Biuletyn WAT
Vol. LVII, Nr 4, 2008

Wyznaczenie dokładnych wartości parametrów dla testu Maurera

KRZYSZTOF MAŃK

Wojskowa Akademia Techniczna,
Wydział Cybernetyki, Instytut Matematyki i Kryptologii
00-908 Warszawa, ul. S. Kaliskiego 2

Streszcznie. Praca ta jest rozwinięciem artykułu Corona i Naccachego *An accurate evaluation of Maurer's universal test.* Oryginalne wyniki wzbogacone zostały o wyprowadzenie potrzebnych formuł dla zaniechanego przypadku bloku jednobitowego i analizę wpływu skończonego, przybliżonego sposobu liczenia nieskończonych sum występujących w prezentowanych formułach. Na koniec zaprezentowano wyniki obliczeń i porównano je z dotychczas znanymi wartościami.
Słowa kluczowe: test statystyczny, test losowości, test Maurera, test entropii
Symbole UKD: 003.26, 519.2

1. Test entropii Maurera

Test Maurera nazywany jest często testem entropii, ze względu na fakt, iż pozwala w przybliżeniu wyznaczyć entropię badanego ciągu binarnego [2].

Test jest określony przez trzy parametry L, Q i K. Sekwencja bitowa jest dzielona na kolejne bloki o długości L bitów. Całkowita długość próbki wynosi $n = L \cdot (Q + K) \cdot 2^L$ bitów. Sekwencja inicjalizująca ma $Q_c = Q \cdot 2^L$ kroków, natomiast test $K_c = K \cdot 2^L$ kroków.

Niech

$$b_i(s^n) = \left[u_{Li}, u_{Li+1}, \ldots, u_{L(i+1)-1}\right]$$

oznacza i-ty blok dla $i = \overline{0, Q_c + K_c - 1}$, gdzie s^n oznacza całą badaną sekwencję. Zakładamy, że dwa bloki są jednakowe, jeśli składają się z takiego samego ciągu binarnego.

W dalszej części przez $\log x$ rozumieć będziemy logarytm przy podstawie 2. Statystyka testowa jest zdefiniowana następująco:

$$f_T(s^n) = \frac{1}{K_c} \sum_{i=Q_c}^{Q_c+K_c-1} \log A_i(s^n),$$

gdzie funkcja $A_i(s^n)$ jest odległością i-tego bloku od jego ostatniego wystąpienia w całym ciągu czyli:

$$A_i(s^n) = \begin{cases} i, & \sim \exists\limits_{j \geqslant 1} b_i(s^n) = b_{i-j}(s^n), \\ \min\{j : j \geqslant 1, b_i(s^n) = b_{i-j}(s^n)\}, & \text{w p.p.} \end{cases}$$

Maurer pokazał, że dla ciągu losowego zmienna losowa

$$X_u = \frac{f_T(s^n) - \mu}{\sigma}$$

ma w przybliżeniu rozkład $N(0,1)$.
Ostatnim krokiem testu będzie więc wyznaczenie wartości dystrybuanty rozkładu $N(0,1)$ w punkcie X_u.

W dalszej części zakłada się, że $Q_c \to \infty$ i $K_c \to \infty$, przy czym można pokazać, że wystarczy przyjąć $Q = 10$ oraz $K > 33$.

Niech ciąg $U^n = U_1, U_2, \ldots, U_n$ będzie idealnym ciągiem zmiennych losowych, dla których można określić prawdopodobieństwo:

$$P\{A_i(U^n) = a\} = \sum_{b \in B^L} P\{b_i(U^n) = b,\ b_{i-1}(U^n) \neq b, \ldots, b_{i-a+1}(U^n) \neq b,\ b_{i-a}(U^n) = b\},$$

dla $a \geqslant 1$, $Q_c \leqslant i \leqslant Q_c + K_c - 1$ oraz $B \in \{0,1\}$.
Dla sekwencji idealnej bloki b_i są niezależne i równomiernie rozłożone, czyli mamy

$$P\{A_i = a\} = 2^{-L}\left(1 - 2^{-L}\right)^{a-1},$$

wobec tego wartość oczekiwana ma postać:

$$\mu_L = E[f_T] = E[\log A_i] = 2^{-L} \sum_{a=1}^{\infty} \left(1 - 2^{-L}\right)^{a-1} \log a. \quad [2]$$

Następny krok to obliczenie wariancji teoretycznej:

$$\sigma^2 = c(L, K_c)^2 \cdot \frac{D^2[\log A_n]}{K_c},$$

gdzie

$$D^2[\log A_i] = \sigma_{A_i}^2 = E\left[(\log A_i)^2\right] - (E[\log A_i])^2$$
$$= 2^{-L}\sum_{a=1}^{\infty}\left(1-2^{-L}\right)^{a-1}(\log a)^2 - (E[\log A_i])^2\,,$$

jest wariancją zmiennej losowej określającej $\log A_i$, zaś

$$c\,(L,K_c)^2 = d\,(L) + \frac{e\,(L)}{K_c},\ [1]$$

jest współczynnikiem opisującym wpływ kowariancji poszczególnych zmiennych losowych $\log A_i$.
Pierwotnie, w pracy [2] Maurera ostatnie wyrażenie miało zupełnie inną postać i było empirycznym oszacowaniem funkcji $c(L,K_c)$, dopiero stosunkowo niedawno Coron i Naccache podali w pracy [1] sposób dokładnego wyznaczenia postaci tej funkcji. Swoje rozważania ograniczyli jednak do przypadków $3 \leqslant L \leqslant 16$, a podane przez nich wartości stałych $d(L)$ oraz $e(L)$ zostały obliczone ze zbyt małą dokładnością, jak na potrzeby prowadzonych przez Laboratorium badań.

W dalszej części uzupełnimy wyniki zawarte w pracy [1] o przypadki $L = 1$ oraz 2, jak również omówimy sposób dokładniejszego obliczenia stałych, pojawiających się w statystyce testowej. Celem naszym jest znalezienie możliwie dokładnych.

Za cel przyjęliśmy dokładność zmiennoprzecinkowego typu *extended* języka C++, czyli $64+1$ bity, co daje do 20 cyfr dziesiętnych – wartości 16 zestawów (dla $L = 1,\ldots,16$) czterech stałych: $E[\log A_n]$, $D^2[\log A_n]$, $d(L)$, $e(L)$.

2. Wyznaczenie współczynnika kowariancji

Pełne wyprowadzenie formuły na $c(L,K_c)^2$, a pośrednio na $d(L)$ i $e(L)$, znaleźć można w pracy [1], ograniczymy się tu do wskazania istotnych elementów użytej metody.

Zgodnie z oznaczeniem przyjętym przez Maurera w oryginalnej pracy [2], wariancję zmiennej losowej, opisującej statystykę testową, wyrażamy jako:

$$\sigma^2 = c(L,K_c)^2 \cdot \frac{D^2[\log A_n]}{K_c},$$

a wówczas $c(L,K_c)^2$ obliczyć można w następujący sposób

$$c(L,K_c)^2 = 1 + \frac{2}{D^2[\log A_n]K_c} \sum_{1 \leqslant i \leqslant j \leqslant K_c} Cov[\log A_{Q+i}, \log A_{Q+j}],$$

a przyjmując $Q_c \to \infty$ możemy przyjąć, że kowariancja pomiędzy zmiennymi losowymi $\log A_{Q+i}$ i $\log A_{Q+j}$ jest jedynie funkcją $k = j - i$ i po zmianie zmiennych $k = j - i$ dostajemy

$$c(L,K_c)^2 = 1 + \frac{2}{D^2[\log A_n]} \sum_{k=1}^{K_c-1} \left(1 - \frac{k}{K_c}\right) Cov[\log A_n, \log A_{n+k}].$$

Kowariancję występującą w sumie liczymy zaś wprost z definicji

$$Cov[\log A_n, \log A_{n+k}] =$$
$$= \sum_{i,j \geqslant 1} \log i \log j \Pr[A_{n+k} = j, A_n = i] - (E[\log A_n])^2.$$

Powyższą sumę autorzy wyznaczyli rozpatrując 5 rozłącznych przypadków. Przyjmując następujące oznaczenia:

$$u = 1 - 2^{-L},$$
$$v = 1 - \frac{1}{2^L - 1},$$
$$h(z,k) = (1-z)\sum_{i=1}^{\infty} z^{i-1} \log(i+k),$$

możemy wcześniejsze wyrażenia zapisać jako:

$$E[\log A_n] = 2^{-L} \sum_{a=1}^{\infty} u^{a-1} \log a = h(u,0),$$
$$D^2[\log A_n] = 2^{-L} \sum_{a=1}^{\infty} u^{a-1} (\log a)^2 - h^2(u,0).$$

Ostatecznie otrzymali oni [1]:

$$Cov[\log A_{Q+i}, \log A_{Q+j}] = u^k \left(h(u,0)(h(v,k) - h(u,k)) \right.$$
$$\left. + 2^{-L} \sum_{a=1}^{\infty} u^{i-1} v^{i-1} \log i (h(u,k+1) - h(v,k+i-1)) \right),$$

na podstawie czego:

$$c(L,K_c)^2 = 1 - \frac{2}{D^2[\log A_n]}\left(p(L,1) - p(L,K_c) - \frac{q(L,1)-q(L,K_c)}{K_c}\right),$$

gdzie

$$p(L,K) = u^{K-1}\sum_{k=1}^{\infty} F(k,L,K)u^{k-1},$$

$$q(L,K) = u^{K-1}\sum_{k=1}^{\infty} G(k,L,K)u^{k-1},$$

$$\begin{aligned} F(k,L,K) &= u^2(h(v,k+K-1)-h(u,k+K))(h(v,0)-v^k h(v,k)) \\ &\quad + u\cdot h(u,0)(h(u,k+K-1)-h(v,k+K-1)), \\ G(k,L,K) &= u(h(v,k+K-1)-h(u,k+K)) \\ &\quad \cdot\left(u(k+K)(h(v,0)-v^k h(v,k)) - 2^{-L}\sum_{i=1}^{k} i\cdot v^{i-1}\log i\right) \\ &\quad + u(k+K-1)h(u,0)(h(u,k+K-1)-h(v,k+K-1)). \end{aligned}$$

Ponieważ wcześniej przyjęliśmy, że $c(L,K_c)^2$ jest postaci $d(L)+\frac{e(L)}{K_c}$, więc z powyższego widać, że mamy

$$d(L) = 1 - 2\frac{p(L,1)-p(L,K_c)}{D^2[\log A_n]},$$

$$e(L) = 2\frac{q(L,1)-q(L,K_c)}{D^2[\log A_n]}.$$

W dalszej części zajmiemy się jeszcze rozpatrzeniem wpływu wyrażeń $p(L,K_c)$ oraz $q(L,K_c)$ na otrzymywane wartości.

Na podstawie przedstawionych wzorów autorzy pracy [1] wyznaczyli numerycznie wartości $d(L)$ i $e(L)$ dla $L = \overline{3,16}$, z niezrozumiałych przyczyn nie wykorzystując ich dla przypadku $L = 2$.
W następnym punkcie powtórzymy ich tok postępowania w celu wyznaczenia $d(1)$ i $e(1)$, który to przypadek rządzi się nieco odmiennymi regułami.

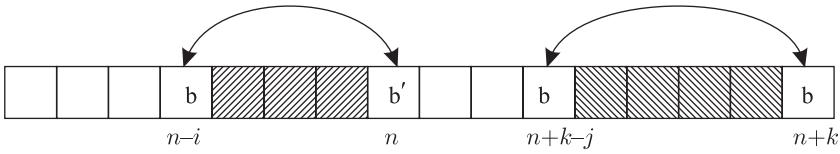
3. Wyznaczenie współczynnika kowariancji dla przypadku $L = 1$

Przypadek bloku jednobitowego jest jakościowo różny od poprzednich, gdyż występują tu tylko dwie możliwe wartości bloku, w związku z czym, niektóre rozpatrywane przypadki redukują się, inne zaś są całkiem niemożliwe. Na początek zauważmy, że dla $L = 1$

$$\Pr[A_m = i] = 2^{-L}(1 - 2^{-L})^{i-1} = \frac{1}{2}\left(1 - \frac{1}{2}\right)^{i-1} = u^i.$$

Obliczać będziemy prawdopodobieństwa $\Pr[A_{n+k} = j, A_n = i]$ dla pięciu różnych przypadków:

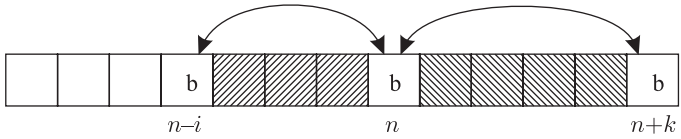
1) rozłączne bloki $1 \leqslant j \leqslant k - 1$



Ponieważ w takim przypadku zdarzenia $A_{n+k} = j$ oraz $A_n = i$ są niezależne, więc

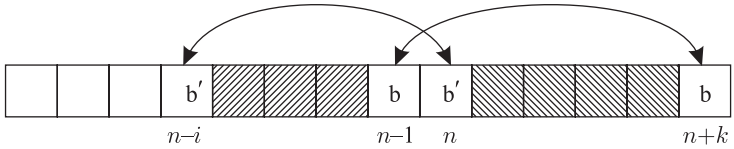
$$\Pr[A_{n+k} = j, A_n = i] = \left(\left(\frac{1}{2}\right)^{i-1} \cdot \frac{1}{2}\right) \cdot \left(\left(\frac{1}{2}\right)^{j-1} \cdot \frac{1}{2}\right) = \left(\frac{1}{2}\right)^{i+j} = u^{i+j},$$

2) następujące po sobie bloki $j = k$



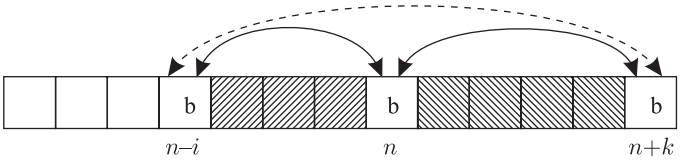
$$\Pr[A_{n+k} = j, A_n = i] = u^i u^j = u^{i+j},$$

3) nakładające się bloki $j = k + 1$, $i \geqslant 2$



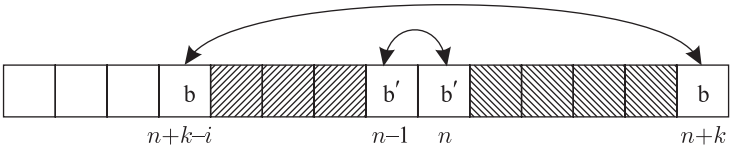
$$\Pr[A_{n+k} = j, A_n = i] = u^{i-1} u u^{k-1} u = u^{i+k} = u^{i+j-1},$$

4) przypadek niemożliwy $j = k + i$



$$\Pr[A_{n+k} = j, A_n = i] = 0,$$

5) bloki zawierające się $i = 1$, $j \geqslant k + 2$



$$\Pr[A_{n+k} = j, A_n = i] = u^j$$

Powyższe wykorzystamy teraz do wyliczenia sumy określającej kowariancję:

$$\begin{aligned} Cov[\log A_n, \log A_{n+k}] &= \sum_{i,j \geqslant 1} \log i \log j \Pr[A_{n+k} = j, A_n = i] - (E[\log A_n])^2 \\ &= \left(u^k \log(k+1) - \sum_{j=k+1}^{\infty} u^j \log j \right) E[\log A_n], \end{aligned}$$

a następnie współczynnika $c(L, K_c)^2$

$$\begin{aligned} c(L, K_c)^2 &= 1 + \frac{2}{D^2[\log A_n]} \sum_{k=1}^{K_c - 1} \left(1 - \frac{k}{K_c}\right) Cov[\log A_n, \log A_{n+k}] \\ &= 1 + \frac{2E[\log A_n]}{D^2[\log A_n]} \left(\sum_{k=2}^{K_c} u^{k-1} \log k - \sum_{j=2}^{\infty} \min\{j-1, K_c - 1\} u^j \log j \right. \\ &\left. - \frac{1}{K_c} \left(\sum_{k=2}^{K_c} (k-1) u^{k-1} \log k - \sum_{j=2}^{\infty} \min\left\{ \frac{j(j-1)}{2}, \frac{K_c(K_c-1)}{2} \right\} u^j \log j \right) \right). \end{aligned}$$

Ponieważ w praktyce K_c jest na tyle duże, że ostatnie wyrażenie można uprościć, przyjmując $K_c \to \infty$, dostajemy:

$$c(L,K_c)^2 = 1 + \frac{2E[\log A_n]}{D^2[\log A_n]} \left(\sum_{j=2}^{\infty} u^{j-1} \log j - \sum_{j=2}^{\infty} (j-1) u^j \log j \right.$$

$$\left. - \frac{1}{K_c} \left(\sum_{j=2}^{\infty} (j-1) u^{j-1} \log j - \sum_{j=2}^{\infty} \frac{j(j-1)}{2} u^j \log j \right) \right)$$

$$= 1 + \frac{2E[\log A_n]}{D^2[\log A_n]} \left(\frac{1+u}{u} E[\log A_n] - \sum_{j=2}^{\infty} j u^j \log j \right)$$

$$+ \frac{2E[\log A_n]}{D^2[\log A_n] K_c} \left(\frac{1}{2} \sum_{j=2}^{\infty} j^2 u^j \log j - \frac{2+u}{2u} \sum_{j=2}^{\infty} j u^j \log j + \frac{1}{u} E[\log A_n] \right).$$

Z powyższego widać, że

$$d(L) = 1 - \frac{2E[\log A_n]}{D^2[\log A_n]} \left(\sum_{j=2}^{\infty} j u^j \log j - \frac{1+u}{u} E[\log A_n] \right),$$

$$e(L) = \frac{2E[\log A_n]}{D^2[\log A_n]} \left(\frac{1}{2} \sum_{j=2}^{\infty} j^2 u^j \log j - \frac{2+u}{2u} \sum_{j=2}^{\infty} j u^j \log j + \frac{1}{u} E[\log A_n] \right),$$

a uwzględniając, że $L = 1$ i $u = 2^{-1}$ dostajemy

$$d(1) = 1 - \frac{2E[\log A_n]}{D^2[\log A_n]} \left(\sum_{j=2}^{\infty} \frac{j \log j}{2^j} - 3E[\log A_n] \right),$$

$$e(1) = \frac{2E[\log A_n]}{D^2[\log A_n]} \left(\sum_{j=2}^{\infty} \frac{j^2 \log j}{2^{j+1}} - 5 \sum_{j=2}^{\infty} \frac{j \log j}{2^{j+1}} + 2E[\log A_n] \right).$$

4. Oszacowanie dokładności obliczania sum

Ze wzorów z punktu 2 widać, że obliczenie stałych w teście sprowadza się do policzenia wielu sum szeregów postaci:

$$\sum_{a=1}^{\infty} u^a \log a, \qquad \sum_{a=1}^{\infty} u^a (\log a)^2,$$
$$\sum_{a=1}^{\infty} a\, u^a \log a, \qquad \sum_{a=1}^{\infty} a^2 u^a \log a.$$

Załóżmy, że każdą z powyższych sum policzyć mamy z bezwzględną dokładnością ε, czyli poszukujemy takiego Δ, że

$$\sum_{a=\Delta}^{\infty} u^{a-1} \log a \leqslant \varepsilon, \qquad \sum_{a=\Delta}^{\infty} u^{a-1} (\log a)^2 \leqslant \varepsilon,$$
$$\sum_{a=\Delta}^{\infty} a\, u^a \log a \leqslant \varepsilon, \qquad \sum_{a=\Delta}^{\infty} a^2 u^a \log a \leqslant \varepsilon.$$

Wykorzystamy rozwinięcie w szereg Taylora funkcji $\log a$

$$\log(a+1) = \log a - \log e \sum_{i=1}^{\infty} \frac{(-1)^i}{i a^i}, \qquad a \geqslant 1,$$

z czego

$$\log(a+1) \leqslant \log a + \frac{\log e}{a}$$

oraz

$$\log(a+1) \geqslant \log a + \log e \left(\frac{1}{a} - \frac{1}{2a^2} \right),$$

jak również następujące sumy

$$\sum_{a=\Delta}^{\infty} u^a = \frac{u^\Delta}{1-u},$$

$$\sum_{a=d}^{\Delta} a\, u^a = \frac{u}{1-u} \left(d u^{d-1} - \Delta u^\Delta + \frac{u^d - u^\Delta}{1-u} \right),$$

$$\sum_{a=\Delta}^{\infty} a\, u^a = \frac{u^\Delta}{1-u} \left(\Delta + \frac{u}{1-u} \right),$$

$$\sum_{a=\Delta}^{\infty} a^2 u^a = \frac{u^\Delta}{1-u}\left(\Delta\left(\Delta + \frac{2u}{1-u}\right) + \frac{u\,(1+u)}{(1-u)^2}\right).$$

Rozważaliśmy również wykorzystanie następującego oszacowania:

$$\frac{\log(\Delta+k)}{\log\Delta} \leqslant \left(\frac{\log(\Delta+1)}{\log\Delta}\right)^k,$$

lecz okazało się, że daje ono, co prawda, bardzo nieznacznie lepsze oszacowania Δ dla małych L, dla większych zaś są one znacząco gorsze od obliczonych dalej.

Posłużymy się też następującymi oszacowaniami:

$$\sum_{a=\Delta}^{\infty} u^a \sum_{t=\Delta}^{a} \frac{1}{t} \leqslant \sum_{a=\Delta}^{\infty} u^a \frac{a-\Delta+1}{\Delta} = \frac{1}{\Delta}\sum_{a=\Delta}^{\infty} u^a a - \frac{\Delta-1}{\Delta}\sum_{a=\Delta}^{\infty} u^a = \frac{u^\Delta}{\Delta(1-u)^2},$$

$$\begin{aligned}
\sum_{t=\Delta}^{\infty} \frac{u^t}{t^k} &= \sum_{w=1}^{\infty} \sum_{t=w\Delta}^{(w+1)\Delta-1} \frac{u^t}{t^k} \leqslant \sum_{w=1}^{\infty} \frac{1}{w^k\Delta^k} \sum_{t=w\Delta}^{(w+1)\Delta-1} u^t \\
&\leqslant \frac{1}{\Delta^k}\sum_{w=1}^{\infty} \frac{1}{w^k} u^{w\Delta} \frac{1-u^\Delta}{1-u} = \frac{1-u^\Delta}{\Delta^k(1-u)} \sum_{w=1}^{\infty} \frac{u^{w\Delta}}{w^k} \\
&\leqslant \frac{1-u^\Delta}{\Delta^k(1-u)}\left(\frac{u^\Delta}{1-u^\Delta} - \sum_{w=2}^{\infty} \frac{w^k-1}{w^k} u^{w\Delta}\right) \\
&\leqslant \frac{1-u^\Delta}{\Delta^k(1-u)}\left(\frac{u^\Delta}{1-u^\Delta} - \frac{2^k-1}{2^k}\frac{u^{2\Delta}}{1-u^\Delta}\right) \\
&\leqslant \frac{u^\Delta}{\Delta^k(1-u)}\left(1 - \frac{2^k-1}{2^k}u^\Delta\right) \leqslant \frac{u^\Delta}{\Delta^k(1-u)},
\end{aligned}$$

(czynnik $\left(1-\frac{2^k-1}{2^k}u^\Delta\right)$ pominięty został ze względu na jego marginalny wpływ i możliwość znacznego uproszczenia wyrażenia),

$$\begin{aligned}
&\sum_{t=\Delta}^{\infty} \frac{u^t}{t^k} = \frac{u^\Delta}{\Delta^k} + u^\Delta \sum_{t=1}^{\infty} \frac{u^t}{(\Delta+t)^k} = \frac{u^\Delta}{\Delta^k} + u^\Delta \sum_{w=0}^{\infty} \sum_{t=w\Delta+1}^{(w+1)\Delta} \frac{u^t}{(\Delta+t)^k} \\
&\geqslant \frac{u^\Delta}{\Delta^k} + u^\Delta \sum_{w=0}^{\infty} \sum_{t=w\Delta+1}^{(w+1)\Delta} \frac{u^t}{(w+2)^k\,\Delta^k} \geqslant \frac{u^\Delta}{\Delta^k}\left(1 + \frac{1-u^\Delta}{1-u}\sum_{w=0}^{\infty} \frac{u^{w\Delta+1}}{(w+2)^k}\right) \\
&\geqslant \frac{u^\Delta}{\Delta^k}\left(1 + \frac{1-u^\Delta}{1-u}u\left(\frac{1}{2^k} + \frac{u^\Delta}{3^k}\right)\right),
\end{aligned}$$

oraz przejściem:

$$\sum_{a=\Delta}^{\infty} f(a)\left(\sum_{t=\Delta}^{a} g(t)\right)^2 = f(\Delta)(g)\Delta))^2$$
$$+ f(\Delta+1)(g(\Delta)+g(\Delta+1))^2 + \ldots + f(\Theta)(g(\Delta)+\ldots+g(\Theta))^2 + \ldots$$
$$= g(\Delta)[f(\Delta)g(\Delta) + f(\Delta+1)(g(\Delta)+g(\Delta+1)) + \ldots + f(\Theta)(g(\Delta)+\ldots$$
$$+ g(\Theta)) + \ldots] + g(\Delta+1)[f(\Delta+1)(g(\Delta)+g(\Delta+1)) + \ldots$$
$$+ f(\Theta)(g(\Delta)+\ldots+g(\Theta)) + \ldots] + \ldots = \sum_{t=\Delta}^{\infty} g(t)\sum_{a=t}^{\infty} f(a)\sum_{w=\Delta}^{a} g(w)$$
$$= \sum_{t=\Delta}^{\infty} g(t)[f(t)(g(\Delta)+\ldots+g(t)) + f(t+1)(g(\Delta)+\ldots$$
$$+ g(t+1)) + \ldots + f(\Theta)(g(\Delta)+\ldots+g(\Theta)) + \ldots]$$
$$= \sum_{t=\Delta}^{\infty} g(t)[g(\Delta)(f(t)+f(t+1)+\ldots) + \ldots + g(t)(f(t)+f(t+1)+\ldots)$$
$$+ g(t+1)(f(t+1)+f(t+2)+\ldots)$$
$$+ g(t+2)(f(t+2)+f(t+3)+\ldots) + \ldots]$$
$$= \sum_{t=\Delta}^{\infty} g(t)\left[\sum_{a=t}^{\infty} f(a)\cdot\sum_{w=\Delta}^{t} g(w) + \sum_{w=t+1}^{\infty} g(w)\sum_{a=w}^{\infty} f(a)\right].$$

Mamy

$$\sum_{a=\Delta}^{\infty} u^a \log a \leqslant u^{\Delta}\log\Delta + \sum_{a=\Delta}^{\infty} u^{a+1}\left(\log\Delta + \log e\sum_{t=\Delta}^{a}\frac{1}{t}\right)$$
$$\leqslant u^{\Delta}\log\Delta + \log\Delta\sum_{a=\Delta}^{\infty} u^{a+1} + \log e\sum_{a=\Delta}^{\infty} u^{a+1}\sum_{t=\Delta}^{a}\frac{1}{t}$$
$$\leqslant u^{\Delta}\log\Delta + \log\Delta\frac{u^{\Delta+1}}{1-u} + \log e\frac{u^{\Delta+1}}{\Delta(1-u)^2}$$
$$\leqslant \frac{u^{\Delta}}{1-u}\left(\log\Delta + \frac{u\log e}{\Delta(1-u)}\right),$$

podobnie

$$\sum_{a=\Delta}^{\infty} u^a (\log a)^2 \leqslant u^\Delta \log^2 \Delta + \sum_{a=\Delta}^{\infty} u^{a+1} \left(\log \Delta + \log e \sum_{t=\Delta}^{a} \frac{1}{t} \right)^2$$

$$\leqslant u^\Delta \log^2 \Delta + \log^2 \Delta \sum_{a=\Delta}^{\infty} u^{a+1} + 2 \log \Delta \log e \sum_{a=\Delta}^{\infty} u^{a+1} \sum_{t=\Delta}^{a} \frac{1}{t}$$

$$+ \sum_{a=\Delta}^{\infty} u^{a+1} \left(\log e \sum_{t=\Delta}^{a} \frac{1}{t} \right)^2 \leqslant \frac{u^\Delta}{1-u} \log^2 \Delta + \frac{2u^{\Delta+1}}{\Delta(1-u)^2} \log \Delta \log e$$

$$+ \log^2 e \sum_{a=\Delta}^{\infty} u^{a+1} \sum_{t=\Delta}^{a} \frac{1}{t} \sum_{w=\Delta}^{a} \frac{1}{w} \leqslant \frac{u^\Delta}{1-u} \log \Delta \left(\log \Delta + \frac{2u \log e}{\Delta(1-u)} \right)$$

$$+ \log^2 e \sum_{t=\Delta}^{\infty} \frac{1}{t} \left(\sum_{w=\Delta}^{t} \frac{1}{w} \cdot \sum_{a=t}^{\infty} u^{a+1} + \sum_{w=t+1}^{\infty} \frac{1}{w} \sum_{a=w}^{\infty} u^{a+1} \right) \leqslant$$

$$\leqslant \frac{u^\Delta}{1-u} \log \Delta \left(\log \Delta + \frac{2u \log e}{\Delta(1-u)} \right)$$

$$+ \log^2 e \sum_{t=\Delta}^{\infty} \frac{1}{t} \left(\frac{t-\Delta+1}{\Delta(1-u)} u^{t+1} + \frac{u^{t+2}}{(1-u)^2 (t+1)} \right)$$

$$\leqslant \frac{u^\Delta}{1-u} \log \Delta \left(\log \Delta + \frac{2u \log e}{\Delta(1-u)} \right)$$

$$+ \frac{\log^2 e}{1-u} \left(\frac{1}{\Delta} \left(\sum_{t=\Delta}^{\infty} u^{t+1} - (\Delta - 1) u \sum_{t=\Delta}^{\infty} \frac{u^t}{t} \right) + \frac{u^2}{1-u} \sum_{t=\Delta}^{\infty} \frac{u^t}{t(t+1)} \right)$$

$$\leqslant \frac{u^\Delta}{1-u} \log \Delta \left(\log \Delta + \frac{2u \log e}{\Delta(1-u)} \right)$$

$$+ \frac{\log^2 e}{1-u} \left(\frac{u^{\Delta+1}}{\Delta(1-u)} - \frac{(\Delta-1) u^{\Delta+1}}{\Delta^2} \left(1 + \frac{1-u^\Delta}{1-u} u \left(\frac{1}{2} + \frac{u^\Delta}{3} \right) \right) \right.$$

$$\left. + \frac{u^{\Delta+2}}{\Delta(\Delta+1)(1-u)^2} \right) \leqslant \frac{u^\Delta}{1-u} \left[\log \Delta \left(\log \Delta + \frac{2u \log e}{\Delta(1-u)} \right) \right.$$

$$+ \frac{\log^2 e}{\Delta} \left(\frac{u^2}{1-u} \left(1 + \frac{1}{(\Delta+1)(1-u)} \right) \right.$$

$$\left. \left. + \frac{u}{\Delta} \left(1 - \frac{(\Delta-1)(1-u^\Delta) u}{1-u} \left(\frac{1}{2} + \frac{u^\Delta}{3} \right) \right) \right) \right].$$

Z kolei dla drugiej pary szeregów mamy:

$$\sum_{a=\Delta}^{\infty} a\, u^a \log a \leqslant u^{\Delta}\Delta\log\Delta + \sum_{a=\Delta}^{\infty} u^{a+1}\,(a+1)\left(\log\Delta + \log e \sum_{t=\Delta}^{a}\frac{1}{t}\right)$$

$$\leqslant u^{\Delta}\Delta\log\Delta + \log\Delta\left(\sum_{a=\Delta}^{\infty} u^{a+1}a + \sum_{a=\Delta}^{\infty} u^{a+1}\right)$$

$$+ \log e\left(\sum_{a=\Delta}^{\infty} u^{a+1}a\sum_{t=\Delta}^{a}\frac{1}{t} + \sum_{a=\Delta}^{\infty} u^{a+1}\sum_{t=\Delta}^{a}\frac{1}{t}\right)$$

$$\leqslant u^{\Delta}\Delta\log\Delta + \log\Delta\left(\frac{u^{\Delta+1}}{1-u}\left(\Delta + \frac{u}{1-u}\right) + \frac{u^{\Delta+1}}{1-u}\right)$$

$$+ \log e\left(\sum_{t=\Delta}^{\infty}\frac{1}{t}\sum_{a=t}^{\infty} u^{a+1}a + \frac{u^{\Delta+1}}{\Delta(1-u)^2}\right)$$

$$\leqslant \frac{u^{\Delta}}{1-u}\log\Delta\left(\Delta + \frac{u}{1-u}\right) +$$

$$+ \log e\left(\sum_{t=\Delta}^{\infty}\frac{1}{t}\frac{u^{t+1}}{1-u}\left(t + \frac{u}{1-u}\right) + \frac{u^{\Delta+1}}{\Delta\,(1-u)^2}\right)$$

$$\leqslant \frac{u^{\Delta}}{1-u}\log\Delta\left(\Delta + \frac{u}{1-u}\right)$$

$$+ \log e\left(\sum_{t=\Delta}^{\infty}\frac{u^{t+1}}{1-u} + \sum_{t=\Delta}^{\infty}\frac{1}{t}\frac{u^{t+2}}{(1-u)^2} + \frac{u^{\Delta+1}}{\Delta(1-u)^2}\right)$$

$$\leqslant \frac{u^{\Delta}}{1-u}\log\Delta\left(\Delta + \frac{u}{1-u}\right)$$

$$+ \log e\left(\frac{u^{\Delta+1}}{(1-u)^2} + \frac{u^2}{\Delta(1-u)^2}\sum_{t=\Delta}^{\infty} u^t + \frac{u^{\Delta+1}}{\Delta(1-u)^2}\right)$$

$$\leqslant \frac{u^{\Delta}}{1-u}\log\Delta\left(\Delta + \frac{u}{1-u}\right)$$

$$+ \log e\left(\frac{u^{\Delta+1}}{(1-u)^2} + \frac{u^{\Delta+2}}{\Delta(1-u)^3} + \frac{u^{\Delta+1}}{\Delta(1-u)^2}\right)$$

$$\leqslant \frac{u^{\Delta}}{1-u}\log\Delta\left(\Delta + \frac{u}{1-u}\right) + \frac{u^{\Delta+1}}{(1-u)^2}\log e\left(1 + \frac{1}{\Delta(1-u)}\right),$$

oraz

$$\sum_{a=\Delta}^{\infty} a^2 u^a \log a \leqslant u^\Delta \Delta^2 \log \Delta + \sum_{a=\Delta}^{\infty} u^{a+1}(a+1)^2 \left(\log \Delta + \log e \sum_{t=\Delta}^{a} \frac{1}{t} \right)$$

$$\leqslant u^\Delta \Delta^2 \log \Delta + \log \Delta \left(\sum_{a=\Delta}^{\infty} u^{a+1} a^2 + 2 \sum_{a=\Delta}^{\infty} u^{a+1} a + \sum_{a=\Delta}^{\infty} u^{a+1} \right)$$

$$+ \log e \left(\sum_{a=\Delta}^{\infty} u^{a+1} a^2 \sum_{t=\Delta}^{a} \frac{1}{t} + 2 \sum_{a=\Delta}^{\infty} u^{a+1} a \sum_{t=\Delta}^{a} \frac{1}{t} + \sum_{a=\Delta}^{\infty} u^{a+1} \sum_{t=\Delta}^{a} \frac{1}{t} \right)$$

$$\leqslant u^{\Delta-b} \Delta^2 \log \Delta + \log \Delta \left(\frac{u^{\Delta+1}}{1-u} \left(\Delta^2 + \frac{2u\Delta}{1-u} + \frac{u(1+u)}{(1-u)^2} \right) \right.$$

$$\left. + 2 \frac{u^{\Delta+1}}{1-u} \left(\Delta + \frac{u}{1-u} \right) + \frac{u^{\Delta+1}}{1-u} \right)$$

$$+ \log e \sum_{t=\Delta}^{\infty} \frac{1}{t} \left(\sum_{a=t}^{\infty} u^{a+1} a^2 + 2 \sum_{a=t}^{\infty} u^{a+1} a + \sum_{a=t}^{\infty} u^{a+1} \right)$$

$$\leqslant u^\Delta \Delta^2 \log \Delta + \frac{u^{\Delta+1}}{1-u} \log \Delta \left(\Delta^2 + \frac{2\Delta}{1-u} + \frac{1+u}{(1-u)^2} \right)$$

$$+ \log e \sum_{t=\Delta}^{\infty} \frac{1}{t} \frac{u^{t+1}}{1-u} \left(t^2 + \frac{2t}{1-u} + \frac{u(1+u)}{(1-u)^2} \right) \leqslant$$

$$\leqslant \frac{u^\Delta}{1-u} \log \Delta \left(\Delta^2 + \frac{2u\Delta}{1-u} + \frac{u(1+u)}{(1-u)^2} \right)$$

$$+ \frac{u}{1-u} \log e \left(\sum_{t=\Delta}^{\infty} u^t t + \frac{2}{1-u} \sum_{t=\Delta}^{\infty} u^t + \frac{1+u}{(1-u)^2} \sum_{t=\Delta}^{\infty} \frac{1}{t} u^t \right)$$

$$\leqslant \frac{u^\Delta}{1-u} \log \Delta \left(\Delta^2 + \frac{2u\Delta}{1-u} + \frac{u\,(1+u)}{(1-u)^2} \right)$$

$$+ \frac{u^{\Delta+1}}{(1-u)^2} \log e \left(\Delta + \frac{u+2}{1-u} + \frac{1+u}{\Delta\,(1-u)^2} \right).$$

Wyznaczymy od razu również oszacowanie z dołu dla pierwszej sumy:

$$\sum_{a=\Delta}^{\infty} u^a \log a \geqslant u^\Delta \log \Delta + \sum_{a=\Delta}^{\infty} u^{a+1} \left(\log \Delta + \log e \sum_{t=\Delta}^{a} \left(\frac{1}{t} - \frac{1}{2t^2} \right) \right)$$

$$\geqslant u^\Delta \log \Delta + \log \Delta \sum_{a=\Delta}^{\infty} u^{a+1} +$$

$$
\begin{aligned}
&+ \log e \left(\sum_{a=\Delta}^{\infty} u^{a+1} \sum_{t=\Delta}^{a} \frac{1}{t} - \frac{1}{2} \sum_{a=\Delta}^{\infty} u^{a+1} \sum_{t=\Delta}^{a} \frac{1}{t^2} \right) \\
&\geqslant \frac{u^{\Delta}}{1-u} \log \Delta + \log e \sum_{t=\Delta}^{\infty} \frac{1}{t} \sum_{a=t}^{\infty} u^{a+1} - \frac{\log e}{2} \sum_{t=\Delta}^{\infty} \frac{1}{t^2} \sum_{a=t}^{\infty} u^{a+1} \\
&\geqslant \frac{u^{\Delta}}{1-u} \log \Delta + \frac{u}{1-u} \log e \sum_{t=\Delta}^{\infty} \frac{u^t}{t} - \frac{u}{1-u} \frac{\log e}{2} \sum_{t=\Delta}^{\infty} \frac{u^t}{t^2} \\
&\geqslant \frac{u^{\Delta}}{1-u} \log \Delta + \frac{u}{1-u} \log e \frac{u^{\Delta}}{\Delta} \left(1 + \frac{1-u^{\Delta}}{1-u} u \left(\frac{1}{2} + \frac{u^{\Delta}}{3} \right) \right) \\
&\quad - \frac{u}{1-u} \frac{\log e}{2} \frac{u^{\Delta}}{\Delta^2 (1-u)} \\
&\geqslant \frac{u^{\Delta}}{1-u} \left(\log \Delta + \frac{u \log e}{\Delta} \left(1 + \frac{1-u^{\Delta}}{1-u} u \left(\frac{1}{2} + \frac{u^{\Delta}}{3} \right) - \frac{1}{2\Delta(1-u)} \right) \right).
\end{aligned}
$$

Rozpatrywać będziemy nierówności:

$$
\frac{u^{\Delta-1}}{1-u} \left(\log \Delta + \frac{u \log e}{\Delta(1-u)} \right) \leqslant \varepsilon, \tag{1}
$$

$$
\begin{aligned}
&\frac{u^{\Delta-1}}{1-u} \left[\log \Delta \left(\log \Delta + \frac{2u \log e}{\Delta(1-u)} \right) \right. \\
&\quad + \frac{\log^2 e}{\Delta} \left(\frac{u^2}{1-u} \left(1 + \frac{1}{(\Delta+1)(1-u)} \right) \right. \\
&\quad \left. \left. + \frac{u}{\Delta} \left(1 - \frac{(\Delta-1)(1-u^{\Delta})u}{1-u} \left(\frac{1}{2} + \frac{u^{\Delta}}{3} \right) \right) \right) \right] \leqslant \varepsilon,
\end{aligned} \tag{2}
$$

$$
\frac{u^{\Delta}}{1-u} \log \Delta \left(\Delta + \frac{u}{1-u} \right) + \frac{u^{\Delta+1}}{(1-u)^2} \log e \left(1 + \frac{1}{\Delta(1-u)} \right) \leqslant \varepsilon, \tag{3}
$$

$$
\begin{aligned}
&\frac{u^{\Delta}}{1-u} \log \Delta \left(\Delta^2 + \frac{2u\Delta}{1-u} + \frac{u(1+u+2u^2-u^3)}{(1-u)^2} \right) \\
&\quad + \frac{u^{\Delta+1}}{(1-u)^2} \log e \left(\Delta + \frac{u+2}{1-u} + \frac{1+u+2u^2-u^3}{\Delta(1-u)^2} \right) \leqslant \varepsilon,
\end{aligned} \tag{4}
$$

które rozwiążemy numerycznie ze względu na Δ.

Poniższa tabela przedstawia wartości Δ uzyskane dla $\varepsilon = 2^{-128}$– przyjęliśmy tak dużą dokładność, gdyż obliczone stałe μ_L oraz σ_{A_i} posłużą następnie do obliczania $d(L)$ i $e(L)$.

Tabela 1

L	$u = 1 - 2^{-L}$	$K_c = 500 \cdot 2^L$	Δ			
			(1)	(2)	(3)	(4)
1	0,5	1000	133	136	139	147
2	0,75	2000	322	330	341	362
3	0,875	4000	698	715	747	798
4	0,9375	8000	1456	1492	1569	1685
5	0,96875	16000	2982	3060	3236	3496
6	0,984375	32000	6060	6221	6619	7189
7	0,9921875	64000	12265	12598	13479	14716
8	0,99609375	128000	24772	25459	27387	30049
9	0,998046875	256000	49980	51389	55577	61274
10	0,9990234375	512000	100781	103664	112705	124837
11	0,99951171875	1024000	203150	209037	228451	254185
12	0,999755859375	2048000	409416	421418	462916	517317
13	0,9998779296875	4096000	824990	849428	937780	1052438
14	0,99993896484375	8192000	1662206	1711901	1899353	2140369
15	0,999969482421875	16384000	3348737	3449686	3846152	4351564
16	0,9999847412109375	32768000	6745934	6950806	7786987	8844538

W powyższej tabeli znajdziemy uzasadnienie stosowania dla $L = 1$ przybliżenia $K_c \to \infty$, które we wszystkich przypadkach jest znacznie większe od wymaganego dokładnością zakresu sumowania. Stosowanie pierwotnej postaci stałoby się uzasadnione dopiero przy wymogu dokładności przekraczającej 10^{-292}.

Ponadto dokonaliśmy porównania pomiędzy wynikami uzyskiwanymi na podstawie przedstawionych oszacowań, a otrzymanymi przez porównanie poszczególnych sum częściowych z sumą 25 mln wyrazów szeregów $\sum_{a=\Delta}^{\infty} (1 - 1/2^L)^a \log a$ oraz $\sum_{a=\Delta}^{\infty} \left(1 - 1/2^L\right)^a a^2 \log a$.

Dla $L = 1$:

Tabela 2

$\varepsilon = 10^{-d}$ d	$\sum_{a=\Delta}^{\infty} (1 - 1/2^L)^a \log a$			$\sum_{a=\Delta}^{\infty} \left(1 - 1/2^L\right)^a a^2 \log a$		
	Δ „rzeczywista”	Δ z oszacowania	błąd %	Δ „rzeczywista”	Δ z oszacowania	błąd %
1	6	7	16,7	15	15	0,0
2	10	11	10,0	19	19	0,0
3	13	13	0,0	23	23	0,0
4	17	17	0,0	27	27	0,0

cd. tabeli 2

$\varepsilon = 10^{-d}$ d	$\sum_{a=\Delta}^{\infty}(1-1/2^L)^a \log a$			$\sum_{a=\Delta}^{\infty}\left(1-1/2^L\right)^a a^2 \log a$		
	Δ „rzeczywista”	Δ z oszacowania	błąd %	Δ „rzeczywista”	Δ z oszacowania	błąd %
5	20	21	5,0	30	31	3,3
6	24	25	4,2	34	35	2,9
7	27	27	0,0	38	39	2,6
8	30	31	3,3	41	41	0,0
9	34	35	2,9	45	45	0,0
10	37	37	0,0	48	49	2,1
15	54	55	1,9	66	67	1,5
20	71	71	0,0	83	83	0,0
30	104	105	1,0	118	119	0,8
40	137	137	0,0	152	153	0,7
50	170	171	0,6	186	187	0,5
60	204	205	0,5	219	219	0,0
70	237	237	0,0	253	253	0,0
80	270	271	0,4	287	287	0,0
90	304	305	0,3	320	321	0,3
100	337	337	0,0	354	355	0,3

Dla $L = 16$:

TABELA 3

$\varepsilon = 10^{-d}$ d	$\sum_{a=\Delta}^{\infty}(1-1/2^L)^a \log a$			$\sum_{a=\Delta}^{\infty}\left(1-1/2^L\right)^a a^2 \log a$		
	Δ „rzeczywista”	Δ z oszacowania	błąd %	Δ „rzeczywista”	Δ z oszacowania	błąd %
1	1074427	1074444	0,0016	3038280	3038310	0,0010
2	1225913	1225926	0,0011	3195887	3195914	0,0008
3	1377330	1377340	0,0007	3353164	3353189	0,0007
4	1528691	1528700	0,0006	3510142	3510165	0,0007
5	1680008	1680015	0,0004	3666849	3666870	0,0006
6	1831287	1831293	0,0003	3823308	3823328	0,0005
7	1982535	1982541	0,0003	3979540	3979558	0,0005
8	2133757	2133762	0,0002	4135563	4135580	0,0004
9	2284956	2284961	0,0002	4291393	4291409	0,0004
10	2436135	2436139	0,0002	4447044	4447059	0,0003
15	3191805	3191808	0,0001	5223019	5223029	0,0002
20	3947216	3947218	0,0001	5995976	5995984	0,0001

cd. tabeli 3

$\varepsilon = 10^{-d}$ d	$\sum_{a=\Delta}^{\infty}(1-1/2^L)^a \log a$			$\sum_{a=\Delta}^{\infty}\left(1-1/2^L\right)^a a^2 \log a$		
	Δ „rzeczywista"	Δ z oszacowania	błąd %	Δ „rzeczywista"	Δ z oszacowania	błąd %
30	5457589	5457591	0,0000	7535593	7535598	0,0001
40	6967613	6967614	0,0000	9069451	9069454	0,0000
50	8477427	8477428	0,0000	10599387	10599389	0,0000
60	9987102	9987103	0,0000	12126477	12126478	0,0000
70	11496679	11496680	0,0000	13651405	13651407	0,0000
80	13006182	13006183	0,0000	15174636	15174638	0,0000
90	14515629	14515630	0,0000	16696498	16696499	0,0000
100	16025029	16025031	0,0000	18217233	18217233	0,0000

Jak widać, w obu przypadkach uzyskaliśmy bardzo dobrą zgodność wyników uzyskanych na podstawie oszacowań i częściowego sumowania każdego z szeregów. Zgodnie z oczekiwaniami względne różnice, jak się okazuje bezwzględne również, największe są dla najmniejszych dokładności, bo i oszacowanie staje się tym dokładniejsze im późniejszego fragmentu szeregu dotyczy. Powyższe wydaje się wystarczającą legitymacją do stosowania dalej otrzymanych tu oszacowań.

5. Obliczanie funkcji $h(z,k)$

Zajmować się będziemy sumą następującego szeregu

$$h(z,k) = (1-z)\sum_{i=1}^{\infty} z^{i-1}\log(i+k),$$

przy czym podstawą logarytmu jest 2. Dla $|z|<1$ szereg ten jest zbieżny, tak zawsze będzie w naszym przypadku.

W szczególności dla $k=0$ dostajemy

$$h(z,0) = (1-z)\sum_{i=1}^{\infty} z^{i-1}\log i.$$

Rozpatrzmy tę samą sumę dla $k+1$

$$\begin{aligned} h(z,k+1) &= (1-z)\sum_{i=1}^{\infty} z^{i-1}\log(i+k+1) \\ &= (1-z)\left(\log(k+2) + z\log(k+3) + z^2\log(k+4) + \ldots\right) = \\ &= (1-z)\frac{1}{z}\left(z\log(k+2) + z^2\log(k+3) + z^3\log(k+4) + \ldots\right) = \end{aligned}$$

$$= \frac{1-z}{z}\left(\log(k+1) + z\log(k+2) + z^2\log(k+3) + z^3\log(k+4) + \ldots\right)$$
$$- \frac{1-z}{z}\log(k+1) = \frac{1-z}{z}\sum_{i=1}^{\infty} z^{i-1}\log(i+k) - \frac{1-z}{z}\log(k+1)$$
$$= \frac{h(z,k) - (1-z)\log(k+1)}{z}.$$

W ten sposób znaleźliśmy rekurencyjną zależność, określającą funkcję $h(z,k)$. Wystarczy więc obliczyć $h(z,0)$, a następnie iteracyjnie wyznaczać wartości funkcji dla kolejnych k. Metoda okazuje się być jednak niestabilna numerycznie. Zobaczmy, jak wyglądać będą kolejne rozwinięcia sporządzone według powyższej reguły:

$$h(z,1) = \frac{h(z,0) - (1-z)\log(1)}{z} = \frac{h(z,0)}{z},$$
$$h(z,2) = \frac{h(z,1) - (1-z)\log 2}{z} = \frac{\frac{h(z,0)}{z} - (1-z)\log 2}{z} =$$
$$= \frac{h(z,0)}{z^2} - \frac{(1-z)\log 2}{z},$$
$$h(z,3) = \frac{h(z,2) - (1-z)\log 3}{z} = \frac{\frac{h(z,0)}{z^2} - \frac{(1-z)\log 2}{z} - (1-z)\log 3}{z}$$
$$= \frac{h(z,0)}{z^3} - \frac{(1-z)\log 2}{z^2} - \frac{(1-z)\log 3}{z},$$
$$\vdots$$
$$h(z,k) = \frac{h(z,0)}{z^k} - (1-z)\sum_{i=2}^{k} z^{i-k-1}\log i.$$

Jak widać, przy zachowaniu możliwości iteracyjnego obliczania kolejnych $h(z,k)$, udało się znaleźć taką postać wyrażenia, że w praktyce możemy obliczać te wartości z taką samą dokładnością, jak w przypadku pierwotnego wzoru.

6. Numeryczne obliczenie współczynników

Obliczanie współczynników testów rozpoczniemy od wartości oczekiwanej i wariancji dla wszystkich wartości L. Ponieważ odpowiadają one odpowiednio pierwszej i drugiej sumie, których zbieżność rozpatrywano w poprzednim punkcie, więc obliczenie ich jest jedynie nieco czasochłonne –

zgodnie z przyjętymi założeniami dla $L = 16$ wymaga zsumowania 6950806 wyrazów szeregu dla każdej z nich.

Przypadek $d(1)$ i $e(1)$ jest z naszego punktu widzenia bardzo prosty, gdyż po wyznaczeniu wartości oczekiwanej $E[\log A_n]$ i wariancji $D^2[\log A_n]$ pozostają do wyznaczenia trzy niezależne sumy, dla których zakresy sumowań wyznaczone zostały w poprzednim punkcie.

Kłopotliwe stają się dopiero obliczenia dla $L > 1$. Jest tak z dwóch powodów, po pierwsze mamy tam do czynienia z nieskończonymi zagnieżdżonymi sumami, a po drugie w pierwotnych wzorach występują człony $p(L, K_c)$ oraz $q(L, K_c)$, których praktycznie rzecz biorąc nie sposób wyznaczyć przed zakończeniem procedury testowej i poznaniem rzeczywistej długości części testowej ciągu.

Ponieważ jednak w teście przyjmuje się, że $K_c \geqslant 500 \cdot 2^L$, więc wystarczy zbadać monotoniczność tych funkcji względem K_c i ocenić ich wartości dla minimalnej wartości.

Jak pokazano w punkcie 2, w wyrażeniach na $d(L)$ oraz $e(L)$ pojawiają się następujące różnice

$$p(L,1) - p(L,K_c) \quad \text{oraz} \quad q(L,1) - q(L,K_c).$$

Rozwijając funkcje $p(L,K)$ oraz $q(L,K)$ dostajemy:

$$\begin{aligned}
p(L,1) - p(L,K_c) &= \sum_{k=1}^{\infty} F(k,L,1)\, u^{k-1} - u^{K_c-1} \sum_{k=1}^{\infty} F(k,L,K_c)\, u^{k-1} \\
&= \sum_{k=1}^{\infty} u^2 \left(h(v,k) - h(u,k+1)\right) \left(h(v,0) - v^k h(v,k)\right) u^{k-1} \\
&\quad + \sum_{k=1}^{\infty} u \cdot h(u,0) \left(h(u,k) - h(v,k)\right) u^{k-1} \\
&\quad - u^{K_c-1} \sum_{k=1}^{\infty} u^2 \left(h(v,k+K_c-1) - h(u,k+K_c)\right) \\
&\quad \cdot \left(h(v,0) - v^k h(v,k)\right) u^{k-1} \\
&\quad - u^{K_c-1} \sum_{k=1}^{\infty} u \cdot h(u,0) \left(h(u,k+K_c-1) - h(v,k+K_c-1)\right) u^{k-1} =
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=1}^{\infty} u^2 \left(h\left(v,0\right) - v^k h(v,k)\right)\left(h\left(v,k\right) - h\left(u,k+1\right)\right.\\
&\quad \left. - u^{K_c-1} h\left(v,k+K_c-1\right) + u^{K_c-1} h\left(u,k+K_c\right)\right) u^{k-1}\\
&\quad + \sum_{k=1}^{\infty} u \cdot h(u,0)\left(h\left(u,k\right) - h(v,k) - u^{K_c-1} h\left(u,k+K_c-1\right)\right.\\
&\quad \left. + u^{K_c-1} h\left(v,k+K_c-1\right)\right) u^{k-1},
\end{aligned}
$$

$$
\begin{aligned}
q(L,1) - q(L,K_c) &= \sum_{k=1}^{\infty} G\left(k,L,1\right) u^{k-1} - u^{K_c-1} \sum_{k=1}^{\infty} G\left(k,L,K_c\right) u^{k-1}\\
&= \sum_{k=1}^{\infty} u\left(h\left(v,k\right) - h\left(u,k+1\right)\right)\left(u\left(k+1\right)\left(h(v,0) - v^k h(v,k)\right)\right.\\
&\quad \left. - 2^{-L} \sum_{i=1}^{k} i \cdot v^{i-1} \log i\right) u^{k-1} + \sum_{k=1}^{\infty} uk \cdot h(u,0)\left(h\left(u,k\right) - h(v,k)\right) u^{k-1}\\
&\quad - u^{K_c-1} \sum_{k=1}^{\infty} (u(h(v,k+K_c-1) - h(u,k+K_c)) \cdot (u(k+K_c)(h(v,0)\\
&\quad - v^k h(v,k)) - 2^{-L} \sum_{i=1}^{k} i \cdot v^{i-1} \log i) u^{k-1})\\
&\quad - u^{K_c-1} \sum_{k=1}^{\infty} u\left(k+K_c-1\right) h(u,0)(h\left(u,k+K_c-1\right)\\
&\quad - h\left(v,k+K_c-1\right)) u^{k-1}\\
&= \sum_{k=1}^{\infty} (u^{k+1}\left(h(v,0) - v^k h\left(v,k\right)\right) \cdot ((k+1)\left(h(v,k) - h\left(u,k+1\right)\right)\\
&\quad - u^{K_c-1}\left(k+K_c\right)\left(h\left(v,k+K_c-1\right) - \left(u,k+K_c\right)\right)))\\
&\quad - \sum_{k=1}^{\infty} (u^k 2^{-L} \sum_{i=1}^{k} i \cdot v^{i-1} \log i \cdot (h(v,k) - h(u,k+1)\\
&\quad - u^{K_c-1} h(v,k+K_c-1) + u^{K_c-1} h(u,k+K_c)))\\
&\quad - \sum_{k=1}^{\infty} u^k h(u,0)(k(h(u,k) - h(v,k))\\
&\quad - u^{K_c-1}(k+K_c-1)(h(u,k+K_c-1) - h(v,k+K_c-1))).
\end{aligned}
$$

Z powyższych widać, że interesujące są relacje w następujących parach, z których w powyższych wzorach tworzone są różnice:

$$\begin{aligned}
&h(v,k) && \text{i} && u^{K_c-1}h\left(v,k+K_c-1\right),\\
&h\left(u,k+1\right) && \text{i} && u^{K_c-1}h\left(u,k+K_c\right),\\
&h\left(u,k\right) && \text{i} && u^{K_c-1}h\left(u,k+K_c-1\right),\\
&(k+1)h(v,k) && \text{i} && u^{K_c-1}(k+K_c)h\left(v,k+K_c-1\right),\\
&(k+1)h(u,k+1) && \text{i} && u^{K_c-1}(k+K_c)h\left(u,k+K_c\right),\\
&kh(u,k) && \text{i} && u^{K_c-1}(k+K_c-1)h\left(u,k+K_c-1\right),\\
&kh(v,k) && \text{i} && u^{K_c-1}(k+K_c-1)h\left(v,k+K_c-1\right),
\end{aligned}$$

przy czym dla par drugiej i trzeciej, czwartej i siódmej oraz piątej i szóstej wystarczające jest rozpatrzenie tylko jednej z nich.

Dla pierwszej z nich mamy:

$$\begin{aligned}
u^{K_c-1}h\left(v,k+K_c-1\right) &= u^{K_c-1}(1-v)\sum_{i=1}^{\infty}v^{i-1}\log\left(i+k+K_c-1\right)\\
&= u^{K_c-1}\left(1-v\right)v^{-k-K_c}\sum_{i=1}^{\infty}v^{i+k+K_c-1}\log\left(i+k+K_c-1\right)\\
&= u^{K_c-1}\left(1-v\right)v^{-k-K_c}\sum_{i=k+K_c}^{\infty}v^{i}\log i\\
&\leqslant u^{K_c-1}\left(\log(k+K_c)+\frac{v\log e}{(k+K_c)(1-v)}\right),
\end{aligned}$$

oczywiste jest, że

$$\underset{u,v\in(0,1),k\geqslant 0,K_c\geqslant 1}{\forall} u^{K_c-1}h\left(v,k+K_c-1\right)\geqslant 0$$

oraz

$$\underset{u,v\in(0,1),k\geqslant 0,K_c\geqslant 1}{\forall} u^{K_c-1}\left(\log\left(k+K_c\right)+\frac{v\log e}{\left(k+K_c\right)\left(1-v\right)}\right)>0$$

i

$$\underset{u,v\in(0,1),k\geqslant 0}{\forall}\lim_{K_c\to\infty} u^{K_c-1}\left(\log\left(k+K_c\right)+\frac{v\log e}{\left(k+K_c\right)\left(1-v\right)}\right)=0,$$

z czego

$$\underset{u,v\in(0,1),k\geqslant 0}{\forall}\lim_{K_c\to\infty} u^{K_c-1}h\left(v,k+K_c-1\right)=0.$$

i z malenia ciągu $u^{K_c-1}\left(\log(k+K_c)+\frac{v\log e}{(k+K_c)(1-v)}\right)$ wynika malenie ciągu $u^{K_c-1}h(v,k+K_c-1)$ dla argumentu K_c, a pozostałych traktowanych jako stałe.

Rozpatrujemy różnicę

$$\begin{aligned}
&u^{K_c}\left(\log(k+K_c+1)+\frac{v\log e}{(k+K_c+1)(1-v)}\right)\\
&\quad-u^{K_c-1}\left(\log(k+K_c)+\frac{v\log e}{(k+K_c)(1-v)}\right)\\
&=u^{K_c-1}\left(u\log(k+K_c+1)-\log(k+K_c)\right.\\
&\quad\left.+\frac{v\log e}{1-v}\left(\frac{u}{k+K_c+1}-\frac{1}{k+K_c}\right)\right)\\
&\leqslant u^{K_c-1}\left((u-1)\log(k+K_c)+\frac{u}{k+K_c}\right.\\
&\quad\left.+\frac{v\log e}{1-v}\left(\frac{u}{k+K_c+1}-\frac{1}{k+K_c}\right)\right),
\end{aligned}$$

dla ostatniego z wyrażeń można, przyjmując $k+K_c=2^d$, dla pewnego $d\in\in\mathbb{R}_+$, pokazać, że wyrażenie w nawiasie jest zawsze ujemne dla $u\in\langle 0{,}5;1)$, co pociąga malenie omawianego ciągu.

Aby dopełnić obraz wpływu składnika $u^{K_c-1}h(v,k+K_c-1)$ na liczoną sumę, oszacujemy jego wartość dla minimalnego $K_c=500\cdot 2^L$ i $k=0$ oraz poszukamy takiego k, aby z oszacowania otrzymać wartość równą 2^{-128}.

W pierwszym przypadku mamy:

$$\begin{aligned}
&u^{K_c-1}h(v,k+K_c-1)\leqslant u^{K_c-1}\left(\log(k+K_c)+\frac{v\log e}{(k+K_c(1-v)}\right)=\Big|_{k=0}\\
&=\left(\frac{2^L-1}{2^L}\right)^{500\cdot 2^L-1}\left(L+\log 500+\frac{\log e}{500}\left(1-\frac{1}{2^{L-1}}\right)\right)\\
&\approx\begin{cases}1{,}9\cdot 10^{-300}, & L=1,\\ 3{,}5\cdot 10^{-219}, & L=5,\\ 1{,}1\cdot 10^{-216}, & L=10,\\ 1{,}8\cdot 10^{-216}, & L=16,\end{cases}
\end{aligned}$$

zaś poszukiwane wartości k wynoszą w przybliżeniu

$$k\approx\begin{cases}2^{2\cdot 10^{262}}, & L=1,\\ 2^{1\cdot 10^{182}}, & L=5,\\ 2^{5\cdot 10^{178}}, & L=10,\\ 2^{4\cdot 10^{178}}, & L=16.\end{cases}$$

Jak widać, dla $k = 0$ składnik ten nie ma w praktyce znaczenia, zaś wartości k, dla których jego wpływ mógłby być widoczny w wynikach obliczeń są tak duże, że dominującą rolę mieć wówczas będzie, dążący do 0, czynnik u^k.

Analogicznie postępujemy dla par drugiej i trzeciej.

Nieco inny przypadek stanowią cztery pozostałe pary, przeanalizujemy teraz ich zachowanie się na przykładzie piątej. Postępując podobnie, jak poprzednio dochodzimy do oszacowania

$$\begin{aligned}
&u^{K_c-1}\,(k+K_c)\,h\,(u,k+K_c)\\
&\quad= u^{K_c-1}(k+K_c)\,(1-u)\sum_{i=1}^{\infty} u^{i-1}\log\,(i+k+K_c)\\
&\quad= u^{K_c-1}\,(k+K_c)\,(1-u)\,u^{-k-K_c-1}\sum_{i=k+K_c+1}^{\infty} u^i\log i\\
&\quad\leqslant u^{K_c-1}\,(k+K_c)\left(\log\,(k+K_c+1)+\frac{u\log e}{(k+K_c+1)\,(1-u)}\right),
\end{aligned}$$

z którego, jak poprzednio, znajdziemy oszacowanie wkładu tego składnika dla $K_c = 500\cdot 2^L$ i $k = 0$ oraz poszukamy takiego k, aby z oszacowania otrzymać wartość równą 2^{-128}. Mamy:

$$\begin{aligned}
&u^{K_c-1}\,(k+K_c)\,h\,(u,k+K_c)\\
&\quad\leqslant u^{K_c-1}\,(k+K_c)\left(\log\,(k+K_c+1)+\frac{u\log e}{(k+K_c+1)\,(1-u)}\right)=\Big|_{k=0}\\
&\quad\approx\left(\frac{2^L-1}{2^L}\right)^{500\cdot 2^L-1}\cdot 500\cdot 2^L\cdot\left(L+\log 500+\frac{(2^L-1)\log e}{500\cdot 2^L+1}\right)\\
&\quad\approx\begin{cases}1{,}9\cdot 10^{-297}, & L=1,\\ 5{,}6\cdot 10^{-216}, & L=5,\\ 5{,}4\cdot 10^{-211}, & L=10,\\ 5{,}8\cdot 10^{-209}, & L=16,\end{cases}
\end{aligned}$$

oraz

$$k\approx\begin{cases}1{,}6\cdot 10^{262}, & L=1,\\ 1{,}2\cdot 10^{182}, & L=5,\\ 5{,}3\cdot 10^{178}, & L=10,\\ 4{,}1\cdot 10^{178}, & L=16.\end{cases}$$

Pomimo występowania dużego czynnika $k + K_c$ i tym razem człon ten ma marginalne znaczenie, znacznie mniejsze wartości występują tylko dla k, choć nadal są one tak duże, że praktycznie niemożliwe do osiągnięcia.

Na podstawie powyższych stwierdziliśmy, że uwzględnianie, podczas obliczania $d(L)$ oraz $e(L)$ składników $p(L, K_c)$ i odpowiednio $q(L, K_c)$ nie wnosi nic do dokładności obliczeń, stąd też w dalszych rozważaniach zostały one pominięte.

Ostatecznie musimy obliczyć dla $L = \overline{2, 16}$ następujące wyrażenia:

$$d(L) = 1 - 2\frac{p(L,1)}{D^2[\log A_n]},$$
$$e(L) = 2\frac{q(L,1)}{D^2[\log A_n]},$$

gdzie

$$p(L,1) = \sum_{k=1}^{\infty}(u(h(v,k) - h(u,k+1))(h(v,0) - v^k h(v,k)) + h(u,0)(h(u,k) - h(v,k)))u^k,$$
$$q(L,1) = \sum_{k=1}^{\infty}\left((h(v,k) - h(u,k+1)) \cdot \left(u(k+1)(h(v,0) - v^k h(v,k)) - 2^{-L}\sum_{i=1}^{k} i \cdot v^{i-1}\log i\right) + k \cdot h(u,0)(h(u,k) - h(v,k))\right)u^k.$$

Powyższe przekształcić można do następującej postaci:

$$p(L,1) = \sum_{k=1}^{\infty}(u \cdot S_1(k) \cdot S_2(k) + h(u,0) \cdot S_3(k)),$$
$$q(L,1) = \sum_{k=1}^{\infty}\left(S_1(k) \cdot \left(u(k+1) \cdot S_2(k) - (1-u)\sum_{i=1}^{k} i \cdot v^{i-1}\log i\right) + k \cdot h(u,0) \cdot S_3(k)\right),$$

gdzie

$$S_1(k) = u^k(h(v,k) - h(u,k+1)),$$
$$S_2(k) = h(v,0) - v^k h(v,k),$$
$$S_3(k) = u^k(h(u,k) - h(v,k)).$$

Kolejnym krokiem będzie znalezienie oszacowań „ogonów" sum $p(L,1)$ i $q(L,1)$, które posłużą do wyznaczenia ostatecznych granic dla obliczeń numerycznych.

Mamy:

$$
\begin{aligned}
S_1(k) &= u^k\left(h(v,k)-h\left(u,k+1\right)\right)\\
&= u^k\left((1-v)\sum_{i=1}^{\infty}v^{i-1}\log(i+k)-(1-u)\sum_{i=1}^{\infty}u^{i-1}\log\left(i+k+1\right)\right)\\
&= \left(\frac{u}{v}\right)^k\frac{1-v}{v}\sum_{i=k+1}^{\infty}v^i\log i-\frac{1-u}{u^2}\sum_{i=k+2}^{\infty}u^i\log i\leqslant\\
&\leqslant u^k\left(\log(k+1)+\frac{v\log e}{(k+1)(1-v)}-\log(k+2)\right.\\
&\quad\left.-\frac{u\log e}{k+2}\left(1+\frac{1-u^{k+2}}{1-u}u\left(\frac{1}{2}+\frac{u^{k+2}}{3}\right)-\frac{1}{2\left(k+2\right)(1-u)}\right)\right)\\
&\leqslant u^k\log e\left(-\frac{1}{k+1}+\frac{1}{2\left(k+1\right)^2}+\frac{v}{(k+1)(1-v)}\right.\\
&\quad\left.-\frac{u}{k+2}\left(1+\frac{1-u^{k+2}}{1-u}u\left(\frac{1}{2}+\frac{u^{k+2}}{3}\right)-\frac{1}{2\left(k+2\right)(1-u)}\right)\right)\\
&\leqslant u^k\log e\left(\frac{1}{k+1}\frac{2v-1}{1-v}+\frac{1}{2(k+1)^2}\right.\\
&\quad\left.-\frac{u}{k+2}\left(1+\frac{1-u^{k+2}}{1-u}u\left(\frac{1}{2}+\frac{u^{k+2}}{3}\right)-\frac{1}{2(k+2)(1-u)}\right)\right),
\end{aligned}
$$

$$
\begin{aligned}
S_2(k) &= h(v,0)-v^kh(v,k)=\\
&= h(v,0)-v^k\left(\frac{h(v,0)}{v^k}-(1-v)\sum_{i=2}^{k}v^{i-k-1}\log i\right)\\
&= (1-v)\sum_{i=2}^{k}v^{i-1}\log i\leqslant h(v,0),
\end{aligned}
$$

$$
\begin{aligned}
S_3(k) &= u^k(h(u,k)-h(v,k))\\
&= u^k\left((1-u)\sum_{i=1}^{\infty}u^{i-1}\log\left(i+k\right)-(1-v)\sum_{i=1}^{\infty}v^{i-1}\log(i+k)\right)\\
&= \frac{1-u}{u}\sum_{i=k+1}^{\infty}u^i\log i-\left(\frac{u}{v}\right)^k\frac{1-v}{v}\sum_{i=k+1}^{\infty}v^i\log i\\
&\leqslant u^k\left(\log(k+1)+\frac{u\log e}{(k+1)(1-u)}-\log(k+1)+\right.
\end{aligned}
$$

$$-\frac{v\log e}{k+1}\left(1+\frac{1-v^{k+1}}{1-v}v\left(\frac{1}{2}+\frac{v^{k+1}}{3}\right)-\frac{1}{2(k+1)(1-v)}\right)\Bigg)$$
$$\leqslant \frac{u^k\log e}{k+1}\left(\frac{u}{(1-u)}-v\left(1+\frac{1-v^{k+1}}{1-v}v\left(\frac{1}{2}+\frac{v^{k+1}}{3}\right)\right.\right.$$
$$\left.\left.-\frac{1}{2(k+1)(1-v)}\right)\right),$$

$$\sum_{i=1}^{k} i\,v^{i-1}\log i \geqslant 2v+3v^2\log 3+\sum_{w=2}^{s-1} w\sum_{i=2^w}^{2^{w+1}-1} i\,v^{i-1}+s\sum_{i=2^s}^{k} i\,v^{i-1}=$$
$$\geqslant 2v+3v^2\log 3+\sum_{w=2}^{s-1} w\frac{v}{1-v}\left(2^w v^{2^w-1}-(2^{w+1}-1)v^{2^{w+1}-1}\right.$$
$$\left.+\frac{v^{2^w}-v^{2^{w+1}-1}}{1-v}\right)+s\frac{v}{1-v}\left(2^s v^{2^s-1}-kv^k+\frac{v^{2^s}-v^k}{1-v}\right)$$
$$\geqslant 2v+3v^2\log 3+\sum_{w=2}^{s-1}\frac{wv^{2^w}}{1-v}\left(2^w\left(1-2\cdot v^{2^w}\right)+\frac{v}{1-v}\left(1-v^{2^w}\right)\right)$$
$$+s\frac{v^{2^s}}{1-v}\left(2^s+\frac{v}{1-v}\right)-\frac{s}{(1-v)^2}v^{k+1}-\frac{s}{1-v}kv^{k+1}$$
$$\geqslant W(s)-\frac{s}{(1-v)^2}v^{k+1}-\frac{s}{1-v}kv^{k+1},$$

gdzie

$$s=\lfloor\log k\rfloor,$$

i

$$W(s)=2v+3v^2\log 3+\sum_{w=2}^{s-1}\frac{w\,v^{2^w}}{1-v}\left(2^w\left(1-2\cdot v^{2^w}\right)+\frac{v}{1-v}\left(1-v^{2^w}\right)\right)$$
$$+s\frac{v^{2^s}}{1-v}\left(2^s+\frac{v}{1-v}\right).$$

Na podstawie powyższych wyznaczymy poszukiwane oszacowania:

$$\sum_{k=\Delta}^{\infty}\left(u\cdot S_1(k)\cdot S_2(k)+h(u,0)\cdot S_3(k)\right)\leqslant\sum_{k=\Delta}^{\infty}u^{k+1}\log e\left(\frac{1}{k+1}\frac{2v-1}{1-v}\right.$$
$$+\frac{1}{2(k+1)^2}-\frac{u}{k+2}\left(1+\frac{1-u^{k+2}}{1-u}u\left(\frac{1}{2}+\frac{u^{k+2}}{3}\right)\right.$$
$$\left.\left.-\frac{1}{2(k+2)(1-u)}\right)\right)\cdot h(v,0)+$$

$$+\sum_{k=\Delta}^{\infty} h(u,0)\frac{u^k\log e}{k+1}\left(\frac{u}{(1-u)}-v\left(1+\frac{1-v^{k+1}}{1-v}v\left(\frac{1}{2}+\frac{v^{k+1}}{3}\right)\right.\right.$$

$$\left.\left.-\frac{1}{2(k+1)(1-v)}\right)\right)\leqslant\frac{u^{\Delta+1}h(v,0)\log e}{(1-u)}\left(\frac{(2v-1)}{(\Delta+1)(1-v)}\right.$$

$$+\frac{1}{2(\Delta+1)^2(1-u)}+\frac{u^{\Delta+4}}{6(\Delta+2)(1-u^2)}$$

$$\left.-\frac{u(2-u)}{2(\Delta+2)}\left(1+\frac{1-u^{\Delta+2}}{1-u}u\left(\frac{1}{2}+\frac{u^{\Delta+2}}{3}\right)\right)+\frac{u^{2\Delta+6}}{3(\Delta+2)(1-u^3)}\right)$$

$$+u^{\Delta}h(u,0)\log e\left(\frac{1}{(\Delta+1)(1-u)}\left(\frac{u}{(1-u)}-\frac{v(2-v)}{2(1-v)}\right.\right.$$

$$\left.+\frac{v}{2(\Delta+1)(1-v)}\right)+\frac{v^{\Delta+3}}{6(\Delta+1)(1-v)(1-uv)}$$

$$\left.+\frac{v^{2\Delta+4}}{3(\Delta+1)(1-v)(1-uv^2)}\right),$$

$$\sum_{k=\Delta}^{\infty}\left(S_1(k)\cdot\left(u(k+1)\cdot S_2(k)-(1-u)\sum_{i=1}^{k}i\cdot v^{i-1}\log i\right)\right.$$

$$\left.+k\cdot h(u,0)\cdot S_3(k)\right)\leqslant\sum_{k=\Delta}^{\infty}\left(u^k\log e\left(\frac{1}{k+1}\frac{2v-1}{1-v}+\frac{1}{2(k+1)^2}\right.\right.$$

$$\left.-\frac{u}{k+2}\left(1+\frac{1-u^{k+2}}{1-u}u\left(\frac{1}{2}+\frac{u^{k+2}}{3}\right)-\frac{1}{2(k+2)(1-u)}\right)\right)$$

$$\left.\cdot\left(uh(v,0)(k+1)-(1-u)\left(W(s)-\frac{s}{(1-v)^2}v^{k+1}-\frac{s}{1-v}kv^{k+1}\right)\right)\right)$$

$$+\sum_{k=\Delta}^{\infty}k\cdot h(u,0)\cdot\frac{u^k\log e}{k+1}\left(\frac{u}{(1-u)}-v\left(1+\frac{1-v^{k+1}}{1-v}v\left(\frac{1}{2}+\frac{v^{k+1}}{3}\right)\right.\right.$$

$$\left.\left.-\frac{1}{2(k+1)(1-v)}\right)\right)\leqslant h(v,0)\log e\sum_{k=\Delta}^{\infty}\left(\left(\frac{2v-1}{1-v}-\frac{u(2-u)}{2(1-u)}\right)u^{k+1}\right.$$

$$\left.+\frac{u^{k+1}}{2(k+1)}+\frac{u^{2k+5}}{6(1-u)}+\frac{u^{3k+7}}{3(1-u)}+\frac{u^{k+2}}{2(k+2)(1-u)}\right)$$

$$-(1-u)\log e\sum_{k=\Delta}^{\infty}\left(\left(\frac{2v-1}{1-v}\frac{u^k}{k+1}+\frac{u^k}{2(k+1)^2}-\frac{u(2-u)}{2(1-u)}\frac{u^k}{k+2}+\right.\right.$$

$$
\begin{aligned}
&+\frac{1}{6(1-u)}\frac{u^{2k+4}}{k+2}+\frac{1}{3(1-u)}\frac{u^{3k+6}}{k+2}+\frac{1}{2(1-u)}\frac{u^{k+1}}{(k+2)^2}\Big)\cdot\\
&\cdot\left(W(s)-\frac{s}{(1-v)^2}v^{k+1}-\frac{s}{1-v}kv^{k+1}\right)\Big)\\
&+h(u,0)\log e\sum_{k=\Delta}^{\infty}\Bigg(\left(\left(\frac{u}{(1-u)}-\frac{v(2-v)}{2(1-v)}\right)\frac{u^k k}{k+1}+\frac{v^3}{6(1-v)}\frac{(uv)^k k}{k+1}\right.\\
&\left.+\frac{v^4}{3(1-v)}\frac{(uv^2)^k k}{k+1}+\frac{v}{2(1-v)}\frac{u^k k}{(k+1)^2}\right)l\\
\leqslant\ &\frac{h(v,0)\log e}{1-u}u^{\Delta+1}\left(\frac{2v-1}{1-v}-\frac{u(2-u)}{2(1-u)}+\frac{1}{2(\Delta+1)}+\frac{u}{2(\Delta+2)(1-u)}\right.\\
&\left.+\frac{u^{\Delta+4}}{6(1-u^2)}+\frac{u^{2\Delta+6}}{3(1-u^3)}\right)-\log e\cdot W(s)u^{\Delta}\left(\frac{u^{\Delta}(2v-1)(1-u)}{(\Delta+1)(1-v)}\right.\\
&\cdot\left(1+\frac{1-u^{\Delta+1}}{1-u}u\left(\frac{1}{2}+\frac{u^{\Delta+1}}{3}\right)\right)+\frac{u^{\Delta}(1-u)}{2(\Delta+1)^2}\left(1+\frac{1-u^{\Delta+1}}{1-u}\right.\\
&\left.\cdot u\left(\frac{1}{4}+\frac{u^{\Delta+1}}{9}\right)\right)-\frac{u(2-u)}{2(\Delta+2)(1-u)}\\
&+\frac{u^{\Delta+4}}{6(\Delta+2)}\left(1+\frac{1-u^{2\Delta+4}}{1-u^2}u\left(\frac{1}{2}+\frac{u^{2\Delta+4}}{3}\right)\right)\\
&+\frac{u^{2\Delta+6}}{3(\Delta+2)}\left(1+\frac{1-u^{3\Delta+6}}{1-u^3}u\left(\frac{1}{2}+\frac{u^{3\Delta+6}}{3}\right)\right)\\
&\left.+\frac{u}{2(\Delta+2)^2}\left(1+\frac{1-u^{\Delta+2}}{1-u}u\left(\frac{1}{4}+\frac{u^{\Delta+2}}{9}\right)\right)\right)+\log e\frac{1-u}{(1-v)^2}su^{\Delta}v^{\Delta+1}\\
&\cdot\left(\frac{2v-1}{(\Delta+1)(1-v)(1-uv)}+\frac{1}{2(\Delta+1)^2(1-uv)}-\frac{u(2-u)}{2(\Delta+2)(1-u)}\right.\\
&\cdot\left(1+\frac{1-u^{\Delta+2}v^{\Delta+3}}{1-uv}uv\left(\frac{1}{2}+\frac{u^{\Delta+2}v^{\Delta+3}}{3}\right)\right)\\
&+\frac{u^{\Delta+4}}{6(\Delta+2)(1-u)(1-u^2v)}+\frac{u^{2\Delta+6}}{3(\Delta+2)(1-u)(1-u^3v)}\\
&\left.+\frac{u}{2(\Delta+2)^2(1-u)(1-uv)}\right)+\log e\frac{1-u}{1-v}su^{\Delta}v^{\Delta+1}\\
&\cdot\left(\frac{1}{1-uv}\left(\frac{2v-1}{(1-v)}-\frac{u(2-u)}{2(1-u)}\right)+\frac{1}{2(\Delta+1)(1-uv)}+\right.\\
&\left.+\frac{u^{\Delta+4}}{6(1-u)(1-u^2v)}+\frac{u^{2\Delta+6}}{3(1-u)(1-u^3v)}+\frac{u}{2(\Delta+2)(1-u)(1-uv)}\right)
\end{aligned}
$$

$$+ h(u,0)\log e u^{\Delta}\left(\left(\frac{u}{(1-u)} - \frac{v(2-v)}{2(1-v)}\right)\frac{1}{1-u} + \frac{v^{\Delta+3}}{6(1-v)(1-uv)} + \frac{v^{2\Delta+4}}{3(1-v)(1-uv^2)} + \frac{v}{2(\Delta+1)(1-u)(1-v)}\right).$$

W tabeli poniżej zamieszczone zostały wartości Δ, dla których na podstawie powyższych oszacowań zachodzą:

$$\sum_{k=\Delta}^{\infty}\left(u\cdot S_1(k)\cdot S_2(k) + h(u,0)\cdot S_3(k)\right) \leqslant 2^{-65}, \tag{1}$$

$$\sum_{k=\Delta}^{\infty}\left(u\cdot S_1(k)\cdot S_2(k) + h(u,0)\cdot S_3(k)\right) \leqslant 2^{-128}, \tag{2}$$

$$\sum_{k=\Delta}^{\infty}\left(S_1(k)\cdot\left(u(k+1)\cdot S_2(k) - (1-u)\sum_{i=1}^{k} i\cdot v^{i-1}\log i\right) + k\cdot h(u,0)\cdot S_3(k)\right) \leqslant 2^{-65}, \tag{3}$$

$$\sum_{k=\Delta}^{\infty}\left(S_1(k)\cdot\left(u(k+1)\cdot S_2(k) - (1-u)\sum_{i=1}^{k} i\cdot v^{i-1}\log i\right) + k\cdot h(u,0)\cdot S_3(k)\right) \leqslant 2^{-128}, \tag{4}$$

przy założeniu, że wartość $h(u,0)$ podana jest dokładnie.

Tabela 4

L	$u = 1-2^{-L}$	$K_c = 500\cdot 2^L$	Δ			
			(1)	(2)	(3)	(4)
2	0,75	2000	149	298	165	317
3	0,875	4000	333	654	374	701
4	0,9375	8000	707	1373	805	1481
5	0,96875	16000	1469	2823	1691	3067
6	0,984375	32000	3019	5751	3514	6287
7	0,9921875	64000	6173	11660	7259	12826
8	0,99609375	128000	12584	23581	14941	26097
9	0,998046875	256000	25608	47627	30691	53025
10	0,9990234375	512000	52055	96122	62951	107642
11	0,99951171875	1024000	105738	193907	128986	218389

Tabela 4

L	$u = 1 - 2^{-L}$	$K_c = 500 \cdot 2^L$	Δ			
			(1)	(2)	(3)	(4)
12	0,999755859375	2048000	214667	391054	264067	442896
13	0,9998779296875	4096000	435624	788472	540225	897907
14	0,99993896484375	8192000	883694	1589515	1104488	1819876
15	0,999969482421875	16384000	1792074	3203936	2256830	3687633
16	0,9999847412109375	32768000	3633184	6457316	4609007	7470641

7. Wyniki obliczeń

W tabelach poniżej zebrane zostały wyniki przeprowadzonych obliczeń. W pierwszej podane są wartości oczekiwane i odchylenia standardowe dla zmiennych losowych $A_i(s^n)$, w drugiej zaś wartości parametrów $d(L)$ i $e(L)$ dla $L = 1, \ldots, 16$.

Pogrubione zostały te cyfry, których nie można było znaleźć w dostępnej literaturze bądź też, gdy w świetle przeprowadzonych obliczeń, podawane na tej pozycji wartości były błędne.

Tabela 5

L	$E[\log A_n]$	$D^2[\log A_n]$
1	0,7326494821174844154	0,6897677849414730957899
2	1,5374382909327386397	1,3377387691100273785
3	2,4016068119756679046	1,90133468673455419743
4	3,3112247204007159797	2, 35773692616648526827
5	4,2534265964727897507	2,70455283913999607332
6	5,2177052498613229973	2,954032399381721807
7	6,1962506541018770827	3,12539186860888834697
8	7,183665553492268639	3,238662160971425896
9	8,1764247579136495	3,3112008794777729186
10	9,1723243081957289788	3,356456906968740799
11	10,170032291924027377	3,3840870306566133265
12	11,16876487440486225 16	3,4006541450941706898
13	12,16807031422367721 43	3,410438009140221767
14	13,167692567127944386	3,416141821707380582
15	14,167488448596030694 2	3,419430397502265927
16	15,167378763677508772	3,4213083424718861382

Tabela 6

L	$d(L)$	$e(L)/2^L$	$e(L)$
1	0,1946340234883123148	0,67053546969724352606	1,341070939394487052
2	0,2363134725179499465	0,559497571818450236	2,23799028727380094399
3	0,2732725**058977388449** 0,2732725	0,4890883**2806285090885** 0,4890883	3, 9127066245028072708
4	0,3045101**315775895468** 0,3045101	0,4435381**2331972225955** 0,4435381	7,0966099731155561529
5	0,3296586**56693816651918** 0,3296587	0,4137195**82350136217 62** 0,4137196	13,2390266352043589638
6	0,3489768**5118084701067** 0,3489769	0,3941337**944526468635** 0,3941338	25.2245628449693992659
7	0,3631815**1997069249365** 0,3631815	0,3813210**3883561493299** 0,3813210	48.80909297095871132
8	0,3732189**2957788234228** 0,3732189	0,3730194**9204189159814** 0,3730195	95.492989962724249124
9	0,3800636**6611343474813** 0,3800637	0,3677118**145424184971** 0,3677118	188.2684490457182705
10	0,3845866**729846703285** 0,3845867	0,3643695**4012381556889** 0,3643695	373.11440908678714255
11	0,3874941**9935746281236** 0,3874942	0,3622979**025861052106** 0,3622979	741.9861044963434713
12	0,3893189**20214368600573** 0,3893189	0,3610335**7213385799147** 0,3610336	1478.793511460282333
13	0,3904405**146005691433 4** 0,3904405	0,3602731**2844583196555** 0,3602731	2951.3574682282554618
14	0,3911176**3381731468 51** 0,3911178	0,3598218**5228368677115** 0,3598216	5895.3212278159240586
15	0,3915201**136403384 3555** 0,3915202	0,3595572**833285827172 38** 0,3595571	11781.9730601109984785
16	0,3917561**504127106571** 0,3917561	0,3594038**5666680925834** 0,3594040	23553.891150516011554

Liczby w powyższych tabelach mają tak dobrane długości, że w każdym przypadku są one konieczne i wystarczające, by komputer przypisał możliwie najdokładniejszą wartość zmiennej typu *extended*.

Jak można zauważyć, rozbieżności pomiędzy literaturowymi a otrzymanymi wartościami nie są zbyt wielkie. Ich wpływ prześledzimy dla przypadku $L = 14$, gdzie te różnice wydają się być największe. Przyjmując $K_c = 500 \cdot 2^{14}$ i poziom istotności testu $\alpha = 0{,}1$ dostajemy następu-

jące progowe wartości statystyki 13,16810877104 dla wartości literaturowych oraz 13,16810877087, czyli różnica pojawia się na 9 miejscu po przecinku, a 11 pozycji znaczącej. Jednak jeśli obliczymy prawdopodobieństwo dla pierwszej z tych wartości według otrzymanych danych, to dostaniemy 0,95000007..., a tu różnica pojawia się już na 8 miejscu znaczącym, oznacza ona, że odrzucilibyśmy o około 0,00000014 przypadków za mało, co daje proporcjonalnie 0,0000014 wszystkich odrzucanych przypadków. Jeśli jednak poziom istotności wyniósłby 0,0001, to różnica taka wyniosłaby 0,0000068 odrzucanych przypadków.

Podsumowując powyższe spostrzeżenia możemy stwierdzić, że wprowadzenie poprawionych wartości współczynników d i e nie zmienia drastycznie otrzymywanych rezultatów, łatwo jednak wyobrazić sobie sytuację, w której te drobne różnice mogłyby stać się przysłowiowym języczkiem u wagi, decydującym o dopuszczeniu generatora tak naprawdę nieprzechodzącego tego testu.

Nawet jeśli powyższe uznamy za skrajnie nieprawdopodobne, to pracę tę powinny bronić wyniki otrzymane dla $L = 1$ oraz 2.

Praca naukowa finansowana ze środków na naukę w latach 2008–2010 jako projekt rozwojowy Nr O R00 0031 06.

Artykuł wpłynął do redakcji w dniu 27.06.2008 r. Zweryfikowaną wersję po recenzji otrzymano w grudniu 2008 r.

LITERATURA

[1] J. S. Coron, D. Naccache, *An accurate evaluation of Maurer's universal test*, Proceedings of SAC 98 (Lecture Notes in Computer Science), Springer-Verlag, 1998.

[2] U. M. Maurer, *A universal statistical test for random bit generator*, Advances in Cryptology, CRYPTO'90. Lecture Notes in Computer Science, vol. 537. Springer-Verlag.

K. MAŃK

Evaluation of exact parameters values for Maurer's test

Abstract. This paper is a development of Coron and Naccache's work entitled *An accurate evaluation of Maurer's universal test.* Original results have been enriched by deriving formulas for one bit block case and analysis of influence of approximate evaluation of infinite sums which occurs in presented formulas. Finally computational results were presented and compared with previous ones.

Keywords: Maurer's test, universal test, statistical test

2000 Mathematics Subject Classification: (primary) 62E20 (secondary) 62Q05