دانشگاه صنعتی خواجه‌نصیرالدین طوسی
دانشکده مهندسی برق

(۳)

ششمین کنفرانس مهندسی برق ایران
۲۲ - ۲۴ اردیبهشت ۱۳۷۷

معرفی یک آزمون خودهمبستگی جدید

محمد دخیل علیان
دانشگاه صنعتی اصفهان
دانشکدهٔ برق وکامپیوتر

محمدرضا عارف
دانشگاه صنعتی شریف
دانشکدهٔ برق

فاکس: ۸۹۱۲۲۵۰ - ۰۳۱
پست الکترونیکی: md-alian@ cc.iut.ac.ir

چکیده

آزمونهای آماری ابزاری برای بررسی خواص دنباله های شبه تصادفی است. دنباله هایی که به عنوان کلید اجرایی در سیستمهای رمز "پی در پی"[1] مورد استفاده قرارمی گیرند باید از لحاظ خواص آماری مطلوب باشند تا اطلاعات نشت یافته به متن رمز شده حداقل شود. در این راستا آزمونهای مختلفی ارائه شده است که در این مقاله ضمن بیان آزمون خودهمبستگی ، آزمون جدیدی که عملکرد آن بسیار مطلوب می باشد ارائه می گردد.

کلمات کلیدی: آزمونهای آماری ، آزمون خودهمبستگی ، رمزکننده های پی در پی ، دنباله های تصادفی.

۱. مقدمه

در بسیاری از کاربردها، از جمله سیستمهای رمز پی در پی استفاده از دنباله هایی که کاملا" تصادفی عمل کنند، از اهمیت قابل توجهی برخوردار می باشد. منظور از یک دنبالهٔ تصادفی، دنباله ای با سمبلهای مستقل ودارای توزیع یکنواخت می باشد(i.i.d[2]). بدلیل محدودیتهای عملی، استفاده از دنباله های تصادفی در این سیستمها میسر نیست و معمولا" از مولدهای خاصی برای تولید دنباله های مورد نظر استفاده می شود. این دنباله ها در واقع شبه تصادفی هستند، به این معنا که در طراحی این مولدها سعی شده است خواص آماری دنباله های تولید شده به دنباله های تصادفی بسیار نزدیک باشد.

باشناخت خواص آماری دنباله های تصادفی، معیارهایی برای دنباله های شبه تصادفی بیان شده است[۳] و متعاقب آن نیز آزمونهای متعددی برای بررسی تصادفی بودن دنباله ها ابداع گردیده است. آزمونهای آماری بر روی بخش کوچکی از دنباله انجام می شود و طی آن، دنباله در آزمون قبول یا رد می گردد. برای ارزیابی یک مولد معمولا" تعداد زیادی دنباله مورد آزمایش قرار می گیرند و لازم است تعداد قابل توجهی از دنباله ها، از آزمون موفق بیرون آیند. ذکر این نکته ضروری است که قبول یا رد دنباله ای در یک آزمون دلیل بر تصادفی بودن یک دنباله نیست، زیرا در این آزمونها رفتار نوعی دنباله های تصادفی مد نظر قرار می گیرد و بدین جهت دنباله هایی که با این رفتار نوعی مطابقت داشته باشند، مورد قبول واقع می گردند.

---

[1] Stream Cipher

[2] Independently and Identically Distributed

آزمون خود همبستگی از جمله آزمونهای مطرح شده می باشد([۲] و[۴]) که در این مقاله به آن پرداخته می شود و متعاقب آن آزمون خودهمبستگی مناسب تری معرفی خواهد شد.

۲. آزمون خودهمبستگی

برای بررسی میزان تصادفی بودن یک دنباله می توان از آزمونهای آماری استفاده نمود. بطور نمونه در یک دنبالهٔ n بیتی انتظار این است که تقریباً $\frac{n}{2}$ بیتها صفر باشد و یا توزیع دو بیتهای ۰۰، ۰۱، ۱۰، ۱۱ در یک دنباله یکنواخت باشد. آزمون فرکانس آزمونی است که توزیع بیتهای صفر ویک را در دنباله مورد بررسی قرار داده و آن را با حالت ایده آل مقایسه می کند[۴]. برای بررسی دو بیتها، سه بیتها و ...، آزمونهای سریال، سریال تعمیم یافته، پوکر و پوکر تعمیم یافته[۵] ابداع شده اند- که هر یک بگونه ای توزیع چند بیتهای مختلف را در دنباله مورد بررسی قرار می دهد. آزمون خودهمبستگی، رنها، مشتقات باینری و ... نمونه های دیگری از اینها می باشند([۲]، [۴] و [۷]) - که از این میان به بیان آزمون خودهمبستگی خواهیم پرداخت.

دنباله های کاملاً تصادفی که مؤلفه های آن مستقل از هم و با توزیع یکنواخت باشند دارای تابع خودهمبستگی غیر همفاز[3] صفر می باشند. بنابر این در دنباله های نوعی تولید شده توسط یک منبع B.S.S[4] انتظار داریم تابع خودهمبستگی غیر همفاز مقدار کوچکی باشد.

تابع خودهمبستگی برای یک دنبالهٔ متناوب $\tilde{S} = \{s_1, s_2, \ldots, s_T, s_1, s_2, \ldots\}$ با دورهٔ تناوب T به صورت زیر تعریف می گردد.

$$C(\tau) = \frac{A-D}{T} = \frac{1}{T}\left(T - 4\sum_{i=1}^{T} s_i + 4\sum_{i=1}^{T} s_i \cdot s_{i+\tau}\right) \qquad (1)$$

که در عبارت فوق A تعداد بیتهای موافق و D تعداد بیتهای مخالف در دنبالهٔ مورد نظر و شیفت یافتهٔ آن می باشد. برای دنبالهٔ با طول محدود n نظیر $S^n = \{s_1, s_2, \ldots, s_n\}$، تابع خودهمبستگی معادل محاسبهٔ تابع خودهمبستگی میان دو

[3] Inphase

[4] Binary Symmetric Source

دنبالهٔ $S_1^{n-\tau} = \{s_1, s_2, \ldots, s_{n-\tau}\}$ و $S_{\tau+1}^n = \{s_{\tau+1}, s_{\tau+2}, \ldots, s_n\}$ می باشد که به صورت زیر بدست می آید:

$$C(\tau) = \frac{A-D}{n-\tau} \qquad (۲)$$

که در رابطهٔ(۲)، A تعداد بیتهای موافق و D تعداد بیتهای مخالف در دو دنباله است. فرض کنید $A(\tau)$ به صورت زیر تعریف شود:

$$A(\tau) = \sum_{i=1}^{n-\tau} s_i \cdot s_{i+\tau} \qquad (۳)$$

در این صورت اگر مولفه های دنبالهٔ S^n مستقل از هم باشند، داریم :

$$\mu_1 = E[A(\tau)] = \frac{n_1^2(n-\tau)}{n^2} \qquad (۴)$$

در عبارت فوق n_1 تعداد یکها در دنبالهٔ S^n می باشد.

بر اساس روابط (۳) و(۴)، آزمونی مطرح شده است که پارامتر کای-دوی[5] آن به صورت زیر بیان شده است [۴]،[۵] :

$$\chi^2_m = \sum_{\tau=1}^{t} \frac{(A(\tau)-\mu_1)^2}{\mu_1} \qquad (۵)$$

اگر دنبالهٔ A^τ را به صورت زیر تعریف کنیم :

$$A^\tau = s_1 \cdot s_{1+\tau}, s_2 \cdot s_{2+\tau}, \ldots, s_{n-\tau} \cdot s_n = a_1, a_2, \ldots, a_{n-\tau} \qquad (۶)$$

در این صورت برای یک τ خاص آزمون کای-دو در صورتی قابل انجام است که مولفه های دنباله A^τ مستقل از هم باشند. در صورت صحت چنین فرضی طبق قضیهٔ حد مرکزی $A(\tau)$ برای n های بزرگ با تقریب خوبی دارای توزیع نرمال می باشد. اما چنین فرضی برای دنبالهٔ A^τ صحیح نیست. به عنوان نمونه در دنبالهٔ A^1 مولفه های مجاور هم مستقل نیستند، زیرا $P(a_i / a_{i+1}) \neq P(a_i)$ $(i = 1,2,\ldots,n-1)$ می باشد.

۳. معرفی آزمون خودهمبستگی جدید

با در نظر گرفتن تعریف تابع خودهمبستگی برای دنبالهٔ S^n (رابطهٔ (۲)) دنبالهٔ C^τ را بصورت زیر تعریف میکنیم:

$$C^\tau = s_1 \oplus s_{1+\tau}, s_2 \oplus s_{2+\tau}, \ldots, s_{n-\tau} \oplus s_n = C_1^\tau, C_2^\tau, \ldots, C_{n-\tau}^\tau \qquad (۷)$$

(که در رابطهٔ(۷) $\oplus$ عملگر XOR می باشد)

با توجه به روابط (۲) و (۷)، تابع خودهمبستگی به صورت زیر تبدیل می شود:

[5] Chi-square

$$C(\tau)=\frac{n_0(\tau)-n_1(\tau)}{n-\tau}=1-\frac{2n_1(\tau)}{n-\tau}=1-\frac{2\sum_{j=1}^{n-\tau}C_j^{\tau}}{n-\tau}$$

$$\tau=1,2,\ldots,n-1$$

(۸)

در عبارت(۸)، $n_0(\tau)$ و $n_1(\tau)$ به ترتیب تعداد صفرها ویکها در دنبالهٔ C^{τ} می باشند.

لم ۱: اگر s_1 ،s_2 ،s_3 سه متغیر تصادفی باینری مستقل با توزیع یکنواخت باشند آنگاه :

الف) متغیر تصادفی $c_1^1=s_1\oplus s_2$ دارای توزیع یکنواخت بوده و مستقل از s_1 و s_2 می باشد.

ب) متغیرهای تصادفی $c_1^1=s_1\oplus s_2$ و $c_1^2=s_1\oplus s_3$ مستقل از هم می باشند.

اثبات: برای اثبات بند الف ، ابتدا ثابت می کنیم c_1^1 دارای توزیع یکنواخت است :

$$P(c_1^1=i)=P(s_1\oplus s_2=i)=P(s_2=i/s_1=0)P(s_1=0)+P(s_2=i\oplus 1/s_1=1)P(s_1=1)$$
$i\in\{0,1\}$

(۹)

با توجه به استقلال s_1و s_2 داریم :

$$P(c_1^1=i)=P(s_2=i)P(s_1=0)+P(s_2=i\oplus 1)P(s_1=1)$$

و بنابراین :

$$P(c_1^1=i)=\frac{1}{4}+\frac{1}{4}=\frac{1}{2} \qquad (۱۰)$$

حال ثابت می کنیم که c_1^1 مستقل از s_1 می باشد. برای این کار فرض کنید $i,j\in\{0,1\}$ باشند، در این صورت خواهیم داشت:

$$P(c_1^1=i/s_1=j)=P(s_2=i\oplus j/s_1=j)=P(s_2=i\oplus j)$$

و با توجه به توزیع s_2 و رابطهٔ(۱۰) داریم :

$$P(c_1^1=i/s_1=j)=P(c_1^1=i)=\frac{1}{2} \qquad (۱۱)$$

بطور مشابه متغیر c_1^1 از s_2 نیز مستقل می باشد.

برای اثبات بند (ب) می توان نوشت :

$$P(c_1^1=i,c_1^2=j)=P(s_2=i,s_3=j/s_1=0)P(s_1=0)+P(s_2=i\oplus 1,s_3=j\oplus 1/s_1=1)P(s_1=1)$$

با توجه استقلال s_1,s_2,s_3 از رابطهٔ فوق داریم :

$$P(c_1^1=i,c_1^2=j)=\frac{1}{8}+\frac{1}{8}=\frac{1}{4} \qquad (۱۲)$$

با توجه به رابطهٔ (۱۰) و (۱۲) نتیجه می گیریم که:

$$P(c_1^1=i,c_1^2=j)=P(c_1^1=i)P(c_1^2=j)=\frac{1}{4} \qquad (۱۳)$$

پس c_1^1 و c_1^2 مستقل می باشند.

■

قضیه ۱: اگر $S^n=s_1,s_2,\ldots,s_n$ یک دنبالهٔ تصادفی باینری با مولفه های مستقل و دارای توزیع یکنواخت باشد آنگاه دنبالهٔ

$$C^{\tau}=s_1\oplus s_{1+\tau},s_2\oplus s_{\tau+2},\ldots,s_{n-\tau}\oplus s_n=C_1^{\tau},C_2^{\tau},\ldots,C_{n-\tau}^{\tau}$$

(۱۴)

نیز یک دنبالهٔ با مولفه های مستقل و توزیع یکنواخت می باشد.

اثبات: با توجه به لم۱ هر یک از مولفه های C^{τ} دارای توزیع یکنواخت است. برای اثبات استقلال مولفه های C^{τ} از یکدیگر کافی است احتمال زیر :

$$P(c_i^{\tau}=b_i/c_1^{\tau}=b_1,c_2^{\tau}=b_2,\ldots,c_{i-1}^{\tau}=b_{i-1},c_{i+1}^{\tau}=b_{i+1},\ldots,c_{n-\tau}^{\tau}=b_{n-\tau})$$
$$i=1,2,\ldots,n-\tau \quad ,b_i\in\{0,1\}$$

(۱۵)

برابر $P(c_i^{\tau}=b_i)$ باشد. برای اثبات میتوان نوشت:

$$P\left(c_i^{\tau}=b_i\Big/\bigcap_{\substack{j=1\\j\neq i}}^{n-\tau}(c_j^{\tau}=b_j)\right)=P\left(s_{i+\tau}=b_i\Big/\bigcap_{\substack{j=1\\j\neq i}}^{n-\tau}(c_j^{\tau}=b_j),s_i=0\right)P(s_i=0)+$$
$$P\left(s_{i+\tau}=b_i\oplus 1\Big/\bigcap_{\substack{j=1\\j\neq i}}^{n-\tau}(c_j^{\tau}=b_j),s_i=1\right)P(s_i=1)$$

(در عبارت فوق $\bigcap$ علامت عطف می باشد)

با توجه به اینکه s_i و $s_{i+\tau}$ مستقل هستند همچنین طبق لم۱ $s_{i+\tau}$ از کلیهٔ c_j^{τ} ها مستقل می باشد. بنابراین داریم:

$$P\left(c_i^{\tau}=b_i\Big/\bigcap_{\substack{j=1\\j\neq i}}^{n-\tau}(c_j^{\tau}=b_j)\right)=\frac{1}{4}+\frac{1}{4}=\frac{1}{2}=P(c_i^{\tau}=b_i) \qquad (۱۶)$$

بنابر این کلیهٔ مولفه های C^{τ} مستقل نیز می باشند.

■

با بکارگیری قضیهٔ۱، قضیهٔ حد مرکزی و رابطهٔ(۸) می توان گفت تابع خودهمبستگی دنبالهٔ S^n، یعنی $C(\tau)$ با افزایش n به سمت یک توزیع نرمال با میانگین و واریانس زیر میل خواهد کرد :

$$(\mu_{\tau},\sigma_{\tau})=(0,\frac{1}{\sqrt{n-\tau}}) \qquad (۱۷)$$

لم۲: اگر دنبالهٔ $S^n=s_1,s_2,\ldots,s_n$ یک دنبالهٔ تصادفی باینری با مولفه های مستقل و دارای توزیع یکنواخت باشد آنگاه به ازای n های به مقدار کافی بزرگ($n\to+\infty$) مقادیر تابع

خودهمبستگی $C(1),C(2),...,C(r)$ $(r<<n)$ دوبدو مستقل می باشند.

اثبات: هر یک از $C(1),C(2),...,C(r)$ در حد به سمت یک متغیر تصادفی نرمال با میانگین صفر و واریانس $\frac{1}{n-1},\frac{1}{n-2}$ و ... $\frac{1}{n-r}$ میل می کند، از طرف دیگر با استفاده از رابطة(۸) داریم :

$$E[C(i)C(j)] = 1 - 2\frac{\sum_{k=1}^{n-i} E(c_k^i)}{n-i} - 2\frac{\sum_{k=1}^{n-j} E(c_k^j)}{n-j} + 4\frac{\sum_{k=1}^{n-i}\sum_{m=1}^{n-j} E(c_k^i c_m^j)}{(n-i)(n-j)} \qquad i \neq j \qquad (۱۸)$$

با توجه به لم۱، c_k^i, c_m^j مستقل از هم بوده، و علاوه بر این با در نظر گرفتن اینکه میانگین و واریانس هر یک از مولفه های دنبالة C^n برابر $\frac{1}{2}$ و $\frac{1}{4}$ می باشد، رابطة(۱۸) برابر صفر می گردد.

$$E[C(i)C(j)] = 0 \qquad (۱۹)$$

پس $C(i)$ و $C(j)$ ناهمبسته می باشند. از آنجا که به ازای n های بزرگ این دو متغیر نرمال هستند، بنابراین ناهمبسته بودن به معنای استقلال ایندو از یکدیگر می باشد.

■

قضیه۲: اگر دنبالة $S^n = s_1,s_2,...,s_n$ یک دنبالة تصادفی باینری با مولفه های مستقل و دارای توزیع یکنواخت باشد آنگاه به ازای n های به مقدار کافی بزرگ($n \to +\infty$) مقادیر تابع خودهمبستگی $C(1),C(2),...,C(r)$ $(r<<n)$ تواماً مستقل می باشند.

اثبات: با توجه به لم۲، در حد ($n \to +\infty$) متغیرهای تصادفی $C(1),C(2),...,C(r)$ دوبدو مستقل می باشند. از طرف دیگر با توجه به نرمال بودن توزیع هر یک از این مقادیر نتیجه می گیریم که $C(1),C(2),...,C(r)$ تواماً مستقل نیز هستند.

■

۳. آزمون کای-دو

در مبحث متغیرهای تصادفی، توزیعی به نام کای-دو مطرح می باشد.این متغیر تصادفی به این نحو تعریف می گردد که اگر X یک متغیر تصادفی نرمال با میانگین μ و واریانس σ^2 باشد، در این صورت متغیر تصادفی $\frac{(X-\mu)^2}{\sigma^2}$ را یک متغیر تصادفی کای-دو (χ^2) با یک درجة آزادی گویند. اگر n کمیت تصادفی $X_1, X_2, ..., X_n$ را که مستقل از هم و با توزیع نرمال هستند را در نظر بگیریم، می توان متغیر تصادفی کای-دوی جدیدی به صورت زیر تعریف نمود:

$$\chi^2 = \sum_{i=1}^{n} \frac{(X_i-\mu_i)^2}{\sigma_i^2} \qquad (۲۰)$$

تعداد اجزاء مستقل تشکیل دهندة تابع $\sum_{i=1}^{n}\frac{(X_i-\mu_i)^2}{\sigma_i^2}$ را درجة آزادی متغیر کای-دو می گویند.

قضیه۳ (جمع پذیری کای-دو)**:** اگر $\chi^2_{v_1}, \chi^2_{v_2}, ..., \chi^2_{v_k}$ کمیتهای مستقل از هم باشند بطوری که هر یک به ترتیب دارای درجات آزادی $v_1, v_2, ..., v_k$ باشند، آنگاه حاصل جمع آنها یعنی :

$$\chi^2_v = \chi^2_{v_1} + \chi^2_{v_2} + ...\chi^2_{v_k} \qquad (۲۱)$$

نیز یک متغیر تصادفی کای-دو با درجة آزادی $v = v_1 + v_2 + ... + v_k$ خواهد شد.

در بسیاری از مسایل عملی هدف ما آزمون کردن دو فرض در مقابل یکدیگر می باشد. در اینگونه مسایل فرض مشخص بودن تابع چگالی احتمال برای یک متغیر تصادفی که نمونه گیری شده است در مقابل این فرض که تابع چگالی احتمال از آن نوع مشخص نباشد، مورد آزمون قرار می گیرد. یک روش آزمون نمودن چنین فرضهای توزیعی، آزمون زیبندگی کای-دو است. در همین ارتباط آزمونهای آماری استاندارد معمولاً با بکارگیری متغیرهای تصادفی چند جمله ای و قضیة زیر تعریف شده اند.

قضیه۴: اگر $(X_1, X_2, ..., X_n)$ یک متغیر تصادفی چند جمله ای با پارامترهای n و $P_1, P_2, ..., P_m$ باشد، که در آن X_i هر یک از مقادیر a_j $(j = 1,2,...,m)$ را با احتمال زیر بگیرد:

$$P(X_i = a_j) = P_j \qquad j = 1,2,...,m \qquad i = 1,2,...,n \qquad (۲۲)$$

در این صورت با تعریف U به صورت رابطة (۲۳):

$$U = \sum_{i=1}^{m} \frac{(N_i - nP_i)^2}{nP_i} \qquad (۲۳)$$

هنگامی که $n \to +\infty$ میل کند، U بسمت توزیع کای-دو با m-1 درجهٔ آزادی میل خواهد کرد. یعنی :

$$\forall k \in R\,,\ \lim_{n \to +\infty} F_U(k) = F_{\chi^2}(k) \qquad (۲۴)$$

که در آن $F_{\chi^2}(k)$ تابع توزیع متغیر تصادفی کای-دو می باشد که برابر است با :

$$F(k) = \int_0^k \frac{2^{-(\frac{m-1}{2})}\, y^{(\frac{m-3}{2})}\, e^{-\frac{y}{2}}}{\Gamma(\frac{m-1}{2})}\, dy \qquad (۲۶)$$

N_i در رابطهٔ(۲۳) تعداد دفعاتی است که a_i در نمونهٔ متغیر تصادفی چند جمله ای ظاهر شده است.

برای انجام آزمون کای-دو و بررسی این فرض که $(X_1, X_2, \ldots, X_n)$ یک نمونه از متغیر تصادفی چند جمله ای با پارامترهای معین $P_1, P_2, \ldots, P_m$ است یا نه، نمونهٔ مورد نظر را اختیار کرده و U را توسط رابطهٔ(۲۳) محاسبه می کنیم. اگر $U > \chi^2_{1-\alpha}$ ، یعنی بزرگتر از $100(1-\alpha)$ امین در صد توزیع کای-دو با m-1 درجهٔ آزادی شد، فرض را رد می کنیم. اگر فرض درست باشد ، احتمال رد شدن آن در آزمون برابر α می باشد. در واقع α احتمال خطای نوع اول می باشد. تا زمانی که $nP_i > 5$ $(i = 1,2,\ldots,m)$ باشد، تقریب کای-دو برای توزیع U کاملاً خوب می باشد[۶].

۴. آزمون خودهمبستگی جدید

برای انجام آزمون خودهمبستگی به جای استفاده از دنبالهٔ A^τ (رابطهٔ(۶)) می توان از دنبالهٔ C^τ (رابطهٔ(۷)) استفاده نمود.همانطور که در قضیهٔ۱ ملاحظه شد تابع خودهمبستگی دنبالهٔ S^n (برای یک τخاص) در حالت ایده آل به سمت یک متغیر تصادفی نرمال با میانگین و واریانس بیان شده در رابطهٔ(۱۷) میل خواهد نمود. بنابراین با توجه به مطالب بخش۳ به ازای n های بزرگ متغیر تصادفی $\chi^2_{ac}(\tau)$ که به صورت زیر تعریف می گردد بسمت یک متغیر تصادفی کای-دو با یک درجهٔ آزادی میل خواهد کرد.

$$\chi^2_{ac}(\tau) = \left[\frac{C(\tau)}{\frac{1}{\sqrt{n-\tau}}}\right]^2 = \frac{(n - \tau - 2\sum_{i=1}^{n-\tau} c_i^\tau)^2}{n-\tau} \qquad (۲۵)$$

برای انجام آزمون خودهمبستگی روی یک دنبالهٔ نمونه نظیر S^n، ابتدا دنبالهٔ C^τ را بدست آورده وبکمک رابطهٔ(۲۵) پارامتر $\chi^2_{ac}(\tau)$ را محاسبه می کنیم. اگر $\chi^2_{ac}(\tau)$ محاسبه شده از $\chi^2_{1-\alpha}$ بزرگتر شد، فرض ناهمبسته بودن دنبالهٔ S^nو دنبالهٔ شیفت یافته اش (یعنی دنبالهٔ $S_1^{n-\tau}$ و $S_{\tau+1}^n$)را رد می کنیم. در غیر این صورت دنبالهٔ S^n از آزمون خودهمبستگی به ازای شیفت مورد نظر عبور می کند. در این آزمون اگر $\alpha = 0.05$اختیار شود، با استفاده از جدول کای-دو مقدار $\chi^2_{0.95}$ برابر ۳/۸۴ خواهد شد. بنابراین دنبالهٔ S^nاز آزمون خودهمبستگی عبور خواهد کرد هر گاه $\chi^2_{ac}(\tau)$ کوچکتر از ۳/۸۴ گردد.

حال می خواهیم آزمونی ترتیب دهیم که شامل تابع خودهمبستگی یک دنباله به ازای شیفتهای مختلف باشد. اگر طول دنبالهٔ S^n به اندازهٔ کافی بزرگ باشد طبق قضیهٔ۲ کلیهٔ متغیرهای $C(1), C(2), \ldots, C(r)$ $(r << n)$ مستقل از هم می باشند. بنابراین در حد کلیهٔ متغیرهای کای-دوی $\chi^2_{ac}(1), \chi^2_{ac}(2), \ldots, \chi^2_{ac}(r)$ نیز مستقل خواهند شد. بدین ترتیب متغیر تصادفی χ^2_{ac} که به صورت رابطهٔ(۲۷) تعریف می شود، طبق قضیهٔ۳،یک متغیر تصادفی کای-دو با r درجهٔ آزادی می باشد.

$$\chi^2_{ac} = \sum_{\tau=1}^{r}\left[\chi^2_{ac}(\tau)\right]^2 = \sum_{\tau=1}^{r}\left[\frac{C(\tau)}{\sigma_{C_\tau}}\right]^2 = \sum_{\tau=1}^{r}\left[\frac{1 - 2\frac{\sum_{j=1}^{n-\tau} c_j^\tau}{n-\tau}}{\frac{1}{\sqrt{n-\tau}}}\right]^2 \qquad (۲۷)$$

در این حالت برای انجام آزمون خودهمبستگی روی یک دنبالهٔ نمونه نظیر S^n، ابتدا دنباله های C^τ $(1 \le \tau \le r)$ را بدست آورده وبکمک رابطهٔ(۲۷) پارامتر χ^2_{ac} را محاسبه می کنیم. اگر χ^2_{ac} محاسبه شده از $\chi^2_{1-\alpha}$ بزرگتر شد، فرض ناهمبسته بودن دنبالهٔ S^nو دنباله های شیفت یافته اش (یعنی دنباله های $S_1^{n-\tau}$ و $S_{\tau+1}^n$ $(1 \le \tau \le r)$)را رد می کنیم. در غیر این صورت دنبالهٔ S^n از آزمون خودهمبستگی به ازای شیفتهای مورد نظر عبور می کند.

۵. خلاصه و نتیجه گیری

در این مقاله ابتدا مقدمه ای در مورد آزمونهای آماری آورده شد. در این میان آزمون خودهمبستگی به طور دقیق تر مورد بررسی قرارگرفت. سپس با توجه به اینکه این آزمون در مواردی ضعیف عمل می کند، با بررسی خواص دنباله های باینری تصادفی ، در حالت ایده آل آزمون اصلاح شدهٔ جدیدی مطرح گردید. این آزمون نسبت به آزمون قبلی کار آمدتر بوده و نتایج این دو آزمون بر روی دنباله های مختلف مؤید این برتری بوده است[۱].

مراجع

[۱] محمد دخیل علیان "طراحی و ارزیابی دنباله های شبه تصادفی غیر خطی در سیستمهای رمز پی در پی "، رسالهٔ دکترا، دانشگاه صنعتی اصفهان، در حال تدوین.

[۲] محمود مدرس هاشمی "طراحی سیستمهای رمز کنندهٔ پی در پی"، پایان نامهٔ کارشناسی ارشد ، دانشگاه صنعتی اصفهان، ۱۳۷۰.

[3] S.W. Golomb, "*Shift Register Sequences*" , Holden-Day , San Fransisco, 1982.

[4] H. Beker and F. Piper ;*Cipher System : The protection of Communication* ,Northwood Books ,1982.

[5] M. Kimberely," *Comparison of Two Statistical Test for Keystream Sequences*" Electronic Letter,Vol.23, No.8, 9th April 1987.

[6] D. Knuth : *The Art of Computer programming* Vol.2 Addison-Wesley ,1981.

[.7] U. Maurer, "*A Universal Statistical test for Random Bit Generators*", Journal of Cryptology,Vol.5, No.2, pp. 89-105, 1992.