Faire Entscheidungen

Ehrhard Behrends

1. Einleitung

Mal angenommen, zwei Freunde sind völlig unentschlossen, was sie mit dem Abend anfangen sollen: Konzert oder Theater?. Eine Münze zu werfen scheidet aus, denn sie wollen selbst aktiv an der Entscheidung mitwirken, und beide sollen gleichberechtigt beteiligt sein. Sie haben die folgende Idee: Auf Kommando heben beide jeweils eine Hand, wobei "zufällig" null, eins,..,fünf Finger ausgestreckt werden (der Einfachheit halber wird der Daumen zum Finger erklärt). Es soll dann die Summe gebildet werden; ist sie gerade, geht es ins Konzert, andernfalls ist Theater angesagt.

Erfüllt das Verfahren die Erwartungen? Mathematisch übersetzt ist das doch die Frage, ob $X+Y \bmod 2$ gleichverteilt ist, wenn X, Y unabhängige, in $\{0, \ldots, 5\}$ gleichverteilte Zufallsvariable sind. (Für den Augenblick wollen wir annehmen, daß diese Umschreibung gerechtfertigt ist, wir kommen in Kapitel 4 darauf zurück.)

Die Antwort ist leicht gegeben, man muß nur alle Möglichkeiten, 0 bis 5 Finger zu heben, systematisch zusammenstellen, allen die gleiche Wahrscheinlichkeit (also 1/36) zuordnen und dann sortieren, welche zu einer geraden bzw. ungeraden Summe führen. Da es jeweils 18 Möglichkeiten gibt, sind beide Wahrscheinlichkeiten gleich 0.5, die Freunde können also mit dem Verfahren zufrieden sein.

Bei einer anderen Gelegenheit wollen die beiden auf ähnliche Weise eine faire Entscheidung zwischen *drei* Alternativen treffen, und das klappt genauso, wenn man nun modulo 3 rechnet. Weitere Verallgemeinerungen bieten sich an, wir formulieren gleich diejenige Fragestellung, von der wir hier ausgehen werden. Gegeben seien natürliche Zahlen k, n und a sowie Wahrscheinlichkeitsmaße $P_1, \ldots, P_k$ auf $\{0, \ldots, n-1\}$. Wir stellen uns die $P_1, \ldots$ als Verteilungen unabhängiger Zufallsvariablen $X_1, \ldots$ vor, d. h. $P(X_\kappa = \nu) = P_\kappa(\{\nu\})$, und dann fragen wir nach der Verteilung von $(X_1 + \cdots + X_k) \bmod a$, also nach den Zahlen $Q(\{\alpha\}) := P((X_1 + \cdots +$

X_k) mod $a = \alpha$) für $\alpha = 0, \ldots, a-1$. In der einleitend gegebenen Interpretation heißt das: k Freunde wollen eine faire Entscheidung zwischen a Alternativen treffen, und sie machen das so, daß sich der κ-te Teilnehmer gemäß P_κ für eine Zahl zwischen 0 und $n-1$ entscheidet, dann werden diese k Zahlen addiert und modulo a ausgewertet.

Es gibt in diesem Zusammenhang einige Fragen, die wir nachstehend behandeln wollen (die Übersetzungen in Probleme zur Freunde-treffen-Entscheidungen-Situation sind naheliegend).

Problem 1: Angenommen, alle P_κ sind die Gleichverteilung auf $\{0, \ldots, n-1\}$. Für welche k, a ist dann Q die Gleichverteilung auf $\{0, \ldots, a-1\}$?

Problem 2: Kann Q auch dann die Gleichverteilung sein, wenn die P_κ *nicht* gleichverteilt sind? Wie sieht das insbesondere im Fall $P_1 = \cdots = P_k$ aus?

Problem 3: Es sei $k = 2$, und P_1 sei vorgegeben. Ist es dann möglich, ein P_2 so zu finden, daß Q die Gleichverteilung ist? Sind auch mehrere Lösungen denkbar?

Problem 1 kann übrigens – wie im oben besprochenen Spezialfall $n = 6$, $k = a = 2$ – in ein kombinatorisches Problem umformuliert werden. Allerdings sehen die dann entstehenden Ausdrücke nur für kleine k, a halbwegs übersichtlich aus, allgemeine Aussagen scheinen so nicht zu gewinnen zu sein. Deswegen werden die Probleme hier ganz anders behandelt, es soll nämlich die Gelegenheit genutzt werden, anhand dieser elementaren Fragestellung einige *Ideen der harmonischen Analysis* kennenzulernen und anzuwenden. Das wird in *Kapitel 2* ausgeführt. Dort wird gleich eine etwas allgemeinere Situation diskutiert, nämlich das Problem der Auswahl im Fall endlicher kommutativer Gruppen (bisher war nur von der $\mathbb{Z}_n$ die Rede). Mit Hilfe der Fouriertransformation können alle aufgeworfenen Probleme vollständig gelöst werden. In *Kapitel 3* dann geht es um beliebige endliche Gruppen, dabei werden Darstellungen und deren Fouriertransformation wichtig. Da wir die Theorie nicht voll entwickeln können, beweisen wir die Ergebnisse unter der – im Einzelfall oft leicht nachprüfbaren Voraussetzung – daß es "genügend viele" Darstellungen gibt. So zeigt sich, daß die unterschiedlichen Phänomene in den Fällen kommutativer bzw. nicht-kommutativer Gruppen durch das unterschiedliche Verhalten von komplexen Zahlen bzw. komplexen Matrizen verursacht werden. Die Arbeit schließt in *Kapitel 5* mit einigen Ergänzungen.

Die zum Verständnis benötigte Mathematik ist elementar, außer grundlegenden Kenntnissen über komplexe Zahlen und Matrizen wird nichts vom Leser erwartet.

2. Der Fall endlicher kommutativer Gruppen

Zunächst geben wir eine natürliche Verallgemeinerung der vorstehenden Überlegungen an: Sei G eine endliche, additiv geschriebene abelsche Gruppe. Wir stellen uns das folgende Problem: Von k "Mitspielern" soll ein Element g aus G so ausgewählt werden, daß alle g die gleiche Wahrscheinlichkeit haben. Das soll so geschehen, daß k Wahrscheinlichkeitsmaße $P_1, \ldots, P_k$ auf G bestimmt werden, und dann werden k Elemente $g_1, \ldots, g_k$ unabhängig so gefunden, daß jeweils g_κ wie P_κ verteilt ist; anschließend wird $g = g_1 + \cdots + g_k$ betrachtet. Bezeichne mit Q wieder die zugehörige Summen-Wahrscheinlichkeit, also $Q(\{g\})$:="Wahrscheinlichkeit, daß bei diesem Verfahren g ausgewählt wird" (eine Formel für Q folgt gleich). Wir wollen dann wissen, unter welchen Bedingungen an die P_κ man zu $Q = U$(=Gleichverteilung) kommt.

Dazu rechnen wir zunächst Q aus. Wir beschränken uns auf den Fall von zwei Wahrscheinlichkeitsmaßen $P, \tilde{P}$, eine Formel für k Maße folgt daraus durch Iteration.

Die Wahrscheinlichkeit, daß ein g_0 speziell als $g + \tilde{g}$ entsteht, ist – Unabhängigkeit der Auswahl vorausgesetzt – $P(\{g\})\tilde{P}(\{\tilde{g}\})$. Nun sind noch die Wahrscheinlichkeiten aller dieser Darstellungsmöglichkeiten zu addieren. Jedes g kann auftreten, und $\tilde{g}$ ist dann gleich $g_0 - g$; insgesamt erhalten wir so $Q(\{g_0\}) = \sum_g P(\{g\})\tilde{P}(\{g_0 - g\})$. Statt Q werden wir $P * \tilde{P}$ schrebien und von der *Faltung* der Wahrscheinlichkeitsmaße $P, \tilde{P}$ sprechen.

Es geht also um Faltungsgleichungen, insbesondere um die Bestimmung von $P_1, \ldots, P_k$ mit $P_1 * \cdots * P_k = U$. Und das wollen wir mit Methoden der harmonischen Analysis behandeln, durch die – im hier betrachteten kommutativen Fall – alles in Fragen über komplexe Zahlen transformiert wird.

Zunächst eine Definition: Eine Abbildung $\chi : G \to \Gamma := \{z \mid z \in \mathbb{C}, |z| = 1\}$ heißt ein *Charakter*, wenn stets $\chi(g + g') = \chi(g)\chi(g')$ gilt. Wir benötigen die folgenden Eigenschaften von Charakteren:

Lemma 2.1

(i) *χ sei ein Charakter, χ sei* nicht *die Konstante* 1. *Dann ist* $\sum_g \chi(g) = 0$.

(ii) *Sind* χ_1, χ_2 *verschiedene Charaktere, so ist* $\sum_g \chi_1(g)/\chi_2(g) = 0$.

(iii) $\chi_1, \dots, \chi_l$ *seien paarweise verschiedene Charaktere. Dann sind sie linear unabhängig im* $\mathbb{C}-$ *Vektorraum der Abbildungen von* G *nach* $\mathbb{C}$*. Insbesonder kann es höchstens* $\mathrm{card}(G)$ *verschiedene Charaktere geben.*

Beweis: (i) Wähle g_0 mit $\chi(g_0) \neq 1$. Da $\{g + g_0 \mid g \in G\}$ mit G übereinstimmt, ist $\sum_g \chi(g) = \sum_g \chi(g + g_0) = \chi(g_0) \sum_g \chi(g)$, also $\sum_g \chi(g) = 0$.

(ii) Beachte, daß χ_1/χ_2 Charakter ist. Wende dann (i) an.

(iii) $a_1, \dots, a_l \in \mathbb{C}$ seien gegeben, so daß $\sum_{\lambda=1\dots,l} a_\lambda \chi_\lambda(g) = 0$ für alle g. Wir teilen die Gleichung durch $\chi_{\lambda_0}(g)$ und summieren über g. (ii) ergibt $0 = \sum_\lambda a_\lambda (\sum_g \chi_\lambda(g)/\chi_{\lambda_0}(g)) = a_{\lambda_0} \mathrm{card}(G)$. □

Es gibt also stets höchsten $\mathrm{card}(G)$ Charaktere. Man kann zeigen, daß diese Zahl immer erreicht wird (für dieses und andere Ergebnisse der harmonischen Analysis vgl. [1],[4],[5]). Der Beweis würde hier zu weit führen, daher werden wir diese Tatsache immer als (eigentlich überflüssige) Extra-Voraussetzung aufnehmen. Bei konkret gegebenem G ist sie in der Regel leicht nachprüfbar. Für die Gruppe $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, die zur Motivation aus Kapitel 1 gehört, sind offensichtlich $\chi_j : \mathbb{Z}_n \to \Gamma, \chi_j(l) := \exp(2\pi jl/n)(j = 0, \dots, n-1)$ paarweise verschiedene Charaktere.

Mit Charakteren können Faltungsgleichungen in Skalargleichungen umgeformt werden. Sei dazu P ein Wahrscheinlichkeitsmaß auf G. Wir definieren – für Charaktere χ – die komplexe Zahl $\hat{P}(\chi)$ als $\sum_g P(\{g\})\chi(g)$ (Achtung: in manchen Büchern wird hier $\bar{\chi}(g)$ statt $\chi(g)$ eingesetzt).

$\hat{P}$ ist eine auf der Menge $\hat{G}$ der Charaktere definierte komplexwertige Abbildung, die die *Fouriertransformation* von P genannt wird.

Lemma 2.2 *Wir setzen voraus, daß es* $\mathrm{card}(G)$ *paarweise verschiedene Charaktere auf* G *gibt.*

(i) *Sind* P_1, P_2 *Wahrscheinlichkeitsmaße auf* G *mit* $\hat{P}_1 = \hat{P}_2$*, so gilt* $P_1 = P_2$.

(ii) *Für Wahrscheinlichkeitsmaße* P_1, P_2 *ist* $\widehat{P_1 * P_2} = \hat{P}_1 \hat{P}_2$.

(iii) *Für die Gleichverteilung* U *gilt* $\hat{U} = \delta$*, wobei* δ *durch* $\delta(\chi) := 1$ *bzw.* $:= 0$ *für* $\chi = 1$ *bzw.* $\chi \neq 1$ *erklärt ist.*

Beweis: (i) Die lineare Hülle der χ ist nach Voraussetzung und Lemma 2.1(iii) n-dimensional und enthält folglich *alle* Funktionen von G nach $\mathbb{C}$. Wähle bei vorgegebenem g_0 eine Linearkombination der Charaktere so, daß die Indikatorfunktion von $\{g_0\}$ entsteht; es soll also $\sum_j a_j\chi_j(g) = 1$ bzw. $= 0$ sein, wenn $g = g_0$ bzw. $g \neq g_0$ ist. Multipliziert man dann die nach Voraussetzung bestehenden Gleichungen $\sum_g P_1(\{g\})\chi_j(g) = \sum_g P_2(\{g\})\chi_j(g)$ mit a_j und summiert auf, so folgt $P_1(\{g_0\}) = \sum_g P_1(\{g\})(\sum_j a_j\chi_j(g)) = \sum_g P_2(\{g\})(\sum_j a_j\chi_j(g)) = P_2(\{g_0\})$.

(ii) Sei χ ein beliebiger Charakter.

$$
\begin{aligned}
(\widehat{P_1 * P_2})(\chi) &= \sum_{g_0}(P_1 * P_2)(\{g_0\})\chi(g_0) \\
&= \sum_{g_0}\sum_{g} P_1(\{g\})P_2(\{g_0 - g\})\chi(g_0) \\
&= \sum_{g_0}\sum_{g} P_1(\{g\})P_2(\{g_0 - g\})\chi(g)\chi(g_0 - g) \\
&= (\sum_{g} P_1(\{g\})\chi(g))(\sum_{g_0} P_2(\{g_0 - g\})\chi(g_0 - g)) \\
&= (\sum_{g} P_1(\{g\})\chi(g))(\sum_{g_0} P_2(\{g_0\})\chi(g_0)) \\
&= \hat{P}_1(\chi)\hat{P}_2(\chi).
\end{aligned}
$$

(iii) Das folgt sofort aus Lemma 2.1(i). □

Nach diesen Vorbereitungen sind alle Fragen leicht zu beantworten:

Satz 2.3 *P und $P_1, \ldots, P_k$ seien Wahrscheinlichkeitsmaße auf einer endlichen kommutativen Gruppe G, für die wir die Existenz von $n := \mathrm{card}(G)$ verschiedenen Charakteren voraussetzen.*

(i) *Ist das k-fache Faltungsprodukt von P mit sich gleich der Gleichverteilung U, so ist notwendig $P = U$.*

(ii) *$P_1 * \cdots * P_k = U$ gilt genau dann, wenn es für jeden von 1 verschiedenen Charakter χ ein κ mit $\hat{P}_\kappa(\chi) = 0$ gibt. Das ist insbesondere dann erfüllt, wenn irgendein P_κ gleich U ist.*

(iii) *Zu P_1 gibt es ein von U verschiedenes P_2 mit $P_1 * P_2 = U$ genau dann, wenn für ein geeignetes $\chi \neq 1$ die Fouriertransformation $\hat{P}_1(\chi)$ verschwindet.*

Beweis: (i) Das folgt unter Verwendung von Lemma 2.2 aus der Tatsache, daß sich für komplexe Zahlen z aus $z^k = 0$ stets $z = 0$ schließen läßt.

(ii) Wieder wird die Aussage auf einfache Eigenschaften von Zahlen zurückgeführt, auch diesmal ist nur wichtig, daß $\mathbb{C}$ nullteilerfrei ist.

(iii) Eine Richtung ist klar: Sind alle $\hat{P}_1(\chi) \neq 0$, so gilt nur für $P_2 = U$, daß $P_1 * P_2 = U$. Sei nun $\chi_0 \neq 1$ ein Charakter mit $\hat{P}_1(\chi_0) = 0$. $\hat{P}_1$ verschwindet dann auch auf $(\chi_0)^{-1} = \overline{\chi_0}$, da die $P_1(\{g\})$ reell sind.

Ein Maß P_2 soll durch $P_2(\{g\}) := 1/n + \epsilon(\chi_0 + \overline{\chi_0})(g)$ erklärt werden, dabei wählen wir $\epsilon > 0$ so, daß diese Zahlen nichtnegativ sind.

Wegen Lemma 2.1(i) ist P_2 wirklich ein Wahrscheinlichkeitsmaß, und der zweite Teil dieses Lemmas garantiert, daß $\hat{P}_2(\chi) = 0$ für $\chi \neq \chi_0, \overline{\chi_0}, 1$. Andererseits gilt $\hat{P}_2(\chi_0) \neq 0$, also ist $P_2 \neq U, \hat{P}_1\hat{P}_2 = \delta$, und so ein P_2 sollte konstruiert werden. □

Für das Ausgangsproblem, zunächst im Fall $n = a$ formuliert, heißt das:

- Soll eine faire Entscheidung zwischen n Alternativen von k Personen dadurch herbeigeführt werden, daß alle gemäß einer festen Verteilung P ein Element in $\{0, \ldots, n-1\}$ wählen und dann die Summe modulo n bilden, so führt dieses Verfahren zur Gleichverteilung auf $\{0, \ldots, n-1\}$ genau dann, wenn P selbst die Gleichverteilung war.

- Sind unterschiedliche Verteilungen $P_1, \ldots, P_k$ zugelassen, so wird das Verfahren alle n Alternativen mit gleicher Wahrscheinlichkeit genau dann liefern, wenn es zu jeder von 1 verschiedenen n−ten Einheitswurzel $\xi_j := \exp(2\pi ij/n), j = 1, \ldots, n-1$, ein κ mit $\sum_{l=0,\ldots,n-1} P_\kappa(\{l\})(\xi_j)^l = 0$ gibt.

- Sind zwei Personen beteiligt und entscheidet sich die erste für P_1, so kann die zweite durch die Wahl $P_2 = U$ immer erreichen, daß das Verfahren insgesamt fair wird. Andere Wahlen für P_2 sind genau dann möglich, wenn $\sum_{l=0,\ldots,n-1} P_1(\{l\})(\xi_j)^l = 0$ für ein $j \in \{1, \ldots, n-1\}$.

  [Ein Beispiel für $n = 6$: Ordnet P_1 den Zahlen $0, \ldots, 5$ die Wahrscheinlichkeiten $0, 0.2, 0.3, 0, 0.2, 0.3$ zu, so verschwindet die Fouriertransformation für $j = 1, 3, 5$, und folglich existieren von U verschiedene P_2 mit $P_1 * P_2 = U$ (z. B. das P_2, das $0, \ldots, 5$ auf $1/3, 0, 1/3, 0, 1/3, 0$ abbildet, es entspricht der Konstruktion aus dem Beweis mit $\epsilon = 1/12, \chi =$ "der zu $j = 3$ gehörige Charakter").

  Ist dagegen P_1 z. B. die Punktmasse auf 0, so gibt es außer $P_2 = U$ keinen Kandidaten.]

Es fehlt noch eine *Ergänzung für den Fall $a \neq n$.* Beachtet man, daß $(X_1 + \cdots + X_k) \bmod a = ((X_1 \bmod a) + \cdots + (X_k \bmod a)) \bmod a$, so hat man nur die vorstehenden Überlegungen auf die $X_\kappa \bmod a$ anzuwenden. Offensichtlich ist auch, daß für ein auf $\{0,\ldots,n-1\}$ gleichverteiltes X die Variable $X \bmod a$ auf $\{0,\ldots,a-1\}$ genau dann gleichverteilt ist, wenn a die Zahl n teilt. Sind also alle P_κ die Gleichverteilung, so ist $a|n$ notwendig und hinreichend dafür, daß alle Alternativen bei der Auswahl die gleichen Chancen haben. (*Deswegen* klappte es mit $a = 2$ und $a = 3$ am Anfang, da war nämlich $n = 6$.)

Hier haben wir uns um die elementar zugänglichen Aspekte im Zusammenhang mit der Gleichverteilung und Faltungen gekümmert. Es sollte jedoch erwähnt werden, daß man eine naheliegende Verallgemeinerung für beliebige kompakte kommutative Gruppen G betrachten kann. Der Kandidat für die Gleichverteilung ist da das *Haarsche Maß* U, das eindeutig bestimmte Wahrscheinlichkeitsmaß mit $U(A) = U(A+x)$ (alle $x \in G, A \subset G$ Borelmenge). Auch hier läßt sich eine Faltung $P_1 * P_2$ von Wahrscheinlichkeitsmaßen P_1, P_2 definieren, und $P_1 * P_2$ entspricht wieder der Verteilung von $g_1 + g_2$, wenn g_1, g_2 gemäß P_1 bzw. P_2 ausgewählt wurden.

Fragen des Typs "$P_1 * P_2 = U$?" können wieder mit Hilfe von *Charakteren* χ behandelt werden, das sind stetige Abbildungen von G nach Γ mit $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$. Die Ergebnisse sind fast wörtlich so wie im hier besprochenen endlichen Fall, insbesondere liefert $P * \cdots * P$ nur dann U, wenn P selbst schon U war. Die Beweise verlangen auch keine neuen Ideen; der technische Aufwand ist allerdings erheblich höher, da Integrale statt Summen zu betrachten sind und die auftretenden Funktionenräume unendlich-dimensional werden.

Als Beispiel für eine Interpretation unter dem Aspekt "Entscheidungen" stelle man sich k Personen vor, die sich mit Hilfe eines fairen Zufallsverfahrens auf eine Zeigerstellung (etwa eine Himmelsrichtung) einigen wollen. Jeder sucht sich eine aus, und am Ende wird die Hintereinanderausführung betrachtet. Das führt auf $G = \Gamma$, und U ist hier das normalisierte Borel-Lebesgue-Maß. Für diese Gruppe sind die Charaktere wieder leicht zu berechnen – es sind genau die Abbildungen $z \mapsto z^m$ mit $m \in \mathbb{Z}$ –, und folglich kann man Probleme im Zusammenhang mit Entscheidungen genauso explizit lösen wie eben im Fall der $\mathbb{Z}_n$.

3. Der Fall beliebiger endlicher Gruppen

Erwartungsgemäß wird alles schwieriger, wenn wir nun auch nichtkommutative endliche Gruppen zulassen. Es soll herausgearbeitet werden, daß für die hier interessierenden Aspekte die neu auftretenden Probleme durch das unterschiedliche Verhalten von Zahlen und Matrizen verursacht werden.

Ab hier sei $(G, \circ)$ eine beliebige endliche Gruppe. Wieder können wir versuchen, gleichverteilt in G dadurch etwas auszusuchen, daß $g_1, \ldots, g_k$ gemäß $P_1, \ldots, P_k$ gewählt werden und dann $g_1 \circ \cdots \circ g_k$ betrachtet wird.

> Konkretes Beispiel: Eine "zufällige" Sitzordnung beim Skat soll durch zwei Spielleiter festgelegt werden, die sich nach persönlichen Zufallsmechanismen für jeweils eine Permutation von $1, 2, 3$ entscheiden; dann wird die Hintereinanderausführung dieser Permutationen gebildet.

Klar, daß die oben gestellten Fragen hier genauso sinnvoll aufgeworfen werden können, wie sieht es aber mit den Antworten aus?

Wieder sei U die Gleichverteilung auf G, wieder ist leicht zu berechnen, wie für Wahrscheinlichkeitsmaße P_1, P_2 die Verteilung der Summe aussieht, wenn wir wie üblich Unabhängigkeit der Auswahl voraussetzen. Das zugehörige Maß wird auch hier mit $P_1 * P_2$ bezeichnet, und man bestimmt seine Werte durch die Formel $P_1 * P_2(\{g_0\}) = \sum_{g_1 \circ g_2 = g_0} P_1(\{g_1\}) P_2(\{g_2\}) = \sum_g P_1(\{g_0 \circ g^{-1}\}) P_2(\{g\})$.

Leider kann man nun nicht Faltungsgleichungen unter Verwendung von Charakteren in Skalargleichungen überführen, denn man kann nicht garantieren, daß es auf G "genügend viele" Charaktere gibt. (Das ist auch nicht zu erwarten, denn ein Charakter kann nicht zwischen den – möglicherweise verschiedenen - Elementen $g_1 \circ g_2$ und $g_2 \circ g_1$ unterscheiden.) Es hilft aber eine neue Idee weiter:

Eine d-dimensionale *Darstellung M von G* ist eine Abbildung, die jedem $g \in G$ eine unitäre $d \times d$-Matrix M_g zuordnet, so daß stets $M_{g_1 \circ g_2} = M_{g_1} M_{g_2}$ gilt (Matrizenprodukt). Schreibt man $M_g = (f_{s,t}(g))_{s,t=1,\ldots,d}$, so heißen die $f_{s,t} : G \to \mathbb{C}$ die *Koeffizientenfunktionen* zu M.

Wieder wird es wichtig sein, daß "genügend viele" Darstellungen existieren. Das ist immer erfüllt (vgl. die angegebene Literatur zur harmonischen Analysis), wir wollen es aber als Extra-Voraussetzung formulieren und im konkreten Einzelfall nachprüfen, um den Lesern einen langen technischen Exkurs zu ersparen. Wir werden voraussetzen, daß es Darstellungen

$M^1, \dots, M^m$ mit den folgenden Eigenschaften gibt[1]:

- Mit d_μ="die Dimension von M^μ" gilt $d_1^2 + \cdots + d_m^2 = n := \mathrm{card}(G)$.
- M^1 ist die triviale Darstellung ($d_1 = 1, f_{1,1}(g) = 1$ für alle g).
- Bezeichnet $(f^\mu_{s,t})_{s,t=1,\dots,d_\mu}$ die Koordinatenfunktionen von M^μ, so sollen diese n Funktionen paarweise orthogonal im folgenden Sinn sein: $1/n \sum_g f^\mu_{s,t} f^{\mu'}_{s't'}(g)$ ist immer Null, außer im Fall $s = s', t = t', \mu = \mu'$; dann soll die Summe $1/d_\mu$ sein.

Wir definieren auch hier eine *Fouriertransformation* für Wahrscheinlichkeitsmaße P: Das ist diejenige Abbildung, die einer Darstellung M die Matrix $\hat{P}(M) := \sum_g P(\{g\}) M_g$ zuordnet.

Lemma 3.1 *Für Wahrscheinlichkeitsmaße P_1, P_2 gilt:*
(i) *Aus $\hat{P}_1(M^\mu) = \hat{P}_2(M^\mu)$ für $\mu = 1, \dots, m$ folgt $P_1 = P_2$.*
(ii) *Für alle Darstellungen M ist $\widehat{P_1 * P_2}(M) = \hat{P}_1(M)\hat{P}_2(M)$.*
(iii) *$\hat{U}(M^1) = 1$, alle anderen $\hat{U}(M^\mu)$ verschwinden.*

Beweis: Das geht genauso wie in Kapitel 2. Es ist nur wichtig, daß – als Folgerung aus den Orthogonalitätsrelationen – jede komplexwertige Funktion auf G Linearkombination der f^μ_{st} ist. □

Für die hier interessierenden Faltungsgleichungen ergibt sich sofort:

Satz 3.2 *Genau dann ist $P_1 * \cdots * P_k$ die Gleichverteilung, wenn alle Matrizenprodukte $[\hat{P}_1(M^\mu)] \cdots [\hat{P}_k(M^\mu)]$ für $\mu = 2, \dots, m$ die Nullmatrix sind.*

Anders als für Zahlen kann man aber für Matrizen A, B aus $AB = 0$ nicht schließen, daß $A = 0$ oder $B = 0$, und deswegen ist nicht klar, ob wir ähnliche Folgerungen ziehen können wie im kommutativen Fall, ob es also zum Beispiel ein Analogon zu Satz 2.3(i) gibt. Positive Ergebnisse kann man erzwingen, indem man durch Forderungen an P garantiert, daß $[\hat{P}(M)]^k = 0$ nur für $\hat{P}(M) = 0$ gilt.

Das ist zum Beispiel dann der Fall, wenn P *symmetrisch* ist, d. h. wenn $P(\{g\}) = P(\{g^{-1}\})$ für alle g ist. Denn da alle M_g unitär sind, ist $M_{(g^{-1})} =$

[1] Das ist die angemessene Verallgemeinerung der Reichhaltigkeitsforderung im kommutativen Fall; dort hatten wir "viele" Charaktere, d. h. eindimensionale Darstellungen postuliert.

$(M_g)^*$(=die zu M_g adjungierte Matrix). Im Falle symmetrischer P ist dann $(\hat{P}(M))^* = \sum_g P(\{g\})M_g^* = \sum_g P(\{g\})M_{(g^{-1})} = \sum_g P(\{g^{-1}\})M_{(g^{-1})} = \hat{P}(M)$, d. h. die hier interessierenden $\hat{P}(M^\mu)$ sind selbstadjungiert, und für derartige Matrizen A darf man wirklich aus $A^k = 0$ auf $A = 0$ schließen. Das zeigt:

Korollar 3.3 *Die üblichen Voraussetzungen seien erfüllt, zusätzlich sei P ein symmetrisches Wahrscheinlichkeitsmaß auf G. Ist dann $P * \cdots * P$ (k-faches Faltungsprodukt) gleich U, so folgt $P = U$.*

Damit ist der allgemeine Fall noch nicht entschieden. Die folgenden Beispiele zeigen aber, daß für nichtkommutative G alles Mögliche passieren kann.

Satz 3.4 *Es gibt nichtkommutative Gruppen G_1, G_2 mit genügend vielen Darstellungen im oben präzisierten Sinn, so daß*

(i) *Auf G_1 gibt es ein Wahrscheinlichkeitsmaß $P \neq U$ mit $P * P = U$.*

(ii) *In G_2 folgt aus $P * P = U$ stets $P = U$.*

Beweis: (i) Sei $G_1 := S_3$, die Gruppe der Permutationen von drei Elementen. Die sechs Elemente von G_1 kürzen wir wie folgt ab:
$0 := \binom{1\,2\,3}{1\,2\,3}, 1 := \binom{1\,2\,3}{3\,1\,2}, 2 := \binom{1\,2\,3}{2\,3\,1}, 3 := \binom{1\,2\,3}{1\,3\,2}, 4 := \binom{1\,2\,3}{3\,2\,1}, 5 := \binom{1\,2\,3}{2\,1\,3}.$

Wir geben explizit die geforderten Darstellungen an: Die ersten beiden sind eindimensional, die dritte ist zweidimensional. Hier die Werte der Funktionen $f^\mu_{s,t}$ (dabei steht w für $\sqrt{3/4}$):

$g:$	0	1	2	3	4	5
f^1_{11}	1	1	1	1	1	1
f^2_{11}	1	1	1	-1	-1	-1
f^3_{11}	1	-0.5	-0.5	-1	0.5	0.5
f^3_{12}	0	$-w$	w	0	$-w$	w
f^3_{21}	0	w	$-w$	0	$-w$	w
f^3_{22}	1	-0.5	-0.5	1	-0.5	-0.5

Wir definieren noch P durch $2P(\{0\}) = 2P(\{4\}) = P(\{2\}) = P(\{5\}) = 1/3$. Eine kanonische Rechnung zeigt, daß die f^μ_{st} zu Darstellungen gehören, daß die Orthogonalitätsrelationen erfüllt sind und daß $P * P = U$. (Zur Kontrolle berechnen wir $\hat{P}(M^3) = (1/12)\begin{pmatrix} 3 & 6w \\ -2w & -3 \end{pmatrix}$, und das ist wirklich eine nilpotente nichttriviale Matrix.)

(ii) G_2 sei die *Quaternionengruppe*. Die besteht aus den acht Elementen $\pm 1, \pm i, \pm j, \pm k$, für die die Gruppenstruktur durch $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$ erklärt ist (die Rechenregeln für ± 1 und $\pm$ sollen so sein, wie man es von komplexen Zahlen gewohnt ist; z. B. ist $k(-i) = -ki = -j$).

Auf G_2 gibt es neben dem trivialen Charakter χ_1 noch drei weitere Charaktere, die hier mit χ_i, χ_j, χ_k bezeichnet werden. Sie sind durch
$\chi_i : \pm 1, \pm i \mapsto 1, \pm j, \pm k \mapsto -1$,
$\chi_j : \pm 1, \pm j \mapsto 1, \pm k, \pm i \mapsto -1$,
$\chi_k : \pm 1, \pm k \mapsto 1, \pm i, \pm j \mapsto -1$
definiert. Und dann gibt es noch eine zweidimensionale Darstellung M. Die ist durch

$$\pm 1 \mapsto \pm E, \pm i \mapsto \pm I, \pm j \mapsto \pm J, \pm k \mapsto \pm K$$

erklärt, wobei E, I, J, K die folgenden Matrizen bezeichnen:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \frac{\sqrt{2}}{2}\begin{pmatrix} i & i \\ i & -i \end{pmatrix}, J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \frac{\sqrt{2}}{2}\begin{pmatrix} -i & i \\ i & i \end{pmatrix}.$$

(Das "i" in diesen Matrizen ist die übliche imaginäre Einheit, die auf den ersten Blick mit dem $i \in G_2$ nichts zu tun hat. Es besteht aber ein Zusammenhang: Die Quaternionengruppe erzeugt die Quaternionen, die $\mathbb{C}$ umfassen.)

Damit ist, auch wenn wir die elementaren Rechnungen hier nicht ausführen werden, die Existenz genügend vieler Darstellungen nachgewiesen.

Sei nun P ein Wahrscheinlichkeitsmaß auf G_2 mit $P*P = U$; es ist $P = U$ zu zeigen. Dazu setzen wir $\tau_\alpha := P(\{\alpha\}) + P(\{-\alpha\})$ für $\alpha = 1, i, j, k$. Da P ein Wahrscheinlichkeitsmaß ist und da nach Satz 3.2 die $(\hat{P}(\chi_\alpha))^2$ und folglich die $\hat{P}(\chi_\alpha)$ für $\alpha = i, j, k$ verschwinden, folgt
$\tau_1 + \tau_i + \tau_j + \tau_k = 1, \tau_1 + \tau_i - \tau_j - \tau_k = 0$,
$\tau_1 - \tau_i + \tau_j - \tau_k = 0, \tau_1 - \tau_i - \tau_j + \tau_k = 0$,
und dieses Gleichungssystem hat als eindeutig bestimmte Lösung $\tau_1 = \tau_i = \tau_j = \tau_k = 1/4$. Wir schreiben daher – mit geeigneten $\delta_1, \delta_i, \delta_j, \delta_k$ – $P(\{\alpha\}) = 1/8 + \delta_\alpha, P(\{-\alpha\}) = 1/8 - \delta_\alpha$.

Werte nun die Identität $P * P = U$ bei 1 aus:

$$1/8 = (1/8 + \delta_1)^2 + (1/8 - \delta_1)^2 + 2 \sum_{\alpha = i,j,k} (1/8 + \delta_\alpha)(-1/8 - \delta_\alpha),$$

also $0 = (\delta_1)^2 - (\delta_i)^2 - (\delta_j)^2 - (\delta_k)^2$. Analog ergibt die Auswertung bei i, j, k die weiteren Gleichungen $0 = \delta_1\delta_i = \delta_1\delta_j = \delta_1\delta_k$. Diese Beziehungen implizieren $\delta_1 = \delta_i = \delta_j = \delta_k = 0$, und das war zu zeigen. □

Die genaue Antwort auf die Frage, ob sich eine Gruppe wie in (i) oder wie in (ii) des vorigen Satzes verhält, wurde in [2] gegeben (s. a. [6]): Für ein nichtkommutatives kompaktes G kann man genau dann stets von $P * P = U$ auf $P = U$ schließen, wenn G ein Produkt aus der Quaternionengruppe und einer Gruppe des Typs $\{0,1\}^I$, (I irgendeine Menge) ist. Die hier bereitgestellten elementaren Methoden reichen aber bei weitem nicht aus, um diesen Charakterisierungssatz zu beweisen.

4. Ergänzungen

Die vorstehenden Kapitel haben uns von einem konkreten Entscheidungsfindungs-Problem bis in die harmonische Analysis nichtkommutativer Gruppen geführt. Die am Anfang aufgeworfenen Fragen konnten vollständig geklärt werden, sogar dann, wenn man die zur Motivation gehörige Gruppe $\mathbb{Z}_n$ durch ein beliebiges kommutatives endliches (oder sogar kompaktes) G ersetzt. Im nichtkommutativen Fall liegen nach der allgemeinen Charakterisierung aus [2] sofort einige Fragen nahe, z. B.: Wann impliziert $U = P * \cdots * P$ (k-faches Faltungsprodukt), daß $P = U$? Welche Zusatzeigenschaften an P garantieren, daß $P = U$ aus $P * P = U$ folgt?

Auch im kommutaiven Fall, selbst für die $\mathbb{Z}_n$, ergeben sich durch Variation der Ausgangssituation schnell noch offene Probleme. Wir denken wieder an die Freunde vom Anfang, die gemeinsam dadurch eine Entscheidung zwischen n Alternativen treffen wollen, daß jeder etwas aus $\{0, \ldots, n-1\}$ auswählt und dann die Summe modulo n als gemeinsame Entscheidung akzeptiert wird. Diesmal wird aber gewünscht, daß die Ergebnisse entsprechend einem vorher vereinbarten Wahrscheinlichkeitsmaß P_0 gefunden werden. In unserer Terminologie heißt das: Diskutiere $P_1 * P_2 = P_0$ bei vorgelegtem P_0. Findet man z. B. zu jedem P_0 ein P mit $P * P = P_0$ (das entspricht dem Fall, daß beide Freunde das gleiche Entscheidungsverfahren verwenden)? Für kleine n kann man das noch leicht diskutieren. Sei etwa $n = 2$. P_0 sei gegeben, und wir fragen nach Zahlen $p, q \geq 0$ (unseren Kandidaten für $P(\{0\}), P(\{1\})$) mit $p + q = 1, p^2 + q^2 = P_0(\{0\}), 2pq = P_0(\{1\})$. Die ersten beiden Bedingungen implizieren die dritte (denn P_0 ist ein Wahrscheinlichkeitsmaß), und die Lösung kann geometrisch leicht gefunden werden: Es geht um die Schnittpunkte der Geraden $p + q = 1$ mit dem Kreis $p^2 + q^2 = P_0(\{0\})$. Es zeigt sich etwa, daß es Lösungen genau dann gibt, wenn $P(\{0\}) \geq 1/2$ ist.

Für beliebige n scheint keine einfache Charakterisierung der P_0, zu denen es P mit $P * P = P_0$ gibt, möglich zu sein. Nur soviel läßt sich sagen: $P * P = P_0$ gilt genau dann, wenn $(\hat{P}(\chi_j))^2 = \widehat{P_0}(\chi_j)$ für $j = 1, \ldots, n-1$. Das macht klar, daß das Problem mit den Wurzeln der $\widehat{P_0}(\chi_j)$ zusammenhängt, und man sieht auch, warum der oben diskutierte Fall $P_0 = U$ zu einem einfach zu behandelnden Problem führt (da sind nämlich alle diese Zahlen Null).

Noch verwickelter ist in diesem Zusammenhang die folgende Fragestellung, die im Fall $P_0 = U$ in Kapitel 2 vollständig diskutiert wurde: Gibt es zu P_1, P_0 ein P_2 mit $P_1 * P_2 = P_0$? Eine Umformulierung mit Hilfe von Charakteren führt auf $\widehat{P_1}(\chi)\widehat{P_2}(\chi) = \widehat{P_0}(\chi)$, und das impliziert die notwendige Bedingung $|\widehat{P_1}(\chi)| \leq |\widehat{P_0}(\chi)|$ für alle χ (da $|\hat{P}(\chi)| \leq 1$). Daher werden die Zahlen $\alpha_j := \widehat{P_0}(\chi_j)/\widehat{P_1}(\chi_j)$ eine Rolle spielen (wir wollen der Einfachheit halber annehmen, daß alle $\widehat{P_1}(\chi_j) \neq 0$ sind), und dann steht man vor dem Problem zu entscheiden, ob die α_j als $\hat{P}(\chi_j)$ für ein geeignetes Wahrscheinlichkeitsmaß P realisiert werden können. Das ist der schwierige Teil, nur für kleine n bieten sich Charakterisierungen an.

Sei z. B. $n = 3$. Für welche α_1, α_2 gibt es $p_0, p_1, p_2 \geq 0$ (die Kandidaten für die Wahrscheinlichkeiten von $0, 1, 2$) mit $p_0 + p_1 + p_2 = 1, p_0 + p_1\xi + p_2\bar{\xi} = \alpha_1, p_0 + p_1\bar{\xi} + p_2\xi = \alpha_2$ (mit $\xi := \exp(2\pi i/3)$)? Es muß $\alpha_1 = \overline{\alpha_2}$ sein, und α_1 muß in der konvexen Hülle C von $1, \xi, \bar{\xi}$ liegen. Für das Ausgangsproblem heißt das: Genau dann ist $P_1 * P_2 = P_0$ für ein geeignetes P_2, wenn $\widehat{P_0}(\chi_1)/\widehat{P_1}(\chi_1)$ in C liegt.

Wir kommen noch einmal auf den Beginn der Arbeit zurück: Faire Entscheidungen durch Fingerheben[2]. Nachträglich wird klar, warum der Daumen als Finger wichtig war. Läßt man ihn nämlich weg, so geht man von $n = 6$ zu $n = 5$ über, und dann sind die Summen modulo 2 nicht meht gleichverteilt. Es sind noch zwei weitere Punkte zu besprechen. Zum einen ist es nicht so, daß man 0 oder $1, \ldots, 5$ Finger (der Daumen zählt wieder mit) gleichverteilt hebt, wenn man sich einbildet, das zu tun. Ungerade Zahlen haben eine höhere Wahrscheinlichkeit als gerade, wohl deswegen, weil $1, 3, 5$ Finger leichter zu strecken sind als 2 oder 4. Damit taucht "Summe gerade" öfter auf als "Summe ungerade", auch wenn beide Teilnehmer um eine gleichverteilte Entscheidung bemüht sind.

[2] Das ist übrigens, glaubt man [3], Seite 69, ein gängiges Entscheidungsverfahren unter Kindern.

Und ganz schwierig wird es, wenn man dieser Frage unabhängig von der Physiologie der Finger auf den Grund gehen möchte: Kann ein Mensch überhaupt zufällig reagieren, kann er etwa ohne Hilfsmittel eine faire Münze simulieren? Mir sind nur ziemlich gekünstelte Lösungen eingefallen, jeder ist herzlich eingeladen, sich eigene Verfahren auszudenken.

LITERATURHINWEISE

[1] P. DIACONIS. *Group representations in probability and statistics.* IMS - Lecture Notes-Monograph Series **11** (1988).

[2] P. DIACONIS, M. SHASHSHAHANI. *On square roots of the uniform distribution on compact groups.* Proc. of the AMS **98** (1986),341-348 .

[3] I. EKELAND. *The broken dice.* University of Chicago Press (1993).

[4] E. HEWITT, K. A. ROSS. *Abstract harmonic analysis I,II.* Springer Verlag, Berlin-Heidelberg-New York (1963).

[5] W. SCHEMPP, B. DRESELER. *Einführung in die harmonische Analyse.* Teubner-Verlag, Stuttgart (1980).

[6] G. TURNWALD. *Roots of Haar measure and topological hamiltonian groups.* Springer Verlag, Lecture Notes in Mathematics **1379** (1989),364-375.

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