Z. Wahrscheinlichkeitstheorie verw. Geb. 16, 1–21 (1970)

Klassifikation der Zufallsgesetze nach Komplexität und Ordnung*

Claus-Peter Schnorr

1. Einleitung und Übersicht

Nachdem in [10, 11] mit der Definition effektiver Zufallstests eine Charakterisierung aller effektiv nachprüfbaren Eigenschaften von Zufallsfolgen gegeben wurde, ist es das Ziel der vorliegenden Arbeit, diese Eigenschaften zu klassifizieren. Die Klassifikation bezüglich der Komplexität, d.h. nach dem technischen Aufwand an Raum bzw. Zeit, der beim Testen der betreffenden Eigenschaft mindestens aufgewendet werden muß, führt zur Definition des Zufallsgrads von Folgen. Er gibt an, in welchem Maße das Verhalten einer Folge dem einer idealen Zufallsfolge nahekommt. Damit werden Klassen berechenbarer Folgen gebildet, die sich in ihrem Verhalten dem idealer Zufallsfolgen immer mehr annähern. Somit gelangt man erstmals zu einem präzisen Konzept einer Pseudozufallszahl. Diese Pseudozufallszahlen sind notwendigerweise aufwendig zu berechnen und könnten im Gegensatz zu den gebräuchlichen Zufallszahlen nicht bei jeder Verwendung erneut berechnet werden. Aber es wäre denkbar, daß man in einem einmaligen aufwendigen Verfahren eine Pseudozufallszahl konstruiert, die sich in allen Rechenprozessen, die eine gewisse Komplexität nicht übersteigen, wie eine ideale Zufallsfolge verhält. Unser Konzept der Pseudozufallszahl ist insofern noch idealisiert als es sich dabei um unendliche Folgen handelt, deren Zufallseigenschaften im allgemeinen in unendlichen Rechenprozessen zum Tragen kommen.

Durch den Begriff der Ordnung eines Fastüberallgesetzes sind wir in der Lage, zu präzisieren, in welchem Sinne den in der statistischen Praxis üblicherweise durchgeführten Tests eine große Bedeutung zukommt. Diese Tests beziehen sich nämlich auf Zufallsgesetze mit der höchsten Ordnung. Allgemein gehören die Zufallsgesetze, welche die relative Grenzhäufigkeit von Ereignissen zum Inhalt haben, zu den Gesetzen von hoher Ordnung. Hierunter fällt insbesondere das starke Gesetz der großen Zahlen.

Um zu einer Komplexitätshierarchie von effektiven Zufallstests zu gelangen, benutzen wir im Prinzip den Ansatz von Hartmanis und Stearns [4]. Wir legen dabei das in [12] eingeführte Modell einer mehrbändrigen Turingmaschine zugrunde, bei dem reine Bandschiebeoperationen zu Sprüngen zusammengefaßt werden können. Die Arbeitsweise dieses Modells entspricht der eines Speichers mit fester Zugriffszeit. Eine Beschreibung des Modells findet sich in Kapitel 2.

* Die Arbeit stellt einen Teil der Habilitationsschrift dar, die der Mathematisch-Naturwissenschaftlichen Fakultät der Universität des Saarlandes vom Verfasser vorgelegt wurde.

Die Komplexität von Zufallsgesetzen und den Zufallsgrad von Folgen definieren wir in Kapitel 3. Eine Folge ist vom Zufallsgrad T (T: $N \to N$ ist eine rekursive, monoton wachsende Funktion), wenn sie alle Zufallstests der Komplexität T besteht. Wir untersuchen Beziehungen zwischen der Komplexität von Folgen und ihrem Zufallsgrad. Die Komplexität einer Folge mit Zufallsgrad T muß selbst stärker wachsen als T. Die Aufgabe, eine Folge mit Zufallsgrad T zu konstruieren erfordert nicht wesentlich mehr Aufwand, als die Aufgabe, eine Folge zu konstruieren, deren Komplexität T übersteigt. Das starke Gesetz der großen Zahlen ist insofern von sehr geringer Komplexität, als die Folgen mit dem niedrigsten von uns betrachteten Zufallsgrad bereits dieses Gesetz erfüllen. Wir zeigen ferner, daß es zu vorgegebener Komplexität keinen universellen Zufallstest (d.h. ein Test, der alle Zufallstests dieser Komplexität umfaßt) gibt, welcher noch von dieser Komplexität ist. Dagegen gibt es einen solchen universellen Test mit einer stärker wachsenden Komplexität.

In Kapitel 4 zeigen wir, daß der Zufallsgrad einer Folge sich bei Transformation der Folge durch eine Auswahlregel i.S. von Mises nicht ändert, sofern nur diese Auswahlregel nicht zu kompliziert ist. Ferner wird bewiesen, daß der Zufallsgrad einer Folge im Gegensatz zur Komplexität nicht von einer beliebig dünnen Teilmenge der Glieder der Folge abhängen kann.

Im Gegensatz zur Komplexität, welche eine rein algorithmische Klassifikation der Fastüberallgesetze liefert, ist die in Kapitel 5 definierte Ordnung eine rein geometrische Eigenschaft der den Fastüberallgesetzen zugehörigen Nullmengen. Kleine Nullmengen haben eine hohe Ordnung. Es werden Operationen untersucht, welche die Ordnung eines Fastüberallgesetzes nicht verändern. Wir zeigen, daß die Klassifikation nach der Ordnung relativ fein ist. Wenn die Ordnungsfunktion G nur geringfügig stärker anwächst als G', dann gibt es Nullmengen der Ordnung G', die nicht in der Vereinigung aller Nullmengen der Ordnung G enthalten sind.

In Kapitel 6 charakterisieren wir die Gesamtheit aller Zufallsgesetze von der höchsten Ordnung. Die Gesetze mit exponentiell wachsenden Ordnungsfunktionen sind gerade Gesetze, welche eng mit der relativen Grenzhäufigkeit von Ereignissen zusammenhängen.

Wir setzen im folgenden die Kenntnis der Arbeiten [10, 11], insbesondere die dort eingeführten Bezeichnungen, voraus.

2. Raum- und Zeitkomplexität rekursiver Funktionen

Wir definieren allgemein Raum- und Zeitkomplexitätsklassen rekursiver Funktionen h: $X^* \to Y^*$. Dabei ist X^* die Menge der endlichen Folgen mit Elementen aus X. Wir erweitern das übliche Modell einer mehrbändrigen Turingmaschine (TM) durch Operationen, die markierte Bandspeicherplätze anspringen, so daß der Arbeitsspeicher einem Speicher mit fester Zugriffszeit nahekommt. Durch diese Abänderung werden die Komplexitätsklassen weniger von der Geometrie der Maschine abhängig. Eine n-bändrige TM soll n zweiseitig unendliche Arbeitsbänder, sowie jeweils ein einseitig unendliches Ein- bzw. Ausgabeband besitzen. Auf dem Eingabeband darf nichts geschrieben, auf dem Ausgabeband darf nichts gelöscht werden. Ferner dürfen Ein- und Ausgabeband nur in eine Richtung bewegt werden.

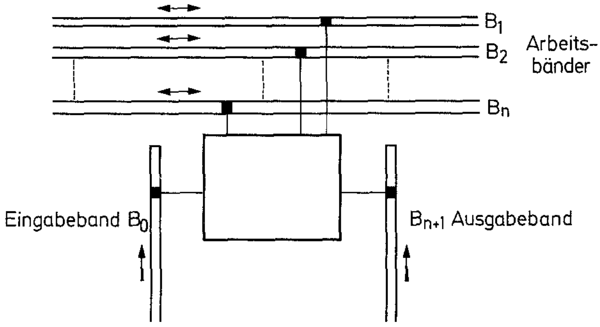

Fig. 1. Eine n-bändrige Turingmaschine

(2.1) **Definition.** Eine n-bändrige TM ist ein 5-Tupel $M=(Z, X, a_0, Z_F, \delta)$ mit (1)–(5).

(1) Z ist eine endliche Menge von Zuständen, $a_0 \in Z$ ist der Anfangszustand, $Z_F \subset Z$ die Menge der Endzustände.

(2) X ist das endliche Alphabet, $\square \in X$ ist das Leerzeichen.

(3) δ: $(Z-Z_F)\times X^{n+1} \to X^{n+1} \times C^{n+2} \times Z$ mit $C=\{-1,0,1\}$ ist die Überführungsfunktion.

(4) Es gelten folgende Einschränkungen:

$$\delta(s_i; x_0, x_1, \ldots, x_n) = (y_1, y_2, \ldots, y_{n+1}; c_0, \ldots, c_{n+1}; s_j)$$

impliziert: $c_0 \neq -1$, $c_{n+1} \neq -1$ und $(y_{n+1} \neq \square \Rightarrow c_{n+1}=1)$.

(5) Zu $x \in X$ und i mit $1 \leqq i \leqq n$ gibt es einen ausgezeichneten Zustand $s(x, i) \in Z$. $Z_i \underset{\text{def}}{=} \{s(x, i) | x \in X\}$.

Die Arbeitsweise von M ergibt sich, indem wir eine Zuordnung

$$\delta\colon (s_i; x_0, x_1, \ldots, x_n) \to (y_1, y_2, \ldots, y_{n+1}; c_0, \ldots, c_{n+1}; s_j)$$

folgendermaßen als Maschinenoperation deuten: s_i ist der augenblickliche Zustand der Maschine. x_k sind die Symbole, über denen sich im augenblicklichen Zustand der Lese-Schreibkopf des Bandes B_k befindet. y_k sind die Symbole, die auf dem Band B_k an die Stelle, die der Lese-Schreibkopf beobachtet, geschrieben werden. c_k gibt die Bewegungsrichtung des Bandes B_k an. Falls $s_i \notin Z_i$ rückt das Band B_k anschließend um eine Einheit nach rechts wenn $c_k=1$, bzw. eine Einheit nach links wenn $c_k=-1$ und bleibt unverändert wenn $c_k=0$. Ist $s_i=s(x, k)$, dann rückt das Band B_k solange nach rechts im Falle $c_k=1$ (links wenn $c_k=-1$), bis der Lese-Schreibkopf über einem Symbol x steht; das Band bleibt unverändert, wenn $c_k=0$. Die Maschine geht sodann in den Zustand s_j über.

$M(x_1 \ldots x_n)$ bezeichnet den Rechenvorgang, der beginnt, wenn (1) die Inschrift $x_1 x_2 \ldots x_n$ fortlaufend in den ersten Zellen des Eingabebandes steht gefolgt von Leersymbolen, (2) die Maschine sich im Zustand a_0 befindet, (3) die Köpfe von B_0 und B_{n+1} sich jeweils über der ersten Zelle des Ein- bzw. des Ausgabebandes befinden und (4) die Arbeitsbänder und das Ausgabeband leer sind. Er bricht ab, wenn ein Endzustand erreicht wird.

(2.2) **Definition.** Die TM M_i berechnet die Funktion h: $X^* \to Y^*$ ($\square \notin Y$), wenn

(1) $M_i(\Lambda)$ abbricht, so daß $h(\Lambda)$ auf dem Ausgabeband steht. $\Lambda \in X^*$ ist das leere Wort.

(2) $M_i(x_1 \ldots x_n)$ zunächst dieselben Operationen ausführt wie $M_i(x_1 \ldots x_{n-1})$, dann $h(x_1 \ldots x_n)$ berechnet und durch ein Leersymbol von $h(x_1 \ldots x_{n-1})$ getrennt auf dem Ausgabeband ausdruckt und dann abbricht.

Als eine Operation der Maschine bezeichnen wir die oben beschriebene Ausführung einer Zuordnung δ: $u \mapsto v$. Wir ordnen einer TM M_i folgende Komplexitätsfunktionen zu:

(2.3) **Definition.**

(1) $R_i^0(x)$ ist die Anzahl der Operationen von $M_i(x)$.

(2) $R_i^1(x)$ ist das Maximum aus der Anzahl der Zellen, die der Rechengang $M_i(x)$ auf den Arbeitsbändern benutzt und den Längen der Worte $h(x(n))$ mit $n \leqq |x|$.

Sei M_i ($i \in N$) eine Aufzählung aller mehrbändrigen TM'en. Dann ordnen wir einer monoton wachsenden Funktion T: $N \to N$ Raum- bzw. Zeitkomplexitätsklassen C_T^μ ($\mu = 0, 1$) von rekursiven Funktionen zu.

(2.4) **Definition.** h: $X^* \to Y^*$ ist in C_T^μ ($\mu = 0, 1$), wenn es eine TM M_i zu h im Sinne von (2.2) und ein $K \in N$ gibt, so daß für alle $x \in X^*$

$$R_i^\mu(x) \leqq K T(K + |x|).$$

Im folgenden setzt die Bezeichnung C_T^μ stets voraus, daß T rekursiv ist, und daß im Falle der Zeitkomplexität ($\mu = 0$) stets $T(n) \geqq n^2$ und im Falle der Raumkomplexität ($\mu = 1$) stets $T(n) \geqq n$ gilt. Somit lassen wir, wie man aus (2.3) entnimmt, gerade alle Komplexitätsklassen C_T^μ zu, die Funktionen h: $X^* \to Y^*$ enthalten, so daß $|h(x)|$ streng monoton mit $|x|$ wächst.

Der Vorteil unserer Modifikation des ursprünglichen Modells der TM liegt darin, daß die Komplexitätsklassen unabhängig von der Anzahl der zugelassenen Arbeitsbänder sind. Es gilt folgender leicht zu beweisender Satz [12].

(2.5) **Satz.** *Sei M_i eine m-bändrige TM zu h: $X^* \to Y^*$, dann gibt es eine einbändrige TM M_j zu h, so daß für alle $x \in X^*$ gilt:*

(1) $$R_j^0(x) \leqq (2+m)\, m\, R_i^0(x),$$

(2) $$R_j^1(x) \leqq m\, R_i^1(x).$$

Im Gegensatz zu den Raumkomplexitätsklassen können die Zeitkomplexitätsklassen von der Anzahl der zugelassenen Sprungmarken, d.h. von der Größe des Alphabets abhängen. Man kann eine TM M mit Alphabet $\bar{X}$ durch eine andere mit einem kleineren Alphabet X simulieren, indem man wie üblich $\bar{X}$ in X^* einbettet. Jede Operation von M, die nicht Sprungoperation ist, läßt sich bzgl. des kleineren Alphabets X so simulieren, daß sie im Rechenablauf jeweils durch eine konstante Anzahl von Operationen bzgl. des Alphabets X ersetzt wird [4]. Eine Sprungoperation muß man dagegen im allgemeinen durch eine Suchprozedur ersetzen. Die Anzahl der dabei ausgeführten Operationen kann man durch die Zahl der beschriebenen Bandspeicherplätze und damit durch die Gesamtzahl der Operationen abschätzen, die M bis dahin ausgeführt hat. Damit erhöht sich die Gesamtzahl der Operationen bei der Simulierung höchstens ins Quadrat. Dieser Quadratfaktor geht stets bei Anwendung einer Diagonalisierungstechnik ein.

Die Definition von Komplexitätsklassen rekursiver Funktionen $h: X^* \to Y^*$ führt insbesondere zu einer Komplexitätsklassifizierung der rekursiven Testfunktionen $F: X^* \to Z(2)$, sowie der rekursiven Folgen in X^∞. Hierzu beschreiben wir eine unendliche Folge über X durch eine Abbildung $h: N \to X$ und identifizieren die natürlichen Zahlen N mit dem von einer einelementigen Menge I erzeugten freien Monoid I^*. Für die so erzeugten Komplexitätsklassen von rekursiven Folgen bzw. von Testfunktionen schreiben wir $C_T^\mu(Fo)$ bzw. $C_T^\mu(TF)$. Ferner bezeichnen wir mit $C_T^\mu(Fu)$ die Komplexitätsklassen rekursiver Funktionen h: $N \to N$. Dabei identifizieren wir den Argumentbereich von h wieder mit I^*. Den Wertebereich von h betten wir in $Z(2)$ ein.

In den Überlegungen der Kapitel 3 und 4, welche auf dieser Komplexitätsklassifizierung beruhen, schlagen sich hauptsächlich einige Abschlußeigenschaften der Komplexitätsklassen nieder, die daraus resultieren, daß der Aufwand an Zeit bzw. Raum nur bis auf einen konstanten Faktor in die Definition der Komplexitätsklassen eingeht. Die benutzten Abschlußeigenschaften sind gerade die in [12] behandelten.

Wir führen Abschätzungen der Komplexität im folgenden nie explizit durch, sondern setzen dabei etwas Verständnis für die Manipulation von Programmen auf TM'en voraus [6, 7].

Grundlegendes zur Komplexitätstheorie rekursiver Funktionen findet sich außer in [4] u. a. in [1] und [5].

3. Die Komplexität von Zufallsgesetzen und der Zufallsgrad von Folgen

In diesem Kapitel definieren wir Klassen von Folgen, die sich in ihrem Verhalten demjenigen idealer Zufallsfolgen beliebig gut annähern.

(3.1) **Definition.** Ein Fastüberallgesetz (FÜG) ist von der (Zeit- bzw. Raum-) Komplexität T, wenn es zu der zugehörigen Nullmenge $\mathfrak{N} \subset X^\infty$ eine rekursive Testfunktion $F: X^* \to Z(2)$ mit $F \in C_T^\mu(TF)$ gibt, so daß $\mathfrak{N} \subset \mathfrak{N}_F$.

(3.2) **Definition.** Es sei C_T^μ eine Komplexitätsklasse, dann ist $[T]_\mu = X^\infty - \bigcup_{F \in C_T^\mu(TF)} \mathfrak{N}_F$ die zu C_T^μ gehörige Komplexitätsklasse von Zufallsfolgen.

Wir sagen, daß die Folgen in $[T]_\mu$ den Zufallsgrad T (bzgl. des Zeit- bzw. Raummaßes) haben. Da z genau dann in $[T]_\mu$ liegt, wenn z alle Zufallstests besteht, die in (Raum- bzw. Zeit-) Komplexität T nicht übersteigen, approximiert eine Folge z das ideale Zufallsverhalten um so besser je höher ihr Zufallsgrad ist. Eine Folge, die jeden Zufallsgrad besitzt, ist gerade eine ideale Zufallsfolge.

(3.3) **Korollar.** *In $[T]_\mu$ gibt es berechenbare Folgen.*

Beweis. Nach Standardmethoden [4] beweist man, daß $C_T^\mu(TF)$ rekursiv aufzählbar ist. Dann gibt es nach (6.2) [10] eine T-Funktion F, so daß $\mathfrak{N}_{F_i} \subset \mathfrak{N}_F$

für alle $F_i \in C_T^\mu(TF)$. Es genügt somit, eine Folge zu berechnen, die nicht in $\mathfrak{N}_F$ liegt. Dies ist nach Satz (6.1) [10] möglich.

Weiterhin folgt, daß die Komplexitätsteinteilung der Zufallsgesetze nicht trivial ist.

(3.4) **Korollar.** *Zu T gibt es FÜG'e, die nicht von der (Raum- bzw. Zeit-) Komplexität T sind.*

Beweis. Wähle die T-Funktion F so, daß $\mathfrak{N}_F \cap [T]_\mu \neq \emptyset$. Dann gilt $\mathfrak{N}_F \not\subset \mathfrak{N}_{F_i}$ für alle $F_i \in C_T^\mu(TF)$.

Mit dem gleichen Argument wie für die Komplexitätsklassen von Folgen kann man auch für die Komplexitätsklassen von Zufallsfolgen die Nicht-Entscheidbarkeit nachweisen (s. [4]).

(3.5) **Korollar.** *Es gibt keinen Algorithmus, der zu einer rekursiven Folge $z \in X^\infty$ entscheidet, ob $z \in [T]_\mu$.*

(3.6) **Satz.** *Zu einem FÜG der (Zeit- bzw. Raum-) Komplexität T gibt es stets eine Folge $z \in C_T^\mu(Fo)$, die dieses Gesetz erfüllt.*

Beweis. Sei $F\colon X^* \to Z(2)$ eine T-Funktion in $C_T^\mu(TF)$, die das betrachtete FÜG repräsentiert. $z = z_1 \dots z_i \dots \in X^\infty$ konstruiere man rekursiv wie im Beweis zu (6.1) [10], so daß

$$F(z_1 \dots z_{i+1}) \leqq F(z_1 \dots z_i\, \alpha) \qquad (\alpha \in X).$$

Dann erfüllt z den Test F. Zur Berechnung von z_{i+1} muß man im wesentlichen $F(z_1 \dots z_i\, \alpha)$ für alle $\alpha \in X$ berechnen. Weil der Aufwand an Zeit bzw. Raum nur bis auf einen konstanten Faktor in die Komplexitätsklassen eingeht, liegt z in derselben Komplexitätsklasse wie F, also in $C_T^\mu(Fo)$. Man kann dies auch unmittelbar aus den in [12] betrachteten Abschlußeigenschaften von C_T^μ folgern.

Obiger Satz läßt sich umkehren.

(3.7) **Satz.** *Sei $z \in C_T^\mu(Fo)$, dann gibt es eine T-Funktion $F \in C_T^\mu(TF)$ mit $z \in \mathfrak{N}_F$.*

Beweis. Wir definieren $F(z(n)) = 2^n$ und $F(x) = 0$, falls $z(|x|) \neq x$. Mit dem gleichen Argument wie zu (3.6) folgt $F \in C_T^\mu(TF)$.

(3.8) **Lemma.** *Wenn $\mathfrak{N}_1$ und $\mathfrak{N}_2$ Nullmengen von der (Raum- bzw. Zeit-) Komplexität T sind, dann ist auch $\mathfrak{N}_1 \cup \mathfrak{N}_2$ von dieser Komplexität.*

Beweis. Aus $F_i \in C_T^\mu(TF)$ $(i = 1, 2)$ folgt $F_1 + F_2 \in C_T^\mu(TF)$.

(3.9) **Satz.** *Es gibt keine maximale Nullmenge von der (Raum- bzw. Zeit-) Komplexität T.*

Beweis. Angenommen $\mathfrak{N}$ sei eine maximale Nullmenge von der (Raum- bzw. Zeit-) Komplexität T. Dann gibt es nach (3.6) eine Folge $z \in C_T^\mu(Fo)$ mit $z \notin \mathfrak{N}$. Zu z gibt es nach (3.7) eine Nullmenge $\overline{\mathfrak{N}}$ von der (Raum- bzw. Zeit-) Komplexität T mit $z \in \overline{\mathfrak{N}}$. Nach (3.8) ist $\mathfrak{N} \cup \overline{\mathfrak{N}}$ ebenfalls von der (Raum- bzw. Zeit-) Komplexität T, im Widerspruch zur Annahme.

Sei $\mathfrak{K}$ eine Klasse effektiver Zufallstests, dann heißt ein Test F universell für $\mathfrak{K}$, wenn für alle $F_i \in \mathfrak{K}$ die Inklusion $\mathfrak{N}_{F_i} \subset \mathfrak{N}_F$ gilt. Innerhalb von $C_F^\mu(TF)$ gibt es nach (3.9) keinen universellen Test zu $C_T^\mu(TF)$. Dagegen gibt es, wie wir bereits wissen, universelle Tests höherer Komplexität zu $C_T^\mu(TF)$. Wir geben eine Abschätzung für die Komplexität solcher universeller Tests.

(3.10) **Satz.** *Es seien C_T^μ, C_S^μ Komplexitätsklassen. f, h: $N \to N$ seien monoton wachsende, unbeschränkte Funktionen in $C_S^\mu(Fu)$ so, daß für $f(n) \geqq i$, $K \leqq h(i)$, $i \in N$ Folgendes gilt:*

$$K^2\, T(K+n)^2 \leqq 2^{-i}\, S(n) \quad \textit{im Falle } \mu=0,$$

$$K T(K+n) \leqq 2^{-i}\, S(n) \quad \textit{im Falle } \mu=1.$$

Dann gibt es in $C_S^\mu(TF)$ eine universelle T-Funktion zu $C_T^\mu(TF)$.

Die obige Bedingung über T und S besagt im wesentlichen, daß die Folgen $KT(n+K)\, S(n)^{-1}$ bzw. $K^2\, T(n+K)^2\, S(n)^{-1}$ für jedes feste $K \in N$ mit wachsendem n konstruktiv und in einer einfachen Abhängigkeit von n und K gegen null konvergieren.

Beweis. Da ähnliche Konstruktionen bereits ausführlich behandelt wurden [4], beschränken wir uns auf eine Beweisskizze. Es gibt eine rekursive Aufzählung (M_i, K_i) $(i \in N)$ aller TM'en M_i, welche eine T-Funktion F_i derart berechnet, daß $R_i^\mu(x) \leqq K_i\, T(K_i + |x|)$ für alle $x \in X^*$ gilt und daß $K_i \leqq h(i)$. Dabei durchlaufe F_i alle T-Funktionen in $C_T^\mu(TF)$.

Sei nun $s \in N$ so gewählt, daß $2^{-s} < p^{-1}$. Wir setzen:

$$F(x) = \sum_{i=1}^{f(|x|)} F_i(x)\, 2^{-2si} + 2^{-sf(|x|)}.$$

Weil f monoton und unbeschränkt wächst, ist F eine universelle Testfunktion zu $C_T^\mu(TF)$ (vgl. den Beweis zu (6.2) [10]). Nach Konstruktion ist M_i mit $i \leqq f(n)$ eine TM, die F_i für alle x mit $f(|x|) \geqq i$ mit einem Aufwand $R_i^0(x)^2 \leqq 2^{-i}\, S(|x|)$ bzw. $R_i^1(x) \leqq 2^{-i}\, S(|x|)$ berechnet. O.B.d.A. kann man annehmen, daß es eine feste TM gibt, die jede der TM'en M_i derart simulieren kann, daß dabei der Zeitaufwand durch $i\, R_i^0(x)^2$, bzw. der Raumaufwand durch $i\, R_i^1(x)$ beschränkt ist. Da der Aufwand für die Additionen, zur Berechnung des Gliedes $2^{-sf(|x|)}$, sowie zum Aufzählen der Folge (M_i, K_i) vernachlässigbar ist, kann man F mit dem (Zeit- bzw. Raum-) Aufwand $R^\mu(x) \leqq C \sum_{i=1}^{f(|x|)} i\, 2^{-i}\, S(|x|)$ berechnen, wobei C eine feste Konstante ist. Also gilt jeweils $F \in C_S^\mu(TF)$.

Aus (3.6) ergibt sich nun sofort folgendes Korollar.

(3.11) **Korollar.** *Es seien T, S, h, f wie in* (3.10). *Dann gibt es eine Folge $z \in [T]_\mu$ mit $z \in C_S^\mu(Fo)$.*

In die (Raum- bzw. Zeit-) Komplexität einer Folge $z \in [T]_\mu$, welche man nach obigem Konstruktionsverfahren erhält, geht im wesentlichen nur der (Raum- bzw. Zeit-) Aufwand ein, mit dem man zu festem X und Y die Berechnung einer jeden Funktion h: $X^* \to Y^*$ in C_T^μ durch eine feste TM simulieren kann. Der dadurch bedingte (Raum- bzw. Zeit-) Aufwand ist aber im Prinzip bereits notwendig, wenn man eine Folge $z \notin C_T^\mu(Fo)$ nach der Cantorschen Diagonalisierungstechnik konstruiert. Damit ist die Aufgabe, eine Folge z vom vorgegebenen

Zufallsgrad T zu konstruieren nicht wesentlich aufwendiger als die darin enthaltene Aufgabe, eine Folge zu konstruieren, deren Komplexität T übersteigt. Diese Folgerung gilt auch, wenn man statt des in Kapitel 2 beschriebenen Modells der TM wie Hartmanis und Stearns [4] ein Modell ohne Sprungbefehle zugrunde legt.

Wir zeigen nun, daß das starke Gesetz der großen Zahlen von geringer Zeit- und Raum-Komplexität ist. Tatsächlich genügen jeweils die Folgen mit dem niedrigsten von uns betrachteten Zufallsgrad (bzgl. des Raum- bzw. Zeitmaßes) bereits diesem Gesetz. Zu $\alpha \in X$ und $x_1 x_2 \ldots x_n \in X^*$ bezeichne $s_\alpha(x_1 \ldots x_n) = \sum_{x_i=\alpha} |x_i|$.

(3.12) **Satz.** (a) *Zeitmaß:* $T(n) \geqq n^2$ *impliziert* $\lim_n s_\alpha(z(n))\, n^{-1} = p^{-1}$ *für alle* $z \in [T]_0$, $\alpha \in X$.

(b) *Raummaß:* $T(n) \geqq n$ *impliziert* $\lim_n s_\alpha(z(n))\, n^{-1} = p^{-1}$ *für alle* $z \in [T]_1$, $\alpha \in X$.

Beweis. Wir benutzen die in (4.5) [11] gegebene Darstellung des starken Gesetzes der großen Zahlen. Sei q rational und $-1 < q < 1$ ferner $\alpha \in X$. Die Testfunktion $F_{q,\alpha}$ wird wie folgt definiert:

$$F_{q,\alpha}(\Lambda) = 1,$$

$$F_{q,\alpha}(x\,\beta) = \begin{cases} F_{q,\alpha}(x)\,(1+q) & \text{falls } \alpha = \beta, \\ F_{q,\alpha}(x)\,(1-q(p-1)^{-1}) & \text{sonst.} \end{cases}$$

Es sei $A \subset [-1, 1]$ eine Menge rationaler Zahlen, so daß sowohl $A \cap [-1, 0]$ als auch $A \cap [0, 1]$ in 0 einen Häufungspunkt hat. Aus dem Beweis zu Satz (4.5) [11] folgt dann:

$\lim_n s_\alpha(z(n))\, n^{-1} = p^{-1}$ gilt genau dann, wenn z alle Tests $F_{q,\alpha}$ mit $q \in A$ besteht.

Nun setzen wir z.B. für A die folgende Menge von Binärzahlen:

$$\{\pm(p-1)\, 2^{-n} | n \in N\}.$$

Dann ist für $q \in A$ $F_{q,\alpha}$: $X^* \to Z(2)$ eine rekursive Funktion. Aus elementaren Abschätzungen (oder aus den in [12] behandelten Abschlußeigenschaften der Komplexitätsklassen) schließt man, daß $F_{q,\alpha} \in C_T^\mu(TF)$ für alle $q \in A$, $\alpha \in X$, sofern nur C_T^μ gemäß unseren Vereinbarungen definiert ist. Hieraus folgt (3.12).

Der obige Satz läßt sich von Elementen aus X auf beliebige Folgen in X^* übertragen. Es seien $x, w \in X^*$ und $|w| = k$. Zu $j < k$ definieren wir:

$$s_{w,j}(x) = \left| \left\{ i \in N \,\middle|\, \begin{matrix} 0 \leqq j + i\,k \leqq |x| - k \\ x \in x(j+i\,k)\, w\, X^* \end{matrix} \right\} \right|.$$

Dies ist die Anzahl mit der w als Teilwort in x vorkommt unter der Nebenbedingung, daß die Länge der vor w stehenden Anfangsfolge in x durch die Länge von w dividiert den Rest j ergibt.

$$s_w(x) \underset{\text{def}}{=} \sum_{j=0}^{k-1} s_{w,j}(x)$$

gibt gerade die Anzahl an, mit der w als Teilwort in x auftritt. Zu rationalem q mit $-1 < q < 1$ definieren wir die Testfunktion $F_{q,w,j}$ wie folgt:

Für $|x|=|w|\,n+j$ mit $n\in N$ definiert man

$$F_{q,w,j}(x)=(1+q)^{s_{w,j}(x)}\left(1-q(p^{|w|}-1)^{-1}\right)^{n-s_{w,j}(x)}.$$

Man verifiziert für $|x|=|w|\,n+j$:

$$F_{q,w,j}(x)=p^{-|w|}\sum_{|v|=|w|}F_{q,w,j}(x\,v).$$

Somit kann man die Definition der Testfunktion $F_{q,w,j}$ durch die Forderung $p\,F_{q,w,j}(y)=\sum_{\alpha\in X}F_{q,w,j}(y\,\alpha)$ für alle $y\in X^*$ vervollständigen.

Sei nun $A\subset[-1,1]$ wieder eine Menge von rationalen Zahlen mit der Eigenschaft, daß $A\cap[-1,0]$ und $A\cap[0,1]$ in 0 einen Häufungspunkt haben. In völliger Analogie zu (4.5) [11] beweist man:

Es gilt genau dann $\lim_n s_{w,j}(z(n))\,n^{-1}=p^{-|w|}\,|w|^{-1}$, wenn z für alle $q\in A$ den Test $F_{q,w,j}$ besteht.

Nun setzt man für A die folgende Menge von Binärzahlen:

$$\{\pm(p^{|w|}-1)\,2^{-n}|n\in N\}.$$

Nun folgt wieder, daß für alle $q\in A$, $w\in X^*$ und $j<|w|$, $F_{q,w,j}$ in $C_T^\mu(TF)$ liegt, sofern nur C_T^μ gemäß unseren Vereinbarungen erklärt ist. Demnach gilt folgendes Korollar:

(3.13) **Korollar.** (a) *Zeitmaß: $T(n)\geqq n^2$ impliziert $\lim_n s_w(z(n))\,n^{-1}=p^{-|w|}$ für alle $z\in[T]_0$ und $w\in X^*$.*

(b) *Raummaß: $T(n)\geqq n$ impliziert $\lim_n s_w(z(n))\,n^{-1}=p^{-|w|}$ für alle $z\in[T]_1$ und $w\in X^*$.*

Zum Abschluß des Kapitels weisen wir noch daraufhin, daß in den Begriff des Zufallsgrads einer Folge die beiden dualen Auffassungen der Komplexität von Folgen eingehen. Die Programmkomplexität der endlichen Abschnitte der Folge gehen, wie in Kapitel 1 [11] gezeigt wurde, implizit über die Struktur der Testfunktion in diesen Begriff ein. Andererseits haben wir in diesem Kapitel enge Beziehungen zwischen der (Raum- bzw. Zeit-) Komplexität von Folgen und ihrem Zufallsgrad nachgewiesen.

4. Abschlußeigenschaften der Komplexitätsklassen von Zufallszahlen

Zunächst formulieren wir eine Untermenge der konstruktiven, maßinvarianten Transformationen und zeigen dann, daß alle Transformationen dieser Klasse nicht aus den Komplexitätsklassen $[T]_\mu$ von Zufallszahlen hinausführen, sofern nur die Komplexität dieser Transformationen durch T beschränkt ist.

(4.1) **Definition.** Eine Funktion $\bar{Q}$: $X^*\to X^*$, die eine konstruktive Transformation Q: $X^\infty\to X^\infty$ erzeugt, heißt eine permutierte Stellenauswahl, wenn für jedes $x\in X^*$ entweder (a) oder (b) erfüllt ist.

(a) $\bar{Q}(x\,\alpha)=\bar{Q}(x)$ für alle $\alpha\in X$,

(b) $\{\bar{Q}(x\,\beta), \beta\in X\}=\{\bar{Q}(x)\,\alpha, \alpha\in X\}$.

Man verifiziert leicht, daß eine permutierte Stellenauswahl $\bar{Q}$ mit $\bar{Q}(\Lambda)=\Lambda$ eine maßinvariante Transformation Q: $X^\infty \to X^\infty$ erzeugt. Beispiele permutierter Stellenauswahlen werden durch die Auswahlregeln im v. Misesschen Sinne erzeugt. Sei nämlich f: $X^* \to \{0,1\}$ eine rekursive Funktion. Dann wird durch

$$\bar{Q}(\Lambda)=\Lambda,$$
$$\bar{Q}(x\alpha)=\begin{cases}\bar{Q}(x)\,\alpha & \text{falls } f(x)=1,\\ \bar{Q}(x) & \text{sonst},\end{cases}$$

eine permutierte Stellenauswahl $\bar{Q}$ erzeugt, sofern nur $|\bar{Q}(z(n))|$ für alle $z\in X^\infty$ mit n unbeschränkt wächst. Ferner folgt aus $f\in C_T^\mu$, daß auch $\bar{Q}$ in C_T^μ liegt.

(4.2) **Satz.** *Sei $\bar{Q}$: $X^* \to X^*$ eine permutierte Stellenauswahl mit $\bar{Q}\in C_T^\mu$, dann gilt: $Q([T]_\mu)\subset[T]_\mu$.*

Beweis. Sei F: $X^* \to Z(2)$ eine T-Funktion mit $F\in C_T^\mu(TF)$. Es genügt eine T-Funktion $\bar{F}\in C_T^\mu(TF)$ zu konstruieren, so daß

(1) $$Q^{-1}(\mathfrak{N}_F)\subset\mathfrak{N}_{\bar{F}}$$

erfüllt ist. Hierzu definieren wir:

$$\bar{F}(x)=F\bar{Q}(x) \qquad (x\in X^*).$$

Weil $\bar{Q}$ eine permutierte Stellenauswahl ist, folgt daß mit F auch $\bar{F}$ die Funktionaleigenschaft einer T-Funktion erfüllt. Berücksichtigt man die Eigenschaft $\bar{Q}(x\alpha)\in\bar{Q}(x)\ (X\cup\Lambda)$ für $x\in X^*$, $\alpha\in X$, dann folgt aus $F\in C_T^\mu(TF)$ und $\bar{Q}\in C_T^\mu$, daß auch $\bar{F}$ in der Komplexitätsklasse $C_T^\mu(TF)$ liegt.

Um nun (1) zu beweisen, benutzen wir, daß es eine rekursive Funktion h: $N\to N$ gibt, so daß $|\bar{Q}(x)|\geqq n$ für alle x mit $|x|\geqq h(n)$. Sei nun $z\in\mathfrak{N}_F$; es ist zu zeigen $Q^{-1}(z)\in\mathfrak{N}_{\bar{F}}$. Wegen $\overline{\lim_n}\, F(z(n))=\infty$ gibt es eine rekursive Funktion g: $N\to N$ und eine unendliche Menge $M\subset N$ so, daß es zu $n\in M$ stets ein $i\leqq g(n)$ gibt mit $F(z(i))\geqq n$. Dann gilt aber für die rekursive Funktion $f=h\circ g$: zu $\bar{z}\in Q^{-1}(z)$ und $n\in M$ gibt es stets ein $i\leqq f(n)$ mit $\bar{F}(\bar{z}(i))\geqq n$. Daraus folgt $\overline{\lim_n}\, \bar{F}(\bar{z}(n))=\infty$ für alle $\bar{z}\in Q^{-1}(z)$ und (1) ist somit bewiesen.

Aus (4.2) folgert man unmittelbar:

(4.3) **Korollar.** *Wenn sich zwei Folgen $z_1, z_2\in X^\infty$ nur in endlich vielen Gliedern unterscheiden, dann gilt stets: $z_1\in[T]_\mu \Leftrightarrow z_2\in[T]_\mu$.*

Ferner ist die Definition der Komplexitätsklassen gerade so gewählt, daß eine Verschiebung von Folgen ihre Komplexität als auch ihren Zufallsgrad nicht ändert.

(4.4) **Korollar.** *Wenn für $x\in X^*$ und $y, z\in X^\infty$ die Relation $xy=z$ gilt, dann folgt: $y\in[T]_\mu \Leftrightarrow z\in[T]_\mu$.*

Nun betrachten wir Abschlußeigenschaften der Komplemente der Komplexitätsklassen von Zufallszahlen. Man übersieht leicht, daß die Abschlußeigenschaft von (4.2) für $X^\infty-[T]_\mu$ nicht gilt. Dagegen ergibt sich aus dem Beweis zu (4.2) gerade, daß die Komplemente der Komplexitätsklassen von Zufallszahlen gegenüber der Umkehrung von permutierten Stellenauswahlen abgeschlossen sind.

(4.5) **Korollar.** *Es sei* $\bar{Q}$: $X^* \to X^*$ *eine permutierte Stellenauswahl mit* $\bar{Q} \in C_T^\mu$, *dann gilt:* $Q^{-1}(X^\infty - [T]_\mu) \subset X^\infty - [T]_\mu$.

Für unendliche Folgen $z \in X^\infty$ weiß man, daß die Komplexität von z wesentlich von einer unendlichen Teilmenge der Glieder von z bestimmt sein kann, welche beliebig dünn im Verhältnis zur Menge aller Glieder von z ist. Denn sei $M \subset N$ eine entscheidbare Menge, dann kann man jede rekursive Folge $z \in X^\infty$ durch Abänderung der Glieder z_i mit $i \in M$ beliebig kompliziert machen. Wir zeigen nun, daß man den Zufallsgrad einer Folge z im allgemeinen nicht dadurch erhöhen kann, daß man eine beliebig dünne Teilmenge der Glieder von z abändert.

(4.6) **Satz.** *Es sei* C_T^μ *eine Komplexitätsklasse und* $z \in C_T^\mu(Fo)$. *Ferner sei* g: $N \to N$ *eine streng monoton wachsende Funktion in* $C_T^\mu(Fu)$ *mit* $\lim_n (g(n) - n) = \infty$. *Dann gehören alle Folgen, die sich von* z *nur in Gliedern* z_i *mit* $i \in g(N)$ *unterscheiden zu* $X^\infty - [T]_\mu$.

Beweis. Für zwei Folgen $x, y \in X^*$ gleicher Länge schreiben $x = y \bmod g$ genau dann, wenn sich x und y nur in Gliedern unterscheiden, deren Index in $g(N)$ liegt.

Durch elementare Abschätzung überzeugt man sich, daß folgende Funktionen von der (Raum- bzw. Zeit-) Komplexität T sind. Wegen $g \in C_T^\mu(Fu)$ ist auch die Funktion f: $N \to N$, die durch

$$f(n) = \begin{cases} 0 & \text{falls } n \in g(N), \\ 1 & \text{sonst}, \end{cases}$$

definiert wird, in $C_T^\mu(Fu)$. Ferner ist wegen $z \in C_T^\mu(Fo)$ die Funktion h: $X^* \to \{0, 1\}$, die durch

$$h(x) = \begin{cases} 0 & \text{falls } x = z(|x|) \bmod g, \\ 1 & \text{sonst}, \end{cases}$$

definiert wird, in der Komplexitätsklasse C_T^μ.

Nun definieren wir die T-Funktion F: $X^* \to Z(2)$:

$$F(\Lambda) = 1,$$

$$F(x\alpha) = \begin{cases} F(x) & \text{falls } f(|x\alpha|) = 0, \\ F(x)2 & \text{falls } f(|x\alpha|) = 1 \quad \text{und} \quad h(x\alpha) = 0, \\ 0 & \text{sonst}. \end{cases}$$

F ist eine T-Funktion in $C_T^\mu(TF)$. Es bleibt zu zeigen, daß alle Folgen in X^∞, die sich von z nur in Gliedern z_i mit $i \in g(N)$ unterscheiden, in $\mathfrak{N}_F$ liegen.

Wegen $\lim_n (g(n) - n) = \infty$ und weil g eine streng monotone, rekursive Funktion ist, gibt es eine rekursive Funktion d: $N \to N$, so daß für $i \geqq d(n)$ stets $g(i) - i \geqq n$ gilt. Wenn sich $y, z \in X^\infty$ nur in Gliedern y_k mit $k \in g(N)$ unterscheiden, dann gilt nach Konstruktion für $i \geqq d(n)$ die Relation $F(y(g(i))) \geqq 2^n$. Dies impliziert aber $\overline{\lim_n} F(y(n)) = \infty$.

5. Die Ordnung eines Fastüberallgesetzes

Wir gehen von der Vorstellung aus, daß die Bedeutung eines Fastüberallgesetzes für die Anwendung dann sehr groß ist, wenn die Eigenschaften von unendlichen Folgen, die das Gesetz beinhaltet, im Mittel bereits an kurzen Folgen sichtbar werden. Dies ist, wie wir noch sehen werden, beim starken Gesetz der sehr großen Zahlen der Fall. Dagegen erfaßt das Gesetz vom iterierten Logarithmus u.a. auch solche Eigenschaften von Folgen, die sich im allgemeinen erst an längeren Folgen bemerkbar machen. Diese intuitive Vorstellung von der Bedeutung eines Fastüberallgesetzes wollen wir nun durch den Begriff der Ordnung präzisieren. Kleinen Nullmengen, wie derjenigen vom starken Gesetz der großen Zahlen, kommt dabei eine hohe Ordnung zu.

Eine positive, monoton wachsende, berechenbare Funktion $G: N \to R^+$ heißt im folgenden *Ordnungsfunktion*. Zu einer T-Funktion F und einer Ordnungsfunktion G bezeichnen wir

$$\mathfrak{N}_{F,G} = \{z \in X^\infty \mid \overline{\lim_n}\, F(z(n))\, G(n)^{-1} > 0\}.$$

(5.1) **Definition.** Eine T-Nullmenge $\mathfrak{N} \subset X^\infty$ heißt von der Ordnung G, wenn es eine T-Funktion F gibt mit $\mathfrak{N} \subset \mathfrak{N}_{F,G}$.

Damit $\mathfrak{N}_{F,G}$ ungleich der leeren Menge sein kann, setzen wir im folgenden stets voraus, daß $G(n+1) \leqq G(n)\, p$.

Wenn die Ordnungsfunktion G beschränkt ist, dann ist jede T-Nullmenge von der Ordnung G. Die folgenden Korollare ergeben sich sofort aus den Definitionen.

(5.2) **Korollar.** *Ist $\mathfrak{N}$ von der Ordnung G und $\overline{\mathfrak{N}} \subset \mathfrak{N}$, dann ist auch $\overline{\mathfrak{N}}$ von der Ordnung G.*

(5.3) **Korollar.** *Wenn für die Ordnungsfunktionen G und $\bar{G}$ die Folge $G(n)\, \bar{G}(n)^{-1}$ mit wachsendem n beschränkt ist, dann ist jede Nullmenge von der Ordnung $\bar{G}$ auch von der Ordnung G.*

Der Begriff der Ordnung eignet sich nicht dazu, berechenbare Folgen nach ihrem Zufallsverhalten zu klassifizieren.

(5.4) **Korollar.** *Sei $z \in X^\infty$ eine rekursive Folge und G eine Ordnungsfunktion. Dann gibt es eine T-Nullmenge $\mathfrak{N}$ der Ordnung G mit $z \in \mathfrak{N}$.*

Beweis. Man definiert $F(z(n)) = p^n$ und $F(x) = 0$ sonst. Dann gilt $z \in \mathfrak{N}_{F,G}$ für jede Ordnungsfunktion G mit $G(n+1) \leqq G(n)\, p$.

(5.5) **Korollar.** *Wenn $\mathfrak{N}_i$ $(i \in N)$ eine rekursiv aufzählbare Folge von Nullmengen der Ordnung G ist, dann ist auch $\bigcup_{i \in N} \mathfrak{N}_i$ von der Ordnung G.*

Beweis. Es sei F_i $(i \in N)$ eine r.a. Folge von T-Funktionen mit $\mathfrak{N}_i \subset \mathfrak{N}_{F_i,G}$. Durch $F(x) = \sum_{i=1}^{|x|} F_i(x)\, p^{-2i} + p^{-|x|}$ wird dann eine T-Funktion definiert, so daß $\bigcup_{i \in N} \mathfrak{N}_i \subset \mathfrak{N}_{F,G}$.

Weil im Komplement einer T-Nullmenge stets rekursive Folgen enthalten sind, folgt aus (5.4) und (5.5):

(5.6) **Korollar.** *Es gibt keine maximale T-Nullmenge zu einer vorgegebenen Ordnung.*

Als erstes zeigen wir nun, daß die Nullmengen i. S. von Brouwer unter allen T-Nullmengen durch ihre Ordnung ausgezeichnet sind.

(5.7) **Satz.** *Eine T-Nullmenge $\mathfrak{N}$ ist genau dann eine Nullmenge i.S. von Brouwer, wenn es eine unbeschränkte Ordnungsfunktion G gibt, so daß $\mathfrak{N}$ von der Ordnung G ist.*

Beweis. Es sei G eine unbeschränkte Ordnungsfunktion und F eine T-Funktion. Wie im Beweis zu (5.2) [10] gezeigt wurde, ist dann $\mathfrak{N}_{F,G}$ eine Nullmenge i.S. von Brouwer. Sei nun umgekehrt $\mathfrak{N}$ Nullmenge i.S. von Brouwer. Im Beweis zu (5.4) in [10] haben wir zu $\mathfrak{N}$ gerade eine T-Funktion $\bar{F}$ und eine rekursive, monoton wachsende, unbeschränkte Funktion $f\colon N\to N$ konstruiert, so daß für alle $z\in\mathfrak{N}$: $\overline{\lim_n}\, \bar{F}(z(n))\, f(n)^{-1}>0$. Daraus folgt: $\mathfrak{N}\subset\mathfrak{N}_{\bar{F},f}$.

Wir wenden uns nun der Frage zu, wie fein die Einteilung der Fastüberallgesetze nach ihrer Ordnung ist.

(5.8) **Satz.** *Es seien G und $\bar{G}$ Ordnungsfunktionen, so daß $G(n)\,\bar{G}(n)^{-1}$ mit n konstruktiv gegen null konvergiert. Dann gibt es eine Nullmenge der Ordnung G, die nicht von der Ordnung $\bar{G}$ ist.*

Beweis. Es gibt eine rekursive Ordnungsfunktion $\tilde{G}$, die als Werte nur ganzzahlige Potenzen von p annimmt und für die sowohl $\tilde{G}(n)\,\bar{G}(n)^{-1}$ als auch $G(n)\,\tilde{G}(n)^{-1}$ mit n konstruktiv gegen null konvergiert. Um eine solche Funktion $\tilde{G}$ zu gewinnen, konstruiere man zunächst eine rekursive, monoton wachsende Funktion $G_0\colon N\to Z(2)$, so daß die Folge $|G_0(n)-\sqrt{G(n)\,\bar{G}(n)}|$ mit wachsendem n beschränkt ist und definiere dann $\tilde{G}(n)=\max\{p^i|p^i\leqq G_0(n)\}$.

O.B.d.A. können wir annehmen, daß $\tilde{G}(0)=1$ und daß $\tilde{G}$ alle Potenzen p^n $(n\in N)$ als Werte annimmt. Die rekursive Funktion $h\colon N\to N$ werde definiert durch: $h(n)=\min\{m|\tilde{G}(m)=p^n\}$.

Nun konstruieren wir eine T-Funktion F, so daß F auf den Folgen der Länge $h(n)$ nur die Werte 0 und $p^n=\tilde{G}\,h(n)$ annimmt und so, daß F die Gleichung $p\,F(x)=\sum_{\alpha\in X}F(x\,\alpha)$ erfüllt. $\delta\in X$ sei dabei ein festes Element.

Für $|x|<h(1)$ gelte $F(x)=1$. Dann definieren wir F rekursiv. Es sei $x\in X^{h(n)}$ und F sei bereits für alle Folgen y mit $|y|<h(n)$ definiert:

$$F(x)\underset{\text{def}}{=}\begin{cases}p^n & \text{falls } x\in X^*\delta,\ F(x(h(n-1)))\neq 0,\\ 0 & \text{sonst}.\end{cases}$$

Weiter definieren wir für x mit $h(n)<|x|<h(n+1)$:

$$F(x)=F(x(h(n))).$$

Nach Konstruktion erfüllt F die Funktionalgleichung $p\,F(x)=\sum_{\alpha\in X}F(x\,\alpha)$. $\mathfrak{N}_{F,G}$ läßt sich folgendermaßen darstellen:

$$\mathfrak{N}_{F,G}=\{z\in X^\infty|F(z(n))=\tilde{G}(n)\text{ f.a. } n\in N\}.$$

Nun zeigen wir, daß $\mathfrak{N}_{F,G}$ nicht von der Ordnung $\bar{G}$ sein kann. Es sei $\bar{F}$ eine beliebige T-Funktion mit $\bar{F}(\Lambda)=1$. Dann kann man eine Folge $z\in X^\infty$ rekursiv so konstruieren, daß für alle $i\in N$ folgendes gilt:

(1) $$F(z(i+1))=\tilde{G}(i+1),$$

(2) $$\bar{F}(z(i+1))=\min\{\bar{F}(z(i)\,\beta)|F(z(i)\,\beta)=\tilde{G}(i+1)\}.$$

Dann folgt einerseits $z\in\mathfrak{N}_{F,G}$ und andererseits beweist man unter Ausnutzung der besonderen Struktur von F durch Induktion über i: $\bar{F}(z(i))\leqq F(z(i))$. Nach Konstruktion von F und z gilt ferner $F(z(i))=\tilde{G}(i)$. Nun folgt direkt, daß $\lim\limits_i \bar{F}(z(i))\,\bar{G}(i)^{-1}=0$ gilt. Damit liegt z nicht in $\mathfrak{N}_{\bar{F},\bar{G}}$.

Bemerkung. Aus obigem Beweis folgt, daß man die Aussage von (5.8) noch verschärfen kann. Für die oben konstruierte Nullmenge $\mathfrak{N}_{F,G}$ der Ordnung G gilt folgendes: für jede Nullmenge $\mathfrak{N}$ der Ordnung $\bar{G}$ gibt es berechenbare Folgen in $\mathfrak{N}_{F,G}$, die nicht in $\mathfrak{N}$ liegen.

Wir verschärfen (5.8) weiter:

(5.9) **Satz.** *Es seien G und $\bar{G}$ wie in* (5.8). *Dann gibt es eine T-Nullmenge der Ordnung G, die nicht in der Vereinigung aller T-Nullmengen der Ordnung $\bar{G}$ enthalten ist.*

Beweis. Wegen (5.4) ist klar, daß es keine rekursive Folge in einer T-Nullmenge der Ordnung G geben kann, die nicht in der Vereinigung aller T-Nullmengen der Ordnung $\bar{G}$ enthalten ist. (5.9) ist daher als Aussage i.S. der Mengenlehre mit Auswahlaxiom zu verstehen. Zum Beweis des Satzes gehen wir von einer Aufzählung F_i ($i\in N$) aller T-Funktionen aus. Eine solche Aufzählung existiert, sie ist aber nicht rekursiv. Man definiert analog zum Beweis von (6.2) [10]:

$$\bar{F}(x)=\sum_{i=1}^{|x|} F_i(x)\,p^{-2i}+p^{-|x|}.$$

Dann erfüllt $\bar{F}$ die Funktionalgleichung $p\,\bar{F}(x)\geqq\sum\limits_{\alpha\in X}\bar{F}(x\,\alpha)$. Die erzeugte Nullmenge

$$\mathfrak{N}_{\bar{F},\bar{G}}=\{z\in X^\infty\,|\,\overline{\lim_n}\,\bar{F}(z(n))\,\bar{G}(n)^{-1}>0\}$$

umfaßt alle T-Nullmengen der Ordnung $\bar{G}$, ist jedoch selbst keine T-Nullmenge. Sei nun $\mathfrak{N}_{F,G}$ die im Beweis zu (5.8) konstruierte Nullmenge der Ordnung G. Dann kann man ebenso wie dort ein $z\in X^\infty$ induktiv derart definieren, daß für alle $i\in N$ folgendes gilt:

(1) $$F(z(i+1))=\tilde{G}(i+1),$$

(2) $$\bar{F}(z(i+1))=\min\{\bar{F}(z(i)\,\beta)|F(z(i)\,\beta)=\tilde{G}(i+1)\}.$$

($\tilde{G}$ sei dabei wie im Beweis zu (5.8) definiert.) Mit der gleichen Argumentation wie im Beweis zu (5.8) folgt dann $z\in\mathfrak{N}_{F,G}$ und $z\notin\mathfrak{N}_{\bar{F},\bar{G}}$. Im Unterschied zum Beweis zu (5.8) ist z jedoch nicht rekursiv, denn $\bar{F}$ ist nicht berechenbar.

6. Eine Charakterisierung der Zufallsgesetze von exponentieller Ordnung

Wollte man die Zufallsgesetze nach ihrer Bedeutung klassifizieren, so würde man sicher den Gesetzen über die relative Grenzhäufigkeit von Ereignissen, insbesondere dem starken Gesetz der großen Zahlen, mit die größte Bedeutung beimessen. Alle statistischen Tests, denen Pseudozufallszahlen im allgemeinen unterworfen werden, entsprechen solchen Gesetzen. V. Mises glaubte sogar bei der Axiomatisierung des Kollektivs auf Zufallsgesetze anderer Art überhaupt verzichten zu können. Es erscheint uns deshalb als eine Bestätigung unserer Theorie, daß, wie wir in diesem Kapitel zeigen werden, ein enger Zusammenhang zwischen den Zufallsgesetzen von exponentieller Ordnung und den Gesetzen über die Grenzhäufigkeit von Ereignissen besteht. Die Folgen, welche alle Zufallsgesetze von exponentieller Ordnung erfüllen, lassen sich durch eine Modifikation der Axiome des v. Misesschen Kollektivs charakterisieren.

Wir sagen, eine Nullmenge $\mathfrak{N}$ ist von *exponentieller Ordnung*, wenn es eine T-Funktion F und ein $k \in N$ gibt, derart daß

$$\mathfrak{N} \subset \{z \in X^\infty \mid \overline{\lim_n}\, F(z(n))\, e^{-nk^{-1}} = \infty\}.$$

Zunächst leiten wir eine spieltheoretische Darstellung der Zufallsgesetze von exponentieller Ordnung her. Wir knüpfen dabei an das Spielmodell (in naivem Sinne) an, das in Kapitel 2 [11] erläutert wurde.

Es sei $X = \{x_1, x_2, \dots, x_p\}$. Zu $x_i \in X$ sei B_i: $X^* \to R^+$ eine berechenbare beschränkte Funktion. Sei $z \in X^\infty$ eine Zufallsfolge. Dann setzt der Spieler in der $n+1$-ten Spielrunde, also nachdem $z(n)$ bekannt ist, den Betrag $B_i(z(n))$ auf das Ereignis $z_{n+1} = x_i$. Die Einsatzfunktionen B_i erzeugen dann zusammen mit dem Anfangsvermögen $V(\Lambda)$ eine Vermögensfunktion V: $X^* \to R$ gemäß der Formel:

$$V(z(n+1)) = \sum_{i=1}^{p} \sum_{k=0}^{n} B_i(z(k))\, \sigma_i(z_{k+1}) + V(\Lambda)$$

mit

$$\sigma_i(z_{k+1}) = \begin{cases} p-1 & \text{falls } x_i = z_{k+1} \\ -1 & \text{sonst.} \end{cases}$$

$V(z(n+1))$ ist das Vermögen nach der $n+1$-ten Spielrunde. Wir stellen an die Einsatzfunktionen keine weiteren Bedingungen, lassen also zu, daß V negative Werte annimmt. Der Gesamteinsatz $E(z_1 \dots z_n)$, den der Spieler in den ersten $n+1$ Spielrunden einsetzt, ergibt sich zu:

$$E(z(n)) = \sum_{i=1}^{p} \sum_{k=0}^{n} B_i(z(k)).$$

(6.1) **Satz.** *Eine Folge $z \in X^\infty$ erfüllt genau dann alle Fastüberallgesetze von exponentieller Ordnung, wenn in jedem Spiel über z bei dem die Einsatzfunktionen berechenbar und beschränkt sind, das Verhältnis zwischen Vermögen und Gesamteinsatz gegen null strebt, sofern nur der mittlere Einsatz pro Spielrunde nicht beliebig klein wird. Das heißt* $\underline{\lim}_n\, E(z(n))\, n^{-1} > 0$ *impliziert* $\lim_n V(z(n))\, E(z(n))^{-1} = 0.$

Der Satz drückt unter anderem aus, wie unvorteilhaft für einen auf Gewinn spielenden Spieler auf die Dauer ein Spiel über einem Zufallsgenerator ist, der lediglich alle Zufallsgesetze von exponentieller Ordnung erfüllt. Denn die Relation zwischen Vermögen und Gesamteinsatz wird für einen ständig einsetzenden Spieler mit Sicherheit immer ungünstiger. Als ersten Teil von (6.1) beweisen wir:

(6.2) **Satz.** *V bzw. E seien als Vermögensfunktionen bzw. als Gesamteinsatz von beschränkten berechenbaren Einsatzfunktionen erzeugt. Es seien $a, b>0$. Dann wird durch*

$$\mathfrak{N}(a,b)=\{z\in X^\infty \mid \underline{\lim}_n E(z(n))\,n^{-1}>a,\ \overline{\lim}_n |V(z(n))\,E(z(n))^{-1}|>b\}$$

eine T-Nullmenge von exponentieller Ordnung definiert.

Beweis. O.B.d.A. nehmen wir an, daß die Differenz der Vermögensfunktion durch $\frac{1}{2}$ beschränkt ist: $|\Delta V(x)|\leqq\frac{1}{2}$ $(x\in X^*)$. Zu einer ganzen Zahl $m\in Z$ ungleich null definieren wir eine Testfunktion $F_m\colon X^*\to R^+$ wie folgt:

$$F_m(\Lambda)=1,$$

$$F_m(x\alpha)=F_m(x)\left(1+m^{-1}\Delta V(x\alpha)\right).$$

Es gilt dann:

$$F_m(z(n))=\exp\left(\sum_{i=1}^{n}\ln\left(1+m^{-1}\Delta V(z(i))\right)\right).$$

Wir betrachten zunächst die Menge

$$\mathfrak{N}^+(a,b)\underset{\text{def}}{=}\{z\in X^\infty \mid \underline{\lim}_n E(z(n))\,n^{-1}>a,\ \overline{\lim}_n V(z(n))\,E(z(n))^{-1}>b\}.$$

Aus der Taylorentwicklung $\ln(1+x)=x-x^2/2+x^3/3-\cdots$ folgt wegen $|\Delta V(x)|\leqq\frac{1}{2}$:

$$\left|\sum_{i=0}^{n-1}\ln\left(1+m^{-1}\Delta V(z(i+1))\right)-m^{-1}\sum_{i=0}^{n-1}\Delta V(z(i+1))\right|$$

$$\leqq m^{-2}\sum_{i=0}^{n-1}\Delta V(z(i+1))^2\leqq m^{-2}\,2^{-1}\sum_{i=0}^{n-1}|\Delta V(z(i+1))|\leqq m^{-2}\,2^{-2}\,n.$$

Wählt man nun m so, daß $a\,b>m^{-1}\,2^{-2}$, dann folgt aus $z\in\mathfrak{N}^+(a,b)$, daß

$$\overline{\lim}_n\, n^{-1}\sum_{i=0}^{n-1}\ln\left(1+m^{-1}\Delta V(z(i+1))\right)\geqq m^{-1}\,\overline{\lim}_n V(z(n))\,n^{-1}-m^{-2}\,2^{-2}$$

$$\geqq m^{-1}\,\overline{\lim}_n V(z(n))\,E(z(n))^{-1}\,E(z(n))\,n^{-1}-m^{-2}\,2^{-2}$$

$$\geqq m^{-1}\,\overline{\lim}_n V(z(n))\,E(z(n))^{-1}\,\underline{\lim}_n E(z(n))\,n^{-1}-m^{-2}\,2^{-2}$$

$$\geqq m^{-1}\,a\,b-m^{-2}\,2^{-2}>0.$$

Daraus folgt, daß es ein $k\in N$ gibt so, daß

$$\overline{\lim}_n F_m(z(n))\,e^{-nk^{-1}}=\infty \qquad \text{für alle } z\in\mathfrak{N}^+(a,b).$$

Somit ist $\mathfrak{N}^+(a,b)$ von exponentieller Ordnung.

Analog zeigt man, daß es ein geeignetes negatives $\bar{m}\in Z$ und ein $\bar{k}\in N$ gibt, so daß für alle

$$z\in\mathfrak{N}^-(a,b)\underset{\text{def}}{=}\{z\in X^\infty|\underline{\lim}_n E(z(n))\,n^{-1}>a,\ \underline{\lim}_n V(z(n))\,E(z(n))^{-1}<-b\}$$

stets $\lim_n F_{\bar{m}}(z(n))\,e^{-n\bar{k}^{-1}}=\infty$ erfüllt ist.

Weil die Vereinigung zweier T-Nullmengen von exponentieller Ordnung wieder eine solche ist, folgt Satz (5.2).

Um den Beweis von (6.1) zu vervollständigen, zeigen wir nun, daß sich umgekehrt jede Nullmenge $\mathfrak{N}$ exponentieller Ordnung in eine Nullmenge der obigen Form $\mathfrak{N}(a,b)$ einbetten läßt.

(6.3) **Satz.** *Zu einer T-Nullmenge $\mathfrak{N}$ von exponentieller Ordnung gibt es stets berechenbare, beschränkte Einsatzfunktionen, sowie $a,b>0$, so daß für die erzeugte Vermögensfunktion V und den Gesamteinsatz E die folgende Inklusion gilt:*

$$\mathfrak{N}\subset\mathfrak{N}(a,b)\underset{\text{def}}{=}\{z\in X^\infty|\underline{\lim}_n E(z(n))\,n^{-1}>a,\ \overline{\lim}_n |V(z(n))\,E(z(n))^{-1}|>b\}.$$

Beweis. Sei F eine T-Funktion. Wir betrachten zu $k\in N$:

$$\mathfrak{N}_F^k\underset{\text{def}}{=}\{z\in X^\infty\,|\,\overline{\lim}_n F(z(n))\,e^{-nk^{-1}}=\infty\}.$$

Es genügt, zu zeigen, daß sich $\mathfrak{N}_F^k$ auf obige Weise einbetten läßt. Durch $\bar{F}(x)=\ln(1+F(x))$ wird eine T-Funktion $\bar{F}$ definiert. Wie im Beweis zu (3.5) [10] gezeigt wurde, kann man zu $\bar{F}$ eine T-Funktion $\tilde{F}$ konstruieren, so daß folgendes gilt:

(i) $\tilde{F}(x)\geqq\bar{F}(x)$ $\quad(x\in X^*)$,

(ii) $|\Delta\tilde{F}|$ ist beschränkt,

(iii) $p\,\tilde{F}(x)=\sum_{\alpha\in X}\tilde{F}(x\,\alpha)$ $\quad(x\in X^*)$.

Nach Konstruktion gilt dann für alle $z\in\mathfrak{N}_F^k$:

$$\overline{\lim}_n \ln(F(z(n))^{n^{-1}})\geqq k^{-1}$$

und somit:

$$\overline{\lim}_n \tilde{F}(z(n))\,n^{-1}\geqq k^{-1}.$$

Wegen (iii) ist $\tilde{F}$ eine Vermögensfunktion, und wegen (ii) kann man beschränkte Einsatzfunktionen B_i finden, die $\tilde{F}$ als Vermögensfunktion erzeugen. Diese Einsatzfunktionen B_i kann man ferner so wählen, daß der erzeugte Gesamteinsatz E die Bedingung $\underline{\lim}_n E(z(n))\,n^{-1}>0$ erfüllt. Denn wenn man alle Einsatzfunktionen B_i gleichmäßig erhöht, ändert sich die erzeugte Vermögensfunktion nicht. Damit ist die Behauptung gezeigt.

Wir geben nun eine äquivalente Formulierung des Satzes (6.1) an, die erkennen läßt, daß es sich bei den Zufallsgesetzen von exponentieller Ordnung im wesentlichen um die Gesetze über die relative Grenzhäufigkeit von Ereignissen handelt. Zu $\alpha,\beta\in X$ bezeichnet

$$\delta_\alpha^\beta=\begin{cases}1 & \text{falls } \alpha=\beta\\ 0 & \text{sonst.}\end{cases}$$

(6.4) **Satz.** *Eine Folge $z \in X^\infty$ erfüllt genau dann alle Zufallsgesetze von exponentieller Ordnung, wenn für jede beschränkte, berechenbare Funktion $H: X^* \to R^+$, für die $\varliminf_n n^{-1} \sum_{i=0}^{n} H(z(i)) > 0$ gilt, die folgende Relation* (R) *für alle $\alpha \in X$ erfüllt ist.*

$$\text{(R)} \qquad \lim_n \left(\sum_{i=0}^{n} H(z(i))\, \delta^{\alpha}_{z_{i+1}}\right) \left(\sum_{i=0}^{n} H(z(i))\right)^{-1} = p^{-1}.$$

Bemerkung. Setzt man für H die konstante Funktion, die nur den Funktionswert 1 annimmt, dann bedeutet (R) gerade, daß das Element $\alpha \in X$ mit der Grenzhäufigkeit p^{-1} in der Folge z vorkommt.

Bemerkung. Auffallend ist die formale Ähnlichkeit der Folgen, welche alle Zufallsgesetze von exponentieller Ordnung erfüllen, zu den Folgen des entsprechenden Kollektivs im v. Misesschen Sinne. Eine Folge $z \in X^\infty$ gehört nämlich genau dann zu dem Kollektiv mit den Grenzhäufigkeiten p^{-1} (im von Church [2] präzisierten Sinne), wenn für alle rekursiven Funktionen $H: X^* \to \{0, 1\}$, welche die Bedingung $\lim_n \sum_{i=1}^{n} H(z(i)) = \infty$ für alle $z \in X^\infty$ erfüllen, die Relation (R) für alle $\alpha \in X$ gilt.

Der *Beweis* von (6.4) beruht auf dem Satz (6.1). Angenommen $z \in X^\infty$ erfüllt für alle obigen H und alle $\alpha \in X$ die Relation (R). Wir zeigen, daß für beliebige berechenbare, beschränkte Einsatzfunktionen B_i: $X^* \to R^+$ $(i = 1, \ldots, p)$, welche die Vermögensfunktion V und den Gesamteinsatz E erzeugen, folgende Implikation gilt:

$$\varliminf_n E(z(n))\, n^{-1} > 0 \Rightarrow \lim_n V(z(n))\, E(z(n))^{-1} = 0.$$

Eine Einsatzfunktion B_i allein genommen erzeugt eine Vermögensfunktion V_i:

$$V_i(z(n+1)) = \sum_{k=0}^{n} B_i(z(k))\, \sigma_i(z_{k+1}), \qquad V_i(\Lambda) = 0$$

und einen Gesamteinsatz E_i:

$$E_i(z(n)) = \sum_{k=0}^{n} B_i(z(k)).$$

Wegen $E = \sum_{i=1}^{p} E_i$ und $V = \sum_{i=1}^{p} V_i + V(\Lambda)$ kann man die Behauptung reduzieren auf:

$$\varliminf_n E_i(z(n))\, n^{-1} > 0 \Rightarrow \lim_n V_i(z(n))\, E_i(z(n))^{-1} = 0 \qquad \text{für } i = 1, \ldots, p.$$

Wir nehmen nun an, daß $\varliminf_n E_i(z(n))\, n^{-1} > 0$. Nach Voraussetzung gilt dann:

$$\text{(1)} \qquad \lim_n \left[\left(\sum_{k=0}^{n} B_i(z(k))\, \delta^{\alpha}_{z_{k+1}}\right) \left(\sum_{k=0}^{n} B_i(z(k))\right)^{-1}\right] = p^{-1} \qquad (\alpha \in X).$$

Ferner gilt:

$$\text{(2)} \qquad V_i(z(n)) = (p-1) \sum_{k=0}^{n-1} B_i(z(k))\, \delta^{x_i}_{z_{k+1}} - \sum_{\substack{k=0 \\ x_i \neq z_{k+1}}}^{n-1} B_i(z(k)).$$

Aus (1) und (2) folgt:

$$\lim_n V_i(z(n))\, E_i(z(n))^{-1} = (p-1)\, p^{-1} - (p-1)\, p^{-1} = 0.$$

Damit ist eine Richtung der Behauptung gezeigt.

Nun nehmen wir umgekehrt an, daß $z \in X^\infty$ für jedes Spiel über z die Aussage von (6.1) erfüllt. Es sei dann $H\colon X^* \to R^+$ eine beliebige, beschränkte, berechenbare Funktion. Es ist zu zeigen:

$$\underline{\lim}_n\, E(z(n))\, n^{-1} > 0 \Rightarrow \lim_n R_i(z(n)) = p^{-1} \qquad \text{für } i = 1, \ldots, p.$$

Dabei benutzen wir folgende Bezeichnungen:

$$E(z(n)) = \sum_{k=0}^{n-1} H(z(k)), \qquad R_i(z(n)) = \sum_{k=0}^{n-1} H(z(k))\, \delta^{x_i}_{z_{k+1}}\, E(z(n))^{-1}.$$

Wir betrachten die Vermögensfunktion V_i, die jeweils von der Einsatzfunktion $B_i = H$ allein erzeugt wird:

$$V_i(z(n)) = \sum_{k=0}^{n-1} H(z(k))\, \sigma_i(z_{k+1}).$$

Die erzeugte Gesamteinsatzfunktion E_i ist jeweils mit E identisch. Wir nehmen nun an, daß $\underline{\lim}_n\, E(z(n))\, n^{-1} > 0$. Dann gilt nach Voraussetzung für festes i:

$$\begin{aligned}
0 &= \lim_n \left[\sum_{k=0}^{n} H(z(k))\, \sigma_i(z_{k+1})\, E(z(n))^{-1} \right] \\
&= \lim_n \Big[(p-1)\, R_i(z(n)) - \sum_{j \neq i} R_j(z(n))\Big] \\
&= \lim_n \Big[p\, R_i(z(n)) - \sum_{j=1}^{p} R_j(z(n))\Big] \\
&= p \lim_n \big[R_i(z(n)) - p^{-1}\big].
\end{aligned}$$

$\Big($Denn es gilt: $\sum_{j=1}^{p} R_j(z(n)) = 1.\Big)$ Es folgt also: $\lim_n R_i(z(n)) = p^{-1}$, q.e.d.

Zum Abschluß bemerken wir noch, daß sich eine Implikation im Satz (6.1) erweitern läßt. Es gilt nämlich:

(6.5) **Satz.** *Es sei $z \in X^\infty$ eine ideale Zufallsfolge i.S. von* (3.2) [10]. *Dann gilt in jedem Spiel über z, bei dem die Einsatzfunktionen berechenbar und beschränkt sind, für das Verhältnis zwischen Vermögen V und Gesamteinsatz E:*

$$\lim_n V(z(n))\, E(z(n))^{-1} = 0,$$

sofern nur $\mathrm{klim}_n\, E(z(n)) = \infty$ *erfüllt ist.*

Mit der gleichen Argumentation wie beim Beweis von Satz (6.4) kann man daraus folgendes Korollar ableiten:

(6.6) **Korollar.** *Es sei* $z \in X^\infty$ *eine ideale Zufallsfolge i.S. von* (3.2) [10]. *Dann folgt für jede berechenbare, beschränkte Funktion* $H: X^* \to R^+$, *für die* $\operatorname{klim}_n \sum_{i=0}^{n} H(z(i)) = \infty$ *erfüllt ist, die Relation:*

$$\lim_n \left[\left(\sum_{i=0}^{n} H(z(i))\, \delta^{\alpha}_{z_{i+1}} \right) \left(\sum_{i=0}^{n} H(z(i)) \right)^{-1} \right] = p^{-1} \qquad (\alpha \in X).$$

Zum Beweis zu (6.5) geht man zunächst wie beim Beweis von (6.2) vor. Es seien die Testfunktionen F_m wie im Beweis zu (6.2) definiert. Wir betrachten die dort abgeleitete Relation:

$$\left| \sum_{i=0}^{n-1} \ln\left(1 + m^{-1} \Delta V(z(i+1))\right) - m^{-1} \sum_{i=0}^{n-1} \Delta V(z(i+1)) \right|$$
$$\leqq m^{-2}\, 2^{-1} \sum_{i=0}^{n-1} |\Delta V(z(i+1))|.$$

Zu $a > 0$ zeigen wir, daß durch

$$\mathfrak{N}^+(a) \underset{\text{def}}{=} \{ z \in X^\infty \mid \operatorname{klim}_n E(z(n)) = \infty,\ \overline{\lim_n}\, V(z(n))\, E(z(n))^{-1} > a \}$$

eine T-Nullmenge definiert wird.

Man wähle m so groß, daß $a > m^{-1}\, 2^{-1}\, p^{-1}$, dann gilt für jedes $z \in \mathfrak{N}^+(a)$:

$$\sum_{i=0}^{n-1} \ln\left(1 + m^{-1} \Delta V(z(i+1))\right) \geqq m^{-1}\, V(z(n)) - m^{-2}\, 2^{-1} \sum_{i=0}^{n-1} |\Delta V(z(i+1))|.$$

Dies impliziert:

$$\overline{\lim_n} \sum_{i=0}^{n-1} \ln\left(1 + m^{-1} \Delta V(z(i+1))\right)$$
$$\geqq m^{-1}\, \overline{\lim_n} \left[V(z(n))\, E(z(n))^{-1}\, E(z(n)) - m^{-1}\, 2^{-1} \sum_{i=0}^{n-1} |\Delta V(z(i+1))| \right]$$
$$\geqq \overline{\lim_n} \left[a\, E(z(n)) - m^{-1}\, 2^{-1}\, p^{-1}\, E(z(n)) \right] m^{-1}.$$

Wegen $a > m^{-1}\, 2^{-1}\, p^{-1}$ und $\operatorname{klim}_n E(z(n)) = \infty$ folgt dann:

$$\operatorname{k}\overline{\lim_n} \sum_{i=0}^{n-1} \ln\left(1 + m^{-1} \Delta V(z(i+1))\right) = \infty.$$

Nach Definition von F_m heißt das: $\operatorname{k}\overline{\lim_n}\, F_m(z(n)) = \infty$. Somit gilt: $\mathfrak{N}^+(a) \subset \mathfrak{N}_{F_m}$.

In analoger Weise zeigt man, daß es zu $a > 0$ ein geeignetes negatives $\bar{m} \in Z$ gibt, so daß die durch

$$\mathfrak{N}^-(a) \underset{\text{def}}{=} \{ z \in X^\infty \mid \operatorname{klim}_n E(z(n)) = \infty,\ \underline{\lim_n}\, V(z(n))\, E(z(n))^{-1} < -a \}$$

definierte Menge $\mathfrak{N}^-(a)$ in der von $F_{\bar{m}}$ erzeugten T-Nullmenge $\mathfrak{N}_{F_{\bar{m}}}$ enthalten ist.

Literatur

1. Blum, M.: A machine-independent theory of the complexity of recursive functions. J. Assoc. comp. Machin. **14**, 322 – 336 (1967).
2. Church, A.: On the concept of a random sequence. Bull. Amer. math. Soc. **46**, 130 – 135 (1940).
3. Davis, H.: Computability and unsolvability. New York-Toronto-London: McGraw-Hill 1958.
4. Hartmanis, J., Stearns, R. E.: On the computational complexity of algorithms. Trans. Amer. math. Soc. **117**, 285 – 306 (1965).
5. Hennie, F. C.: One-tape, off-line turing machine computations. Inform. and Control **8**, 553 – 578 (1965).
6. Hermes, H.: Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit. Berlin-Göttingen-Heidelberg: Springer 1961.
7. Hotz, G., Walter, H.: Automatentheorie und formale Sprachen. Mannheim-Zürich: Bibliographisches Institut 1968.
8. Mises, R. v.: Grundlagen der Wahrscheinlichkeitsrechnung. Math. Zeitschrift **5**, 52 – 99 (1919).
9. Schnorr, C. P.: Eine Bemerkung zum Begriff der zufälligen Folge. Z. Wahrscheinlichkeitstheorie verw. Geb. **14**, 27 – 35 (1969).
10. – Über die Definition effektiver Zufallstests. Teil I. Z. Wahrscheinlichkeitstheorie verw. Geb. **15**, 297 – 312 (1970).
11. – Über die Definition effektiver Zufallstests. Teil II. Z. Wahrscheinlichkeitstheorie verw. Geb. **15**, 313 – 328 (1970).
12. – Komplexität von Algorithmen mit Anwendung auf die Analysis. Erscheint in Arch. math. Logik Grundlagenforsch.

Priv.-Doz. Dr. Claus-Peter Schnorr
Institut für Angewandte Mathematik
Universität des Saarlandes
D-6600 Saarbrücken 15

(Eingegangen am 14. Juli 1969)