Über das Fälschen von Würfeln

Ehrhard Behrends

1. Einleitung

Wir gehen aus von einem handelsüblichen Würfel, also einem, auf dessen Seiten die Zahlen von 1 bis 6 aufgedruckt sind. Er soll *fair* genannt werden, wenn alle Zahlen mit gleicher Wahrscheinlichkeit, d.h. mit Wahrscheinlichkeit $1/6$, beim Würfeln erscheinen. Bekanntlich lassen sich Würfel aber auch manipulieren: Durch Verwendung inhomogener Materialien, Magneten usw. können die Wahrscheinlichkeiten verändert werden.

Wenn zwei faire Würfel vorliegen und sie gleichzeitig geworfen werden, ergeben sich als Augensumme Zahlen zwischen 2 und 12, und es ist nicht schwer, für jede dieser Zahlen k die Wahrscheinlichkeit des Auftretens auszurechnen. Man addiert einfach die Wahrscheinlichkeiten derjenigen Möglichkeiten, die zum Ergebnis k führen, wobei man die Wahrscheinlichkeit jedes einzelnen Zahlenpaares als $1/36$ ansetzt. So ergeben sich für $2, 3, \ldots, 11, 12$ die Werte $1/36, 2/36, \ldots, 2/36, 1/36$.

Wie sieht das bei gefälschten Würfeln aus? Auch da kann man die Augensummen-Wahrscheinlichkeiten leicht bestimmen, und diese Zahlen werden offensichtlich im allgemeinen von $1/36, 2/36, \ldots, 2/36, 1/36$ verschieden sein.

Als Ausgangspunkt für die in diesem Artikel zu besprechenden Ergebnisse wollen wir zwei mit den Summen-Wahrscheinlichkeiten zusammenhängende Probleme formulieren. Als erstes stellen wir uns die Frage, ob es durch geeignetes Fälschen zweier Würfel möglich ist, daß für die Augensumme die Ergebnisse $2, \ldots, 12$ alle die gleiche Wahrscheinlichkeit haben. Und dann kümmern wir uns um das Problem, ob sich - geschicktes Fälschen vorausgesetzt - die Summen bei manipulierten Würfeln genauso verhalten können wie die zweier fairer, ob also als Summen-Wahrscheinlichkeiten auch dann $1/36, 2/36, \ldots, 2/36, 1/36$ auftreten können, wenn nicht notwendig die Wahrscheinlichkeiten für $1, \ldots, 6$ auf beiden Würfeln jeweils $1/6$ sind.

Es wird sich herausstellen, daß die Antwort in beiden Fällen "nein" lautet. Der Beweis ist mit elementaren Mitteln leicht zu führen, hier soll es aber um eine jeweils naheliegende Verallgemeinerung gehen. Um die zu formulieren, numerieren wir unsere Würfel zunächst um: Statt mit $1,\ldots,6$ sollen sie mit $0,\ldots,5$ beschriftet sein. Klar, daß das inhaltlich nicht das Geringste ändert, später werden aber dadurch einige Formulierungen etwas übersichtlicher. Als nächstes gehen wir von einem Würfel mit sechs Flächen zu einem mit n Flächen über, wobei n irgendeine natürliche Zahl ist; die Flächen sind dann von 0 bis $n-1$ durchnumeriert. (Um so etwas zu realisieren, könnte man eine kleine Säule verwenden, deren Querschnitt ein regelmäßiges n-Eck ist, und "würfeln" bedeutet dann, diese Säule über den Tisch zu rollen.) Und schließlich wollen wir auch die Sprache der Wahrscheinlichkeitsrechnung verwenden. Aus einem "n-Würfel" mit der Beschriftung $0,\ldots,n-1$ wird ein Wahrscheinlichkeitsmaß auf $\{0,\ldots,n-1\}$, das wir uns durch Vorgabe der Zahlen $p_j := P(\{j\})$ definiert denken, und zum "Würfeln mit zwei Würfeln" müssen wir uns daran erinnern, wie man die Verteilung der Summe unabhängiger Zufallsvariablen berechnet. Hier liest sich das so: Sind Wahrscheinlichkeitsmaße auf $\{0,\ldots,n-1\}$ durch $p_0,\ldots,p_{n-1}$ und auf $\{0,\ldots,m-1\}$ durch $q_0,\ldots,q_{m-1}$ gegeben, so korrespondiert "Summe der Augenzahlen" zu einem Wahrscheinlichkeitsmaß auf $\{0,\ldots,n+m-2\}$, wobei sich die Wahrscheinlichkeiten für $j=0,\ldots,n+m-2$ als $r_j = p_0q_j + p_1q_{j-1} + \cdots + p_jq_0$ berechnen lassen; dabei ist hier und im folgenden $p_i = q_j := 0$ für $i \geq n, j \geq m$ gesetzt.

Nach diesen Vorbereitungen können wir die obigen Probleme wie folgt verallgemeinern:

Problem 1: Fälschen zum Simulieren der Gleichverteilung

Es seien n und m natürliche Zahlen. Gibt es Wahrscheinlichkeiten $p_0,\ldots,p_{n-1}$ bzw. $q_0,\ldots,q_{m-1}$, so daß alle $r_j := p_0q_j+p_1q_{j-1}+\cdots+p_jq_0, j = 0,\ldots,n+m-2$ gleich sind?

Problem 2: Fälschen mit dem Ziel, die Summe fairer Würfel zu simulieren

Seien $k,n,m \in \mathbb{N}$ mit $n+m=2k$. Ist es möglich, Wahrscheinlichkeiten $p_0,\ldots,p_{n-1}$ und $q_0,\ldots,q_{m-1}$ so zu finden, daß die $p_0q_j + p_1q_{j-1} + \cdots + p_jq_0, j=0,\ldots,2n-2$ so sind wie bei der Summe zweier Gleichverteilungen auf $\{0,\ldots,k-1\}$, also gleich $1/k^2, 2/k^2,\ldots,2/k^2,1/k^2$?

Das erste Problem geht auf eine Frage von P. Lévy zurück. Eine erste Antwort stammt von Raikov ([9]): Ist k eine Primzahl, so gibt es keine nichttriviale Lösung (d.h. eine mit $n,m>1$). Dieses Ergebnis ist in mehreren Lehrbüchern zu finden, die sich mit der Darstellung von Zufallsvariablen durch Summen unabhängiger Variablen beschäftigen (z.B. in [1],[6],[7],[8]). Weniger bekannt scheint zu sein, daß das Problem in der allgemeinen Form auch schon vor langer Zeit untersucht wurde (in [3], zitiert meines Wissens nach nur in [7]). Der vergleichsweise einfach zu behandelnde Fall $n = m = 6$ ist in der Verkleidung des zu Beginn geschilderten Würfelproblems Standard-Übungsaufgabe in der elementaren Wahrscheinlichkeitstheorie; die älteste Quelle scheint mir [4] zu sein.

Das zweite Problem ist nur in [10] untersucht worden und wird dort im Spezialfall $n = m = k$ vollständig gelöst. (Dort gibt es allerdings einen Fehler: Dem Computerprogramm ist entgangen, daß es nichttriviale Lösungen auch für den Fall $n = m = k = 13$ gibt.)

Der Aufbau ist wie folgt. In *Kapitel 2* werden die Probleme in Fragen über Polynome bzw. in eine Aussage der elementaren Zahlentheorie (additive Darstellbarkeit von Zahlen) umformuliert. *Kapitel 3* enthält eine vollständige Lösung des Problems 1, wobei auch der Fall von mehr als zwei Würfeln erledigt wird. Die Methoden sind ähnlich wie in [3] (wo es allerdings nur um zwei Würfel geht).

Das Problem 2 wird in *Kapitel 4* gelöst. Der Zugang ist etwas elementarer als in [10], dadurch wird die Beweisstrategie etwas klarer; wie dort wird auch hier nur der Spezialfall $n = m = k$ vollständig diskutiert. In *Kapitel 5* schließlich gibt es noch einige Ergänzungen: Erweiterungen der vorher bewiesenen Ergebnisse, aber auch weitere Informationen zum Thema "Manipulieren von Würfeln".

Von den Lesern wird an Vorkenntnissen zum Verständnis nur recht elementare Mathematik erwartet. Komplexe Zahlen spielen eine wichtige Rolle, und bei der Erklärung, wie ich zu der Aussage von Lemma 4.1(i) komme (allerdings nicht für den Beweis), sollte man sich an die Hauptachsentransformation erinnern.

2. Übersetzung des Problems in Fragen über Polynome und die Darstellbarkeit von Zahlen

Nachstehend werden Polynome $P(x) = p_0 + p_1 x + \cdots + p_{n-1} x^{n-1}$ mit nichtnegativen Koeffizienten eine wichtige Rolle spielen. Derartige Polynome entsprechen eineindeutig den Wahrscheinlichkeitsmaßen auf $\{0, \ldots, n-1\}$, wenn wir noch $p_0 + \cdots + p_{n-1} = 1$ verlangen.

Für die Behandlung unserer Probleme ist die folgende elementare Tatsache wichtig: Sind $P(x) = p_0 + p_1 x + \cdots + p_{n-1} x^{n-1}$ und $Q(x) = q_0 + q_1 x + \cdots +$

$q_{m-1}x^{m-1}$ Polynome, die zu Wahrscheinlichkeitsmaßen auf $\{0,\ldots,n-1\}$ bzw. $\{0,\ldots,m-1\}$ gehören, so korrespondiert zu dem in der Einleitung behandelten Wahrscheinlichkeitsmaß auf $\{0,\ldots,n+m-2\}$ (der Summenverteilung) gerade das Polynom $P(x)Q(x)$.

Problem 1 wird also so übersetzt: Gibt es zu vorgelegten Zahlen n, m Polynome $P(x) = p_0+p_1x+\cdots+p_{n-1}x^{n-1}$ und $Q(x) = q_0+q_1x+\cdots+q_{m-1}x^{m-1}$ mit nichtnegativen Koeffizienten, so daß die Summe der Koeffizienten 1 ist und $P(x)Q(x) = (1+x+\cdots+x^{n+m-2})/(n+m-1)$? Oder gleichwertig (nachdem die auftretenden Polynome mit $1/p_{n-1}, 1/q_{m-1}$ bzw $n+m-1$ multipliziert wurden): Kann man $1+x+\cdots+x^{n+m-2}$ als Produkt $A(x)B(x)$ schreiben, wobei $A(x) = a_0+\cdots+a_{n-2}x^{n-2}+x^{n-1}, B(x) = b_0+\cdots+b_{m-2}x^{m-2}+x^{m-1}, a_j, b_j \geq 0$?

Die Übersetzung von *Problem 2* lautet entsprechend: Gibt es zu $k \in \mathbb{N}$ Polynome $A(x) = a_0+\cdots+a_{n-2}x^{n-2}+x^{n-1}, B(x) = b_0+\cdots+b_{m-2}x^{m-2}+x^{m-1}$ mit $a_j, b_j \geq 0$ und $A(x)B(x) = (1+x+\cdots+x^{k-1})^2$?

In beiden Fällen spielen also Polynome der Form $C(x) = 1+x+\cdots+x^{k-1}$ eine Rolle. Da $(1-x)C(x) = 1-x^k$ gilt, sind die Nullstellen von $C(x)$ bekannt: Es handelt sich um die von 1 verschiedenen k-ten Einheitswurzeln, also die Zahlen $\zeta_j := \exp(2\pi ij/k), j = 1,\ldots,k-1$. Damit kennen wir aber auch die Nullstellen der in der Problemumformulierung auftauchenden Polynome $A(x), B(x)$, es muß sich ebenfalls um die ζ_j handeln. Das hat interessante Konsequenzen:

Lemma 2.1 *$A(x) = a_0+\cdots+a_{n-2}x^{n-2}+x^{n-1}$ und $B(x) = b_0+\cdots+b_{m-2}x^{m-2}+x^{m-1}$ seien Polynome mit $a_j, b_j \geq 0$.*

(i) *Gilt $A(x)B(x) = 1+x+\cdots+x^{n+m-2}$ oder, falls $n+m$ die Form $2k$ hat, $A(x)B(x) = (1+x+\cdots+x^{k-1})^2$, so ist $a_j = a_{n-1-j}$ $(j = 0,\ldots,n-1)$ sowie $b_j = b_{m-1-j} (j = 0,\ldots,m-1)$.*

(ii) *Aus $A(x)B(x) = 1+x+\cdots+x^{n+m-1}$ folgt zusätzlich $a_j, b_j \in \{0,1\}$ für alle j.*

Beweis:

(i) Betrachten wir etwa das Polynom $A(x)$. Es soll $A(x) = x^{n-1}A(1/x)$ gezeigt werden, woraus dann durch Koeffizientenvergleich alles folgt. Wir wissen schon, daß alle Nullstellen ζ von $A(x)$ Einheitswurzeln sind und daß 1 *keine* Nullstelle ist. Da die Koeffizienten von A reell sind, ist mit ζ auch die konjugiert komplexe Zahl $\overline{\zeta}$ Nullstelle. Nun ist $|\zeta| = 1$, und deswegen stimmt $\overline{\zeta}$ mit $1/\zeta$ überein. Durch Betrachtung der Ableitungen von $A(x)$, die auch

Polynome mit reellen Koeffizienten sind, folgt noch, daß die Nullstellen ζ und $\overline{\zeta}$ mit der gleichen Vielfachheit auftreten.

All das liefert die für uns wichtigen Informationen über die $n-1$ Faktoren in der kanonischen Darstellung $\prod(x-\zeta)$ von $A(x)$ (ζ durchläuft dabei die Nullstellen von $A(x)$, wobei die Vielfachheiten zu berücksichtigen sind):

- Ersetzt man in dem Produkt jedes ζ durch $1/\zeta$, so treten die gleichen Faktoren auf; das ergibt $x^{n-1}A(1/x) = x^{n-1}\prod(1/x-\zeta) = \prod(1-\zeta x) = \prod(-\zeta)\prod(x-1/\zeta) = A(0)A(x)$.

- Im Produkt $A(0) = \prod(-\zeta)$ existiert zu jedem nicht-reellen Faktor $-\zeta$ ein Faktor $-\overline{\zeta}$, und als reeller Faktor ist nur $-(-1)$ möglich; folglich ist dieses Produkt gleich 1.

So ist wirklich $x^{n-1}A(1/x) = A(x)$ gezeigt.

(ii) Aus $a_j, b_j \geq 0$ folgt sofort durch Betrachtung des Koeffizienten des Produkts bei x^j, daß $a_j, b_j \in [0,1]$.

Angenommen, es gäbe einen Index j mit $0 < a_j < 1$. Bezeichnet j_0 das kleinste j mit dieser Eigenschaft, so ist – wegen Teil (i) – $j_0 > 0$. Nun ist $b_l + b_{l-1}a_1 + \cdots + b_1 a_{l-1} + a_l = 1$ für $l = 1, \cdots, n+m-2$ (wobei wir wieder $a_i, b_j = 0$ für $i \geq n, j \geq m$ gesetzt haben). Aus dieser Gleichung folgt durch Induktion nach l: $b_l \in \{0,1\}$ für $l = 0, \ldots, j_0 - 1$ sowie $0 < b_{j_0} < 1$.

Das hat aber einen Widerspruch zur Folge, wenn wir nun den Koeffizienten von x^{m-1} im Produkt auswerten, wobei wir Teil (i) des Lemmas anwenden: $1 = b_{m-1} + b_{m-2}a_1 + \cdots + b_{m-1-j_0}a_{j_0} \cdots \geq b_{m-1} + b_{m-1-j_0}a_{j_0} = 1 + b_{j_0}a_{j_0} > 1$. □

Wegen 2.1(i) müssen wir uns bei der Behandlung unserer Probleme eins und zwei nur um Polynome kümmern, die von vorn nach hinten die gleichen Koeffizienten haben wie umgekehrt. In Analogie zur entsprechenden Bezeichnung bei Worten spricht man dann von *Palindrom*-Polynomen.

Teil (ii) des Lemmas führt noch zu einer weiteren Vereinfachung von Problem 1. Von den Koeffizienten von $A(x)$ und $B(x)$ sind sicher nur die Indizes i, j interessant, für die $a_i = 1 = b_j$. Setze $\Pi_A := \{i | a_i = 1\}, \Pi_B := \{j | b_j = 1\}$. $A(x)B(x) = 1 + x + \cdots + x^{n+m-2}$ heißt dann, daß jedes $j \in \{0, \ldots, n+m-2\}$ auf eindeutige Weise als $j = j_1 + j_2, j_1 \in \Pi_A, j_2 \in \Pi_B$, geschrieben werden kann. Und so hat sich Problem 1 in ein Problem der elementaren Zahlentheorie verwandelt.

3. Fälschen zum Simulieren der Gleichverteilung

Wir fassen noch einmal zusammen, wobei wir das bisher behandelte Problem 1 leicht verallgemeinern:

Problem 1': Es seien $s, k_1, \ldots, k_s$ natürliche Zahlen und $k_0 := k_1 + \cdots + k_s$. Gibt es Mengen $\Pi_\sigma \subset \{0, \ldots, k_\sigma\}$, so daß jedes j in $\{0, \ldots, k_0\}$ eindeutig als $j = j_1 + \cdots + j_s$ mit $j_\sigma \in \Pi_\sigma$ geschrieben werden kann? Wir werden $\Pi_1, \ldots, \Pi_s$ in so einem Fall eine $(k_1, \ldots, k_s)$*-Familie (zu* $\{0, \ldots, k_0\}$*)* nennen.

Zu welchen k_0 gibt es $s \geq 2, k_1, \ldots, k_s \in \mathbb{N}$ mit $k_1 + \cdots + k_s = k$, so daß eine $(k_1, \ldots, k_s)$-Familie existiert?

> Der bisher diskutierte Fall entspricht $s = 2, k_1 = n - 1, k_2 = m - 1$. Die Verallgemeinerung ist eine Umformulierung der Frage, ob man die Gleichverteilung auf $\{0, \ldots, k_0\}$ durch Fälschen von s Würfeln erzeugen kann. Lemma 2.1 rechtfertigt zwar zunächst nur die Übersetzung im Falle zweier Würfel, enthält aber auch schon die allgemeinere Variante, wenn man es im Falle von s Polynomen $A_1(x), \ldots, A_s(x)$ auf $A_1(x)$ und $A_2(x)A_3(x) \cdots A_s(x)$ anwendet.

Einige einfache Beispiele und Tatsachen ergeben sich schnell. Zum Beispiel müssen alle Π_σ die Zahlen 0 und k_σ enthalten, da andernfalls 0 bzw. k_0 überhaupt nicht darstellbar wären. Andererseits: Außer 0 gibt es *keine* Zahl j, die in mehr als einem Π_σ enthalten ist (denn sonst hätte j zwei verschiedene Darstellungen). Damit ist übrigens die Frage nach der Existens einer $(5, 5)$-Familie (d.h. Problem 1 für gefälschte sechsseitige Würfel) bereits negativ beantwortet.

Sei α_σ das kleinste strikt positive Element von Π_σ. Da alle α_σ voneinander verschieden sind und mindestens eins gleich 1 sein muß (warum?), dürfen wir annehmen, daß $1 = \alpha_1 < \cdots < \alpha_s$. In so einem Fall wollen wir von einer $(k_1, \cdots, k_s)$*-Familie in kanonischer Reihenfolge* sprechen.

Hier ein Beispiel: $\Pi_1 := (111), \Pi_2 := (1001)$ ist eine $(2, 3)$-Familie in kanonischer Reihenfolge für (111111). (Ab hier verschlüsseln wir Teilmengen von $\{0, \ldots, r\}$ durch die Werte der zugehörigen charakteristischen Funktion; die eben angegebenen Π_1, Π_2 zum Beispiel sind also die Mengen $\{0, 1, 2\}, \{0, 3\}$). Entsprechend sind $(1111), (10001), (10000000100000001)$ eine $(3, 4, 16)$-Familie und $(110011), (101)$ eine $(5, 2)$-Familie (beide in kanonischer Reihenfolge).

Übrigens wollen wir ausdrücklich den Fall $s = 1$ zulassen, die *triviale Familie.*

Wir beschreiben nun alle Möglichkeiten, Familien in kanonischer Reihenfolge zu finden (womit Problem 1' dann vollständig gelöst sein wird). Zunächst geben wir einen konkreten Algorithmus an, solche Familien zu finden, und dann zeigen wir im schwierigeren zweiten Teil, daß alle so entstehen.

Sei $k_0 \in \mathbb{N}$. Wir nehmen an, daß $k_0+1 = g_1 \cdots g_t$ als Produkt natürlicher Zahlen mit $t, g_1, \ldots, g_t \geq 2$ geschrieben ist (Achtung: Die Reihenfolge der g_j wird sich als wichtig erweisen). Dann kann jedes $j \in \{0, \cdots, k_0\}$ auf eindeutige Weise als $j = j_1 + j_2 g_1 + j_3 g_2 g_1 + \cdots + j_t g_{t-1} \cdots g_1$ geschrieben werden, wo $0 \leq j_\tau < g_\tau$. Das ist eine offensichtliche Verallgemeinerung der wohlbekannten g-adischen Entwicklung, die dem Fall $g = g_1 = \cdots = g_t$ entspricht.

In unserer Terminologie heißt das: Setzt man $\widehat{\Pi}_1 := \{0, \ldots, g_1-1\}, \widehat{\Pi}_2 := \{0, g_1, 2g_1, \ldots, (g_2-1)g_1\} =: g_1\{0, \ldots, g_2-1\}$, allgemein $\widehat{\Pi}_\tau := (g_{\tau-1}g_{\tau-2} \cdots g_1)\{0, \cdots, g_\tau - 1\}$ sowie $\widehat{k}_\tau := (g_\tau - 1)g_{\tau-1} \cdots g_1$ für $\tau = 1, \ldots, t$, so ist $(\widehat{\Pi}_1, \ldots, \widehat{\Pi}_t)$ eine $(\widehat{k}_1, \ldots, \widehat{k}_t)$-Familie. Sie ist in kanonischer Reihenfolge, da $g_1 < g_2 g_1 < \cdots$.

Sei nun $2 \leq s \leq t$ und $\Delta_1, \ldots, \Delta_s$ eine disjunkte Zerlegung von $\{1, \ldots, t\}$ in nichtleere Teilmengen, derart daß kein Δ_σ zwei aufeinanderfolgende Zahlen enthält und jeweils das kleinste Element von Δ_σ kleiner als das von $\Delta_{\sigma+1}$ ist (z. B. $\{1\}, \{2\}, \{3\}$ im Fall $s = t = 3$ oder $\{1, 3\}, \{2\}$ für $s = 2, t = 3$). So etwas soll in diesem Abschnitt eine *alternierende s-Zerlegung von* $\{1, \ldots, t\}$ heißen.

Setze $\Pi_\sigma := \sum_{\tau \in \Delta_\sigma} \widehat{\Pi}_\tau$; dabei ist die Summe von Zahlenmengen M, N als $M + N := \{m + n | m \in M, n \in N\}$ erklärt. Es ist offensichtlich, daß dann $\Pi_1, \ldots, \Pi_s$ eine $(k_1, \ldots, k_s)$-Familie mit $k_1 + \cdots + k_s = k_0$ ist, wenn wir $k_\sigma := \sum_{\tau \in \Delta_\sigma} \widehat{k}_\tau$ definieren. Unsere Voraussetzung an die Δ_σ impliziert auch sofort, daß sie kanonisch geordnet ist.

So also erhält man Beispiele. Zum späteren Zitieren wollen wir die eben gefundene Familie *die zu* $(g_1, \ldots, g_t; \Delta_1, \ldots, \Delta_s)$ *gehörige Familie* nennen.

Beispiel:

Sei $k_0 = 23$ und k_0+1 als $4 \cdot 2 \cdot 3$ geschrieben. Dann ist $\widehat{\Pi}_1 = (1111), \widehat{\Pi}_2 = (10001), \widehat{\Pi}_3 = (10000000100000001)$. Die einzige alternierende 3-Zerlegung ($\Delta_i = \{i\}$) führt zur $(3, 4, 16)$-Familie $\widehat{\Pi}_1, \widehat{\Pi}_2, \widehat{\Pi}_3$, und die eindeutig bestimmte 2-Zerlegung von $\{1, 2, 3\}$, also $\{1, 3\}, \{2\}$, liefert $(111100001111000011111), (10001)$.

2. Wieder sei $k_0 = 23$, diesmal versuchen wir es mit $k_0 + 1 = 2 \cdot 2 \cdot 3 \cdot 2$. Hier sind die $\widehat{\Pi}_\tau$ wie folgt: $\widehat{\Pi}_1 = (11), \widehat{\Pi}_2 = (101), \widehat{\Pi}_3 = (100010001), \widehat{\Pi}_4 =$

(1000000000001). Die alternierende 2-Zerlegung $\{1,3\},\{2,4\}$ führt auf die $(9,14)$-Familie (1100110011), (101000000000101).

Schwieriger ist die Umkehrung, wir formulieren sie als

Theorem 3.1 *Sei $\Pi_1,\ldots,\Pi_s$ eine $(k_1,\ldots,k_s)$-Familie in kanonischer Reihenfolge.*

(i) *Es gibt $t\ge 1, g_1,\ldots,g_t>1$ mit $k+1=g_1\cdots g_t$ und eine alternierende s-Zerlegung $\Delta_1,\ldots,\Delta_s$ von $\{1,\ldots,t\}$, so daß $\Pi_1,\ldots,\Pi_s$ die zu $(g_1,\ldots,g_t;\Delta_1,\ldots,\Delta_s)$ gehörige Familie ist.*

(ii) *$\Pi_1,\ldots,\Pi_s$ bestimmen $(g_1,\ldots,g_t,\Delta_1,\ldots,\Delta_s)$ eindeutig.*

Der Beweis folgt gleich, zunächst benötigen wir als Vorbereitung zwei Lemmata.

Lemma 3.2 *Es seien $r,k_0\in\mathbb{N}, r<k_0$, und $\Pi\subset\{0,\ldots,k_0-r\}$ so, daß $\{0,\ldots,r\},\Pi$ eine (r,k_0-r)-Familie ist. Dann ist $r+1$ ein Teiler von k_0+1, und Π ist die Menge $(r+1)\{0,\ldots,n-1\}$, wo $n:=(k_0+1)/(r+1)$.*

Beweis: Die Eindeutigkeit der Darstellung impliziert $|j'-j''|>r$ für verschiedene Elemente j',j'' aus Π, und wegen der Forderung, daß alle Elemente aus $\{0,\ldots,k_0\}$ als Summen von Elementen aus $\{0,\ldots,r\}$ bzw. Π darstellbar sein sollen, können die Lücken nicht größer als $r+1$ sein. □

Lemma 3.3 *$\Pi,\tilde\Pi$ sei eine zulässige Familie für $\{0,\ldots,k_0\}$ mit $1\in\Pi$. Wähle r so, daß $\{0,\ldots,r\}\subset\Pi$, aber $r+1\notin\Pi$. Dann gilt*

(i) *$r+1\in\tilde\Pi$.*

(ii) *Aus $\{i,i+1,\ldots,i+r'\}\subset\Pi$ folgt $r'\le r$.*

(iii) *Für $i\in\Pi$ mit $i-1\notin\Pi$ ist $\{i,\ldots,i+r\}\in\Pi$.*

(iv) *$r+1$ teilt jedes $j\in\tilde\Pi$ und jedes $j'\in\Pi$ mit $j'-1\notin\Pi$.*

Beweis: (i) Das ist klar, da sonst $r+1$ nicht als Summe darstellbar wäre.

(ii) Wäre einmal $\{i,\ldots,i+r+1\}\in\Pi$, so hätte $i+r+1$ zwei verschiedene Darstellungen als j_1+j_2 mit $j_1\in\Pi, j_2\in\tilde\Pi$, nämlich als $(i+r+1)+0$ und als $i+(r+1)$.

(iii) Angenommen, das wäre nicht der Fall. $i\in\Pi$ soll das kleinste Element sein, wo zwar $i-1\notin\Pi$, aber $\{i,\ldots,i+r\}\not\subset\Pi$; für $i'\in\Pi, i'<i, i'-1\notin\Pi$ gilt also $\{i',\ldots,i'+r\}\subset\Pi$. Wähle r' so groß wie möglich, daß $\{i,i+1,\ldots,i+r'\}\subset\Pi$, nach Annahme ist dann $r'<r$.

Schreibe $i + r' + 1$ als $j_1 + j_2$ mit $j_1 \in \Pi, j_2 \in \tilde{\Pi}$. Wegen $j + r' + 1 \notin \Pi$ ist $j_2 > 0$ und folglich $j_2 \geq r + 1$. Also ist $j_1 < i$. Wir behaupten, daß $j_1 - 1 \notin \Pi$. Im Fall $j_1 = 0$ ist das klar, und im Fall $j_1 > 0$ betrachten wir die Identität $i + r' = (i + r') + 0 = (j_1 - 1) + j_2$. Sie bedeutet im Fall $j_1 - 1 \in \Pi$ zwei verschiedene Darstellungen von $i + r'$. Also ist $j_1 \in \Pi, j_1 - 1 \notin \Pi, j_1 < i$, und daraus dürfen wir $\{j_1, \ldots, j_1 + r\} \in \Pi$ folgern. Insbesondere gilt $j_1 + (r - r') \in \Pi$ und $j_1 + (r - r') < i$ (wegen $i - 1 \notin \Pi$), und das verschafft uns zwei verschiedene Darstellungen von $i + r + 1$ als $i + (r + 1)$ und als $(j_1 + r - r') + j_2$, wo $i, j_1 + r - r' \in \Pi, r + 1, j_2 \in \tilde{\Pi}$. Dieser Widerspruch zeigt (iii).

(iv) Setze $\Pi' := \{i \in \Pi | i - 1 \notin \Pi\}$, wobei $\Pi' = \{0\}$ möglich ist. Wegen (ii) und (iii) ist jedes $j \in \Pi$ eindeutig als $j' + j''$ darstellbar, wo$j' \in \{0, \ldots, r\}$ und $j'' \in \Pi'$. Folglich ist $(\{0, \ldots, r\}, \Pi' + \tilde{\Pi})$ eine zulässige Familie, und die Behauptung folgt aus dem vorstehenden Lemma. □

Wir kommen nun zum *Beweis von Theorem 3.1*, wir führen ihn durch Induktion nach k_0. Für $k_0 = 0$ ist alles klar, und wir nehmen an, daß k_0 nun so vorgelegt ist, daß die Aussage für alle $\tilde{k}_0 < k_0$ schon bewiesen ist; weiter sei eine zulässige Familie wie im Theorem gegeben. Da die triviale Familie zu $(k_0 + 1, \{1\})$ gehört, dürfen wir $s \geq 2$ annehmen.

Um 3.1(i) zu zeigen, sind $g_1, \ldots, g_t \geq 2$ und eine disjunkte Zerlegung $\Delta_1, \ldots, \Delta_s$ von $\{1, \ldots, t\}$ so zu finden, daß $g_1 \cdots g_t = k_0 + 1$ und

(1) $\Delta_\sigma \neq \emptyset$ für alle σ.

(2) Kein Δ_σ enthält zwei aufeinanderfolgende Elemente.

(3) Das kleinste Element von Δ_σ ist kleiner als das kleinste Elment von $\Delta_{\sigma+1}$.

(4) Setzt man $\widehat{\Pi}_\tau := (g_{\tau-1} \cdots g_1)\{0, \ldots, g_\tau - 1\}$, so ist $\Pi_\sigma = \sum_{\tau \in \Delta_\sigma} \Pi_\tau$.

Dazu definieren wir $\Pi := \Pi_1$ und $\tilde{\Pi} := \Pi_2 + \cdots + \Pi_s$. Nach Annahme ist $1 \in \Pi$, so daß wir Lemma 3.3 anwenden dürfen: Es gibt ein $r \geq 1$ so, daß (mit den Bezeichnungen des Lemmas) $\Pi = \{0, \ldots, r\} + \Pi'$, und $r + 1$ teilt alle Elemente von $\Pi' + \tilde{\Pi}$. Insbesondere teilt $r + 1$ das größte Element n von $\Pi + \tilde{\Pi}$, und damit teilt $r + 1$ auch $k_0 + 1 = n + r + 1$.

Setze $\tilde{k}_0 := n/(r + 1)$; das ist unser Kandidat, um die Induktionsvoraussetzung anzuwenden. Wir definieren $\tilde{\Pi}_1 := \Pi'/(r + 1)$
$(:= \{j/(r + 1) | j \in \Pi'\}), \tilde{\Pi}_\sigma := \Pi_\sigma/(r + 1)$ für $\sigma > 1$. Wir nehmen für den Augenblick an, daß alle $\tilde{\Pi}_\sigma$ mindestens zwei Elemente enthalten. (Tatsächlich könnte $\tilde{\Pi}_1 = \{0\}$ sein, wenn nämlich $\Pi_1 = \{0, \ldots, r\}$ war; um diese Möglichkeit kümmern wir uns gleich). Dann bildet $\tilde{\Pi}_1, \ldots, \tilde{\Pi}_s$ eine $(\tilde{k}_1, \ldots, \tilde{k}_s)$-

Familie für $\{0,\ldots,\tilde{k}_0\}$, wobei $\tilde{k}_1 := (k_1 - r)/(r+1, \tilde{k}_\sigma := k_\sigma/(r+1)$ für $\sigma > 1$.

Darauf wird nun die Induktionsvoraussetzung angewandt. (Die bezieht sich zwar nur auf Familien in kanonischer Reihenfolge, doch drückt sich das eventuell notwendige Umsortieren nur dadurch aus, daß für die hier relevanten Δ-Mengen nicht notwendig die kleinsten Elemente eine monotone Folge bilden.) Die gesuchten $g_1,\ldots,g_t$ entstehen nun so, daß man zu den g's der Induktionsvoraussetzung die Zahl $r+1$ als erstes Element hinzunimmt, und die Δ-Mengen entstehen aus den jetzt gefundenen durch Translation um 1 (wobei man zu Δ_1 noch 1 hinzufügen muß). Daß dann wirklich (1) bis (4) erfüllt sind, ist unschwer einzusehen. Beim Nachweis, daß Δ_1 keine zwei aufeinanderfolgenden Elemente enthält muß man sich an $r+1 \notin \Pi_1$, d.h. $1 \notin \tilde{\Pi}_1$ erinnern.

Der Fall $\Pi' = \{0\}$ erfordert nur geringe Modifikationen, insbesondere ist $\Delta_1 := \{1\}$ zu setzen.

(ii) Auch das wird durch Induktion gezeigt. $\Pi_1,\ldots,\Pi_s$ sei in kanonischer Reihenfolge und entstehe sowohl aus $(g_1,\ldots,g_t;\Delta_1,\ldots,\Delta_s)$ als auch aus $({g'}_1,\ldots,{g'}_{t'};{\Delta'}_1,\ldots,{\Delta'}_s)$. Dann ist $g_1 = {g'}_1$ die eindeutig bestimmte Zahl r, für die $\{0,\ldots,r\} \subset \Pi_1$, aber $r+1 \notin \Pi_1$. Konstruiere dann $\tilde{\Pi}_1,\ldots,\tilde{\Pi}_s$ wie im vorstehenden Beweis. Die dafür nach Induktionsannahme gesicherte Eindeutigkeit der Darstellung liefert sofort $(g_1,\ldots,g_t;\Delta_1,\ldots,Ds) =$
$({g'}_1,\ldots,{g'}_{t'};{\Delta'}_1,\ldots,{\Delta'}_s)$. □

Für alle, die von dem eher technischen Beweis verwirrt sind, folgt hier eine

Zusammenfassung:

Starte mit einer $(k_1,\ldots,k_s)$-Familie $\Pi_1,\ldots,\Pi_s$ (sie muß nicht in kanonischer Reihenfolge sein). $\sigma(1)$ sei das σ, für das $1 \in \Pi_\sigma$, und $g_1 - 1$ wird als dasjenige r definiert, für das $\{0,\ldots,r\} \subset \Pi_{\sigma(1)}$, aber $r+1 \notin \Pi_{\sigma(1)}$. Betrachte eine neue Familie $\Pi_1^{(2)},\ldots,\Pi_s^{(2)}$, wo $\Pi_{\sigma(1)}^{(2)} := \{i \in \Pi_{\sigma(1)} | i-1 \notin \Pi_{\sigma(1)}\}, \Pi_\sigma^{(2)} := \Pi_\sigma/g_1$ für $\sigma \neq \sigma(1)$ (dabei kann $\Pi_{\sigma(1)}^{(2)} = \{0\}$ sein). So wie $\sigma(1)$ und g_1 aus $\Pi_1,\ldots,\Pi_s$ entstanden, werden nun $\sigma(2)$ und g_2 aus $\Pi_1^{(2)},\ldots,\Pi_s^{(2)}$ gewonnen. Das Verfahren setze man fort, solange noch von $\{0\}$ verschiedene $\Pi_\sigma^{(\tau)}$ auftreten.

So erhält man $g_1,\ldots,g_t,\sigma(1),\ldots,\sigma(t)$. Setzt man noch $\Delta_\sigma :=$

$\{\tau|\sigma(\tau) = \sigma\}$, so ist das eine alternierende s-Zerlegung, und die vorgelegte Famile entsteht aus $(g_1, \ldots, g_t; \Delta_1, \ldots, \Delta_s)$.

Beispiel: Seien $\Pi_1 = (1100110011), \Pi_2 = (101000000000101)$.
Wir erhalten
$\sigma(1) = 1, g_1 = 2, \Pi_1^{(2)} = (10101), \Pi_2^{(2)} = (11000011)$;
$\sigma(2) = 2, g_2 = 2, \Pi_1^{(3)} = (111), \Pi_2^{(3)} = (1001)$;
$\sigma(3) = 1, g_3 = 3, \Pi_1^{(4)} = (0), \Pi_2^{(4)} = (11)$;
$\sigma(4) = 2, g_4 = 2, \Pi_1^{(5)} = (0), \Pi_2^{(5)} = (0)$.
Damit ist Π_1, Π_2 diejenige Familie, die aus $(2, 2, 3, 2; \{1, 3\}, \{2, 4\})$ entsteht.

Für den Fall $s = 2$ formulieren wir unsere Ergebnisse noch als

Korollar 3.4 *Es seien k_1, k_2, k_0 natürliche Zahlen mit $k_1 + k_2 = k_0$ sowie $\Pi_1 \subset \{0, \ldots, k_1\}, \Pi_2 \subset \{0, \ldots, k_2\}$ mit $1 \in \Pi_1$, so daß jedes $j \in \{0, \ldots, k_0\}$ eindeutig als $j = j_1 + j_2$ mit $j_1 \in \Pi_1, j_2 \in \Pi_2$ geschrieben werden kann. Dann gibt es $g_1, \ldots, g_t$ mit $g_1 \cdots g_t = k_0 + 1$, so daß*
$k_1 = (g_1 - 1) + (g_3 - 1)g_2g_1 + (g_5 - 1)g_4g_3g_2g_1 \cdots$,
$k_2 = (g_2 - 1)g_1 + (g_4 - 1)g_3g_2g_1 + (g_6 - 1)g_5g_4g_2g_3g_1 \cdots$.
Rekursiv erhält man k_1, k_2 so: Setze $k_1{}' := g_t - 1, k_1{}'' := 0, k_\tau{}' := g_{t-\tau+1}k_{\tau-1}{}'' + g_{t-\tau+1} - 1, k_\tau{}'' := g_{t-\tau+1}k_{\tau-1}{}'$ für $\tau = 2, \ldots, t$. Dann ist $(k_1, k_2) = (k_t{}', k_t{}'')$ oder $(k_1, k_2) = (k_t{}'', k_t{}')$, je nachdem, ob t gerade oder ungerade ist.

Das ist also die Lösung, die wir für Problem 1 anbieten können: Genau dann kann man einen fairen $(k_0 + 1)$-seitigen Würfel durch die Summe eines $(k_1 + 1)$-seitigen und eines $(k_2 + 1)$-seitigen Würfels simulieren, wenn k_1, k_2 wie vorstehend beschrieben aus einer multiplikativen Darstellung von $k_0 + 1$ entstehen.

4. Problem 2: Fälschen mit dem Ziel, die Summe fairer Würfel zu simulieren

Wir fixieren n, m, k mit $n + m = 2k$ und kümmern uns um die Existenz nichtnegativer a_i, b_j, so daß $A(x)B(x) = (1 + a_1x + \cdots + a_{n-1}x^{n-1})(1 + b_1x + \cdots + b_{m-1}x^{m-1}) = (1 + x + \cdots + x^{k-1})^2$; den trivialen Fall $n = m = k, a_i = b_j = 1$ wollen wir dabei nicht berücksichtigen. Beispiele für solche Situatiuonen liefert Kapitel 3: Ist $1 + x + \cdots + x^{k-1} = A_0(x)B_0(x)$ mit nichttrivialen $A_0(x), B_0(x)$, so ist $(A_0(x))^2, (B_0(x))^2$ eine zulässige Wahl für $A(x), B(x)$ in der hier vorliegenden Situation. Die Identität $(1+x)(1+x^2) = 1+x+x^2+x^3$ etwa ergibt eine Möglichkeit, die Summe von zwei fairen vierseitigen Würfel als Summe gefälschter Würfel (mit drei bzw. fünf Flächen) zu simulieren. So werden sicher nicht alle $A(x), B(x)$ entstehen (insbesondere keine Beispiele im Fall $n = m$), und deswegen muß das Problem noch etwas näher analysiert werden, um zu einer allgemeinen Beweisstrategie zu kommen.

Dazu erinnern wir uns daran, daß die Nullstellen von $A(x)$ und $B(x)$ k-te Einheitswurzeln sind und daß mit jedem ζ auch $\overline{\zeta}$ Nullstelle sein muß. Schreibt man also $1 + x + \cdots + x^{k-1}$ als Produkt $(1 - \eta_1 x + x^2)(1 - \eta_2 x + x^2)\cdots(1 - \eta_l x + x^2)(1 + x)$ (der letzte Faktor tritt nur dann auf, wenn k gerade ist), so werden $A(x)$ und $B(x)$ ebenfalls aus derartigen Faktoren zusammengesetzt sein, und insgesamt – für $A(x)$ und $B(x)$ zusammen – muß jedes der Polynome $1 - \eta_1 x + x^2, 1 - \eta_2 x + x^2, \ldots, 1 - \eta_l x + x^2$ (und evtl $1 + x$) genau zweimal aufgetreten sein.

Unser Problem lautet also wie folgt: Sei $k \in \mathbb{N}$ und $\zeta_j := \exp(2\pi j/k)$ für $j = 1, \ldots, k-1$. Wir setzen $\eta_j := \zeta_j + \overline{\zeta_j}$ und $l := k/2 - 1$ bzw. $l := (k-1)/2$ für gerades bzw. ungerades k. Ist dann die Folge $1 - \eta_1 x + x^2, 1 - \eta_1 x + x^2, \ldots, 1 - \eta_l x + x^2, 1 - \eta_l x + x^2$ (die für gerades k noch um $1 + x, 1 + x$ fortzusetzen ist) *so* disjunkt in zwei Teile zu zerlegen, daß beim Ausmultiplizieren Polynome $(n-1)$–ten und $(m-1)$-ten Grades mit nichtnegativen Koeffizienten entstehen?

Wie man zeigen kann, daß das für "kleine" n, m, k nur auf die triviale Weise geht, wird später im Beweis von Theorem 4.2 erläutert werden. Ansonsten sind Beispiele für nichttriviale Zerlegungen leicht durch Ausprobieren zu finden, etwa im Fall $k = 6, n = 8, m = 4$: $1 + 2x + \cdots + 2x^9 + x^{10} = (1 + 2x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 2x^6 + x^7)(1 + x^3) = (1 + x^2 + x^3 + x^4 + x^5 + x^7)(1 + 2x + 2x^2 + x^3)$. Verzichtet man auf die Bedingung $n = m$, so scheint es für jedes k zahlreiche $A(x), B(x)$ zu geben; das legen jedenfalls die mit Computerhilfe gefundenen Ergebnisse nahe, Beweise gibt es dazu vorläufig nicht. Die Suche wird dabei durch folgende Beobachtung etwas eingeschränkt: Ist k ungerade, so sind nur quadratische Faktoren zu berücksichtigen, d. h. auch n und m müssen ungerade sein; und ist k gerade, so müssen $A(x), B(x)$ beide den Faktor $1 + x$ enthalten, denn andernfalls könnten keine Polynome ungeraden Grades entstehen.

Wir betrachten nun nur noch den Fall $n = m = k$. ζ, ζ' seien zwei benachbarte, nicht-reelle k-te Einheitswurzeln, und $\eta := \zeta + \overline{\zeta}, \eta' := \zeta' + \overline{\zeta'}$.

Dann ist $1+x+\cdots+x^{k-1} = (1-\eta x+x^2)(1-\eta' x+x^2)C_0(x)$ für ein geeignetes Polynom $C_0(x)$. Wir werden versuchen, $A(x)$ und $B(x)$ als $(1-\eta' x+x^2)(1-\eta' x+x^2)C_0(x)$ und $(1-\eta x+x^2)(1-\eta x+x^2)C_0(x)$ zu definieren. Dann ist klar, daß beide Polynome Grad $k-1$ haben und daß $A(x)B(x)$ auf nicht-triviale Weise $(1+x+\cdots+x^{k-1})^2$ darstellt. Warum aber sollten die Koeffizienten nicht-negativ sein. Betrachten wir etwa $A(x)$. Es ist doch, wenn wir $C(x) := (1-\eta' x+x^2)C_0(x), \epsilon := \eta' - \eta$ setzen, $A(x) = (1-(\eta+\epsilon)x+x^2)C(x)$, und $(1-\eta x+x^2)C(x) = 1+x+\cdots+x^{k-1}$ *hat* nichtnegative Koeffizienten. Für "kleines" ϵ, d. h. "großes" k, sollten dann aus Stetigkeitsgründen auch in $A(x)$ keine negativen Koeffizienten vorkommen.

Dieses Störungsargument wollen wir etwas präzisieren. Dazu fixieren wir das bisherige ζ, setzen wie bisher $\eta := \zeta + \overline{\zeta}$ und schreiben das dann auftretende $C(x)$ als $1 + c_1 x + \cdots + c_{k-4}x^{k-4} + x^{k-3}$.

Im Polynom $(1-\eta x+x^2)C(x)$ sind alle Koeffizienten 1 , und wir möchten, daß sie in $(1-(\eta+\epsilon)x+x^2)C(x)$ nichtnegativ sind. Das läuft auf $\epsilon c_j \leq 1$ hinaus, und damit ist zu hoffen, daß wir eine Abschätzung für die $|c_j|$ finden können, die es uns gestattet, $|(\eta-\eta')c_j| \leq 1$ zu beweisen.

Zunächst ist nicht klar, waraum das gehen sollte: Für große k kann zwar $\eta-\eta'$ als beliebig klein angenommen werden, doch könnten die c_j gleichzeitig zu groß werden. Daß die Idee aber dennoch zu verwirklichen ist, wird durch das folgenden Lemma vorbereitet:

Lemma 4.1

(i) *Es gilt* $c_j = \frac{\zeta^2}{(1-\zeta)(\overline{\zeta}-\zeta)}\zeta^j + \frac{\overline{\zeta}^2}{(1-\overline{\zeta})(\zeta-\overline{\zeta})}\overline{\zeta}^j + \frac{1}{(1-\zeta)(1-\overline{\zeta})}$ *für* $j = 0, \ldots$.

(ii) *Die* c_j *liegen im Intervall* $[\frac{1}{2-\eta} - \frac{2}{(2-\eta)\sqrt{2+\eta}}, \frac{1}{2-\eta} + \frac{2}{(2-\eta)\sqrt{2+\eta}}]$. *Insbesondere sind die* $|c_j|$ *durch* $\varphi(\eta) := \frac{1}{2-\eta} + \frac{2}{(2-\eta)\sqrt{2+\eta}}$ *beschränkt.*

Beweis:

(i) Durch Koeffizientenvergleich folgt rekursiv: $c_0 = 1, c_1 = 1+\eta, c_2 = 1+\eta c_1, c_3 = 1+\eta c_2 - c_1, \ldots, c_j = 1+\eta c_{j-1} - c_{j-2}$, wobei wir den letzten Ausdruck nach der Festsetzung $c_{-1} = c_{-2} = 0$ für alle j verwenden dürfen.

Die behauptete Gleichung ist nun leicht zu erledigen: Man definiere d_j als den rechts stehenden Ausdruck und rechne direkt nach, daß $d_{-1} = d_{-2} = 0, d_j = 1+\eta d_{j-1} - d_{j-2}$; klar daß dann $d_j = c_j$ für alle j gelten muß.

Interessanter als der vorstehende Beweis ist der Weg, wie die Formel gefunden wurde. Hier eine Skizze: Ich habe für jedes j den Vektor $w_j := \binom{c_{j+1}}{c_j}$ betrachtet und dann $w_{j+1} = Mw_j + \binom{1}{0}$ als Rekursionsformel erhalten, wobei M die Matrix $\begin{pmatrix} \eta & 1 \\ -1 & 0 \end{pmatrix}$ bezeichnet. Alles läuft dann auf die Bestimmung von $(E+M+M^2+\cdots+M^{j-1})\binom{1}{0}$ hinaus, und dafür wurde die Formel für die geometrische Reihe angewandt: $(E-M^j)(E-M)^{-1}\binom{1}{0}$. Dabei darf $E-M$ wirklich invertiert werden, denn die Determinante ist $2-\eta>0$. Nun sind die Eigenwerte von M gerade die Zahlen $\zeta,\overline{\zeta}$. Also kann M auf Hauptachsen transformiert werden, und die Einträge der M^j kann man leicht durch $\zeta^j,\overline{\zeta}^j$ ausdrücken.

(ii) Mit $\xi := \frac{2\zeta^2}{(1-\zeta)(\overline{\zeta}-\zeta)}$ besagt (i), daß c_j der um $\frac{1}{(1-\zeta)(1-\overline{\zeta})} = 1/(2-\eta)$ verschobene Realteil von $\xi\zeta^j$ ist. (Das läßt übrigens eine interessante Interpretation zu: Die c_j sind die Realteile von gewissen oder allen Punkten eines regulären k-Ecks, das $1/(2-\eta)$ als Mittelpunkt und $2|\xi|$ als Durchmesser hat; wieviele Ecken dabei wirklich auftreten, hängt davon ab, wieviele verschiedene ζ^j vorkommen.)

Folglich liegt c_j im Intervall $[1/(2-\eta)-|\xi|, 1/(2-\eta)+|\xi|]$, und die Behauptung folgt aus $|\xi| = \frac{2}{(2-\eta)\sqrt{2+\eta}}$. □

Als Folgerung aus dem Lemma und den vorstehenden Überlegungen erhalten wir so Teil (i) des folgenden Theorems, durch das Problem 2 im Fall $n=m$ vollständig gelöst wird;

Theorem 4.2

(i) *Es gebe zwei nichtreelle k-te Einheitswurzeln ζ,ζ' so, daß die Zahlen $\eta := \zeta+\overline{\zeta}, \eta' := \zeta'+\overline{\zeta'}$ verschieden sind und $|\varphi(\eta)|, |\varphi(\eta')| \leq 1/|\eta-\eta'|$ gilt. Dann ist Problem 2 nichttrivial lösbar.*

(ii) *Diese Bedingung ist für alle $k\geq 12$ erfüllt.*

(iii) *Auch für $k=10$ läßt sich das Problem auf die angegebene Weise lösen, auch wenn die Abschätzung in (i) für keine Wahl von ζ,ζ' gilt.*

(iv) *Für die noch verbleibenden k gibt es keine nichttrivialen Lösungen.*

Zusammen: Man kann die Summe zweier Gleichverteilungen auf $\{0,\ldots,k-1\}$ nichttrivial als Summe von Verteilungen auf $\{0,\ldots,k-1\}$ genau dann erzeugen, wenn k nicht zur Menge $\{1,\ldots,9,11\}$ gehört.

Beweis: Für den Nachweis von (ii) bemerken wir zunächst, daß φ auf $[-1,2[$ monoton steigt, da die Ableitung dort positiv ist. Insbesondere gilt für $-1\leq\eta\leq 0$ die Abschätzung $\varphi(\eta)\leq\varphi(0)=(1+\sqrt{2})/2$.

Wir wollen nun eine untere Schranke für die k suchen, so daß folgende Konstruktion möglich ist: Man findet zwei benachbarte k-te Eineitswurzeln

$\zeta, \overline{\zeta}'$, so daß für die zugehörigen η, η' sowohl $\eta, \eta' \in [-1, 0]$ als auch $|\eta - \eta'| \leq 2/(1 + \sqrt{2})$ gilt.

Sind ζ und ζ' die l-te und die $(l+1)$-te k-te Einheitswurzel, so ist $|\eta - \eta'| = 2|\cos(2\pi l/k) - \cos(2\pi(l+1)/k| \leq 4\pi/k$, wobei wir für die Abschätzung den Mittelwertsatz verwendet haben. So erhalten wir die Bedingung $k \geq 2\pi(1 + \sqrt{2}) \approx 15.17$, und folglich ist (i) für alle $k \geq 16$ erfüllt.

Die verbleibenden Fälle werden durch konkrete Rechnung erledigt: Für $k = 12, 13, 14, 15$ ist die Bedingung (i) erfüllt, wenn wir sie jeweils auf die 4-te und 5-te k-te Einheitswurzel anwenden. Für $k = 10$ ist (i) nicht erfüllbar. Trotzdem kann man auch hier durch die gleiche Idee eine nichttriviale Darstellung von $(1+x+\cdots+x^9)^2$ als Produkt zweier Polynome 5-ten Grades gefunden werden: Man muß nur ζ, ζ' als 3-te und 4-te 10-te Einheitswurzeln wählen (explizit ist das in [10] ausgerechnet).

Der Nachweis von (iv) könnte ebenfalls einem Computer anvertraut werden (und das ist sicherheitshalber auch wirklich geschehen), läßt sich mit etwas Geduld aber auch ohne Rechnerhilfe führen. Als Beispiel betrachten wir $k = 8$: Lassen sich $1 - \sqrt{2}x + x^2, 1 - \sqrt{2}x + x^2, 1 + x^2, 1 + x^2, 1 + \sqrt{2}x + x^2, 1 + \sqrt{2}x + x^2, 1 + x, 1 + x$ zu zwei Polynomen $A(x), B(x)$ 7-ten Grades mit nichtnegativen Koeffizienten zusammenfassen, so daß beide von $1 + x + \cdots + x^7$ verschieden sind? Angenommen, so eine Zerlegung würde existieren. Da der Grad jeweils 7 ist, muß $1 + x$ Faktor von $A(x)$ und $B(x)$ sein, andererseits muß mindestens einer der irreduziblen Faktoren in $A(x)$ oder $B(x)$ quadratisch vorkommen, denn sonst würde der triviale Fall vorliegen. Die Möglichkeit, daß $(1 - \sqrt{2}x + x^2)^2$ als Faktor vorkommt, scheidet aus, denn sowohl in $(1 - \sqrt{2}x + x^2)^2(1 + x^2)(1 + x)$ als auch in $(1 - \sqrt{2}x + x^2)^2(1 + \sqrt{2}x + x^2)(1 + x)$ gibt es negative Koeffizienten. Würde schließlich $(1 + \sqrt{2}x + x^2)^2$ in (zum Beispiel) $A(x)$ vorkommen, so wäre $B(x) = (1 - \sqrt{2}x + x^2)^2(1 + x^2)(1 + x)$ oder $= (1 - \sqrt{2}x + x^2)(1 + x^2)^2(1 + x)$, und in beiden Fällen treten negative Koeffizienten auf. □

5. Einige Ergänzungen und Probleme

Die hier behandelten Probleme kamen in der Verkleidung der gefälschten Würfel daher. Wie schon erwähnt, ist das ein Spezialfall der allgemeineren Fragestellung, ob und wie man vorgelegte Zufallsvariable als Summen unabhängiger Zufallsvariablen schrieben kann. Das ist fundamental wichtig, wenn man Grenzwertsätze der Wahrscheinlichkeitsrechnung systematisch studieren möchte.

Manipulierte Würfel trifft man aber auch noch an anderen Stellen in der Literatur. Man kann etwa die hier betrachteten Probleme variieren, indem man andere Beschriftungen der Würfel zuläßt ([5], Problem IV.1). Interessant ist in diesem Zusammenhang auch das folgende Paradoxon. Dazu betrachten wir faire Würfel W, W' (jede Seite soll also mit gleicher Wahrscheinlichkeit gewürfelt werden), auf deren Seiten Zahlen stehen. Wir nennen W *günstiger* als W' (Schreibweise: $W \succ W'$), wenn die Wahrscheinlichkeit, daß W ein größeres Ergebnis als W' anzeigt, größer als 0.5 ist. Paradox ist nun, daß günstiger" nicht transitiv ist. Zum Beispiel: Man kann die Zahlen von 1 bis 18 so auf den Flächen dreier gewöhnlicher Würfel W, W', W'' verteilen, daß $W \succ W' \succ W'' \succ W$. Weitere Informationen dazu findet man in [11].

Schließlich soll noch auf [2] hingewiesen werden, wo in verschiedenen Artikeln zum Thema "Zufall" auch mehrfach vom gefälschten Würfel die Rede ist.

Es folgen nun einige Ergänzungen zu den Problemen dieser Arbeit. Zunächst zu Problem 1. Da kann man sich etwa fragen, wie es mit der Eindeutigkeit der Fälschungsmöglichkeiten aussieht. In Abhängigkeit von den zahlentheoretischen Eigenschaften von k_0, k_1, k_2 kann das sehr unterschiedlich sein. So liefert etwa eine systematische Rechnung für $k_0 = 11$, daß es verschiedene $(3, 8)$-Familien, aber nur eine $(5, 6)$-Familie gibt. Man kann die Rekursionsformel aus Korollar 3.4 heranziehen um einzusehen, daß für alle k_0, für die 12 Teiler von $k_0 + 1$ ist, k_1, k_2 mit $k_1 + k_2 = k_0$ so existieren, daß es zwei verschiedene (k_1, k_2)-Familien gibt. (Beweisidee: Aus der Rekursionsformel folgt, daß eine Darstellung von $k_0 + 1$ als $2 \cdot 2 \cdot 3 \cdots$ zu (k_2, k_1) führt, wenn die Darstellung $4 \cdot 3 \cdots$ das Ergebnis (k_1, k_2) geliefert hat. Für $36|(k_0 + 1)$ gilt sogar: $9 \cdot 4 \cdots$ führt zum gleichen Ergebnis wie $3 \cdot 2 \cdot 2 \cdot 3 \cdots$, und gilt $150|(k_0 + 1)$, so erzeugen $5 \cdot 5 \cdot 6 \cdots$ und $10 \cdot 3 \cdot 5 \cdots$ das gleiche (k_1, k_2)-Paar.) So gibt es eine Reihe von – mit Computerhilfe – leicht zu entdeckenden Phänomenen, die mit Teilbarkeitseigenschaften zusammenhängen, für die ich aber keine allgemeine Lösung anzubieten habe.

Man kann sich auch fragen, ob Fälschen "oft" möglich ist: Für wieviele k_1, k_2 mit $k_1 + k_2 = k_0 \leq k'$ gibt es (k_1, k_2)-Familien? Ich konnte zeigen, daß der Anteil für k' gegen Unendlich gegen Null geht (der Beweis ist etwas technisch, deswegen soll er hier nicht ausgeführt werden).

Nun zu Problem 2. Da wäre interessant zu wissen, wie man bei gegebenen k, m, n mit $m + n = 2k$ leicht entscheiden kann, ob das Problem für diese Konstellation lösbar ist oder nicht. In Kapitel 4 habe ich schon einige Beobachtungen zusammengestellt, eine systematische Untersuchung steht aber noch aus.

Mit den hier entwickelten Methoden kann auch – wenigstens im Prinzip – ein allgemeineres Problem behandelt werden: Die Summe von r Würfeln mit jeweils k Seiten soll die Summe aus r fairen Würfeln simulieren (Beschriftung auf allen Würfeln von 0 bis $k-1$). Geht das nur auf die triviale Weise? Die zu erwartende Übersetzung ist natürlich die Frage, ob man anders als auf triviale Weise $(1 + x \cdots + x^{k-1})^r$ als Produkt von Polynomen $(k-1)$-ten Grades mit nichtnegativen Koeffizienten schreiben kann. (Man könnte auch – in leichter Verschärfung – verlangen, daß keines der Polynome gleich $1 + x + \cdots + x^{k-1}$ ist). Für "kleine" k zeigen Überlegungen in Analogie zum Beweis von Theorem 4.2(iv), daß das nicht gehen kann. Und für "große" k kann wieder die Technik aus Kapitel 4 verwendet werden.

> Im Fall $r = 3$ etwa muß man jetzt von *drei* benachbarten k-ten Einheitswurzeln ζ, ζ', ζ'' ausgehen und mit den zugehörigen η-Werten das Polynom $1 + x + \cdots + x^{k-1}$ als $(1 - \eta x + x^2)(1 - \eta' x + x^2)(1 - \eta'' x + x^2)D(x)$ schreiben. Für die Polynome $(1 - \eta x + x^2)^2(1 - \eta' x + x^2)D(x), (1 - \eta x + x^2)(1 - \eta'' x + x^2)^2 D(x), (1 - \eta' x + x^2)^2(1 - \eta'' x + x^2)D(x)$ kann man dann durch das gleiche Störungsargument wie vorher nachweisen, daß für genügend großes k nichtnegative Koeffizienten zu erwarten sind.

Etwas präziser ausgedrückt heißt das: Zu jedem r gibt es ein K_r, so daß sich für jedes $k \geq K_r$ Summen von r echt gefälschten Würfeln wie Summen fairer Würfel verhalten können. Der Beweis liefert noch, daß K_r als $(r-1)16$ gewählt werden kann. Die verbleibenden k in $\{1, \ldots, K_r - 1\}$ müssen mit Computerhilfe jeweils gesondert untersucht werden.

Abschließend soll darauf hingewiesen werden, daß man beide Probleme im Prinzip auch für andere Verteilungen als die Gleichverteilung untersuchen kann. Die Verallgemeinerung von Problem 2 lautet so: $P(x) = p_0 + p_1 x + \cdots + p_{k-1} x^{k-1}$ sei ein Polynom mit nichtnegativen Koeffizienten. Kann man $(P(x))^2$ in nichttrivialer Weise als $A(x)B(x)$ durch zwei Polynome $(k-1)$-ten Grades mit ebenfalls nichtnegativen Koeffizienten darstellen? Das hängt in naheliegender Weise von der Nullstellenverteilung von $P(x)$ ab. Haben zum Beispiel alle Nullstellen nichtpositiven Realteil, so gibt es eine Fülle von Möglichkeiten für die Wahl von $A(x)$ und $B(x)$. Andererseits kann es etwa bei beliebig großem k keine nichttrivialen Zerlegungen für $(1+x^{k-1})^2$ geben. Es wäre interessant zu wissen, welche Eigenschaften der Nullstellen verantwortlich sind. Dabei wird es sich im allgemeinen nicht nur um Einheitswurzeln handeln, und deswegen stehen die in dieser Arbeit verwendeten Techniken nicht zur Verfügung.

LITERATURHINWEISE

[1] P. BILLINGSLEY. *Probability and Meeasure.* John Wiley and Sons (1995).

[2] I. EKELAND. *The broken dice.* University of Cicago Press (1993).

[3] M. KRASNER, B. RANULAC. *Sur une proprieté du polynomes de division du cercle.* C. R. Acad. Sc. Paris **204** (1937),397-399.

[4] G. LETAC. *Problèmes de probabilité.* Presses universitaires de France, Paris (1970).

[5] G. LETAC. *Integration and probability by P. Malliavin.* Springer Verlag, New York, Berlin, Heidelberg (1995), .

[6] V. LINNIK. *Decomposition of probability distributions.* Oliver&Boyd, London (1964).

[7] V. LINNIK, L. OSTROVSKI. *Decomposition of random variables and vectors.* AMS, Translations of MAth. Monographs **48** (1977).

[8] E. LUKACZ. *Developments in characteristic function theory.* Charles Griffin&Company, London (1983).

[9] D. A. RAIKOV. *One property of cyclotomic polynomials.* Matem. sb. **2/44** (1937),379-382 .

[10] L. ROBERTSON, R. SHORTT, S. LANDRY. *Dice with fair sum.* Am. Math. Monthly **95** (1988), 316-328.

[11] G. SZEKELY. *Paradoxes in probability theory and mathematical statistics.* Reidel Publishing Comp., Boston (1986).

I. Mathematisches Institut, Freie Universität Berlin, Arnimallee 2–6,
D-14195 Berlin, Germany; e-mail: behrends@math.fu-berlin.de