسته، مشتق‌پذیر و متقارن نسبت به خط $x=0.5$ باشد، آنگاه تابع‌چگالی احتمال متغیر تصادفی $Y = a^k X \ mod\ 1$ ($k = 0,1,2,\cdots$ ، $a = 2,4,6,\cdots$) الف) نسبت به خط $y=0.5$ متقارن است. ب) با افزایش k، متغیر تصادفی Y به سمت یک متغیر تصادفی با توزیع یکنواخت میل خواهد نمود[۱]

به منظور استفاده از قضیهٔ۱ و تشابه رفتار دنباله‌های آشوبی با نمونه‌های یک متغیر تصادفی مثالی را مورد بررسی قرار می‌دهیم. فرض کنید $f_X(x)$ تابع چگالی احتمال متغیر تصادفی X باشد که به صورت(۱۰) تعریف شده است. $f_X(x)$ دارای محور تقارن $x=0.5$ می‌باشد، بنابراین قضیهٔ۱ برای آن برقرار است. حال رفتار متغیر تصادفی $Y = 10^k X \ mod\ 1$ را از طریق شبیه سازی مورد بررسی قرار می‌دهیم، برای اینکار ابتدا متغیر تصادفی X را شبیه سازی کرده و به کمک آن Y را به ازای kهای مختلف تولید می‌کنیم. برای تولید متغیر تصادفی X کافی است یک متغیرتصادفی یکنواخت در فاصله (۰،۱) را به تابع $F_X^{-1}(u) = \frac{1}{2}\left\{\sin\left[\pi(u-\frac{1}{2})\right]+1\right\}$ اعمال نماییم.

شکل (۱-الف) تابع‌چگالی احتمال حاصل شده از شبیه سازی متغیر X را نشان می‌دهد- که نظیر تابع(۱۰) می‌باشد. با اعمال تابع $Y = 10^k X \ mod\ 1$ به نمونه‌های X توابع چگالی Y به ازای kهای مختلف بدست می‌آید. در شکل(۱-ب)، (۲-ج)و (۲-د) این توابع که در شبیه سازی بدست آمده، نشان داده شده‌اند. همانطور که ملاحظه می‌شود با افزایش k تابع چگالی احتمال $f_{Y,k}(y)$ به تدریج به سمت یک توزیع یکنواخت میل نموده است(شکل(۱-د) را ملاحظه نمایید).

حال نگاشت لجستیک را در نظر می‌گیریم. دنبالهٔ حاصل شده توسط این نگاشت یعنی $x_0, f^1(x_0), f^2(x_0), \cdots$ دارای یک رفتار تصادفی نظیر متغیر X می‌باشد. از آنجا که این نگاشت یک نگاشت ارگادیک با تابع چگالی‌پایای(۱۱) است، انتظار داریم، نتایج قضیهٔ۱ برای دنباله‌های ترمی تولید شده، توسط چنین نگاشتی برقرار باشد. شبیه سازی و تولید دنباله‌های آشوبی توسط نگاشت $g(x)$ و بدست آوردن تابع چگالی نمونه‌ها نشان می‌دهد که رفتار دنباله‌ها و نمونه‌های متغیرتصادفی X کاملاً با یکدیگر شباهت دارد. شکلهای(۲-الف) الی (۲-د) نتایج این شبیه سازی را نشان می‌دهد. برای بررسی تابع احتمال هریک از ارقام اعشاری یک متغیر تصادفی در فاصلهٔ[۰،۱] قضیهٔ ۲را می‌توان بیان نمود:

قضیه ۲: اگر X یک متغیر تصادفی پیوسته در فاصلهٔ[۰،۱] با تابع توزیع $F_X(x)$ باشد، در این‌صورت تابع احتمال متغیر تصادفی $Y = \left[a^k X\right] mod\ \ a$ به صورت زیر خواهد شد[۱]

$$\underset{y=0,1,2,\ldots,a-1}{P_{Y,k}(y)} = P(Y=y) = \sum_{i=0}^{a^{k-1}-1}\left(F_X\left(\frac{m+y+1}{a^i}\right) - F_X\left(\frac{m+y}{a^i}\right)\right) \tag{۲۰}$$

علاوه بر این اگر $f_X(x)$ نسبت به خط $x=0.5$ متقارن باشد، در این صورت داریم

$$P_{Y,k}(y) = P_{Y,k}(a-1-y) \quad y = 0,1,\cdots,a-1 \qquad k = 1,2,\cdots \tag{۲۱}$$

([.] در صورت قطب نشان دهندهٔ جزء صحیح می‌باشد)

در قضیهٔ۲ با شرط تقارن $f_X(X)$ نسبت به خط $x=0.5$، به سادگی می‌توان ثابت نمود که تابع احتمال متغیرتصادفی $Y=\left[a^k X\right] mod \quad a$ با افزایش k به سمت یک متغیر تصادفی گسستهٔ یکنواخت میل خواهد نمود[۱] یعنی:

(۲۲)

$$\lim_{k \to +\infty} P_{Y,k}(Y=y)=a^{-1} \qquad y=0,1,\cdots,a-1$$

بنابراین انتظار داریم آنتروپی Y با افزایش k به سمت $log_2 a$ میل کند. یعنی:

(۲۳)

$$\lim I_k(Y)=-\lim \sum_{y=0}^{a-1} P_{Y,k}(y) log_2\left[P_{Y,k}(y)\right]=log_2 a$$

به عنوان مثال آنتروپی متغیرتصادفی $Y=\left[10^k X\right] mod \ 10$ به ازای kهای مختلف و برای متغیرتصادفی X با تابع‌چگالی (۱۰) به صورت جدول(۱) محاسبه شده است. همانطور که ملاحظه می‌شود، آنتروپی $I_k(Y)$ با افزایش k سریعاً به سمت $log_2 10$ میل می‌کند.

برای بررسی استقلال ارقام اعشاری متغیرهای تصادفی قضیهٔ زیر را بیان نموده‌ایم.

قضیه ۳: اگر Y یک متغیر تصادفی پیوسته یکنواخت روی[۰،۱] باشد، کلیه متغیرهای تصادفی زیر مستقل از هم می‌باشند[۱]

$$D_k=\left[a^k Y\right] \ mod \ a \quad k=1,2,\cdots$$

دنباله‌های آشوبی تولید شده توسط نگاشتهای ارگادیک اساساً با یک متغیر تصادفی متفاوت می‌باشند. ولی از آنجا که رفتار تصادف‌گونهٔ این نگاشتها مشابه با متغیرهای‌تصادفی توسط یک تابع‌چگالی توصیف می‌گردد، بنابر این چگونگی رفتار متغیرهای‌تصادفی کمکی در توجیه رفتار مؤلفه‌های دنباله‌های تولید شده توسط نگاشتهای آشوبی خواهد بود. البته نتایج بیان شده در حالت کلی برای این دنباله‌ها برقرار نیست، چرا که در هر حال دنباله‌های آشوبی توسط حالت اولیه خود کاملاً مشخص بوده و رفتار نامنظم آنها به خاطر شرایط خاص غیرخطی بودن نگاشت می‌باشد. اما از آنجا که رفتار ایستان مؤلفه‌های این دنباله‌ها نظیر نمونه‌های یک متغیر تصادفی با تابع احتمالی معلوم می‌باشد، نتایجی مشابه با آنچه در قضایای این بخش مطرح نمودیم برای این دنباله‌ها دور از انتظار نمی‌باشد.

۴- اثر محدودیت دقت‌محاسبات بر رفتار تناوبی و تابع‌همبستگی

ویژگی نگاشتهای آشوبی نظیر غیرقابل پیش‌بینی بودن،از جمله ویژگیهای جالب توجه در کاربردهای عملی، از جمله رمزنگاری می‌باشد. از آنجا که در بکارگیری این نگاشتها همواره با خطای گردکردن و یا به عبارتی محدود بودن دقت محاسبات مواجه هستیم، لذا در این بخش این موضوع مورد بررسی قرار می‌گیرد.

هنگامی‌که دقت محاسبات r رقم اعشار (در مبنای a) باشد، حداکثر a^r حالت مختلف برای ارقام بعد از ممیز اعشار قابل تصور است. به عبارت دیگر با یک سیستم گسسته با تعداد حالات محدود مواجه می‌باشیم. در پیاده‌سازی نگاشت $g(x)$ و تولید دنباله‌های مورد نظر، این واقعیت باعث بروز سیکلهایی با دورهٔ تناوب محدود می‌گردد. خوشبختانه نتایج عملی پیاده‌سازی این نگاشتها حاکی از آن است که رفتار نامنظم نگاشتها مستقل از حالت اولیه، با تابع‌چگالی پایای نگاشت تطابق دارد. این نتیجه به نوعی حاکی از اعتبار تئوری ارگادیک می‌باشد. دنباله‌ای که توسط نگاشتی با دقت r رقم اعشار توسط یک کامپیوتر تولید می‌گردد، دارای رفتار غیرتناوبی است و تکرارهای تابع روی یک ناحیه باعث ایجاد شبه مدارهایی[1] (یا دنباله‌هایی با طول گذرای اولیه، که نهایتاً به یک دنبالهٔ متناوب یا سیکل ختم می‌شوند) می‌گردد که با تقریب مناسبی نظیر سیکلهایی است که توسط دنباله‌های آشوبی ایجاد می‌گردد. بنابر این با اتکا بر تابع‌چگالی پایاء می‌توان خواص آماری دنباله‌هایی که توسط یک نگاشت آشوبی توسط کامپیوتر و با دقت محدود بدست می‌آیند را مورد بررسی قرار داد.

در بخش قبل تابع‌چگالی پایای نگاشت لجستیک که توسط کامپیوتر و با دقت چهارده رقم اعشار حاصل شده بود در شکل(۲) مشخص گردید. این اشکال علاوه بر نشان دادن رفتار نامنظم این دنباله‌ها، تطابق رفتار دنباله‌های تولید شده را با تابع چگالی مربوطه نشان می‌دهد. در مورد دیگر نگاشتهای مطرح شده در این فصل نیز رفتاری مشابه وجود دارد. نکته مهمی که در پیاده‌سازی نگاشتها وجود دارد، چگونگی رفتار تناوبی دنباله‌هاست. گردکردن اعداد هنگام محاسبه نگاشتها، نظیر یک نویز بر رفتار نگاشت اثر می‌گذارد ولی یکی از اثرات آن تغییر ساختار

---

1 - Pseudo orbit

تناوبی مدارهای دنباله‌های آشوبی است گردکردن اعداد باعث ایجاد دنباله‌های غیرتناوبی می‌شود که پس از طی تکرارهای بی‌شمار سرانجام به یک دنبالهٔ متناوب و یا به یک نقطه ثابت ختم می‌گردد

در شبیه‌سازیهای انجام شده، برای تولید هر دنباله ابتدا یک حالت اولیه به‌صورت تصادفی در فاصله دامنهٔ تعریف نگاشت انتخاب و سپس تعدادی مؤلفه از دنباله به عنوان حداکثر طول گذرای اولیه در نظر گرفتیم که آن را L_{in} می‌نامیم. پس از مشاهدهٔ L_{in} مؤلفهٔ اول به جستجوی سیکلهای نهایی و اندازه‌گیری دوره تناوب آنها پرداختیم. در شبیه‌سازی نگاشت لجستیک با رابطهٔ $g(x) = 4x(1-x)$ ابتدا دقت محاسبات ده رقم اعشار در نظر گرفته شد(در مبنای ده). نتایج شبیه سازیها نشان داد، اگر L_{in} کمتر از 10^5 باشد، عملاً تعداد قابل توجهی از دنباله‌های مورد آزمایش به سیکل نهایی نمی‌رسند. به عبارت دیگر این دنباله‌ها دارای طول گذرای اولیهٔ بیش از 10^5 می‌باشند. هنگامی‌که L_{in} برابر 10^6 انتخاب شود، تقریباً تمامی دنباله‌ها به سیکلهای نهایی خود خواهند رسید. با در نظر گرفتن ۱۰۰۰ دنباله و $L_{in} = 10^6$، ۵ سیکل نهایی با دوره تناوبهای ۶۹۶۴۰۱، ۷۵۱۷۷و ۲۲۴۶۳۱مشاهده گردید و ۸۳۴ دنباله نهایتا به سیکل با دوره تناوب ۲۲۴۶۳۱ختم شده‌اند. از میان دنباله‌های مورد آزمایش دو دنباله به سیکل نهایی نرسیده‌اند، به عبارت دیگر دو دنباله دارای طول اولیهٔ گذرایی بیش از 10^6 بودند(یا سیکل نهایی آنها دورهٔ تناوبی بیش از 10^6 داشته است). با افزایش L_{in} به 10^7 و تکرار آزمایش کلیهٔ دنباله‌ها به سیکلهای نهایی خود می‌رسند. نکتهٔ حایز اهمیت دیگر در این است که سیکل با دوره تناوب ۱ در نتایج ظاهر می‌شود. حال دقت محاسبات را چهارده رقم اعشار در نظر می‌گیریم. علاوه بر افزایش طول گذاری اولیه دوره تناوب سیکلها نیز افزایش می‌یابد. در این حالت با در نظرگرفتن L_{in} به اندازه 10^7 مولفه، حدود ۹۷۲دنباله از هزار دنباله مورد آزمایش به سیکل نهایی خود نرسیدند به عبارت دیگر طول گذاری اولیه آنها بیش از 10^7 بوده است. اگر L_{in} برابر 10^8 مؤلفه در نظر گرفته شود، نتایج حاصل از آزمایش ۱۰۰دنباله نشان می‌دهد که تمامی آنها به سیکلهای نهایی خود می‌رسند. از این میان بیش از نصف دنباله‌ها با طول گذاری نسبتاً بزرگ نهایتاً به دنبالهٔ تماماً صفر خواهند رسید (سیکل با دورهٔ تناوب ۱) و اکثریت قریب به اتفاق دنباله‌های باقیمانده نیز به سیکلی با دوره تناوب ۱۵۷۸۴۵۲۱ختم می‌شوند. اگر دقت محاسبات به ۲۰رقم اعشار افزایش یابد، آزمایشهای مختلف نشان داد که با در نظر گرفتن L_{in} تا اندازهٔ 10^8 هیچیک از دنباله‌های مورد آزمایش به سیکلهای نهایی نرسیدند. افزایش L_{in} به میزانی بیش از 10^8 مؤلفه، زمان شبیه‌سازی را بسیار طولانی و غیرعملی خواهد نمود. بنابر این نتایج شبیه‌سازی نگاشت لجستیک به‌وضوح نشان می‌دهند که با افزایش دقت محاسبات، طول گذاری اولیه ودوره تناوب سیکلهای نهایی نیز افزایش می‌یابد. با توجه به مطالب بخش۲ اگر پارامتر نگاشت لجستیک(μ) اندکی کمتر از چهار باشد، باز هم رفتار دنباله‌های تولید شده آشوبی خواهد بود. حال اگر نگاشت لجستیک را به شکل $(4-\varepsilon)x(1-x)$ در نظر بگیریم، نقیصه بیان شده رفع می‌شود. نتایج شبیه سازی نشان داد که اگر دقت محاسبات چهارده رقم اعشار و $\varepsilon = 10^{-12}$ باشد، بازای $L_{in} = 10^7$ هیچ سیکل نهایی مشاهده نشد. اگر L_{in} برابر 10^8 مؤلفه در نظر گرفته شود، نتایج حاصل از ۱۰۰دنبالهٔ نمونه نشان داد که ۹۸ دنباله نهایتاً به سیکلی با دوره تناوب ۶۳۲۶۱۵۳۱ختم می‌شوند. البته نتایج این شبیه‌سازی نشان داد که سیکلهای نهایی اگر چه دارای دوره تناوب یکسانی هستند ولی لزوما همگی دنباله‌ها به یک سیکل یکسان ختم نمی‌شوند. این نتایج نشان می‌دهد که اولاً با انتخاب مناسب ε می‌توان اثر سیکلهای با دوره تناوب یک (تماما صفر) را حذف نمود و ثانیاً دوره تناوب سیکل نهایی و طول گذاری اولیه را نیز افزایش داد. در این حالت اگر دقت محاسبات ۲۰رقم اعشار و مثلاً $\varepsilon = 10^{-18}$ باشد به ازای $L_{in} = 10^8$ هیچ سیکلی نهایتاً مشاهده نشد. در مورد نگاشتهای دیگر نیز این بررسیها انجام گرفته و نتایج مشابهی حاصل شده است[۱].

در انتهای این بخش نتایج آزمایشهای شبیه سازی در مورد همبستگی دنباله‌های آشوبی را مورد بررسی قرار می‌دهیم. همانطور که دیدیم تابع همبستگی نگاشتهای لجستیک، مثلثی و چبی‌چف به‌صورت تابع ضربه گسسته بوده و تابع همبستگی نگاشت بکر نیز به‌صورت نمایی میرا می‌گردد. برای بررسی اثر محدودیت دقت محاسبات بر روی تابع همبستگی نگاشتها، صد دنباله بطول ۱۰۰۰۰ مؤلفه- که حالتهای اولیهٔ آنها به‌صورت تصادفی انتخاب شده بودند- مورد آزمایش قرار گرفتند.

نتایج شبیه سازی نگاشتهای لجستیک، مثلثی، بکر وچبی‌چف در جدول(۲) درج شده است. همانطور که ملاحظه می‌گردد، $c(0)$ بدست آمده با نتایج نظری کاملاً مطابقت دارد، در مورد نگاشتهای لجستیک، مثلثی و چبی‌چف مقادیر $c(m)$ به ازای مقادیر $m \neq 0$ بسیار کوچک ودر حد انتظار می‌باشد. در مورد نگاشت بکر نیز مقادیر نسبتاً بزرگتر می‌باشند که با توجه به رابطهٔ(۲۰) قابل توجیه می‌باشد.آنچه در مجموع

می‌توان بیان نمود این است که اگر دقت محاسبات در پیاده‌سازی نگاشتها مناسب انتخاب گردد، به ازای حالتهای اولیه مختلف اولاً دنباله‌ها غالباً پس از طی طول گذاری قابل توجه سرانجام به سیکلهای با دورهٔ تناوب بزرگ ختم می‌شوند. ثانیاً رفتار نامنظم و تصادفی دنباله‌ها به خوبی توسط تابع چگالی پایا توصیف می‌گردند و ثالثاً دنباله‌های تولید شده از لحاظ تابع همبستگی نیز مطلوب می‌باشند. در این میان تنها نگاشت بکر از جهت تابع همبستگی قدری ضعیف می‌باشد.

۵- خلاصه و نتیجه گیری

استفاده از نگاشتهای آشوبی با توجه به خصوصیات جالب توجه آنها به عنوان ابزاری برای تولید دنبالهٔ کلید اجرایی در سیستمهای رمز قابل بررسی است[۱]. رفتار نامنظم و تصادف‌گونهٔ مؤلفه‌های دنبالهٔ آشوبی توسط تابع چگالی پایا توصیف می‌شوند، همانطور که نمونه‌های یک متغیر تصادفی با تابع‌چگالی احتمال. از آنجا که قصد ما بکارگیری این دنباله‌ها برای تولید دنباله‌های باینری شبه‌تصادفی است، چگونگی رفتار مؤلفه‌های آنها -که در عمل به صورت اعدادی حقیقی با دقت محدود هستند- حایز اهمیت می‌باشد. بدین جهت با تکیه بر نگاشتهای ارگادیک و چهار نگاشت لجستیک، مثلثی، بکر، و چبی‌چف و با توجه به شباهت تابع‌چگالی پایا و تابع‌چگالی احتمال، خواص جالب توجهی از متغیرهای تصادفی استخراج گردید. اگر نمونه‌های این متغیرهای تصادفی را به صورت اعداد حقیقی با دقت نامحدود فرض کنیم، ملاحظه نمودیم که ارقام با وزن کمتر نمونه‌ها سریعاً دارای توزیع یکنواختی خواهند شد و آنتروپی ارقام سریعاً به سمت $log_2 a$ میل می‌کنند، از طرف دیگر با یکنواخت شدن توزیع ارقام، ثابت نمودیم که ارقام مستقل از یکدیگر نیز خواهند شد. مشابهت رفتاری مؤلفه‌های یک دنبالهٔ آشوبی با نمونه‌های یک متغیر تصادفی، این انتظار را بوجود می‌آورد که اولاً ارقام با وزن کمتر مؤلفه‌های یک دنبالهٔ آشوبی دارای توزیع یکنواخت‌تری باشند و ثانیاً ارقام با وزن کمتر وابستگی کمتری نسبت به یکدیگر داشته باشند. نتایج شبیه‌سازیها به خوبی نشان می‌دهد که دنباله‌های تولید شده توسط نگاشتهای آشوبی دارای چنین ویژگیهایی می‌باشند. این حقیقت کمک مؤثری در تولید دنباله‌های باینری با خواص آماری مطلوب و امنیت بالا خواهد بود[۱]. از جمله نکات حایز اهمیت در این بررسی، تاثیر محدود بودن دقت محاسبات در پیاده‌سازی نگاشتها و چگونگی رفتار نقاط تناوبی و تابع همبستگی می‌باشد. همانطور که ملاحظه گردید، در نگاشتهای مورد نظر با افزایش دقت محاسبات طول گذاری اولیه دنباله‌ها بزرگتر شده و دورهٔ تناوب سیکلهای نهایی نیز افزایش می‌یابد و نهایتاً دنباله‌های آشوبی به سیکلهای با دورهٔ تناوب بسیار بزرگی ختم می‌گردند. از جمله معایب این پیاده‌سازیها بروز سیکلهای با دورهٔ تناوب یک (یا احیاناً دورهٔ تناوب کوچک) می‌باشد که باید به نحو مناسبی از ایجاد آن جلوگیری نمود. این چاره‌اندیشی لزوم بررسی دقیق رفتار تناوبی دنباله‌ها را ضروری می‌نماید. بنابراین باید چگونگی رفتار تناوبی دنباله‌ها و تأثیر دقت محدود بر روی آن از لحاظ نظری کاملاً مشخص گردد و یا حداقل کرانی برای دورهٔ تناوب دنباله‌های اثبات گردد. در مورد تابع‌همبستگی نیز نتایج شبیه‌سازی نشان می‌دهد که دنباله‌های تولید شده توسط نگاشتهای لجستیک، مثلثی و چبی‌چف با تقریب خوبی ناهمبسته می‌باشند و در مورد نگاشت بکر نیز با توجه به رابطهٔ تابع همبستگی این نگاشت، نتایج قابل قبول می‌باشند.

۵-مراجع

[۱] محمد دخیل‌علیان "*ارزیابی دنباله‌های شبه تصادفی و طراحی مولدهای آشوبی*" ، دانشگاه صنعتی اصفهان، دانشکدهٔ برق و کامپیوتر، رسالهٔ دکترا، آبان ۱۳۷۷.

[2] Devaney R.L., An Introduction to Chaotic Dynamically Systems, *Second Edition,Addison Wesley, 1989.*

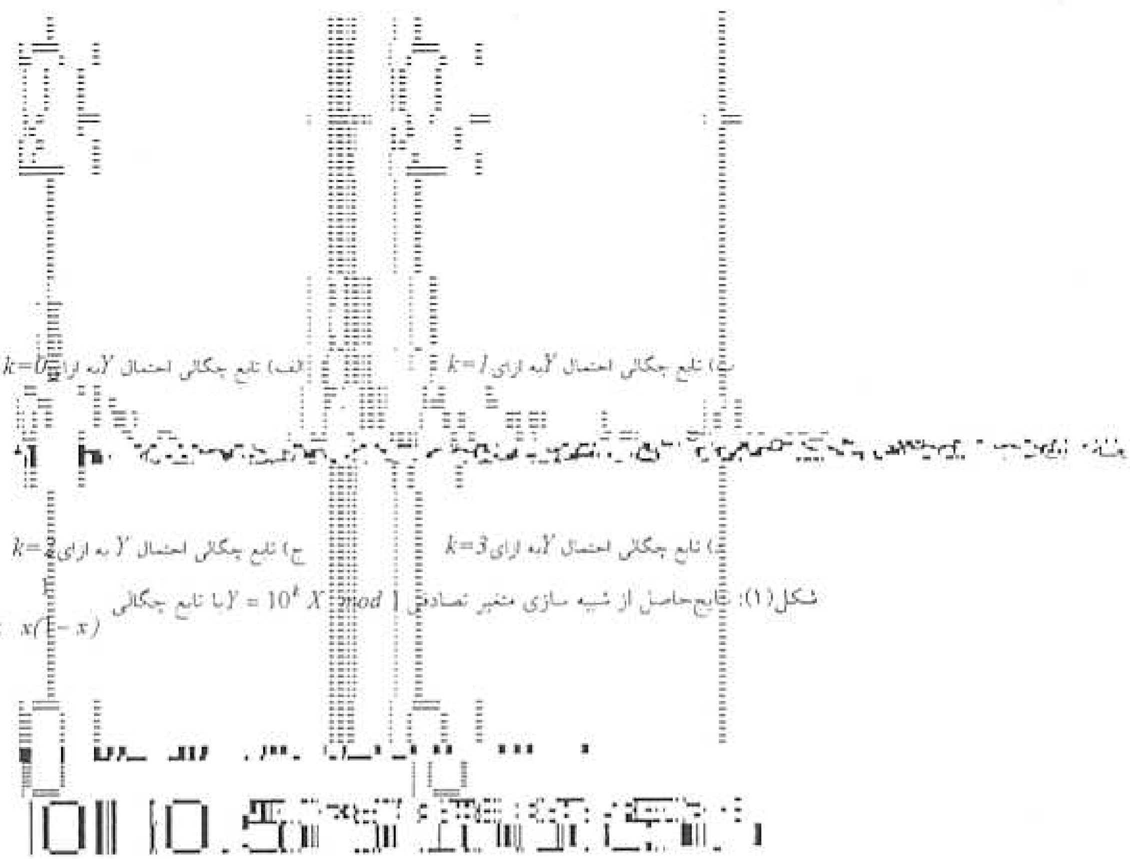
[3] Hao Bai-Lin, CHAOS II, *Word Scientific Pub. Co. Singapore, 1990.*

[4] Schuster H.G., Deterministic Chaos, *Third augmented edition, Weiheim, New York, VCH, 1995.*

[5] Walker W.T., Chaotic Pseudo-Random Sequences and Radar, *Ph.D. Thesis University of Arizona,1993.*

[6] Kohada T. and Tsunenda A., "Pseudo-Noise Sequence by Chaotic Nonlinear Maps and Their Correlation Properties", ICICE Transaction on communication ,E76-B, pp.855-863, 1993.

[7] Parker T.S. and Chua L.O., "Chaos: A Tutorial for Engineers", IEEE Proceeding , vol.75, No.8,August 1987.



$k=0$ الف) تابع چگالی احتمال Y به ازای

$k=1$ ب) تابع چگالی احتمال Y به ازای

$k=2$ ج) تابع چگالی احتمال Y به ازای

$k=3$ د) تابع چگالی احتمال Y به ازای

شکل(۱): نتایج حاصل از شبیه سازی متغیر تصادفی $Y = 10^k X \ mod\ 1$ با تابع چگالی $f_X(x) = \frac{1}{\pi \sqrt{x(1-x)}}$

الف) تابع چگالی پایای نگاشت لجستیک

$k=1$ ب) تابع چگالی پایای Y به ازای

$k=2$ ج) تابع چگالی پایای Y به ازای

$k=3$ د) تابع چگالی پایای Y به ازای

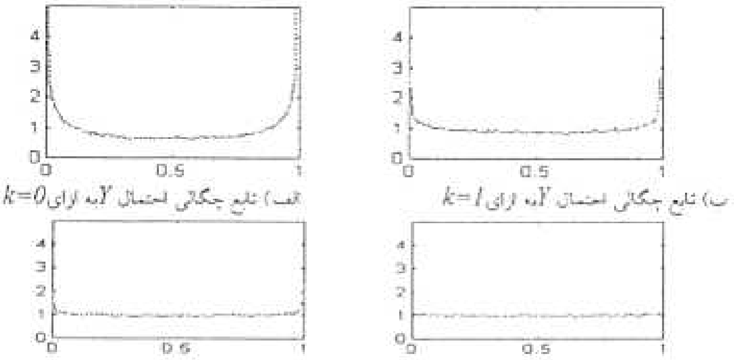
شکل(۲): نتایج حاصل از شبیه سازی نگاشت لجستیک و تبدیلهای $Y = 10^k X \ mod\ 1$.

جدول(۱):آنتروپی متغیر تصادفی Y به ازای kهای مختلف($log_2 10 \approx 3.321928$).

k	۱	۲	۳	۴	۵	۶	۷
$I_k(Y)$	۳/۱۲۹۱۱۸	۳/۳۰۱۵۸۲	۳/۳۱۹۷۸۶	۳/۳۲۱۷۱۰	۳/۳۲۱۹۰۶	۳/۳۲۱۹۲۵	۳/۳۲۱۹۲۷

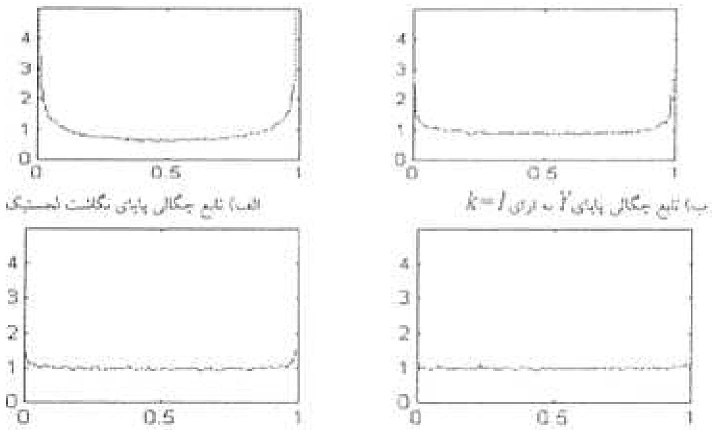
جدول (۲): میانگین و مقادیر تابع همبستگی حاصل از شبیه‌سازی نگاشتها. طول دنباله‌ها = ۱۰۰۰۰ و تعداد دنباله‌ها در هر آزمایش=۱۰۰۰

چبی چف مرتبه۳	چبی چف مرتبه۲	بیکر	مثلثی	لجستیک	
5.8456 E-5	2.1104 E-4	0.50025	0.5013	0.5003	میانگین
0.5000	0.5000	0.0836	0.0836	0.1250	c(0)
6.6813 E-4	1.0355 E-4	0.0415	-4.4110 E-6	1.9840 E-4	c(1)
-2.1934 E-4	-1.0938 E-3	0.0207	6.6712 E-4	-9.8317 E-5	c(2)
1.2288 E-4	-6.6742 E-4	0.0102	3.9161 E-4	1.1307 E-4	c(3)
6.6337 E-6	4.8914 E-4	0.0054	2.3718 E-4	-1.6438 E-4	c(4)
-6.4974 E-4	-2.0921 E-4	0.0028	3.1134 E-4	-8.9336 E-5	c(5)
-1.3345 E-4	-1.3628 E-4	0.0014	2.4425 E-4	9.1525 E-6	c(6)
3.1173 E-4	-1.2978 E-4	0.0007	1.8810 E-4	1.5818 E-4	c(7)
3.9597 E-4	8.1855 E-4	3.7374 E-4	1.3996 E-4	-6.6496 E-5	c(8)
-3.9259 E-4	5.3741 E-4	2.69051 E-6	1.0095 E-5	7.7023 E-5	c(9)
2.3553E-4	-7.3941 E-4	1.0470 E-4	2.6434 E-4	2.3467 E-5	c(10)



الف) تابع چگالی احتمال Y به ازای $k=0$ — ب) تابع چگالی احتمال Y به ازای $k=1$ — ج) تابع چگالی احتمال Y به ازای $k=2$ — د) تابع چگالی احتمال Y به ازای $k=3$

شکل(۱): نتایج حاصل از شبیه سازی متغیر تصادفی $Y = 10^k X \mod 1$ با تابع چگالی $f_X(x) = \frac{1}{\pi\sqrt{x(1-x)}}$



الف) تابع چگالی پایای نگاشت لجستیک — ب) تابع چگالی پایای Y به ازای $k=1$ — ج) تابع چگالی پایای Y به ازای $k=2$ — د) تابع چگالی پایای Y به ازای $k=3$

شکل(۲): نتایج حاصل از شبیه سازی نگاشت لجستیک و تبدیلهای $Y = 10^k X \mod 1$.

جدول(۱): آنتروپی متغیر تصادفی Y به ازای kهای مختلف ($\log_2 10 \approx 3.321928$)

k	۱	۲	۳	۴	۵	۶	۷
$I_k(Y)$	۳/۱۲۹۱۱۸	۳/۳۰۱۵۸۴	۳/۳۱۹۷۸۶	۳/۳۲۱۷۱۰	۳/۳۲۱۹۰۶	۳/۳۲۱۹۲۵	۳/۳۲۱۹۲۷

جدول (۲): میانگین و مقادیر تابع همبستگی حاصل از شبیه‌سازی نگاشتها: طول دنباله‌ها = ۱۰۰۰۰ و تعداد دنباله‌ها در هر آزمایش=۱۰۰۰

چبی چف مرتبهٔ۳	چبی چف مرتبهٔ۲	بکر	تنتی	لجستیک	
5.8456 E-3	2.1104 E-4	0.50025	0.5013	0.5003	میانگین
0.5000	0.5000	0.0836	0.0836	0.1250	c(0)
6.6813 E-4	1.0355 E-4	0.0415	-4.4110 E-6	1.9840 E-4	c(1)
-2.1934 E-4	-1.0938 E-3	0.0207	6.6712 E-4	-9.8317 E-5	c(2)
1.2288 E-4	-6.6742 E-4	0.0102	3.9161 E-4	1.1307 E-4	c(3)
6.6337 E-6	4.8914 E-4	0.0054	2.3718 E-4	-1.6438 E-4	c(4)
-6.4974 E-4	-2.0921 E-4	0.0028	3.1134 E-4	-8.9336 E-5	c(5)
-1.3345 E-4	-1.3628 E-4	0.0014	2.4425 E-4	9.1525 E-6	c(6)
3.1173 E-4	-1.2978 E-4	0.0007	1.8810 E-4	1.5818 E-4	c(7)
3.9597 E-4	8.1855 E-4	3.7374 E-4	1.3996 E-4	-6.6496 E-5	c(8)
-3.9259 E-4	5.3741 E-4	2.69051 E-6	1.0095 E-5	7.7023 E-5	c(9)
2.3553E-4	-7.3941 E-4	1.0470 E-4	2.6434 E-4	2.3467 E-5	c(10)