Sacks of dice with fair totals

Ian Morrison
Department of Mathematics
Fordham University
Bronx, NY 10458
morrison@fordham.edu

1. Introduction

In this paper, a die is a finite probability space whose outcomes are non-negative integers and that may have any probability distribution. A fair die is one for which all outcomes are equally likely. A sack is a finite set of independent dice and a sack is called fair if, when the dice are rolled, all totals are equally likely. More precise definitions are given in section 2, where we set up all our notation and review the results of Gasarch and Kruskal [4] cited below.

Over 60 years ago, the familiar fact that a pair of fair cubical dice has totals that are unfair prompted J. B. Kelly to pose in American Mathematical Monthly problem E 925 [5], the converse question "Can unfair dice have fair totals?" which has a negative answer. A number of papers [1, 3–7] reviewed in Remark 2.5, have considered this question for more general sacks. Most involve conditions on the possible orders of the dice in a sack that guarantee unfairness and very few examples of fair sacks were known.

Gasarch and Kruskal [4], however, asked, "What common structure do all fair sacks share?" and showed that all dice in a fair sack must be *semifair*. Most sacks of semifair dice are, however, not fair. Indeed, we will see in Corollary 5.1 that most semifair dice do not lie in *any* fair sack. Gasarch and Kruskal proved that a sack of semifair dice is fair exactly when it has a global property that we call Uniqueness of Totals: exactly one roll yields each total. Their work does not provide any way to test for this property other than brute force enumeration of the totals of all rolls and, although they gave examples of fair sacks with this property, they found no systematic construction.

This paper provides such a construction. In section 3, we give, in Proposition 3.7, an explicit procedure that yields all known fair sacks and many more, usually in many ways. In section 4, we prove our main results, Theorem 4.1, which produces the sacks of section 3 in a canonical way, and Theorem 4.2 asserting that Theorem 4.1 produces *all* fair sacks. Finally, in section 5, we give a few applications. Our methods are completely elementary, relying principally on a systematic exploitation of Uniqueness of Totals.

2010 *Mathematics Subject Classification.* Primary 60C05, 12D05.
Key words and phrases. fair, dice.

2. Background on fair sacks

Notation and terminology We use two indexing shorthands, $[n] := \{0, 1, \ldots, n\}$ and $\langle n \rangle := \{1, \ldots, n\}$. In what follows, we index sides of dice by $j \in [n]$, dice in sacks by $i \in \langle m \rangle$, and factors in products by $h \in \langle \ell \rangle$, and parts of partitions by $g \in \langle k \rangle$. In our constructions, factors and parts often index dice too.

The *t-fair polynomial* is $\psi_t(x) := 1 + x + \cdots + x^t = \left(\frac{1-x^{t+1}}{1-t}\right)$. Its quotient form shows that the roots of $\psi_t(x)$ are exactly the $(t+1)^{\text{th}}$ roots of unity, except for 1. We expand polynomials in lower-to-higher degree order as in the first form.

A *n-die* $\mathbf{d}$ is a probability space of order $n+1$ with outcomes or *sides* indexed by $j \in [n]$ having real probabilities $p_{\mathbf{d}}(j) \in [0,1]$ summing to 1 and with $p_{\mathbf{d}}(n) > 0$. When there is no risk of confusion, we drop the subscript $\mathbf{d}$. Note that our choices of largest side n and order $n+1$ are "off by one" from the conventions in [4] so that, in many formulas for sacks of dice below, we do not need to correct by the number of dice. Second, we will confound the die $\mathbf{d}$ and the polynomial $\mathbf{d}(x) = \sum_{j=0}^{n} p(j) x^j$: the positivity of $p(n)$, ensures that $\deg\big(\mathbf{d}(x)\big) = n$. A polynomial arising from some $\mathbf{d}$ in this way we call a *die polynomial*. The polynomial $\mathbf{d}(x)$ is also the generating function of a tautological random variable $D_{\mathbf{d}}$ defined by $D_{\mathbf{d}}(j) = j$.

A die is *fair* if all $p_{\mathbf{d}}(j)$ are equal, in which case the monic scaling of $\mathbf{d}(x)$ is $(k+1)\mathbf{d}(x) = \psi_k(x)$. A die is *semifair* if $\mathbf{d}(x)$ is palindromic ($p(j) = p(n-j)$) and if all non-zero $p(j)$ are equal (hence equal to $p(n)$ and $p(0)$). This notion is borrowed directly from [4] except that we use semifair as a more evocative replacement for the term "nice" used there.

Remark 2.1. For $\mathbf{d}$ semifair, the monic scaling of $\mathbf{d}(x)$ is obtained from $\psi_n(x)$ by setting to 0 a palindromic set of the interior coefficients, hence leaving at least 2 coefficients non-zero.

A *sack* $\mathbf{S}$ of size $m_{\mathbf{S}}$ is an *ordered* set of *independent* dice $\mathbf{d}_i$ of orders n_i indexed by $i \in \langle m_{\mathbf{S}} \rangle$. To simplify notation, we omit reference to $\mathbf{S}$ when it is understood and write, for example, m for $m_{\mathbf{S}}$. The *total* of $\mathbf{S}$ is the sum $t = \sum_{i \in \langle m \rangle} n_i$. Each $\mathbf{S}$ has a product sample space $\mathbf{J}$ indexed by $\mathbf{j} = (j_1, j_2, \ldots, j_m) \in \prod_{i \in \langle m \rangle} [n_i]$ equipped with product probability distribution $p(\mathbf{j}) = \prod_{i \in \langle m \rangle} p_{\mathbf{d}_i} j_i$ and projection maps $\mathrm{pr}_i : \mathbf{J} \to [n_i]$. On $\mathbf{J}$, we define *die random variables* $X_i(\mathbf{j}) := \big(D_i \circ \mathrm{pr}_i\big)(\mathbf{j}) = j_i$ and a *total random variable* $T(\mathbf{j}) := \sum_{i \in \langle m \rangle} X_i = \sum_{i \in \langle m \rangle} j_i$.

By definition, X_i has generating function $\mathbf{d}_i(x)$. Since the generating function of a sum of independent random variables is the product of their generating functions (cf. [2, p. 180, Theorem 6]), the total T has the degree t generating function

$$\mathbf{T}(x) = \prod_{i \in \langle m \rangle} \mathbf{d}_i(x) = \sum_{s=0}^{t} \Bigg(\sum_{T(\mathbf{j}) = s} p(\mathbf{j}) \Bigg) x^s \,. \tag{2.2}$$

In words, "sacks with totals $\mathbf{T}(x)$ correspond to ordered factorizations of $\mathbf{T}(x)$ into dice polynomials". Note that $\mathbf{T}(x)$ is also the polynomial of a t-die which we call the *total die* of the sack $\mathbf{S}$. More generally, any subset of $\langle m \rangle$ determines both a sack and a total die.

The Gasarch-Kruskal Theorem A sack $\mathbf{S}$ is *fair* if its total die $\mathbf{T}$ is fair—that is, all totals are equally likely to appear when the dice in $\mathbf{S}$ are rolled—so that $(t+1)\mathbf{T}(x) = \psi_t(x))$.

The main result of Gasarch and Kruskal states:

Theorem 2.3 ([4, Corollary 5]). *The sack* $\mathbf{S}$ *is fair if and only if:*

(1) *Each die* $\mathbf{d}_i$ *is semifair.*
(2) **(Uniqueness of Totals)** *For each s, there is a unique* $\mathbf{j}$ *for which* $T(\mathbf{j}) = s$ *and* $p(\mathbf{j}) \neq 0$*. Equivalently, exactly one term in the sum defining the coefficient of* x^s *in (2.2) is non-zero.*

For each die and total, we can use Uniqueness of Totals to define $\sigma_{\mathbf{d}}(s)$ as the degree of the factor from $\mathbf{d}(x)$ in the unique term of degree s in $\mathbf{T}(x)$. We obtain, for each die, a *factor degree* function $\sigma_{\mathbf{d}} : [t] \to [t]$.

The key point in the Theorem is that fairness of $\mathbf{S}$ implies semifairness of the $\mathbf{d}_i(x)$. Given this, all the non-zero $p(\mathbf{j})$ have a common value, since each is a product of one non-zero coefficient from each $\mathbf{d}_i(x)$. Hence, each total must arise from the same number of such products. But the totals 0 and t arise, respectively, only from the products of the 0^{th} and ${n_i}^{\text{th}}$ coefficients in each d_i.

This argument suggests a more convenient normalization of the polynomials of semifair dice and fair sacks: replace $\mathbf{T}(x)$ and each $\mathbf{d}_i(x)$ by their monic scalings. Since the probability condition allows us to recover the scalings, we lose nothing by assuming this and will do so henceforth. The equation $\mathbf{T}(x) = \prod_{i \in \langle m \rangle} \mathbf{d}_i(x)$ continues to hold, but now all $p(\mathbf{j})$ equal either 0 or 1 with exactly one of the latter giving each total.

One further easy consequence comes up often enough to merit a corollary. If a fair sack contains a die with a non-zero x^s term for any $s > 0$, then the total s arises from rolling s on this die and 0 on all the others. Hence, by Uniqueness of Totals,

Corollary 2.4. **(Uniqueness of Terms)** *A fair sack can contain at most one die with non-zero* x^s *term for any* $s \in \langle t \rangle$ *and contains such a die if and only if* x^s *does not arise as a product of terms of strictly lower degree. In particular, there is always a unique die with non-zero* x *term.*

Remark 2.5. Since a semifair die of order n has a nonzero x^{n-1} term *no two dice in a fair sack can have the* same *order* n. We digress for a moment to document work of several earlier authors (most mutually unaware of each other) on special cases of this result. Almost all the arguments use inequalities involving the side probabilities to reach a contradiction. This is the approach of Moser and Wahab [5] to show there is no fair pair of dice of order 6. Dudewicz and Dann [3], although they do not cite [5], noted that, for identical cubical dice, the conclusion is a "well-known" exercise and cited the text of Parzen [7], where this is Problem 9.12. They prove that no fair sack (other than a singleton) can have *all* dice of equal order n by showing that the total $n-1$ must have probability strictly greater than $\frac{1}{t+1}$.[1] Their

[1] Their title suggests, incorrectly, that no fair sacks exist as does the mysterious claim in the last line of the paper that "similar results" hold for general sacks.

result is reproved (but not cited) by Chen, Rao and Shreve [1] by showing that there must be a pair of totals whose probabilities differ by at least $\left|\frac{m-1}{m^2n}\right|$. The stronger claim that all orders must be distinct was first proved by Gasarch and Kruskal [4], who incorrectly attribute it to Chen, Rao and Shreve, by casting the argument for the $s = n - 1$ case of Corollary 2.4 as a series of inequalities.

We should also mention a overlapping result. No fair sack can contain more than one die of even order, because such dice have polynomials of odd degree which must have a real root and $\psi_t(x)$ has no real roots for odd t and exactly one for even t. This argument first occurs (for order 6) in the proof of Finch and Halmos [5] that there is no fair pair of dice of order 6 and is also found in [4] and [6].

We conclude this section with a lemma that plays a key role in the proof of our main result, Theorem 4.2, and that we state in the notation used in this application.

Lemma 2.6. *Suppose that* $\mathbf{S}$ *is fair and that* $p_\gamma(s) = p_\gamma(s') = 1$ *with* $s \neq s'$ *and* $p_{\gamma'}(s'+u) = 1$ *with* $\gamma' \neq \gamma$*. Then* $p_{\mathbf{d}}(s+u) = 0$ *for every* $\mathbf{d} \neq \gamma$

Proof. If $p_{\mathbf{d}}(s'+u) = 1$, we would get two distinct terms of degree $s + s' + u$, one with $\sigma_\gamma = s$, $\sigma_{\gamma'} = s' + u$ and all other factors of degree 0, and the other with $\sigma_\gamma = s'$, $\sigma_{\mathbf{d}} = s + u$ and all other factors of degree 0. □

3. Constructing fair sacks

From fair sacks to factorizations The key to applying Theorem 2.3 is to define an *ordered factorization* of $t+1$ of size ℓ to be tuple $\mathbf{a} := (a_1, a_2, \ldots, a_\ell)$ for which

$$\prod_{h \in \langle \ell \rangle} a_h = t + 1, \quad \text{and with each } a_h \text{ at least 2.} \tag{3.1}$$

Any fair sack $\mathbf{S}$ yields on ordered factorization $\mathbf{a_S}$ of the same size by taking a_h to be the number of non-zero coefficients of $\mathbf{d}_h(x)$. In (3.1), the equation holds because each side counts the number of non-zero terms $p(\mathbf{j})$ in (2.2) and the inequalities hold by Remark 2.1. We immediately get the last statement of [4, Corollary 9]: for $t+1$ prime, the only fair sack is a single fair t-die.

We can simplify this idea as "fair sacks give ordered factorizations". In other words, there is a function from fair sacks to factorizations. The first step in our construction of fair sacks is to show that this map is surjective: that is, "ordered factorizations give fair sacks". In fact, we do a bit more in Corollary 3.3. While the map from fair sacks to factorizations is not injective, the Corollary constructs a section. That is, from each factorization $\mathbf{a}$ we construct a factorization sack and show that it is fair. Then in Proposition 3.7, we give a more general construction of fair sacks that uses an ancillary partition. In section 4, we show that every fair sack arises from the construction for a canonical factorization and partition.

From factorizations to fair sacks As for sacks, we try to simplify notation by omitting reference to an ordered factorization $\mathbf{a}$ when possible. We first associate to any ordered factorization $\mathbf{a}$ of $t+1$ a *factorization* sack $\mathbf{S_a}$ of the same size.

Lemma 3.2. *Fix an ordered factorization* $\mathbf{a}$ *of* $t+1$ *of size* ℓ. *For* $h \in \langle \ell+1 \rangle$, *define* $b_h := \prod_{h'<h} a_{h'}$ *and note that, by hypothesis,* $t+1 = b_{\ell+1}$. *For* $h \in \langle \ell \rangle$, *define* $\mathbf{d}_h(x) := \psi_{a_h}(x^{b_h})$ *and* $\mathbf{e}_h(x) := \prod_{h' \leq h} \mathbf{d}_{h'}(x)$. *Then* $\mathbf{e}_h(x) = \psi_{b_{h+1}}(x)$. *In particular,* $\mathbf{e}_\ell(x) = \psi_{t+1}(x)$.

Proof. Observe that the roots of $\mathbf{d}_h(x)$ are exactly the ${b_h}^{\text{th}}$ roots of all non-trivial ${a_h}^{\text{th}}$ roots of unity or, equivalently, all $b_h {a_h}^{\text{th}}$ roots of unity of order not dividing b_h or, again equivalently, all the ${b_{h+1}}^{\text{st}}$ roots of unity of order not dividing b_h. By induction on h, the roots of $\mathbf{e}_h(x)$ are exactly the non-trivial ${b_{h+1}}^{\text{st}}$ roots of unity. Since both sides are monic polynomials with the same roots, $\mathbf{e}_h(x) = \psi_{b_{h+1}}(x)$. □

Corollary 3.3. *If* $\mathbf{a}$ *is an ordered factorization of* $t+1$ *of size* ℓ, *let* $\mathbf{S_a}$ *be the* factorization sack *of size* ℓ *whose dice are defined by* $\mathbf{d}_h(x) := \psi_{a_h}(x^{b_h})$. *Then,* $\mathbf{S_a}$ *is a fair sack with total* t.

As an example, we take the case $t+1 = 12$.

Table 3.4 Ordered factorizations $\mathbf{a}$ of 12 and their fair sacks $\mathbf{S_a}$

$a_1 \cdot a_2 \cdot \ldots \cdot a_\ell$	$\mathbf{d}_1(x) \cdot \mathbf{d}_2(x) \cdot \ldots \cdot \mathbf{d}_\ell(x))$
$2 \cdot 2 \cdot 3$	$(1+x)(1+x^2)(1+x^4+x^8)$
$2 \cdot 3 \cdot 2$	$(1+x)(1+x^2+x^4)(1+x^6)$
$2 \cdot 6$	$(1+x)(1+x^2+x^4+x^6+x^8+x^{10})$
$3 \cdot 2 \cdot 2$	$(1+x+x^2)(1+x^3)(1+x^6)$
$3 \cdot 4$	$(1+x+x^2)(1+x^3+x^6+x^9)$
$4 \cdot 3$	$(1+x+x^2+x^3)(1+x^4+x^8)$
$6 \cdot 2$	$(1+x+x^2+x^3+x^4+x^5)(1+x^6)$
12	$(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11})$

We note an equation that follows from Lemma 3.2 by dividing the $h=v$ case by the $h=u$ case and canceling those $\mathbf{d}_{h'}(x)$ that are factors of both $\mathbf{e}_v(x)$ and $\mathbf{e}_u(x)$.

$$\prod_{h=u}^{v} \mathbf{d}_h(x) = \frac{\psi_{b_{v+1}}(x)}{\psi_{b_u}(x)} \tag{3.5}$$

This has a consequence that we will need later.

Corollary 3.6. *If* $\mathbf{a}$ *is obtained from an ordered factorization* $\mathbf{a}'$ *of size* ℓ *by replacing consecutive factors* $a'_u \cdot \ldots \cdot a'_v$ *by their product. Then,* $\mathbf{d}_h(x) = \mathbf{d}'_h(x)$ *for* $1 \leq h < u$, $\mathbf{d}_u(x) = \prod_{h=u}^{v} \mathbf{d}'_h(x)$ *and* $\mathbf{d}_h(x) = \mathbf{d}'_{h+v-u}(x)$ *for* $u < h \leq \ell - v + u$.

Proof. By construction, we have $a_h = a'_h$ for $1 \leq h < u$, $a_u = \prod_{h=u}^{v} a'_h$, and $a_h = a_{h+v-u}$ for $u < h \leq \ell - v + u$. Hence $b_h = b'_h$ for $h \leq u$ and $b_{u+1} = b'_u \prod_{h=u}^{v} a'_h = b'_{v+1}$ and $b_h = b_{h+v-u}$ for $u < h \leq \ell - v + u$. Thus, only the formula for $\mathbf{d}_u(x)$ is not immediate. We may view $\mathbf{d}_u(x)$ as the left side of (3.5) applied to $\mathbf{a}$ with $v = u$ and the product $\prod_{h=u}^{v} \mathbf{d}'_h(x)$ as the left side of (3.5) applied to $\mathbf{a}'$. The formula for the b_{u+1} says that these two instances of (3.5) have equal right hand sides. Hence they have equal left hand sides. □

Factorization-partition sacks Next, we give a recipe that uses a partition of ℓ to produce additional fair sacks of smaller sizes from the factorization sack $\mathbf{S_a}$. Let $\Pi := [\pi_i, \pi_2, \ldots, \pi_k]$ be a partition of ℓ which we will view both as a disjoint union decomposition $\{1, 2, \ldots, n\} = \dot{\bigcup}_{g=1}^{k} \pi_g$ and as a surjective function from $\langle n \rangle \to \langle k \rangle$ with fiber π_g over g.

To each part of Π, we associate a die $\mathbf{d}_g(x) = \prod_{h \in \pi_g} \mathbf{d}_h(x)$ which, by (2.2), is simply the total die of the subsack of $\mathbf{S_a}$ associated to π_g. To the pair $(\mathbf{a}, \Pi)$, we associate the *factorization-partition* sack $\mathbf{S}_{\mathbf{a},\Pi} := (\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_k)$ consisting of the total dice of the parts of Π, and we say that such sacks arise from $\mathbf{a}$.

Proposition 3.7. (1) *Every factorization-partition sack is fair.*
(2) *Every factorization-partition sack arises from an ordered* prime *factorization.*

Proof. Because Π simply partitions the $\mathbf{d}_h(x)$ into disjoint groups with products $\mathbf{d}_g(x)$, the product of all the $\mathbf{d}_h(x)$ and of all of the $\mathbf{d}_g(x)$ are equal. The former, by Lemma 3.3, equals $\psi_t(x)$. Hence, the sack $\mathbf{S}_{\mathbf{a},\Pi}$ is also fair.

To see the second statement, first construct an ordered prime factorization $\mathbf{a}'$ by simply replacing each a_h by an ordered prime factorization, writing the factors of a_1 first, then those of a_2 and so on. By an inductive application of Corollary 3.6, the product of the dice polynomials associated to the prime factors of any a_h equals $\mathbf{d}_h(x)$. This implies that if Π' is the partition with m parts π'_g each consisting of all the prime factors of the a_h in π_g, then the dice associated to the g^{th} parts of Π and Π' are equal. ☐

To illustrate this construction, we again take the case $t + 1 = 12$. The proof of Proposition 3.7(2) shows that if all the parts of the partition are intervals of $\langle n \rangle$, then we will just get the factorization sack associated to the products of primes in these intervals: these are already in Table 3.4. For example, for the ordered factorization $2 \cdot 2 \cdot 3$ with dice factorization $(1 + x)(1 + x^2)(1 + x^4 + x^8)$, we get the $4 \cdot 3$ line from $\Pi = [\{1, 2\}, \{3\}]$, the $2 \cdot 6$ line from $\Pi = [\{1\}, \{2, 3\}]$ and the 12 line from $\Pi = [\{1, 2, 3\}]$.

Thus, only the partition $\Pi = [\{1, 3\}, \{2\}]$ applied to the length 3 factorizations yields new fair sacks. From $2 \cdot 2 \cdot 3$, we get the sack $(1 + x + x^4 + x^5 + x^8 + x^9)(1 + x^2)$; from $2 \cdot 3 \cdot 2$, the sack $(1 + x + x^6 + x^7)(1 + x^2 + x^4)$; and, from $3 \cdot 2 \cdot 2$, the sack $(1 + x + x^2 + x^6 + x^7 + x^8)(1 + x^3)$.

We next recover the roster of examples of fair sacks on p.137 of [4] from our construction, indicating the factorization (and the partition, if any parts are not singletons) followed by the location in the roster in parentheses: $2 \cdot i$ (2); $i \cdot 2$ (3); $3 \cdot i$ (4); $2 \cdot 2 \cdot i$ via $[\{1, 3\}, \{2\}]$ (5); $3 \cdot 4$ and $2 \cdot 2 \cdot 3$ via $[\{1, 3\}, \{2\}]$ (first paragraph after 5); $2 \cdot 2 \ldots \cdot 2$ (second paragraph after 5).

4. The Main Theorems

The goal of this section is to prove that Proposition 3.7 constructs all fair sacks. We actually do a bit more. The proof of the proposition shows that a fair sack can arise from several factorizations: we can replace any interval of consecutive factors a_h lying in the same part π_g by their product. This motivates us to define a partition Π of $\mathbf{a}$ to be *interval free* if no part contains consecutive elements of $\langle \ell \rangle$. In the example with $t+1=12$ above, the interval free partitions are those with all parts singletons and the partition $\Pi = [\{1,3\},\{2\}]$ that yielded the 3 new fair sacks. Although, a priori, requiring interval freeness eliminates only the ambiguity arising above from collapsing consecutive factors, Theorem 4.1 shows that it yields a canonical construction of each factorization-partition sack. Then in Theorem 4.2, we prove, conversely, that every fair sack arises from this construction.

Theorem 4.1. *Every factorization-partition sack arises from an interval free partition of an ordered factorization and the sack determines both the interval free partition and the factorization.*

Proof. We give a simple recipe for modifying any factorization and any partition of it to obtain a new factorization and an interval free partition without changing either the number of parts or any of the associated dice. If any of the given parts contains consecutive factors, replace these by their product in the factorization and assign this product factor to the part formerly containing the consecutive factors, leaving all other parts unchanged. The partition of the collapsed factorization that this produces is interval free. An application of Corollary 3.6 like that used in proving Proposition 3.7(2) shows that the polynomial associated to each product factor in the new factorization will be the product of the polynomials associated to the consecutive factors that it replaces. Hence, the dice associated to each of the corresponding old and new parts will be equal and the sack they form will be unchanged.

We will prove the uniqueness of the interval free realization for a given sack $\mathbf{S}$ by induction on the size ℓ of the factorization $\mathbf{a}$. If this number is 1, we have a fair die. Otherwise, observe that, by Uniqueness of Terms (Corollary 2.4), there is a unique part π_g whose die $d_{\pi_g}(x)$ has non-zero x coefficient. In the construction of factorization sacks, only the die $d_1(x)$ has non-zero x-coefficient so 1 must lie in π_g. I claim that a_1 is the smallest s such that coefficient of x^s in $d_{\pi_g}(x)$ equals 0. No smaller power can have a zero coefficient because $d_1(x) = \psi_{a_1}(x)$ is a factor. Again, by construction, only the die $d_2(x)$ has non-zero x^{a_1} coefficient. So if this coefficient were non-zero in $d_{\pi_g}(x)$, then $d_2(x)$ would be a factor and hence 2 would also lie in π_g, contradicting the interval freeness of Π. Thus $\mathbf{S}$ determines both a_1 and the index g of the part containing 1.

Now we replace $t+1$ by $t'+1 := \frac{t+1}{a_1}$, define an ordered factorization $\mathbf{a}'$ of $t'+1$ by deleting a_1 from $\mathbf{a}$, and define an interval free partition Π' of $n-1$ by first deleting 1 from π_g (and deleting π_g from Π if it is now empty) and then shifting all parts left 1. This yields an interval free realization of a sack $\mathbf{S}'$, also determined by $\mathbf{S}$, but with ℓ reduced by 1. By induction, $\mathbf{S}'$ determines $\mathbf{a}'$ and Π'. But from $\mathbf{a}'$ and a_1 we recover $\mathbf{a}$ and from Π' and the index g of the part containing 1 (or the fact that 1 lay in a deleted part), we recover Π. □

Theorem 4.2. *Every fair sack* $\mathbf{S}$ *of size* k *and total* t *equals* $\mathbf{S}_{\mathbf{a},\Pi}$ *for* Π *an interval free partition with* k *parts of an ordered factorization* $\mathbf{a}$ *of* $t+1$.

The basic idea of the proof is suggested by the proof of uniqueness in Theorem 4.1: use Uniqueness of Totals—Theorem 2.3(2)—to read off the factors a_h of $\mathbf{a}$ in succession from $\mathbf{S}$, associating each to a die to build the interval free Π. Carrying this out requires a somewhat delicate induction which we now explain.

Given an ℓ-tuple $\mathbf{a} := (a_1, a_2, \ldots, a_\ell)$ with each $a_h > 1$, define $b_h = \prod_{h'<h} a_{h'}$, setting $b_1 = 1$ as in Lemma 3.2 and call such a tuple a *partial factorization*. A map $\Pi : \langle \ell \rangle \to \langle k \rangle$ (thought of as the set of dice in $\mathbf{S}$) such that no consecutive elements have the same image is a *partial interval free partition*. Note that we do not require that $b_{\ell+1}$ divide $(t+1)$ nor that Π be surjective. We say that $(\mathbf{a}', \Pi')$ *extends* $(\mathbf{a}, \Pi)$ if the initial ℓ values of both $\mathbf{a}'$ and Π' match those of $\mathbf{a}$ and Π.

Given a pair $(\mathbf{a}, \Pi)$, define $\mathbf{f}_g(x) := \prod_{h \in \pi_g} \psi_{a_h}(x^{b_h})$ for $g \in \langle k \rangle$; if g is not in the image of Π, then $\mathbf{f}_g(x) = 1$. A pair $(\mathbf{a}, \Pi)$ gives a *partial realization* of $\mathbf{S}$ if the $b_{\ell+1}$-term in $\mathbf{d}_{\Pi(\ell)}(x)$ is zero, and if

$$\mathbf{f}_g(x) \equiv \mathbf{d}_g(x) \mod \left(x^{b_{\ell+1}}\right) \text{ for } g \in \langle k \rangle \,. \tag{4.3}$$

The vanishing of the $b_{\ell+1}$-term will be used to inductively extend partial realizations. The conditions in (4.3) have two implications for the degree $b_{\ell+1}$ truncations of the $\mathbf{d}_g(x)$. Their product contains a unique term of each degree less than $b_{\ell+1}$ and contains no term of degree $b_{\ell+1}$ or higher, in both cases because this is true by construction for the product of the $\mathbf{f}_g(x)$ by Lemma 3.2.

Suppose that we have a partial realization for which $b_{\ell+1} \geq t+1$. Then, (4.3) implies that $\mathbf{d}_g(x) = \mathbf{f}_g(x)$ for each $g \in \langle k \rangle$ since any $\mathbf{d}_g(x)$ has degree at most t. This has three consequences. First, the product of all the $\mathbf{f}_g(x)$ has degree $b_{\ell+1} - 1$ by Lemma 3.2 while the product of all the $\mathbf{d}_g(x)$ has degree t; thus $b_{\ell+1} = t+1$ and hence $\mathbf{a}$ is a factorization of $t+1$. Second, for each g, there must be an h such that $\Pi(h) = g$ so the fibers of Π determine an interval free partition. Finally, from the definition of the $\mathbf{f}_g(x)$, we see that $\mathbf{S} = \mathbf{S}_{\mathbf{a},\Pi}$.

A base for an induction on the order ℓ of $\mathbf{a}$ is provided for $\ell = 0$ by setting $\mathbf{f}_g(x) = 1$ for all g. So Theorem 4.2 will follow by induction if we prove:

Claim 4.4. *A partial realization* $(\mathbf{a}, \Pi)$ *of* $\mathbf{S}$ *of order* ℓ *with* $b_{\ell+1} < t+1$ *can be extended to one of order* $\ell+1$.

Proof. To warm up let's find the die $\mathbf{d}_{\Pi(1)}$ and the factor a_1. By Uniqueness of Terms, there is a unique $\mathbf{d}_\gamma(x)$ with a non-zero x term. We set $\Pi(1) = \gamma$ and let a_1 be the smallest power whose coefficient in this die equals 0. Since $b_2 = a_1$, the b_2 term in $\mathbf{d}_{\Pi(1)}(x)$ is zero. Applying Uniqueness of Terms again, no other die in $\mathbf{S}$ can have a non-zero x^s-term for $1 \leq s < a_1 = b_2$ which shows that (4.3) holds. So both conditions for a partial realization hold.

The idea of the general inductive step is similar. Given $(\mathbf{a}, \Pi)$ of order ℓ, We first find Π'. The second consequence of (4.3) implies that $x^{b_{\ell+1}}$ does not arise as a product of lower degree terms in the $\mathbf{d}_g(x)$. By Uniqueness of Terms for $\mathbf{S}$, there must be a unique die $\mathbf{d}_\gamma(x)$ with non-zero $x^{b_{\ell+1}}$ term. We define $\Pi'(\ell+1) = \gamma$. The condition that the $b_{\ell+1}$-term in $\mathbf{d}_{\Pi(\ell)}(x)$ is zero ensures that $\Pi(\ell) \neq \Pi'(\ell+1)$. This and the interval freeness of Π show that Π' is interval free.

Next, we define $a_{\ell+1}$ to be the smallest positive integer such that the $a_{\ell+1}b_{\ell+1}$ term in $\mathbf{d}_\gamma(x)$ is 0. Again, this guarantees the first condition for a partial realization. To make the rest of the argument easier to read, set $\alpha = a_{\ell+1}$ and $\beta = b_{\ell+1}$, write $p_g(s)$ for $p_{\mathbf{d}_g}(s)$, allowing any $s \leq t$ by setting $p_g(s) = 0$ if $s \geq k_d$ and use $\mathbf{d}_{g'}$ to indicate any die other than $\mathbf{d}_\gamma$. We will check that the equations (4.3) known inductively for $(\mathbf{a}, \Pi)$ imply those needed for $(\mathbf{a}', \Pi')$.

Restating (4.3) in terms of the coefficients p_g, we must check that

$$(4.5) \quad p_{g'}(r\beta + s) = 0 \text{ and } p_\gamma(r\beta + s) = p_\gamma(s) \text{ for } 1 \leq r < \alpha \text{ and } 0 \leq s < \beta.$$

The inductive hypothesis tells us that this holds when $r = 0$, and by construction, it holds for $s = 0$—that is, $p_\gamma(r\beta) = 1 = p_\gamma(0)$. Moreover, we know from (4.3) for $(\mathbf{a}, \Pi)$ that the product of the terms of degrees less than β in all the $\mathbf{d}_g(x)$ contains a unique term of every total degree less than β and no terms of higher degree.

We carry out a double induction, first on r and then on $\sigma := \sigma_\gamma(s)$—that is, over the set S_γ of degrees (up to β) of terms of γ. The second induction carries an additional hypothesis which we now explain. Let $S_{\sigma,r} := \{s + r\beta \mid \sigma_\gamma(s) = \sigma\}$: this set has smallest element $\sigma + r\beta$. At the σ-stage in the induction, we will show that:

(1) $p_\gamma(\sigma + r\beta) = 1$ and that $p_g(s) = 0$ for all g and all larger $s \in S_{\sigma,r}$.
(2) At each stage, the set of $s + r\beta$ for which $r\beta \leq \sigma_\gamma(s) \leq \sigma + r\beta$ is exactly the union of all $S_{\sigma',r}$ with $\sigma' \leq \sigma$.

The first statement for all $\sigma \in S_\gamma$ gives (4.5) because, by the inductive hypothesis from (4.3), the union of $S_{\sigma,0}$ over $\sigma \in S_\gamma$ is the set $0 \leq s < \beta$. One consequence of (4.5) for a fixed choice of r is that a term in $\mathbf{T}(x)$ has total degree of the form $s + r\beta$ with $0 \leq s < \beta$ if and only if the degree of its γ-factor has the same form. Ensuring this is the only reason an induction on r is needed. The second statement thus implies that at each stage no product of factors of lower degree gives a term of degree $\sigma + r\beta$.

We now come to the key step, showing that $p_\gamma(\sigma + r\beta) = 1$. This holds by construction for $\sigma = 0$. For $\sigma > 0$, the last sentence in the preceding paragraph implies, by Uniqueness of Terms, that we must have $p_g(\sigma + r\beta) = 1$ for a unique g and we need to check that $g = \gamma$. Pick the largest h in π_γ for which σ is divisible by b_h: this h is also the smallest h for which the σ-term of $\mathbf{d}_\gamma(x)$ picks up a non-constant term from the factor $\psi_{a_h}(x^{b_h})$ of $\mathbf{d}_\gamma$. By construction, $\sigma' := \sigma - b_h$ is also in S_γ and, by induction, we know that $p_\gamma(\sigma' + r\beta) = 1$. If $\Pi(h+1) = \gamma'$, then, again by construction, $p_{\gamma'}(b_{h+1}) = 1$ and $p_\gamma(b_{h+1} - b_h) = 1$. Moreover, since Π is interval free, $\gamma' \neq \gamma$. These choices allow us to apply Lemma 2.6 with $s = \sigma' + r\beta = \sigma + r\beta - b_h$, $s' = b_{h+1} - b_h$ and $u = b_h$. The Lemma then says that $p_g(s + u) = p_g(\sigma + r\beta) = 1$ can *only* hold if $g = \gamma$ as required.

Figure 4.6 illustrates this step graphically in two examples with $b_{\ell+1} = 72$. Each line describes a die with the first line giving γ. The terms are represented as a sequence of dots, starting in degree 0 on the left, with non-zero terms shown as large black dots and multiples of β are indicated by vertical black lines. The colored dots are the σ that we are trying to prove correspond to non-zero terms of γ with the color used to distinguish the different values of h above. Arrows of the same color are drawn from each σ to the $\sigma' = \sigma - b_h$ that we know is non-zero inductively and from the $(b_{h+1} - b_h)$-term of γ to the b_{h+1}-term of γ'.

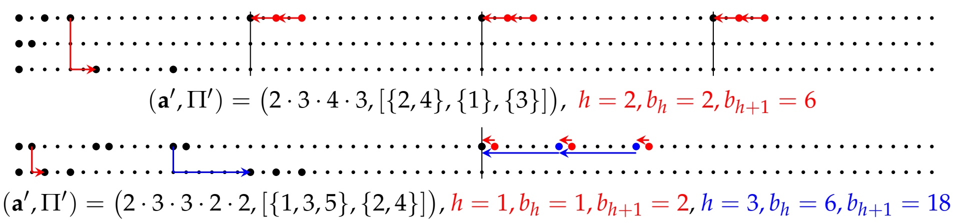

Figure 4.6 Non-zero coefficients of degrees differing by $+b_h$ and by $-b_h$

Given that $p_\gamma(\sigma + r\beta) = 1$, we can produce the terms in $S_{\sigma,r}$ from those in $S_{\sigma,0}$ by replacing the γ-factor x^σ by $x^{\sigma + r\beta}$. Moreover, for any $s \in S_{\sigma,r}$ greater than $\sigma + r\beta$, the degree s term arises as a product of factors of lower degree. By Uniqueness of Terms, we must have $p_g(s) = 0$ for all g for all such s so (1) holds for σ. Moreover, no terms other than those in $S_{\sigma,r}$ can have $\sigma_\gamma(s) = \sigma + r\beta$ so (2) holds too. □

5. **Applications**

Knowing how to construct all sacks yields restrictions on the dice in fair sacks. We give several illustrative corollaries below.

Viewing the Gasarch-Kruskal Theorem as saying that "Every die in a fair sack is semifair" naturally suggests the question, "Does every semifair die occur in a fair sack?". The answer is usually negative, and the simplest examples are the dice $\mathbf{d}_s(x) = 1 + x^s + x^{2s-1} + x^{3s-1}$ for $s \geq 2$. For $\mathbf{d}_2(x) = 1 + x^2 + x^3 + x^5$, we simply have to note that, by Uniqueness of Terms, the sack must also contain a die of the form $(1 + x + \dots)$ and then the total x^3 arises in two ways. For $\mathbf{d}_3(x) = 1 + x^3 + x^5 + x^8$, we need to argue that, since there is a unique die with an x term, an x^2 term cannot arise as a product of lower degree factors. Hence there is a also a die with an x^2 term and this would give two ways to obtain x^5. Similar arguments fail, however, for $\mathbf{d}_4(x) = 1 + x^4 + x^7 + x^{11}$ because there are fair sacks for which no die has an x^3 term. However, if so, then x^3 must arise as a product of lower degree factors and hence the x and x^2 terms occur in two *different* dice in the sack, again giving us two ways to produce x^7. As s increases, handling $\mathbf{d}_s(x)$ in this way requires considering increasingly large numbers of other dice. Theorem 4.2 provides a criterion that lets us read off, directly from $\mathbf{d}(x)$, whether it lies in a fair sack and that immediately shows that no $\mathbf{d}_s(x)$ does.

Corollary 5.1. *A die* $\mathbf{d}$ *lies in a fair sack if and only if* $\mathbf{d}(x) = \prod_{h=1}^{\ell} \psi_{a_j}(x^{b^j})$ *with* $a_j b_j | b_{j+1}$ *for* $1 \leq j < \ell$*. In particular, the degrees of all non-zero terms of* $\mathbf{d}(x)$ *are multiples of the smallest positive such degree.*

Proof. Any die in a factorization-partition sack has the claimed form, hence the first statement follows from Theorem 4.2. It immediately implies the second. □

As an example of a new restriction on the orders of dice in a fair sack, we sharpen the lower bound for the largest size of a die in a fair sack in Corollary 9 of [4].

Corollary 5.2. *If p is the smallest prime dividing $t+1$, then a fair sack with total t always contains a die of order at least $(t+1)(1-\frac{1}{p})+1$. In particular, every fair sack with total t contains a die of order at least $\frac{t+1}{2}+1$.*

Proof. Realize $\mathbf{S}$ as a partition-canonical sack associated to a prime factorization $\mathbf{a}$ of size ℓ. The polynomial $\psi_{a_\ell}(x^{b_\ell})$ is a factor of the $\mathbf{d}_g(x)$ associated to the part π_g containing ℓ. As $\deg\big(\psi_{a_\ell}(x^{b_\ell})\big) = (a_\ell - 1)b_\ell = (t+1) - b_\ell = (t+1)(1-\frac{1}{a_\ell})$, the degree of $\mathbf{d}_g(x)$ is at least this large. Since $a_\ell \leq p$, the corresponding die has order at least $(t+1)(1-\frac{1}{p})+1$. □

Finally, each die in a factorization-partition sack is itself the total die of the subsack determined by its part. This motivates the following definition which leads to our most striking corollary.

A die is *atomic* if it is not the total die of any sack of size 2 or more, and a sack is atomic if all its dice are. Every die $\mathbf{d}$ is the total die of an atomic sack, that we call an *atomization* of $\mathbf{d}$, by a standard argument. (If $\mathbf{d}$ is not itself atomic, then it is the total die of a sack of dice, all of strictly smaller orders. By induction, all of these have atomizations whose union is an atomic sack with total $\mathbf{d}$.) Atomizations are not usually unique: for example, in view of (3) of the next Corollary, the die in the last line of Table 3.4 has 3 atomizations, given in lines 1, 2, and 4. The atomizations of a sack $\mathbf{S}$ are the sacks obtained by atomizing, in any way, all the dice in $\mathbf{S}$. All have the same totals as $\mathbf{S}$.

Corollary 5.3. (1) *Any atomization of a fair sack is fair.*
(2) *The atomic dice that lie in some fair sack are those of the form $\psi_p(x^b)$ with p prime.*
(3) *The atomic fair sacks are the factorization sacks of ordered prime factorizations $\mathbf{a}$.*
(4) *Every atomic fair sack of size n contains a unique fair subsack $\mathbf{S}_{n'}$ of each size $n' \leq n$ consisting of dice associated to the first n' factors in $\mathbf{a}$.*

Proof. The first assertion holds because totals are preserved under atomization. The arguments in the proof of Proposition 3.7 show that only factorization sacks associated to prime factorizations can be atomic. If a die in such a sack was not itself atomic, then by atomizing it we would obtain a fair sack contradicting Theorem 4.2. This proves the second and third assertions. Lemma 3.2 implies the fairness of the subsacks $\mathbf{S}_{n'}$ in the last statement. Uniqueness follows by induction on n. If a fair subsack of size $n' < n$ does not contain the die $\mathbf{d}_n$ associated to the last factor in $\mathbf{a}$, its intersection with $\mathbf{S}_{n-1}$ is fair subsack of size n' that, inductively, must equal $\mathbf{S}_{n'}$. Otherwise, we get a contradiction by removing $\mathbf{d}_n$ to get a fair subsack of size $n'-1$ of $\mathbf{S}_{n-1}$. By induction, this sack is $\mathbf{S}_{n'-1}$ which does not contain $\mathbf{d}_{n-1}$. But adding $\mathbf{d}_n$ back to $\mathbf{S}_{n'-1}$ yields an unfair sack because the total b_{n-1} does not occur. □

We close by noting an open question for the reader. We can factor the dice $\mathbf{d}_s(x)$ defined before Corollary 5.1 as $\mathbf{d}_s(x) = (1 + x^s)(1 + x^{2s-1}) = \psi_2(x^s)\psi_2(x^{2s-1})$. By (2) above this gives an atomization and, at least for small s, there are no others.[2] All other atomizations of semifair dice not lying in a fair sack that we have found contain only semifair dice, but this does not follow from (2) above and we have not found any proof. So we close by asking the reader, "*Must every semifair die have a semifair atomization?*" or, more greedily, "*Is semifairness closed under atomization?*".

Acknowledgements Part of this work was completed while the author was on a Fordham University Faculty Fellowship and visiting the Vietnam Institute for Advanced Studies in Mathematics, Galatasaray University and the Universitá di Firenze. I thank all of these institutions for their support, and Nguyễn Hữu Dự, Ayberk Zeytin and Giorgio Ottaviani for their personal hospitality. I am also grateful to Abe Smith and Dave Swinarski for helpful conversations.

References

[1] Guantao Chen, M. Bhaskara Rao, and Warren E. Shreve, *Can One Load a Set of Dice So That the Sum Is Uniformly Distributed?*, Math. Mag. **70** (1997), no. 3, 204–206. MR1573243 ←1, 4

[2] Kai Lai Chung, *Elementary probability theory with stochastic processes*, 3rd ed., Springer-Verlag, New York, 1979. Undergraduate Texts in Mathematics. MR560506 (81k:60002) ←2

[3] Edward J. Dudewicz and Robert E. Dann, *Equally Likely Dice Sums Do Not Exist*, The American Statistician **26** (1972), no. 4, 41–42. ←1, 3

[4] William I. Gasarch and Clyde P. Kruskal, *When Can One Load a Set of Dice so That the Sum Is Uniformly Distributed?*, Math. Mag. **72** (1999), no. 2, 133–138. MR1573382 ←1, 2, 3, 4, 6, 11

[5] J. B. Kelly, Leo Moser, J. H. Wahab, J. V. Finch, and P. R. Halmos, *E925*, Amer. Math. Monthly **58** (1951), no. 3, 191–192. ←1, 3, 4

[6] Ian Morrison and David Swinarski, *Can you play a fair game of craps with a loaded pair of dice?* (2013), available at arXiv:abs/1308.6816. ←1, 4

[7] Emanuel Parzen, *Modern probability theory and its applications*, A Wiley Publication in Mathematical Statistics, John Wiley & Sons Inc., New York, 1960. MR0112166 (22 #3021) ←1, 3

[2] The roots of $\psi_2(n) = 1 + x^n$ are those $2n^{\text{th}}$ roots of unity that are not n^{th} roots of unity, from which its irreducible factors over $\mathbb{R}$ are easily found. To find all atomizations of $\mathbf{d}_s(x)$ by brute force, we simply enumerate all partitions of the factors for both $n = s$ and $n = s - 1$, find those for which the product of the factors in each part has all coefficients non-negative (and hence gives a die polynomial), and eliminate any that themselves contain non-atomic dice.