On the forged dice

Ehrhard Behrends

Abstract

It is a well–known exercise in elementary probability that it is impossible to forge two ordinary dice with numbers $1, \ldots, 6$ in such a way that when one throws both and takes the sum one gets the numbers $2, 3, \ldots, 12$ all with the same probability.

Now let $m \in I\!N$. We will investigate for what families $k_1, \ldots, k_s \in I\!N$, $s > 1$, with $k_1 + \cdots + k_s = m$ there are probabilities $P_1, \ldots, P_s$ on $\{0, \ldots, k_1\}, \ldots, \{0, \ldots, k_s\}$, respectively, such that $P_1 * \cdots * P_s$ is the uniform distribution on $\{0, \ldots, m\}$; the preceding assertion is just the statement that for $m = 10$, $k_1 = k_2 = 5$ there are no such probabilities.

It will be shown how the $k_1, \ldots, k_s$ for which $P_1, \ldots, P_s$ exist can be described explicitly (and how the P_σ look like in this case) in terms of the divisors of $m + 1$.

In the case $s = 2$ the description reads as follows: Write $m + 1 = g_1 \cdots g_t$ and define inductively $k_1' := g_t - 1$, $k_1'' := 0$, $k_\tau' := g_{t-\tau+1} k_{\tau-1}'' + g_{t-\tau+1} - 1$, $k_\tau'' = g_{t-\tau+1} k_{\tau-1}'$ for $\tau = 2, \ldots, t$; then $k_1 := k_t'$, $k_2 := k_t''$ admit P_1, P_2, and whenever the uniform distribution on $\{0, \ldots, m\}$ can be obtained by convolving probabilities P_1, P_2 on $\{0, \ldots, k_1\}$ and $\{0, \ldots, k_2\}$ with $k_1 + k_2 = m$, then the tuple (k_1, k_2) can be obtained as (k_t', k_t'') (or (k_t'', k_t')) as above.

Many devisors give rise to many families $k_1, \ldots, k_s$ so that our description can be considered as an extension of an old result of Raikov's (which states that no $k_1, \ldots, k_s$ exist if $m + 1$ is prime).

Our original problem is equivalent with representing $1 + x + \cdots + x^m$ as a product of polynomials $A_1, \ldots, A_s$ with nonnegative coefficients. Hence we get a catalogue of all such factorizations, and the explicit form of the measures P_σ (they are uniform on subsets of $\{0, \ldots, k_\sigma\}$) gives rise to an explicit description of the partition of the $(m + 1)$–th roots of unity different from 1 which correspond to the factorization $1 + x + \cdots + x^m = A_1(x) \cdots A_s(x)$.

1. Introduction

Since the beginning of this century it has been of interest to decide whether a given distribution can be written in a nontrivial way as the convolution of two other distributions or, equivalently, whether a random variable is the sum of two independent variables. In particular the case of infinitely divisible distributions has been studied thoroughly because of its importance for generalizations of the central limit theorem. See [5], [6] and [8] for an extensive discussion of these connections and many historical comments.

The first example of an indecomposable distribution was given 1937 by Raikov [7] who showed that the uniform distribution on $\{0, \ldots, m\}$ cannot be written nontrivially as a convolution product provided that $m + 1$ is prime. By using an elementary result on lattice–like distributions (see e.g. th. 5.1.1 in [5]) one can easily show that this is equivalent with the assertion that there are no $k_1, k_2 \in I\!N$ with $k_1 + k_2 = m$ such that there exist probability measures P_1, P_2 on $\{0, \ldots, k_1\}$, $\{0, \ldots, k_2\}$ with $P_1 * P_2 =$ uniform.

It has been also well–known for many years that it is impossible for $n \in I\!N$ to find P_1, P_2 on $\{0, \ldots, n\}$ such that $P_1 * P_2$ is uniform on $\{0, \ldots, 2n\}$; students in elementary probability often make acquaintance with this fact in the disguise of the "forged dice". The oldest reference seems to be [3], the same author treats this question under a different viewpoint in [4].

The present note is devoted to the problem whether for $m, k_1, \ldots, k_s \in I\!N$ with $k_1 + \cdots + k_s = m$ there are $P_1, \ldots, P_s$ on $\{0, \ldots, k_1\}, \ldots, \{0, \ldots, k_s\}$, respectively, such that $P_1 * \cdots * P_s$ is uniform. In *section 2* we study reformulations in terms of factorizations of polynomials which will enable us to reduce our investigation to a question concerning unique additive representations of natural numbers. *Section 3* contains the characterization we aim for in the framework of elementary number theory, and in *section 4* we describe the necessary modifications to treat the variants dealing with probabilities and with roots of unity. This section contains also the discussion of some consequences, e.g.: If there exist P_1, P_2, are they uniquely determined? (No, they aren't.) Is it likely or is it a rare event that, given m, k_1, k_2 with $k_1 + k_2 = m$ there are P_1, P_2 on $\{0, \ldots, k_1\}$, $\{0, \ldots, k_2\}$ such that $P_1 * P_2$ is the uniform distribution? (It is rather unlikely for large m).

2. Preparations

Let $m, k_1, \ldots, k_s \in I\!N$ be given such that $k_1 + \cdots + k_s = m$. Suppose that there exist probability measures P_σ on $\{0, \ldots, k_\sigma\}$, $\sigma = 1, \ldots, s$ such that $P_1 * \cdots * P_s$ is uniform. Let P_σ be defined by the numbers $p_j^\sigma := P_\sigma(\{j\})$, $\sigma = 1, \ldots, s$, $j = 0, \ldots, k_\sigma$. Then $\prod_{\sigma=1}^{s} (p_0^\sigma + p_1^\sigma x + \cdots + p_{k_\sigma}^\sigma x^{k_\sigma}) = \frac{1}{m+1}(1 + x + \cdots + x^m)$ so that – after dividing by $\prod p_{k_\sigma}^\sigma$ – it follows that $1 + x + \cdots + x^m$ can be written as a product $A_1(x) \cdots A_s(x)$ where the degree of A_σ is k_σ, the leading coefficient is one, and all coefficients are nonnegative. The converse is also true: whenever $1 + x + \cdots + x^m$ is decomposed in this way (we will speak of a *nonnegative* $(k_1, \ldots, k_s)$*–decomposition*) we get $P_1, \cdots, P_s$ such that $P_1 * \ldots * P_s$ is the uniform distribution on $\{0, \ldots, m\}$.

2.1 Lemma *Let $1 + x + \cdots + x^m = A_1(x) \cdots A_s(x)$ be a nonnegative $(k_1, \ldots, k_s)$–decomposition, where $A_\sigma(x) = a_0^\sigma + a_1^\sigma x + \cdots + a_{k_\sigma - 1}^\sigma x^{k_\sigma - 1} + x^{k_\sigma}$.*
(i) The A_σ have the following palindrome property:
$a_j^\sigma = a_{k_\sigma - j}^\sigma$ for $j = 0, \ldots, k_\sigma$. In particular $a_0^\sigma = 1$.
(ii) $a_j^\sigma \in \{0, 1\}$ for all σ, j.

Proof Clearly we may assume that $s = 2$ (by considering A_σ, $(\prod_{\sigma' \neq \sigma} A_{\sigma'})$). We will write A, B and k, n instead of A_1, A_2 and k_1, k_2 and the coefficients will be denoted by $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$.

(i) The roots of $1 + x + \cdots + x^m$ are precisely the $w_j := \exp(2\pi i j/(m+1))$, $j = 1, \ldots, m$. Now let w be a root of A. Since the a_κ are real, $\overline{w}$ is also a root, but since $w = w_\ell$ for a suitable ℓ it follows that $\overline{w} = 1/w$. Hence $A(x) = \prod(x - 1/w)$, where the w run through the roots of A. From this it follows easily that $x^k A(1/x) = A(x)$, and this is just (i) for the polynomial A.

(ii) We have $a_\kappa, b_\nu \geq 0$ and hence $a_\kappa, b_\nu \in [0, 1]$. Suppose that, e.g., some a_κ lies in $]0, 1[$. Let κ_0 be the smallest κ for which this happens; note that $\kappa_0 > 0$ since, by (i), $a_0 = 1$.

By assumption $1 = b_j + b_{j-1} a_1 + \cdots + b_1 a_{j-1} + a_j$ for $j = 1, \ldots, m$ (where $b_\nu = 0$ for $\nu > n$ and $a_\kappa = 0$ for $\kappa > k$) and from this we get by induction on j that $b_0, b_1, \ldots, b_{\kappa_0 - 1} \in \{0, 1\}$, $0 < b_{\kappa_0} < 1$. This yields a contradiction when evaluating

the coefficient of x^n:
$1 = b_n + b_{n-1}a_1 + \cdots + b_{n-\kappa_0}a_{\kappa_0} + \cdots \geq 1 + b_{n-\kappa_0}a_{\kappa_0} > 1$ (since, by (i), $b_{n-\kappa_0} = b_{\kappa_0}$).

Note The proof shows that (i) is also valid if the A_σ have real (and not necessarily nonnegative) coefficients. For (ii), however, reality is not sufficient to have "simple" coefficients (e.g. $1 + x + x^2 + x^3 + x^4 = (1 - 2\cos(\frac{2\pi}{5})\,x + x^2)(1 - 2\cos(\frac{4\pi}{5})\,x + x^2)$.

In view of 2.1 (ii) nonnegative $(k_1, \ldots, k_s)$–decompositions of $1 + x + \cdots + x^m$ are in one–to–one correspondence with families of sets $\Pi_\sigma \subset \{0, \ldots, k_{\sigma\}}$ $(\sigma = 1, \ldots, s)$ such that every $j \in \{0, \ldots, m\}$ has a *unique* representation $j = j_1 + \cdots + j_s$ with $j_\sigma \in \Pi_\sigma$. In particular the product of the cardinalities of the Π_σ is $m + 1$, and this proves that there are no decompositions if $m + 1$ is prime (Raikov [7]).

It is also now clear that in the case of admissible $k_1, \ldots, k_s$ the k's have to be pairwise different: one has $k_\sigma \in \Pi_\sigma$ for all σ, and $k_{\sigma_1} = k_{\sigma_2}$ would give rise to two different representations of k_{σ_1} as $j_1 + \cdots + j_s$ with $j_\sigma \in \Pi_\sigma$.

3. The characterization theorem

Families $\Pi_1, \ldots, \Pi_s$ as above (i.e. $\Pi_\sigma \in \{0, \ldots, k_\sigma\}$, $(j_1, \ldots, j_s) \longmapsto j_1 + \cdots + j_s$ is a bijection between $\Pi_1 \times \cdots \times \Pi_s$ and $\{0, \ldots, m\}$) will be called *admissible* $(k_1, \ldots, k_s)$–*families*. In view of the description we have in mind it is convenient to observe that two different Π_σ have only 0 in their intersection so that the numbers $\alpha_\sigma :=$ "the smallest strictly positive element of Π_σ" are different for different σ. We will say that the $\Pi_1, \ldots, \Pi_s$ are *canonically ordered* if $\alpha_1 < \alpha_2 < \cdots < \alpha_s$ (note that always $\alpha_1 = 1$). Occasionally it will be convenient to regard $(\{0, \ldots, m\})$ also as an admissible family (where $s = 1$, $k_1 = m$).

Part 1: A construction to obtain admissible families

Let $m + 1$ be written as $m + 1 = g_1 g_2 \cdots g_t$ with $t, g_\tau > 1$. Then every $j \in \{0, \ldots, m\}$ can uniquely be represented as $j = j_1 + j_2 g_1 + j_3(g_2 g_1) + \cdots + j_t(g_{t-1} \cdots g_1)$ with $0 \leq j_\tau < g_\tau$; in the case $g_1 = g_2 = \cdots = g_t =: g$ this reduces to the well–known g–adic representation of j.

This can be rephrased as: $\widehat{\Pi}_1, \ldots, \widehat{\Pi}_t$ is an admissible $(\widehat{k}_1, \ldots, \widehat{k}_t)$–family, where $\widehat{\Pi}_1 = \{0, \ldots, g_1 - 1\}$, $\widehat{\Pi}_2 = \{0, g_1, 2g_1, \ldots, (g_2 - 1)\, g_1\}, \ldots, \widehat{\Pi}_\tau = (g_{\tau-1} g_{\tau-2} \cdots g_1)\, \{0, \ldots, g_\tau - 1\}$ and $\widehat{k}_\tau = (g_\tau - 1)\, g_{\tau-1} g_{\tau-2} \cdots g_1$. This family is canonically ordered since $1 < g_1 < g_2 g_1 < \cdots$.

Now let $2 \le s \le t$ be given and $\Delta_1 \cup \cdots \cup \Delta_s$ be a partition of $\{1, \ldots, t\}$ into nonvoid subsets such that no Δ_σ contains two consecutive elements and such that the smallest element of Δ_σ is smaller than the smallest element of $\Delta_{\sigma+1}$; we will speak of an *alternating s–partition* for short.
Put $\Pi_\sigma := \sum_{\tau \in \Delta_\sigma} \widehat{\Pi}_\tau$. Then every $j \in \{0, \ldots, m\}$ can uniquely be represented as $j_1 + \cdots + j_s$ with $j_\sigma \in \Pi_\sigma$ so that $\Pi_1, \ldots, \Pi_s$ is an admissible family (in fact a $(k_1, \ldots, k_s)$–family with $k_\sigma := \sum_{\tau \in \Delta_\sigma} \widehat{k}_\tau$). This family is canonically ordered by our assumption on the Δ_σ.

Summing up we arrive at

3.1 Definition *Suppose that $m + 1 = g_1 \cdots g_t$ $(t, g_\tau > 1)$ and that $\Delta_1 \cup \cdots \cup \Delta_s$ is an alternating s–partition of $\{1, \ldots, t\}$. Then the family $\Pi_1, \ldots, \Pi_s$ just constructed will be called the family derived from $(g_1, \ldots, g_t;\ \Delta_1, \ldots, \Delta_s)$. It is a canonically ordered $(k_1, \ldots, k_s)$–family, where $k_\sigma = \sum_{\tau \in \Delta_\sigma} (g_\tau - 1)\, g_{\tau-1} \cdots g_1$.*

Examples (Here we will express subsets Π of $\{0, \ldots, k\}$ by the values of the characteristic functions; e.g. $(1\,1\,0\,0\,0\,0\,1\,1)$ stands for the subset $\{0, 1, 6, 7\}$ of $\{0, \ldots, 7\}$).

1. $m = 23$, $m + 1 = 4 \cdot 2 \cdot 3$, i.e. $t = 3$, $(g_1, g_2, g_3) = (4, 2, 3)$. Here
   $\widehat{\Pi}_1 = (1\,1\,1\,1)$, $\widehat{\Pi}_2 = (1\,0\,0\,0\,0\,1)$, $\widehat{\Pi}_3 = (1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1)$.

   There is only one alternating 3–partition of $\{1, 2, 3\}$, nameyl $\Delta_i = \{i\}$, and this gives rise to the $(3, 4, 16)$–family $\widehat{\Pi}_1$, $\widehat{\Pi}_2$, $\widehat{\Pi}_3$. Also there is only one alternating 2–partition in this case: $\Delta_1 = \{1, 3\}$, $\Delta_2 = \{2\}$, and we obtain the $(19, 4)$–family $((1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1), (1\,0\,0\,0\,1))$.

2. Again with $m = 23$, let us try $m + 1 = 2 \cdot 2 \cdot 3 \cdot 2$ $(t = 4, (g_1, g_2, g_3, g_4) = (2, 2, 3, 2))$. Here the $\widehat{\Pi}_\tau$ are as follows:
   $\widehat{\Pi}_1 = (1\,1)$, $\widehat{\Pi}_2 = (1\,0\,1)$, $\widehat{\Pi}_3 = (1\,0\,0\,0\,1\,0\,0\,0\,1)$, $\widehat{\Pi}_4 = (1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1)$.

There is the obvious alternating 4–partition which gives rise to the $(1,2,8,12)$–family $(\widehat{\Pi}_1,\widehat{\Pi}_2,\widehat{\Pi}_3,\widehat{\Pi}_4)$. As an example of an alternating 3–partition consider $\Delta_1=\{1,4\}$, $\Delta_2=\{2\}$, $\Delta_3=\{3\}$;
this leads to the $(13,2,8)$–family $((1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1), \widehat{\Pi}_2,\widehat{\Pi}_3)$.
And there is only one alternating 2–partition: $\Delta_1=\{1,3\}$, $\Delta_2=\{2,4\}$; this yields the $(9,14)$–family $((1\,1\,0\,0\,1\,1\,0\,0\,1\,1), (1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1))$.

Part 2: Every admissible family can be obtained in this way

3.2 Theorem *Let $(\Pi_1,\ldots,\Pi_s)$ be an admissible $(k_1,\ldots,k_s)$–family; assume that it is canonically ordered (cf. the definition from the beginning of this section).*

(i) There are $t\geq 1$, $g_1,\ldots,g_t>1$ with $m+1=g_1\cdots g_t$ and an alternating s–partition $\Delta_1,\ldots,\Delta_s$ of $\{1,\ldots,t\}$ such that $(\Pi_1,\ldots,\Pi_s)$ is the family derived from $(g_1,\ldots,g_t;\Delta_1,\ldots,\Delta_s)$ in the sense of 3.1.

(ii) $(\Pi_1,\ldots,\Pi_s)$ uniquely determine $(g_1,\ldots,g_t;\Delta_1,\ldots,\Delta_s)$.

Hence there are precisely as many admissible families as there are $(g_1,\ldots,g_t)$ with $m+1=g_1\cdots g_t$ and alternating partitions of $\{1,\ldots,t\}$.

The proof will depend on the following lemmas.

3.3 Lemma *Suppose that $(\{0,\ldots,r\},\Pi)$ is an admissible family for $\{0,\ldots,m\}$, i.e. every $j\in\{0,\ldots,m\}$ can uniquely be written as $j=j_1+j_2$ with $0\leq j_1\leq r$ and $j_2\in\Pi$. Then $(r+1)|(m+1)$ and, with $n:=(m+1)/(r+1)$, the set Π is just the set $\{0,r+1,2(r+1),\ldots,(n-1)(r+1)\}$.*

Proof Uniqueness of the representation $j=j_1+j_2$ implies that $|j-j'|>r$ for $j,j'\in\Pi$, and gaps larger than $r+1$ in Π would contradict the possibility of such representations.

3.4 Lemma *Let $(\Pi,\widetilde{\Pi})$ be an admissible family for $\{0,\ldots,m\}$ with $1\in\Pi$. Let $r\geq 1$ be such that $\{0,\ldots,r\}\subset\Pi$ but $r+1\notin\Pi$. Then*

(i) $r+1\in\widetilde{\Pi}$.

(ii) Suppose that $\{i,i+1,\ldots,i+r'\}\subset\Pi$; then $r'\leq r$.

(iii) *Let $i \in \Pi$ be such that $i-1 \notin \Pi$; then $i, i+1, \ldots, i+r \in \Pi$.*

(iv) *For $j \in \widetilde{\Pi}$ and $j' \in \Pi$ such that $j'-1 \notin \Pi$ one has $r+1 \mid j$, $r+1 \mid j'$.*

Proof This lemma is the crucial step towards the proof of 3.2. Particularly important is part (iii).

(i) This is obvious.

(ii) Suppose that, for some $i \in \Pi$, one would have $i, i+r+1 \in \Pi$. Then this would yield two different representations of $i+r+1$ as j_1+j_2 with $j_1 \in \Pi$ and $j_2 \in \widetilde{\Pi}$, namely $(i+r+1)+0$ and $i+(r+1)$, a contradiction.

(iii) Suppose that (iii) does not hold; let $i \in \Pi$ be the smallest element such that $i-1 \notin \Pi$, but $i \in \Pi$, $i, i+1, \ldots, i+r \in \Pi$ is *not* true. Choose a maximal r' such that $i, i+1, \ldots, i+r' \in \Pi$; by assumption $r'+1 \leq r$. Write $i+r'+1$ as j_1+j_2 with $j_1 \in \Pi$, $j_2 \in \widetilde{\Pi}$. Since $i+r'+1 \notin \Pi$ we have $j_2 > 0$ and thus $j_2 \geq r+1$. This gives $j_1 < i$.

We claim that $j_1 - 1 \notin \Pi$. This is clear if $j_1 = 0$ and if $j_1 > 0$ we consider the identity $i+r' = (i+r')+0 = (j_1-1)+j_2$ which shows that $j_1 - 1 \in \Pi$ would yield two different representations of $i+r'$ by elements of Π and $\widetilde{\Pi}$. Thus $j_1 \in \Pi$, $j_1 - 1 \notin \Pi$ and $j_1 < i$. Since i was the smallest element for which (iii) does not hold it follows that $j_1, j_1+1, \ldots, j_1+r \in \Pi$. In particular we have $j_1+(r-r') \in \Pi$ as well as $j_1+(r-r') < i$ which leads to two different representations of $i+r+1$: $i+r+1 = i+(r+1) = (j_1+(r-r'))+j_2$ $(i, j_1+(r-r') \in \Pi,\ r+1, j_2 \in \widetilde{\Pi})$. This contradiction proves (iii).

(iv) Let $\Pi' := \{i \mid i \in \Pi, i-1 \notin \Pi\}$ (possibly $\Pi' = \{0\}$). By (ii) and (iii) every $j \in \Pi$ can uniquely be written as $j = j' + j''$ with $j' \in \{0, \ldots, r\}$ and $j'' \in \Pi'$. Hence every $j \in \{0, \ldots, m\}$ has a unique representation $j = j_1 + j_2$ with $j_1 \in \{0, \ldots, r\}$ and $j_2 \in \Pi' + \widetilde{\Pi}$. Thus the assertion follows from the preceding lemma.

Proof of the theorem We proceed by induction on m. The theorem is obviously true for $m = 1$, and we will assume that it has already been proved for all $s \geq 2$ and all $\widetilde{m} < m$.

Let $s \geq 2$ and $(\Pi_1, \ldots, \Pi_s)$ be a canonically ordered $(k_1, \ldots, k_s)$–family for $\{0, \ldots, m\}$.

In order to prove (i) we have to exhibit $g_1, \ldots, g_t$ with $g_1 \cdots g_t = m+1$ and a partition of $\{1, \ldots, t\}$ as $\Delta_1 \dot{\cup} \cdots \dot{\cup} \Delta_s$ such that

(1) $\Delta_\sigma \neq \emptyset$

(2) for no σ and no j one has $j, j+1 \in \Delta_\sigma$

(3) the smallest element of Δ_σ is smaller than the smallest element of $\Delta_{\sigma+1}$

(4) with $\widehat{\Pi}_\tau := g_{\tau-1}\cdots g_1\{0,\ldots,g_\tau - 1\}$ one has $\Pi_\sigma = \sum_{\tau\in\Delta_\sigma} \widehat{\Pi}_\tau$ for all σ.

To this end consider $\Pi := \Pi_1$ and $\widetilde{\Pi} := \Pi_2 + \cdots + \Pi_s$. By assumption $1 \in \Pi_1$ so that we may apply Lemma 3.3: there is an $r \geq 1$ such that $\Pi = \{0,\ldots,r\} + \Pi'$, and $r+1$ divides all elements of $\Pi' + \widetilde{\Pi}$. In particular $r+1$ divides the largest element n of $\Pi' + \widetilde{\Pi}$, and since $m = n + r$ this means that $(r+1) \mid (m+1)$. Let $\widetilde{m} := (m-r)/(r+1)$ (= our candidate to apply the induction hypothesis). We set $\widetilde{\Pi}_1 := \Pi'/(r+1)$, $\widetilde{\Pi}_\sigma := \Pi_\sigma/(r+1)$ for $\sigma > 1$ and suppose for the moment that all $\widetilde{\Pi}_\sigma$ are different from zero (in fact $\widetilde{\Pi}_1$ could be zero: this happens if Π_1 was just $\{0,\ldots,r\}$, we will discuss this case later). Then $(\widetilde{\Pi}_1,\ldots,\widetilde{\Pi}_s)$ constitutes an admissible $(\widetilde{k}_1,\ldots,\widetilde{k}_s)$–family for $\widetilde{m}$; here $\widetilde{k}_1 := (k_1 - r)(r+1)$, $\widetilde{k}_\sigma := k_\sigma/(r+1)$ for $\sigma > 1$, and all these numbers are strictly positive. We want to apply our induction hypothesis, but the $\widetilde{\Pi}_1,\ldots,\widetilde{\Pi}_s$ are not necessarily canonically ordered (they will have this property possibly only after a suitable permutation). Nevertheless, if we neglect the possible permutation, there are $\widetilde{g}_1,\ldots,\widetilde{g}_{\widetilde{t}}$ with $\widetilde{g}_1\cdots\widetilde{g}_{\widetilde{t}} = \widetilde{m}+1$ and nonvoid disjoint subsets $\widetilde{\Delta}_\sigma$ of $\{1,\ldots,\widetilde{t}\}$ with $\widetilde{\Delta}_1 \cup\cdots\cup \widetilde{\Delta}_s = \{1,\ldots,\widetilde{t}\}$ such that no $\widetilde{\Delta}_\sigma$ contains consecutive $j, j+1$, and $\widetilde{\Pi}_\sigma = \sum_{\tau\in\widetilde{\Delta}_\sigma} \widetilde{g}_{\tau-1}\cdots\widetilde{g}_1\{0,\ldots,\widetilde{g}_\tau - 1\}$.

By the definition of the $\widetilde{\Pi}_\sigma$ this means that $\Pi_\sigma = \sum_{\tau\in\widetilde{\Delta}_\sigma} \widetilde{g}_{\tau-1}\cdots\widetilde{g}_1(r+1)\{0,\ldots,\widetilde{g}_\tau - 1\}$ for $\sigma > 1$, and $\Pi_1 = (\sum_{\tau\in\widetilde{\Delta}_1} \widetilde{g}_{\tau-1}\cdots\widetilde{g}_1(r+1)\{0,\ldots,\widetilde{g}_\tau - 1\}) + \{0,\ldots,r\}$.

Now note that $m+1 = (r+1)(\widetilde{m}+1)$ so that $m+1 = g_1 g_2\cdots g_t$ if we set $g_1 := r+1$, $t := \widetilde{t}+1$, $g_\tau := \widetilde{g}_{\tau-1}$ for $\tau > 1$. Also $\Pi_\sigma = \sum_{\tau\in\Delta_\sigma} g_{\tau-1}\cdots g_1\{0,\ldots,g_\tau - 1\}$ is valid if we put $\Delta_1 := \{1\} \cup \{\tau+1 \mid \tau \in \widetilde{\Delta}_1\}$, $\Delta_\sigma := \{\tau+1 \mid \tau \in \widetilde{\Delta}_\sigma\}$ for $\sigma > 1$. This is nearly that which has to be shown, only (2) and (3) remain to be proved. (2) needs a verification only for $\sigma = 1$, and there it is the assertion that $1 \notin \widetilde{\Delta}_1$. But this is just the statement $r+1 \notin \Pi_1$ which is clear from the construction.

And (3) follows from the fact that the $\Pi_1,\ldots,\Pi_s$ are in canonical order: by assumption

α_σ, the smallest positive element of Π_σ, is smaller than $\alpha_{\sigma+1}$ = the smallest positive element of $\Pi_{\sigma+1}$. But from our construction, $\alpha_\sigma = g_{\tau_\sigma - 1} \cdots g_1$, where $\tau_\sigma = \min \Delta_\sigma$, so that $\alpha_\sigma < \alpha_{\sigma+1}$ gives $\tau_\sigma < \tau_{\sigma+1}$.

It remains to treat the necessary modifications if $\Pi' = \{0\}$. In this case we proceed similarly, but we only have to consider the $\widetilde{\Pi}_2, \ldots, \widetilde{\Pi}_s$ above which give rise to $\widetilde{g}_1, \ldots, \widetilde{g}_{\widetilde{t}}$ and $\{1, \ldots, \widetilde{t}\} = \widetilde{\Delta}_2 \dot{\cup} \cdots \dot{\cup} \widetilde{\Delta}_s$ according to the induction hypothesis. Construct the Δ_σ from the $\widetilde{\Delta}_\sigma$ as above for $\sigma > 1$ and put additionally $\Delta_1 := \{1\}$.

The proof of (i) is complete, let us turn to the uniqueness part (ii). So suppose that $\Pi_1, \ldots, \Pi_s$ is a canonically ordered $(k_1, \ldots, k_s)$–family, derived from $(g_1, \ldots, g_t; \Delta_1, \ldots, \Delta_t)$ and also from $(\widetilde{g}_1, \ldots, \widetilde{g}_{\widetilde{t}}; \widetilde{\Delta}_1, \ldots, \widetilde{\Delta}_{\widetilde{t}})$. Then $g_1 = \widetilde{g}_1$ since this number is by construction that integer r for which $\{0, \ldots, r\} \subset \Pi_1$ but $r+1 \notin \Pi_1$. Now pass as in the proof of (i) from $\Pi_1, \ldots, \Pi_s$ to $\widetilde{\Pi}_1, \ldots, \widetilde{\Pi}_s$; it should be clear how uniqueness of the representation of $\widetilde{\Pi}_1, \ldots, \widetilde{\Pi}_s$ (more precisely: of its canonically ordered rearrangement) gives rise to uniqueness for the original family so that it is simple to establish (ii) by induction.

In order to illustrate the theorem it seems to be convenient first to *summarize our proof.* Let us start with an admissible $(k_1, \ldots, k_s)$–family $\Pi_1, \ldots, \Pi_s$. We do not assume that it is canonically ordered. Define $\sigma(1)$ to be that number σ for which $1 \in \Pi_\sigma$ and $g_1 := r + 1$, where r is such that $\{0, \ldots, r\} \in \Pi_{\sigma(1)}$, $r + 1 \notin \Pi_{\sigma(1)}$. Now define a new family, $\Pi_1^{(2)}, \ldots, \Pi_s^{(2)}$ by $\Pi_\sigma^{(2)} := \Pi_\sigma / g_1$ for $\sigma \neq \sigma(1)$, and $\Pi_{\sigma(1)}^{(2)} := \{i \mid i \in \Pi_{\sigma(1)}, \, i - 1 \notin \Pi_{\sigma(1)}\} / g_1$ (it might happen that $\Pi_{\sigma(1)}^{(2)} = \{0\}$). Suppose that $g_1, \ldots, g_\tau$, $\sigma(1), \ldots, \sigma(\tau)$ and $\Pi_1^{(\tau+1)}, \ldots, \Pi_s^{(\tau+1)}$ already have been constructed. If this is not the family $\{0\}, \ldots, \{0\}$ there is a unique $\sigma(\tau + 1)$ with $1 \in \Pi_{\sigma(\tau+1)}^{(\tau+1)}$, and $g_{\tau+1}$ will be one plus that number r for which $\{0, \ldots, r\} \in \Pi_{\sigma(\tau+1)}$, $r + 1 \notin \Pi_{\sigma(\tau+1)}^{(\tau+1)}$. Pass from $\Pi_\sigma^{(\tau+1)}$ to $\Pi_\sigma^{(\tau+2)}$ similarly as we have got the $\Pi_\sigma^{(2)}$ from the Π_σ (where $\sigma(\tau+1)$ has to be treated in a different way than the other indices). Thus we find $g_1, \ldots, g_t$, $\sigma(1), \ldots, \sigma(t)$ until this reduction stops with $\Pi_\sigma^{(t+1)} = \{0\}$ (all σ). Then, with $\Delta_\sigma := \{\tau \mid \sigma(\tau) = \sigma\}$ the original family is derived from $(g_1, \ldots, g_t; \Delta_1, \ldots, \Delta_t)$, and if the $\Pi_1, \ldots, \Pi_s$ have been in canonical order the $\Delta_1, \ldots, \Delta_t$ will automatically be an alternating partition.

As an example consider the family constructed after definition 3.1,
i.e. $\Pi_1 = (1\,1\,0\,0\,1\,1\,0\,0\,1\,1)$, $\Pi_2 = (1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1)$.

With the previously introduced notation we get:

$\sigma(1) = 1\,,\quad g_1 = 2\,;\quad \Pi_1^{(2)} = (1\,0\,1\,0\,1)\,,\quad \Pi_2^{(2)} = (1\,1\,0\,0\,0\,0\,1\,1)\,;$

$\sigma(2) = 2\,,\quad g_2 = 2\,,\quad \Pi_1^{(3)} = (1\,1\,1)\,,\quad \Pi_2^{(3)} = (1\,0\,0\,1)\,;$

$\sigma(3) = 1\,,\quad g_3 = 3\,;\quad \Pi_1^{(4)} = (0)\,,\quad \Pi_2^{(4)} = (1\,1)\,;$

$\sigma(4) = 2\,,\quad g_4 = 2\,;\quad \Pi_1^{(5)} = (0)\,;\quad \Pi_2^{(5)} = (0)\,.$

It follows that Π_1, Π_2 is derived from $(2, 2, 3, 2; \{1, 3\}, \{2, 4\})$ (which in this case we knew in advance).

In the case $s = 2$ the $\sigma(\tau)$ will be alternating, e.g. $\sigma(1) = \sigma(3) = \cdots = 1$, $\sigma(2) = \sigma(4) = \cdots = 2$ (if $1 \in \Pi_1$) or vice versa (if $1 \in \Pi_2$). This gives immediately the

3.5 Corollary *Let m, k_1, k_2 be such that $m = k_1 + k_2$ and that there are $\Pi_1 \subset \{0, \ldots, k_1\}$, $\Pi_2 \subset \{0, \ldots, k_2\}$ such that every $j \in \{0, \ldots, m\}$ can uniquely be written as $j = j_1 + j_2$ with $j_1 \in \Pi_1$, $j_2 \in \Pi_2$; suppose that $1 \in \Pi_1$. Then there are $g_1, \ldots, g_t$ with $g_1 \cdots g_t = m + 1$ for which one has*

$k_1 = (g_1 - 1) + (g_3 - 1)\, g_2 g_1 + (g_5 - 1)\, g_4 g_3 g_2 g_1 + \cdots\,,$

$k_2 = (g_2 - 1)\, g_1 + (g_4 - 1)\, g_3 g_2 g_1 + (g_6 - 1)\, g_5 g_4 g_3 g_2 g_1 + \cdots\,.$

k_1, k_2 can also be obtained as follows: Put $k_1' := g_t - 1$, $k_1'' := 0$, $k_\tau' := g_{t-\tau+1} k_{\tau-1}'' + g_{t-\tau+1} - 1$, $k_\tau'' := g_{t-\tau+1} k_{\tau-1}'$ for $\tau = 2, \ldots, t$; then $(k_1, k_2) = (k_t', k_t'')$ or $= (k_t'', k_t')$ (depending on whether t is even or odd).

4. Consequences

A. For what $(k_1, \ldots, k_s)$ are there admissible families?

Let $(\widetilde{k}_1, \ldots, \widetilde{k}_s)$ be fixed and $m := \widetilde{k}_1 + \cdots + \widetilde{k}_s$. Is there an admissible $(\widetilde{k}_1, \ldots, \widetilde{k}_s)$–family in canonical order? One has to check all decompositions of $m+1$ as $m+1 = g_1 g_2 \cdots g_t$ and all alternating s–partitions of $\{1, \ldots, t\}$ to decide whether one possibility leads to $(\widetilde{k}_1, \ldots, \widetilde{k}_s)$. If the canonical order is of no importance, it has to be calculated whether a permutation of the family derived from $(g_1, \ldots, g_t; \Delta_1, \ldots, \Delta_s)$ leads to a family with the desired properties.

Examples

1) Is there an admissible $(5,8)$–family? There are only two decompositions of $5+8+1=14$: $2\cdot 7$ and $7\cdot 2$. They lead (with the help of cor. 35) to the $(1,12)$–family $((1\,1),\,(1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1)$ and the $(6,7)$–family $((1\,1\,1\,1\,1\,1\,1),\,(1\,0\,0\,0\,0\,0\,0\,1))$, respectively. Hence there is no $(5,8)$–family.

2) Let's check the existence of $(3,8)$–families. The decompositions of $3+8+1$ as $2\cdot 6$, $6\cdot 2$, $3\cdot 4$, $4\cdot 3$, $2\cdot 2\cdot 3$, $2\cdot 3\cdot 2$, $3\cdot 2\cdot 2$ lead to $(1,10)$–, $(5,6)$–, (2,9)–, (3,8)–, (9,2)–, (7,4)–, (8,3)–families. Therefore there are even two different (3,8)–families Π_1,Π_2 (but only one where $1\in\Pi_1$):
$((1\,1\,1\,1),(1\,0\,0\,0\,1\,0\,0\,0\,1))$ and $((1\,0\,0\,1),(1\,1\,1\,0\,0\,0\,1\,1\,1))$.

B. Are the $(k_1,\ldots,k_s)$–families unique if there exist any?

The preceding example shows that there can be different (k_1,k_2)–families. It might be, however, that there is always at most one canonically ordered (k_1,k_2)–family as in this example. But this is not the case; the following proposition shows how non–uniqueness is caused by certain divisors of $m+1$:

4.1 Proposition

(i) Suppose that $12\mid(m+1)$. Then there exist k_1,k_2 with $k_1+k_2=m$ for which there are two different (k_1,k_2)–families (Π_1,Π_2) (one where $1\in\Pi_1$, and another where $1\in\Pi_2$).

(ii) Let m be such that $36\mid(m+1)$ or $150\mid(m+1)$. Then one can find k_1,k_2 with $k_1+k_2=m$ such that there exist two different canonically ordered (k_1,k_2)–families.

Proof

(i) Let $h_1\cdots h_{\tilde t}$ be any decomposition of $(m+1)/12$. Then $4\cdot 3\cdot h_1\cdots h_{\tilde t}$ and $3\cdot 2\cdot 2\cdot h_1\cdots h_{\tilde t}$ are decompositions of $m+1$ which we denote by $g_1\cdot\cdots\cdot g_t$ and $g_1^*\cdots g_{t^*}^*$. Let (k_1,k_2) and (k_1^*,k_2^*) be the pairs which arise according to cor. 3.5. Then $(k_1,k_2)=(k_2^*,k_1^*)$ which follows from the second part of this corollary: Denote the k'_τ,k''_τ obtained by using the g's or the g^*'s by k'_τ,k''_τ and $k^{*'}_\tau,k^{*''}_\tau$, respectively.

Then $(k'_{\widetilde{t}}, k''_{\widetilde{t}}) = (k^{*\prime}_{\widetilde{t}}, k^{*\prime\prime}_{\widetilde{t}}) =: (\alpha, \beta)$, since the g's and the g^*'s have the same last $\widetilde{t}$ elements. There are still two resp. three induction steps left to get (k_1, k_2) resp. (k_1^*, k_2^*), and an explicit calculation gives $(k_1, k_2) = (k_2^*, k_1^*) = (12\alpha{+}3, 12\beta{+}8)$.
(Let's abbreviate the technique of the preceding paragraph by saying that $3 \cdot 2 \cdot 2 \cdot \cdots$ gives rise to (k_2, k_1) if $4 \cdot 3 \cdots$ gives rise to (k_1, k_2).)

It is now clear why (i) holds.
Note that even more is true: what we have done with $4 \cdot 3 \cdots$ and $3 \cdot 2 \cdot 2 \cdots$ can also be repeated with $3 \cdot 4 \cdots$ and $2 \cdot 2 \cdot 3 \cdots$ so that there are in fact more examples than claimed.

(ii) The idea is the same, but this time $9 \cdot 4$ and $3 \cdot 2 \cdot 2 \cdot 3$ are of importance: $9 \cdot 4 \cdots$ and $3 \cdot 2 \cdot 2 \cdot 3 \cdots$ lead to the *same* (k_1, k_2) (the situation is different to that of (i) since in this case the number of the factors is modulo 2 the same).
For the assertion concerning 150 one has to check that $5 \cdot 5 \cdot 6 \cdots$ and $10 \cdot 3 \cdot 5 \cdots$ lead to the same (k_1, k_2).

Notes

1) The simplest concrete example to apply (ii) is $m = 35$: There are two $(8, 27)$–families (Π_1, Π_2) with $1 \in \Pi_1$, namely
((1 1 1 1 1 1 1 1 1), (1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1)),
((1 1 1 0 0 0 1 1 1), (1 0 0 1 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 1 0 0 1)).
2) The properties of $12, 36, 150$ in this proposition have been found by trial and error. We have no idea how one could produce systematically $a_1 \cdots a_r$, $b_1, \cdots, b_s$ such that $a_1 \cdots a_r = b_1 \cdots b_s$, and $a_1 \cdots a_r \cdots$ lead to the same (k_1, k_2) as $b_1 \cdots b_s \cdots$.

C. Are there many (k_1, k_2) with $k_1 + k_2 = m$ which admit admissible families?

The answer depends on m, of course. Recall our systematic enumeration of the (k_1, k_2) with $k_1 + k_2 = 11$ for which there are admissible (k_1, k_2)–families: here one has such families for *all* (k_1, k_2) (not in every case, however, one has $1 \in \Pi_1$; this happens only when $k_1 = 1, 2, 3, 5, 7, 8, 9$). There are other examples, here is the complete list for the $m < 255 : m = 3, 5, 7, 11, 15, 23, 31, 35, 47, 63, 71, 95, 127, 143, 191, 215$. For some of

these m the phenomenon can easily be understood; whenever m is of the form $2^\ell - 1$, then for all (k_1, k_2) with $k_1 + k_2 = m$ admissible families exist. The easiest way to explain this is to remember the proofs in section 3. Admissible families arise when one groups together the $\widehat{\Pi}_\tau$, and one has only to notice that every k_1 can be obtained by taking the sum over a suitable subset of $\{1, 2, 4, 8, \ldots\}$.
We cannot offer any number theoretical explanation concerning the other m with this property.

But what is the answer if we consider a "general" m, i.e. an m chosen "at random". More precisely, define

$$M_{m_0} = \{(k_1, k_2) \mid k_1 + k_2 \le m_0\} \text{ and } \widehat{M}_{m_0} =$$
$$\{(k_1, k_2) \mid k_1 + k_2 \le m_0, \text{ there is an admissible } (k_1, k_2)\text{–family}\}:$$

what about $\mu_{m_0} := \text{card}\, \widehat{M}_{m_0} / \text{card}\, M_{m_0}$ for large m_0?

To this end we have to calculate the number of

$$(g_1, \ldots, g_t) \quad \text{such that} \quad g_1 \cdots g_t = m + 1\,.$$

4.2 Lemma *Suppose that $m+1$ is square–free, i.e. there are pairwise different primes $p_1, \ldots, p_\ell$ with $p_1 \cdots p_\ell = m+1$. Denote by β_ℓ* the number of ordered tuples $(g_1, \ldots, g_t)$ with $g_1 \ldots g_t = m + 1$, where t runs through $1, 2, \ldots, \ell$.

(i) $\beta_\ell = \alpha_1^\ell + \alpha_2^\ell + \cdots + \alpha_\ell^\ell$, where the α's can be obtained as follows: $\alpha_1^\ell := 1$ for all ℓ, $\alpha_j^\ell := j\,(\alpha_j^{\ell-1} + \alpha_{j-1}^{\ell-1})$ for $j < \ell$, $\alpha_\ell^\ell := \ell!$

(ii) $\beta_\ell \le 2^{\ell-1}\ell!$.

Proof

(i) Put α_t^ℓ = the number of $(g_1, \ldots, g_t)$ with $g_1 \cdots g_t = m + 1$ (which obviously only depends on ℓ and not on $m+1$). Then it is easy to check that the α's satisfy the above relations.

(ii) From (i) it follows that $\alpha_j^\ell \le \ell\,(\alpha_j^{\ell-1} + \alpha_{j-1}^{\ell-1})$ for $1 < j < \ell$, and this is valid for *all* j if we put $\alpha_{-1}^\ell := 0$, $\alpha_{\ell+1}^\ell := 0$. Thus $\beta_\ell \le 2\ell\beta_{\ell-1}$, and this gives (ii).

Note Here are the first β's: $\beta_1 = 1$, $\beta_2 = 3$, $\beta_3 = 13$, $\beta_4 = 75$, $\beta_5 = 541$.

By cor. 3.5 there are precisely β_ℓ admissible different (k_1, k_2)–families in canonical order; one of these is the trivial (m)–family $(\{0, \dots, m\})$, and there might be different families for the same values of (k_1, k_2). If $m + 1 = p_1 \cdots p_\ell$ with primes which are not necessarily distinct then the number of different $(g_1, \dots, g_t)$ with $g_1 \cdots g_t = m + 1$ is $\leq \beta_\ell$ (a precise calculation seems to be difficult). In any case we know: If $(m + 1)$ is built up from ℓ primes, then the number of different (k_1, k_2)–families for $\{0, \dots, m\}$ is $\leq \beta_\ell$. By a result of Erdös and Kac ([2], or [1], p. 395 and p. 399) one knows that ℓ is of magnitude $\log \log m$, and combining this with 4.2 (ii) and with the help of Stirling's formula we get $\mu_{m_0} \longrightarrow 0$.

D. Factorizations of the uniform distribution

Here is the solution of the problem we started with (the set $\{0, g, 2g, \dots, rg\}$ in this theorem is a typical set $\widehat{\Pi}_\tau$ in the notation of part 1 of section 3):

4.3 Theorem *Let $k_1, \dots, k_s, m$ be such that $k_1 + \cdots + k_s = m$. There are probabilities $P_1, \dots, P_s$ on $\{0, \dots, k_1\}, \dots, \{0, \dots, k_s\}$ such that $P_1 * \cdots * P_s$ is the uniform distribution on $\{0, \dots, m\}$ iff there are subsets $\Pi_\sigma \subset \{0, \dots, k_\sigma\}$ such that every $j \in \{0, \dots, m\}$ can uniquely be written as $j = j_1 + \cdots + j_s$ with $j_\sigma \in \Pi_\sigma$. In this case the P_σ are uniform on such Π_σ, and each P_σ is of the form $P_{\sigma,1} * \cdots * P_{\sigma,t_\sigma}$, where the $P_{\sigma,\tau}$ are uniform distributions on sets of the form $\{0, g, 2g, \dots, rg\}$. The possible $(k_1, \dots, k_s)$, $\Pi_1, \dots, \Pi_s$ are described in section 3.*

E. Factorizations of $1 + x + \cdots + x^m$ into polynomials with nonnegative coefficients

4.4 Theorem *If $1 + x + \cdots + x^m$ is written as $A_1(x) \cdots A_s(x)$, where the A_σ have nonnegative coefficients and leading coefficient 1, then each A_σ is a product of polynomials of the form $1 + x^g + \cdots + x^{rg}$. Consequently the only possibility to write $\{\xi \mid \xi^{m+1} = 1, \xi \neq 1\}$ as a disjoint union $W_1 \dot\cup \cdots \dot\cup W_s$ such that $\prod_{\xi \in W_\sigma} (x - \xi)$ have nonnegative coefficients for all σ is to choose the W_σ as disjoint unions of sets of the form "all r'th roots of all ξ such that $\xi^{g+1} = 1$, $\xi \neq 1$".*

References

[1] P. Billingsley: *Probability and measure.* John Wiley and Sons 1995.

[2] P. Erdös, M. Kac: *On the Gaussian law of errors in the theory of additive functions.* Proc. Nat. Acad. Sci USA 25, 1933, 206–207.

[3] G. Letac: *Problèmes de Probabilité.* Paris, Presses Universitaires de France, 1970.

[4] G. Letac: *Integration and Probability by P. Malliavin.* Springer Verlag, New York, Berlin, Heidelberg, 1995.

[5] V. Linnik: *Decomposition of probability distributions.* Oliver & Boyd, London 1964.

[6] E. Lukacz: *Developments in characteristic function theory.* Charles Griffin & Company, London 1983.

[7] D.A. Raikov: *One property of cyclotomic polynomials.* Matem. sb. 2 (44), 1937, 379–382.

[8] G. Szekely: *Paradoxes in probability theory and mathematical statistics.* D. Reidel Publishing Company, Boston 1986.

Ehrhard Behrends
I. Mathematisches Institut
Arnimallee 3
D – 14195 Berlin