Diss. ETH Nr. 8500

EIN MODIFIZIERTER TAUSWORTHE GENERATOR

A B H A N D L U N G

zur Erlangung des Titels eines

DOKTORS DER MATHEMATIK

der

EIDGENOESSISCHEN TECHNISCHEN HOCHSCHULE ZUERICH

vorgelegt von

Günter Hobein

Dipl. Math. ETH

geboren am 7. September 1950

von Zürich ZH

angenommen auf Antrag von :

Prof. Dr. H. Bühlmann, Referent

Prof. Dr. H. R. Künsch, Korreferent

1988

K U R Z F A S S U N G

Wie der Titel angedeutet, wird in dieser Arbeit Tausworthe's Zufallszahlengenerator aus dem Jahr 1965 abgeändert : Während die Erzeugung der beiden Primärfolgen $(a_k)_{k \in I}$ oder $(\alpha_k)_{k \in I}$ unverändert übernommen wird, werden bei der Bildung der Sekundärfolgen, also der $(Y_k)_{k \in I}$ oder $(W_k)_{k \in I}$, neu auch nicht überlappende Binär-Zahlwörter zugelassen. So entsteht eine Folge abhängiger Zufallszahlen, abhängig von einem frei wählbaren Shiftparameter s , $s \geq 1$, anstelle des festen Vorschubs q , mit $q \geq L$ bei Tausworthe, L ist die Anzahl Binärstellen der Zufallszahl Y_k oder W_k.

In Kapitel 1 werden dann die Resultate des Artikels von Tausworthe für den neuen Ansatz umgeschrieben und einige weitere Resultate hinzugefügt, in Kapitel 2 die Momente sämtlicher auftretender Zufallsfolgen, auch die von Summenfolgen bestimmt. In Kapitel 3 wird der Vergleich mit einem "ideal" erzeugten Generator (i.i.d. - Fall) vorgenommen auf der Basis von Distanzen zwischen Verteilungsfunktionen. In Kapitel 4 werden Methoden untersucht, um aus den korrelierten Zufallsgrössen unkorrelierte zu erhalten : Das ist einmal mit den klassischen Ansätzen der Linearen Algebra möglich, indem man die Covarianzmatrizen diagonalisiert; dazu werden zwei Verfahren in einer geschlossenen Art angeführt. Ferner gibt es einem direkten Weg über den Durbin-Levinson-Algorithmus, der hier ebenfalls zur Anwendung gelangt. In Kapitel 5 werden schliesslich Ueberlegungen zur asymptotischen Normalität der Tausworthe-Folgen angestellt.
Die meisten in der ganzen Arbeit entwickelten Resultate wirken auf den ursprünglichen Tausworthe-Generator zurück. In den Beispielen, Kapitel 6, werden schliesslich Paare abhängiger Sekundärfolgenelemente ihren unkorrelierten Analoga für verschiedene Parameter gegenübergestellt.

A B S T R A C T

As mentioned in the title the author modifies Tausworthe's random number generator of 1965. While the generation of the primary sequences like $(a_k)_{k \in I}$ or $(\alpha_k)_{k \in I}$ has not been changed, the construction of the secondary sequences like $(Y_k)_{k \in I}$ or $(W_k)_{k \in I}$ has been modified in the following way : The binary words of which the random numbers are built are no longer non-overlapping pieces of the primary sequences as they are in Tausworthe's article. We here propose to take just one or two, generally speaking s , new elements to construct the following random number, instead of going always q steps forward, with $q \geq L$ like Tausworthe does; s is called shiftparameter, L means the number of binary digits used in a single Y_k or W_k.

In chapter 1 the results of Tausworthe are reformulated due to our new approach and some more are added, in chapter 2 the moments have been calculated for all sorts of sequences, even for the sequences of partial sums. In chapter 3 the author compares the existing random number sequences with an ideally generated sequence on the basis of distances between the distribution functions. In chapter 4 the question is discussed in how far the correlated random numbers can be transformed into their uncorrelated counterparts. Here are two classical approaches being presented in a closed way to diagonalize covariance matrices of the stationary random sequences as well as the Durbin-Levinson-Algorithmus is applied. In chapter 5 some remarks follow concerning the asymptotical normality. Most results derived in all chapters are also valid for the original Tausworthe-generator. The examples in chapter 6 finally show pairs of dependent correlated random numbers in comparison with pairs of dependent uncorrelated ones.