USING BINARY FACTORIZATIONS TO CONNECT ADDITIVE SYSTEMS AND FAIR SACKS OF DICE

Abstract. Suppose we have polynomials or power series, none equal to 1, with a product that has coefficients of only 1 and such that each has coefficients of only 0 and 1. We define this to be a binary factorization, which we use to connect additive systems and fair sacks of dice, two seemingly unrelated mathematical topics. After establishing the relationship between these three topics, we get new results by translating known results about additive systems and fair sacks of dice.

1. Introduction.

There are many mathematical results that have been discovered and later independently rediscovered. One recent example has gone unnoticed until now because the results involve additive systems and fair sacks of dice, two topics that appear to be far apart. To bridge the gap, we introduce a third topic.

Definition. A *finite binary factorization* is a set of polynomials whose product is $1 + X + X^2 + \cdots + X^{s-1}$, where s is a positive integer, such that each polynomial has coefficients that are only 0 and 1, and no polynomial equals 1. We also say that the set is a binary factorization of size s.

Problem 1. Find a unique form for every finite binary factorization.

After we define additive systems and fair sacks of dice, which we delay for now, we will see that recent structure theorems for additive systems [2] and fair sacks of dice [3] give the same solution to this problem. What we find particularly interesting is that each structure theorem actually solves a generalization of Problem 1, but not the same generalization. We look at the structure theorems for binary factorizations, additive systems, and fair sacks of dice in Sections 2, 3, and 4, respectively. Finally in Section 5 we see how additional results on additive systems translate to binary factorizations and to fair sacks of dice. To first get a feel for the subject, we invite readers to complete the following.

Exercises.

(1) Show that the only binary factorizations of size 6 are $\{1 + X, 1 + X^2 + X^4\}$, $\{1 + X + X^2, 1 + X^3\}$, and $\{1 + X + X^2 + X^3 + X^4 + X^5\}$.

(2) Given a finite binary factorization, consider the product of only some of the polynomials. Prove that the number of terms in the product equals the product of the number of terms in each polynomial. In particular, conclude that there is only one binary factorization of size s if s is prime.

(3) Use the previous exercise to identify the 11 binary factorizations of size 12. To show that no others exist, you may wish to use the structure theorem for binary factorizations in Section 2. (More generally, after Section 3 we can count the number of binary factorizations of size s by rephrasing in terms of additive systems and then consulting [4].)

2. Binary Factorizations.

In order to discuss one of the generalizations Problem 1, we need to redefine a binary factorization so that its size can be ∞. For us, a *power series* is a formal sum $\sum_{n=0}^{\infty} c_n X^n$ with each c_n real. We almost never substitute a real number for X in such an infinite sum, so we ignore convergence. Let $\Psi_\infty(X) = 1+X+X^2+X^3+\cdots$, and for a positive integer s, let $\Psi_s(X) = 1 + X + X^2 + \cdots + X^{s-1}$.

Definition. A set $\{f_i(X)\}_{i\in I}$ is a *binary factorization* if

(1) $\prod_{i\in I} f_i(X) = \Psi_s(X)$, where s is a positive integer or ∞, and
(2) for all $i \in I$, $f_i(X)$ is a power series (or polynomial) with every coefficient 0 or 1, and with $f_i(X) \neq 1$.

We also say that the set is a binary factorization of size s.

We should mention that the notation $\Psi_s(X)$ matches [3], and we have chosen the term size to align with [2]. Let us begin with a few simple observations about a binary factorization $\{f_i(X)\}_{i\in I}$. First, since the constant term of $\Psi_s(X)$ is 1, the same must be true for every $f_i(X)$. Second, the index set I can be empty. Throughout this paper we use the convention that a product of no objects equals 1, so the empty set is the unique binary factorization of size 1. Also, the index set could instead be infinite. For example, the reader can verify that if $I = \{1, 2, 4, 8, 16, \ldots\}$, then $\prod_{i\in I}(1 + X^i) = \Psi_\infty(X)$, so that $\{1 + X^i\}_{i\in I}$ is a binary factorization of size ∞.

Remark 2. For a binary factorization $\{f_i(X)\}_{i\in I}$, the product of any subset, say $g(X) = \prod_{i\in I_0} f_i(X)$, has coefficients 0 and 1 only. To see this, let $h(X) = \prod_{i\in I\setminus I_0} f_i(X)$ and notice that both $g(X)$ and $h(X)$ are nonzero power series whose coefficients are nonnegative integers. Our conclusion now follows from observing that $g(X)\,h(X) = \Psi_s(X)$, which has coefficients 0 and 1 only.

In the following example we use the $\Psi_s(X)$ to write a binary factorization. Eventually we will see how to do this uniquely for every binary factorization.

Example 3. $\{1 + X^2 + X^4, 1 + X + X^6 + X^7\}$ is a binary factorization size 12 that can also be written as $\left\{\Psi_3(X^2), \Psi_2(X)\,\Psi_2(X^6)\right\}$.

The usefulness of the $\Psi_s(X)$ is based on the property that for b a positive integer and a a positive integer or ∞,

$$\Psi_b(X)\,\Psi_a\left(X^b\right) = \Psi_{ab}(X). \tag{2.1}$$

To prove this, first notice that for positive integers c and d, $(1 - X)\,\Psi_c(X) = 1-X^c$, or substituting X^d for X, $(1 - X^d)\,\Psi_c(X^d) = 1 - X^{cd}$. Therefore if a and b are positive integers,

$$(1 - X)\,\Psi_b(X)\,\Psi_a\left(X^b\right) = \left(1 - X^b\right)\Psi_a\left(X^b\right) = 1 - X^{ab} = (1 - X)\,\Psi_{ab}(X),$$

and dividing by $1 - X$ gives us (2.1). The case of $a = \infty$ is nearly the same, where we additionally use $(1 - X^d)\,\Psi_\infty(X^d) = 1$ to get

$$(1 - X)\,\Psi_b(X)\,\Psi_\infty\left(X^b\right) = \left(1 - X^b\right)\Psi_\infty\left(X^b\right) = 1 = (1 - X)\,\Psi_\infty(X).$$

To find binary factorizations using (2.1), suppose, for some $a_0, a_1, \ldots, a_{L-1}$, that we define $b_j = a_0 a_1 \cdots a_{j-1}$ for all $0 \le j \le L$. In particular, $b_0 = 1$ by our convention on empty products. We require each a_j to be an integer greater than 1, except that we also allow $a_{L-1} = \infty$, in which case $b_L = \infty$. Then we can use $\Psi_{b_j}(X)\,\Psi_{a_j}\left(X^{b_j}\right) = \Psi_{b_{j+1}}(X)$ to get

$$\prod_{j=0}^{L-1} \Psi_{a_j}\left(X^{b_j}\right) = \Psi_{b_1}(X) \prod_{j=1}^{L-1} \Psi_{a_j}\left(X^{b_j}\right) = \Psi_{b_2}(X) \prod_{j=2}^{L-1} \Psi_{a_j}\left(X^{b_j}\right)$$

$$= \Psi_{b_3}(X) \prod_{j=3}^{L-1} \Psi_{a_j}\left(X^{b_j}\right) = \cdots = \Psi_{b_{L-1}}(X)\,\Psi_{a_{L-1}}\left(X^{b_{L-1}}\right) = \Psi_{b_L}(X).$$

Similarly, for an infinite sequence of integers $a_0, a_1, a_2, \ldots$, each greater than 1, define $b_j = a_0 a_1 \cdots a_{j-1}$ for all nonnegative integers j. We claim that $\prod_{j=0}^{\infty} \Psi_{a_j}\left(X^{b_j}\right) = \Psi_\infty(X)$. To see this, let L be a positive integer. By the above calculation, $\prod_{j=0}^{\infty} \Psi_{a_j}\left(X^{b_j}\right) = \Psi_{b_L}(X) \prod_{j=L}^{\infty} \Psi_{a_j}\left(X^{b_j}\right)$. The constant term of each $\Psi_{a_j}\left(X^{b_j}\right)$ is 1, and if $j \geq L$, then all other terms have degree at least b_L. Thus the term 1 is the only term of degree less than b_L in the product $\prod_{j=L}^{\infty} \Psi_{a_j}\left(X^{b_j}\right)$. This implies that for every nonnegative integer $N < b_L$, the coefficient of X^N is the same in $\prod_{j=0}^{\infty} \Psi_{a_j}\left(X^{b_j}\right)$ and in $\Psi_{b_L}(X)$, i.e., every such coefficient is 1. Since $b_L \to \infty$ as $L \to \infty$, $\prod_{j=0}^{\infty} \Psi_{a_j}\left(X^{b_j}\right) = \Psi_\infty(X)$.

We now introduce terminology to capture the ideas above.

Definition. Let L be a nonnegative integer or ∞. Suppose we have a sequence of L terms $\left(a_j\right)_{0 \leq j < L}$ such that each a_j is an integer greater than 1, except that we also allow $a_{L-1} = \infty$ if $0 < L < \infty$.

Define $b_j = a_0 a_1 \cdots a_{j-1}$ for all $0 \leq j < L$, and define b_L to be the product of all the a_j. In particular, $b_0 = 1$, and $b_L = \infty$ if and only if either $L = \infty$ or $0 < L < \infty$ and $a_{L-1} = \infty$. Then the sequence of L terms $\left(\Psi_{a_j}\left(X^{b_j}\right)\right)_{0 \leq j < L}$ is a Ψ-*sequence*, and it is generated by $\left(a_j\right)_{0 \leq j < L}$. We say the size of this Ψ-sequence is b_L.

In this definition, the empty sequence of integers generates the empty Ψ-sequence, and this is the only Ψ-sequence for $L = 0$ and the only Ψ-sequence of size 1. If $\left(\Psi_{a_j}\left(X^{b_j}\right)\right)_{0 \leq j < L}$ is a Ψ-sequence of size s, then we have already shown that the product of the terms is $\Psi_s(X)$, and thus the set $\left\{\Psi_{a_j}\left(X^{b_j}\right)\right\}_{0 \leq j < L}$ is a binary factorization of size s.

In Section 5 we will see how to determine whether an arbitrary binary factorization can be ordered to give a Ψ-sequence. To see now that this is not always possible, recall Example 3. Since $1 + X + X^6 + X^7$ cannot be written in the form $\Psi_{a'}\left(X^{b'}\right)$, neither ordering of $\left\{\Psi_3\left(X^2\right), \Psi_2(X)\,\Psi_2\left(X^6\right)\right\}$ gives a Ψ-sequence. This binary factorization, however, is closely related to $\Psi_2(X)$, $\Psi_3\left(X^2\right)$, $\Psi_2\left(X^6\right)$, which is the Ψ-sequence generated by 2, 3, 2. We have simply replaced the first and last term of this Ψ-sequence by their product.

This type of replacement works quite generally. If we replace some elements of a binary factorization by their product, then we have another binary factorization, since the new polynomial has coefficients 0 and 1 only by Remark 2. In the case that we begin with a binary factorization that is a Ψ-sequence, such replacements are not particularly useful if we replace adjacent terms by their product. For instance, consider $\Psi_{a_1}(X)$, $\Psi_{a_2}\left(X^{a_1}\right)$, $\Psi_{a_3}\left(X^{a_1 a_2}\right)$, which is generated by the arbitrary sequence a_1, a_2, a_3. We have $\Psi_{a_1}(X)\,\Psi_{a_2}(X^{a_1}) = \Psi_{a_1a_2}(X)$ and $\Psi_{a_2}(X^{a_1})\,\Psi_{a_3}(X^{a_1a_2}) = \Psi_{a_2a_3}(X^{a_1})$ by using (2.1), where in the latter case we used X^{a_1} in place of X. Thus if we replace the first two terms or last two terms of the Ψ-sequence, we get respectively the Ψ-sequences generated by a_1a_2, a_3 or a_1, a_2a_3.

It is convenient to use partitions to formalize replacements. That is, given a partition of the terms of some Ψ-sequence, we replace the terms in every partition element by their product. The examples above correspond to the partitions $\left\{\left\{\Psi_3\left(X^2\right)\right\}, \left\{\Psi_2\left(X\right), \Psi_2\left(X^6\right)\right\}\right\}$, $\left\{\left\{\Psi_{a_1}(X), \Psi_{a_2}(X^{a_1})\right\}, \left\{\Psi_{a_3}(X^{a_1a_2})\right\}\right\}$, and $\left\{\left\{\Psi_{a_1}(X)\right\}, \left\{\Psi_{a_2}(X^{a_1}), \Psi_{a_3}(X^{a_1a_2})\right\}\right\}$. In order to avoid replacements that could have been created by starting with a different Ψ-sequence, we require that no partition element contains two consecutive terms of the Ψ-sequence. We call these *nonconsecutive* partitions. When we use such a partition to replace terms of a Ψ-sequence, we say we have *nonconsecutive products*, and with this terminology at last we can state a solution to Problem 1, except generalized from finite binary factorizations to any binary factorizations.

Theorem (Structure of binary factorizations)**.** *A binary factorization can be written uniquely as nonconsecutive products of* Ψ*-sequences.*

That is,

(1) nonconsecutive products of a Ψ-sequence give a binary factorization, and
(2) every binary factorization is the set of products that are created from a unique nonconsecutive partition of a unique Ψ-sequence.

Note that above when we established (1), we also showed that the size of the binary factorization equals the size of the Ψ-sequence. For (2), the uniqueness is not difficult, but existence takes a fair amount of work. Rather than providing a proof, we connect binary factorizations to additive systems.

3. First connection: additive systems.

For a set A of positive integers, consider the power series $1 + \sum_{n\in A} X^n$. Its coefficients are all 0 and 1, its constant coefficient is 1, and if A is nonempty then it is not equal to 1. That is, it is exactly the type of power series that might occur in a binary factorization. We can recover A from any such power series as the set of integers that appear as exponents of its nonzero, nonconstant terms. For instance, $1+X^2+X^4$ and $1+X+X^6+X^7$ correspond to $\{2,4\}$ and $\{1,6,7\}$ respectively. We saw in Example 3 that the set of these two polynomials is a binary factorization of size 12, and this is equivalent to the fact that the collection of sets $\left\{\{2,4\},\{1,6,7\}\right\}$ is an additive system of size 12.

Definition. Let s be a positive integer or ∞. A collection of nonempty disjoint sets of positive integers is an *additive system* of size s if the following hold.

(1) Every nonnegative integer less than s can be written in one and only one way as a sum of numbers from the collection, with at most one number selected from each set.
(2) For every integer greater than or equal to s, there are no ways to write s as such a sum.

This definition uses the convention that an empty sum equals 0, just as earlier we defined empty products to be 1. To count how many ways nonnegative integers can be written as the type sum in this definition, we can use the following simple result.

Proposition 4. *Let* $\{A_i\}_{i\in I}$ *be a collection of sets of positive integers, and define* $f_i(X) = 1+\sum_{n\in A_i} X^n$ *for all* $i \in I$*. For any nonnegative integer* N*, the coefficient of* X^N *in* $\prod_{i\in I} f_i(X)$ *is equal to the number of ways to write* N *as a sum of numbers from* $\{A_i\}_{i\in I}$*, with at most one number selected from each* A_i*.*

Note that when I is an infinite set, the coefficient of X^N might be ∞.

Proof. Write $f_i(X) = \sum_{n=0}^{\infty} c_{i,n} X^n$ for each $i \in I$. The coefficient of X^N in $\prod_{i\in I} f_i(X)$ equals $\sum \prod_{i\in I} c_{i,n_i}$, where the sum is over all $\{n_i\}_{i\in I}$ such that each n_i is a nonnegative integer and $N = \sum_{i\in I} n_i$. Since $c_{i,n} = 1$ if $n \in \{0\} \cup A_i$ and otherwise $c_{i,n} = 0$, this equals the number of ways to choose $\{n_i\}_{i\in I}$ such that $N = \sum_{i\in I} n_i$ and $n_i \in \{0\} \cup A_i$ for all i. By discarding all n_i such that $n_i = 0$, this tells us the number of ways to write N as the sum of numbers from $\{A_i\}_{i\in I}$, with at most one number selected from each A_i. □

Proposition 4 immediately tells us how rephrase the definition of an additive system by using power series.

Theorem 5. *Let* $\{A_i\}_{i\in I}$ *be a collection of nonempty disjoint sets of positive integers, and define* $f_i(X) = 1 + \sum_{n\in A_i} X^n$ *for all* $i \in I$*. Then the collection* $\{A_i\}_{i\in I}$ *is an additive system if and only if* $\left\{f_i(X)\right\}_{i\in I}$ *is a binary factorization.*

Here is Theorem 1 of [2].

Theorem (Structure of additive systems)**.** *An additive system can be written uniquely as a mixed quotient of a British number system.*

We could give careful definitions of British number systems and mixed quotients. Instead, however, consider the correspondence we have already established. A set A of positive integers corresponds to $1 + \sum_{n\in A_i} X^n$, and conversely we can recover A as the set of integers that appear as exponents of its nonzero, nonconstant terms. Using this, a British number system is an ordered sequence of sets that corresponds to a Ψ-sequence, and taking a mixed quotient of this corresponds to creating nonconsecutive products. That is, readers can write down these definitions based on our work in Section 2 and then verify that they are exactly the definitions in [2]. Also see Table 1 below in Section 5. Since the above theorem for additive systems is proved in [2], this establishes our structure theorem for binary factorizations.

Now we turn to the relationship between binary factorizations and fair sacks of dice.

4. Second connection: fair sacks of dice.

We begin this section by defining some terminology. A *die* is a probability space $\mathbf{d}$ whose outcomes are finitely many nonnegative integers. A *face* of $\mathbf{d}$ is an outcome that occurs with positive probability. We do not assume that the faces are equally probable. Given a finite set of dice $\{\mathbf{d}_i\}_{i\in I}$, for which we always assume the $\mathbf{d}_i$ are independent, notice that adding the outcomes of the dice gives a new probability space whose outcomes are also finitely many nonnegative integers. That is, this sum is itself a die, which we call the *sack* of the dice and write as the set $\{\mathbf{d}_i\}_{i\in I}$. (In [3] a sack was not treated as a die, but this is a minor change.) The sack of no dice is the die whose only face is 0.

For example, suppose $\mathbf{d}_1$ has faces 0, 1, and 2, each with probability $\frac{1}{3}$, and $\mathbf{d}_2$ has faces 0, 1, 2, 3, and 4, each with probability $\frac{1}{5}$. Then the sack $\{\mathbf{d}_1, \mathbf{d}_2\}$ has faces 0, 1, 2, 3, 4, 5, and 6, with respective probabilities $\frac{1}{15}$, $\frac{2}{15}$, $\frac{3}{15}$, $\frac{3}{15}$, $\frac{3}{15}$, $\frac{2}{15}$, and $\frac{1}{15}$. For example, the face 4 can be achieved in 3 ways, as $0+4$, $1+3$, and $2+2$, and each way has probability $\frac{1}{15}$.

We use polynomials to represent dice as follows. Suppose $f(X) = c_0 + c_1X + \cdots + c_tX^t$ is a nonzero polynomial such that $c_0, c_1, \ldots, c_t$ are nonnegative real numbers. Then to $f(X)$ we associate the die $\mathbf{d}$ in which the outcome n has probability $\frac{c_n}{f(1)}$. We have that the sum of the probabilities is 1 since $f(1) = c_0 + c_1 + \cdots + c_t$, and the faces of $\mathbf{d}$ are those n such that $c_n \neq 0$. We say that $f(X)$ *represents* $\mathbf{d}$. (If $f(1) = 1$, then $f(X)$ is the generating function of $\mathbf{d}$.) Every die can be represented by a polynomial, and this polynomial is unique up to multiplication by a positive constant.

In a moment we prove that a sack of dice can be represented by the product of polynomials that represent the individual dice. For example, $\mathbf{d}_1$ and $\mathbf{d}_2$ as defined above can be represented by $f_1(X) = 1+X+X^2$ and $f_2(X) = 1+X+X^2+X^3+X^4$, and the sack $\{\mathbf{d}_1, \mathbf{d}_2\}$ is represented by $f_1(X)f_2(X) = 1 + 2X + 3X^2 + 3X^3 + 3X^4 + 2X^5 + X^6$. Since $f_1(1)f_2(1) = 15$, we see again from the term $3X^4$ that in this sack of two dice, the face 4 occurs with probability $\frac{3}{15}$.

Proposition 6. *Let I be a finite set, and suppose that for each $i \in I$ we have a die $\mathbf{d}_i$ represented by a polynomial $f_i(X)$. Then the product $\prod_{i\in I} f_i(X)$ represents the sack of dice $\{\mathbf{d}_i\}_{i\in I}$.*

Proof. Write $f_i(X) = \sum_{n=0}^{t_i} c_{i,n}X^n$ for $i \in I$, so that the probability of outcome n for die $\mathbf{d}_i$ is $\frac{c_{i,n}}{f_i(1)}$ if $n \in \{0, 1, \ldots, t_i\}$ and otherwise is zero. Let $g(X) = \prod_{i\in I} f_i(X)$, and let N be a nonnegative integer. We must show that the probability of outcome N in the sack of dice is equal to the coefficient of X^N in $g(X)$ divided by $g(1)$. Certainly if $N > \sum_{i\in I} t_i$, then both these quantities are 0, so assume $N \le \sum_{i\in I} t_i$. The probability of N in the sack of dice is $\sum\prod_{i\in I}\frac{c_{i,n_i}}{f_i(1)} = \frac{1}{g(1)}\sum\prod_{i\in I} c_{i,n_i}$, where both sums are over all $\{n_i\}_{i\in I}$ such that each n_i is a nonnegative integer with $n_i \le t_i$ and $N = \sum_{i\in I} n_i$. Notice, however, that the coefficient of X^N in $g(X)$ is this second sum $\sum\prod_{i\in I} c_{i,n_i}$, completing our proof. □

Let us say that a die is *unbiased* if its faces occur with equal probability and that a die is *fair* if it is unbiased and its faces are $\{0, 1, \ldots, s-1\}$ for some positive integer s. Recalling that a sack of dice is itself a die, this also defines a fair sack of dice. It is important to distinguish a fair sack of dice from a sack of fair dice. For example, $\{\mathbf{d}_1, \mathbf{d}_2\}$ as defined above is a sack of fair dice but not a fair sack of dice. It turns out that a sack of two or more fair dice, each with at least two faces, is never a fair sack. This is a simple consequence of the structure theorem of [3], which we give below. It was known earlier, as discussed at the end of Section 2 of [3].

If a die $\mathbf{d}$ is represented by $f(X)$, then $\mathbf{d}$ is unbiased if and only if $f(X)$ is a positive constant times a polynomial whose coefficients are all 0 or 1, and $\mathbf{d}$ is fair if and only if $f(X)$ is a positive constant times $\Psi_s(X)$ for some positive integer

s. Just as Proposition 4 gave us Theorem 5 above, now Proposition 6 gives us the following.

Theorem 7. *Suppose $\{\mathbf{d}_i\}_{i\in I}$ is a sack of dice, with each $\mathbf{d}_i$ represented by a polynomial $f_i(X)$. Then the sack $\{\mathbf{d}_i\}_{i\in I}$ is fair if and only if $\prod_{i\in I} f_i(X)$ is a positive constant times $\Psi_s(X)$ for some positive integer s.*

Earlier we used a one-to-one correspondence between sets of positive integers and certain power series. It is useful to have a similar correspondence between dice and nonzero polynomials with nonnegative coefficients, so we will choose one polynomial among those that represent a die. We could use the generating function, i.e., requiring $f_i(1) = 1$, but we choose instead to make $f_i(X)$ monic, following the convention of [3]. With that choice, an unbiased die is represented by a polynomial whose coefficients are all 0 and 1, and a fair die (or a fair sack of dice) is represented by $\Psi_s(X)$ for some positive integer s. With this convention, we can translate some additional terminology of [3]. A factorization sack corresponds to a Ψ-sequence, and an interval free partition corresponds to nonconsecutive products. (Again see Table 1, below.) As with additive systems, the reader can write down definitions of these terms based on these correspondences and then verify that they agree with [3]. Our structure theorem for binary factorizations, when restricted to finite size, is then equivalent to the following.

Theorem (Structure of fair sacks of unbiased dice)**.** *A fair sack of unbiased dice can be written uniquely as an interval free partition factorization sack.*

Let us compare this to the following, which is Theorem 5.1 of [3].

Theorem (Structure of fair sacks of dice)**.** *A fair sack of dice can be written uniquely as an interval free partition factorization sack.*

That is, this is a stronger theorem because it additionally gives the important fact that a fair sack of dice contains only unbiased dice. This fact was proved many years earlier [1, Corollary 5], was used in [3] to prove the structure of fair sacks of dice, and can be translated to polynomials as follows.

Theorem 8. *Suppose $\{f_i(X)\}_{i\in I}$ is a finite set of polynomials with each $f_i(X)$ monic and having nonnegative real coefficients. If $\prod_{i\in I} f_i(X) = \Psi_s(X)$ for some s, then each $f_i(X)$ has coefficients that are only 0 and 1. (Consequently, if also $f_i(X) \neq 1$ for all i, then $\{f_i(X)\}_{i\in I}$ is a binary factorization.)*

Before we move on, let us consider possible extensions. In Theorem 8, we know $s \neq \infty$ because $\Psi_s(X)$ is a product of finitely many polynomials. What if some $f_i(X)$ are power series that are not polynomials? What if there are infinitely many $f_i(X)$ such that $f_i(X) \neq 1$ for infinitely many i? In either case, $\prod_{i\in I} f_i(X) = \Psi_s(X)$ would imply $s = \infty$. Let us see that in neither case does the conclusion of Theorem 8 have to hold.

Proposition 9. *Let $f(X) = \sum_{n=0}^{\infty} c_n X^n$ be a power series such that $1 = c_0 \geq c_1 \geq c_2 \geq \cdots \geq 0$ and $f(X) \neq \Psi_\infty(X)$. Then there exist positive integers $n_1 < n_2 < n_3 < \cdots$ and positive real numbers $d_1, d_2, d_3, \ldots$ such that $f(X)\prod_{j=1}^{\infty}\left(1 + d_j X^{n_j}\right) = \Psi_\infty(X)$.*

If we apply this when $0 < c_{n'} < 1$ for some n', then neither proposed extension of Theorem 8 works because we get $\Psi_\infty(X)$ when we multiply $f(X)$ either by the single power series $\prod_{j=1}^{\infty}\left(1 + d_j X^{n_j}\right)$ or by infinitely many binomials $1 + d_j X^{n_j}$.

Proof. We claim that for all positive integers r, there exist positive integers $n_1 < n_2 < \cdots < n_r$ and positive real numbers $d_1, d_2, \ldots, d_{r-1}$ such that in $f(X)\prod_{j=1}^{r-1}\left(1+d_jX^{n_j}\right)$, the coefficients are nonnegative and nonincreasing, with exactly the first n_r equal to 1 (i.e., up to but not including the coefficient of X^{n_r}). Concluding the proposition from this claim then involves the same reasoning we used above to show that the product of a Ψ-sequence with $L=\infty$ is $\Psi_\infty(X)$.

For $r=1$, our claim holds because we use $f(X) \neq \Psi_\infty(X)$ to define n_1 to be the smallest integer such that $c_{n_1} \neq 1$. Now we continue by induction. Assume the claim for some $r \geq 1$. Then in $f(X)\prod_{j=1}^{r-1}\left(1+d_jX^{n_j}\right)$, the coefficients of $1, X, \ldots,$ and X^{n_r-1} equal 1, and the coefficient of X^{n_r} is nonnegative and less than 1. Let d_r be 1 minus this coefficient of X^{n_r}. Then d_r is positive and it is a routine calculation to show that in $f(X)\prod_{j=1}^{r}\left(1+d_jX^{n_j}\right)$, the coefficients are nonnegative and nonincreasing, with the coefficients of $1, X, \ldots, X^{n_r}$ equal to 1 but with the coefficient of X^{2n_r} less than 1. We complete our induction step by defining n_{r+1} to be the smallest integer such that the coefficient of $X^{n_{r+1}}$ is not 1, which means $n_r < n_{r+1} \leq 2n_r$.

□

Open Question. Let $f(X)=\sum_{n=0}^{\infty} c_nX^n$ be a power series with all $c_n \geq 0$ and $c_0 > 0$. When is it possible to find $g(X)=\sum_{n=0}^{\infty} d_nX^n$ with all $d_n \geq 0$ such that $f(X)\,g(X)=\Psi_\infty(X)$? Equivalently, when does the power series $\frac{\Psi_\infty(X)}{f(X)}$ have all nonnegative coefficients?

In this question we are looking for a necessary and sufficient condition for the existence of $g(X)$. If $c_0=1$, then Proposition 9 tells us that a sufficient condition is $c_0 \geq c_1 \geq c_2 \geq \cdots \geq 0$. This condition is sufficient even without assuming $c_0=1$ because we can multiply $f(X)$ and $g(X)$ by positive constants. This condition, however, is not necessary.

Exercise. Let $c_2 \geq 0$ and $f(X)=1+\frac{1}{2}X+c_2X^2$. Prove that $c_2 \leq \frac{3}{4}$ if and only if there exists $g(X)=\sum_{n=0}^{\infty} d_nX^n$ with all $d_n \geq 0$ such that $f(X)\,g(X)=\Psi_\infty(X)$. (Hint: for one direction, multiply first by $1+\frac{1}{2}X$ and then use our sufficient condition above.)

We conclude this section by returning to a topic from Section 1. The structure theorem for binary factorizations solved a more general problem than Problem 1 because it gave a unique form for all binary factorizations, not just the finite ones. How does Theorem 8, which is translated from fair sacks of dice, solve a different generalization? We still conclude the same unique form, i.e., nonconsecutive products of a Ψ-sequence, but starting with less. Rather than assuming we have a binary factorization of finite size, we start with a set polynomials with product $\Psi_s(X)$ for some positive integer s, such that each polynomial is monic, not equal to 1, and has nonnegative real coefficients.

5. Benefiting from the connections.

We have introduced two important one-to-one correspondences. First, in Section 3 we paired a set A of positive integers with $1+\sum_{n\in A} X^n$, so that, by Theorem 5, an additive system corresponds to a binary factorization. Second, in Section 4 we paired a die with the unique monic polynomial that represents it. This similarly allows us to use Theorem 7 to tell us that a fair sack of dice corresponds to a binary factorization of finite size, provided that we use the additional fact that every die in a fair sack must be unbiased. In this section we translate other results for additive systems into results about binary factorizations and fair sacks of dice.

To begin, consider that an additive system is uniquely determined or almost uniquely determined by the union of its sets. By "almost" we mean that there can be up to two additive systems with the same union. To be precise, we give the following theorem, which is derived from Theorems 9 and 10 of [2].

Theorem (Uniqueness for additive systems)**.** *Let U be the union of the sets of an additive system.*

(1) If there exist positive integers M and N such that the $M+1$ largest elements of U are N, $2N$, $\ldots$, $(M+1)N$, then exactly one other additive system has union U. Specifically, there exists a unique additive system $\{A_i\}_{i\in I}$ of size N such that $\{A_i\}_{i\in I}\cup\left\{\{N,2N,\ldots,(M+1)N\}\right\}$ and $\{A_i\}_{i\in I}\cup\left\{\{N,2N,\ldots,MN\},\{(M+1)N\}\right\}$ are the two additive systems with union U.

(2) Otherwise there is no other additive system with union U.

To translate this to binary factorizations, let us see what can correspond to the union of sets of an additive system. Let $\left\{f_i(X)\right\}_{i\in I}$ be a binary factorization. For $i\in I$, $f_i(X)$ has a constant term 1 and has no other term in common with any term of some other $f_{i'}(X)$. Thus every coefficient of $\sum_{i\in I}\left(f_i(X)-1\right)$ is 0 or 1, and we call this the *positive term sum* of the binary factorization. Notice that if $f_i(X)=1+\sum_{n\in A_i}X^n$, then the positive term sum of $\left\{f_i(X)\right\}_{i\in I}$ corresponds to $\sum_{n\in\bigcup_{i\in I}A_i}X^n$. We can now restate the above theorem.

Theorem (Uniqueness for binary factorizations)**.** *Let $F(X)$ be the positive term sum of a binary factorization.*

(1) If there exist positive integers M and N such that $F(X)$ equals $X^N+X^{2N}+\cdots+X^{(M+1)N}$ plus a polynomial of degree less than N, then exactly one other binary factorization has positive term sum $F(X)$. Specifically, there exists a unique binary factorization $\left\{f_i(x)\right\}_{i\in I}$ of size N such that $\left\{f_i(x)\right\}_{i\in I}\cup\left\{\Psi_{M+2}\left(X^N\right)\right\}$ and $\left\{f_i(x)\right\}_{i\in I}\cup\left\{\Psi_{M+1}\left(X^N\right),\Psi_2\left(X^{(M+1)N}\right)\right\}$ are the two binary factorizations with positive term sum $F(X)$.

(2) Otherwise there is no other binary factorization with positive term sum $F(X)$.

In order to translate this to fair sacks of dice, we define the *die faces* of a fair sack of dice to be the single set containing all faces that appear on any die in the sack. If a sack of fair dice corresponds to the additive system $\{A_i\}_{i\in I}$, then the die faces are $\{0\}\cup\left(\bigcup_{i\in I}A_i\right)$. Also let us adopt from [3] a term that corresponds to the size of a binary factorization or additive system. We define the *total* of a fair sack of dice to be s if the faces of the fair sack are $\{0,1,\ldots,s-1\}$.

Theorem (Uniqueness for fair sacks of dice)**.** *Let U be the die faces of a fair sack of dice.*

(1) If there exist positive integers M and N such that the $M+1$ largest elements of U are N, $2N$, $\ldots$, $(M+1)N$, then there exists exactly one

other sack of fair dice with die faces U. Specifically, the two sacks start with a unique fair sack of dice with total N and add either an unbiased die with faces $\{0, N, 2N, \ldots, (M+1)N\}$ or two unbiased dice with faces $\{0, N, 2N, \ldots, MN\}$ and $\{0, (M+1)N\}$.

(2) *Otherwise there is no other fair sack of dice with die faces U.*

In the three uniqueness theorems above, suppose we have case (1). The two additive systems or binary factorizations or fair sacks of dice can be distinguished by their size (or total, for a fair sack of dice), because in the notation of (1), the two sizes are $(M+2)N$ and $2(M+1)N$. We can instead distinguish them by looking at the number of objects (i.e., the number of sets, power series, or dice). In the case of binary factorizations, we can rephrase this to say that when I is finite, a binary factorization $\{f_i(X)\}_{i\in I}$ is uniquely determined by $\sum_{i\in I} f_i(X)$. Indeed, in this sum the constant term is the number of elements in I and the remaining terms form the positive term sum.

When that there exists at least one additive system with union U, [2] gives an explicit construction of the one or two additive systems. In the notation and terminology of [2], the additive systems are $\mathfrak{C}_U$ and, if $\mathfrak{C}_U$ is reducible, its reduction. This construction can be adapted in order to find binary factorizations given only the positive term sum, or to find fair sacks of dice given only the set of die faces.

binary factorization $\{f_i(X)\}$	additive system $\{A_i\}$	fair sack of dice $\{\mathbf{d}_i\}$
power series $f_i(X)$	set A_i	die $\mathbf{d}_i$
size	size	total
Ψ-sequence	British number system	factorization sack
product	quotient	partition
nonconsecutive products	mixed quotient	interval free partition
positive term sum	union	die faces

Table 1. Equivalences

Now let us recall that an arbitrary binary factorization can be uniquely expressed as nonconsecutive products of a Ψ-sequence. The relationship between the binary factorization and the Ψ-sequence is closely related to imposing a "ceiling," in the sense that we "cap off" the binary factorization to values below various positive integers N. Similar statements hold for additive systems and fair sacks of dice, and we make all of these precise in the following theorems. The first is a reworded and condensed version of Proposition 7 and Theorem 8 of [2], and then we translate to binary factorizations and fair sacks of dice.

Theorem (Capping the sets of an additive system). *Let $\{A_i\}_{i\in I}$ be an additive system. For a positive integer N and $i \in I$, let $A_i^{<N}$ be the set of elements of A_i that are less than N, and let $I_N = \left\{i \in I \colon A_i^{<N} \neq \emptyset\right\}$.*

(1) *We can order the A_i so that they form a British number system if and only if $\left\{A_i^{<N}\right\}_{i\in I_N}$ is an additive system for every positive integer N.*

(2) *Fixing a positive integer N such that $N \in A_i$ for some $i \in I$, the following are equivalent.*

(a) *N is an element of one of the sets of the unique British number system for which $\{A_i\}_{i\in I}$ is a mixed quotient.*
(b) *$\left\{A_i^{<N}\right\}_{i\in I_N}$ is an additive system of size N.*
(c) *$\left\{A_i^{<N}\right\}_{i\in I_N}$ is an additive system.*
(d) *$\sum_{i\in I_N}\max A_i^{<N}$ is less than N.*

In the notation of [2], $\left\{A_i^{<N}\right\}_{i\in I_N}$ is written $\mathfrak{A}_{<N}$, where $\mathfrak{A}=\{A_i\}_{i\in I}$.

Theorem (Capping the power series of a binary factorization)**.** *Let $\left\{f_i\left(X\right)\right\}_{i\in I}$ be a binary factorization. For a positive integer N and $i\in I$, let $f_i^{<N}\left(X\right)$ be the sum of the terms of $f_i\left(X\right)$ whose degree is less than N, and let $I_N=\left\{i\in I\colon f_i^{<N}\left(X\right)\neq 1\right\}$.*

(1) *We can order the $f_i\left(X\right)$ so that they form a Ψ-sequence if and only if $\left\{f_i^{<N}\left(X\right)\right\}_{i\in I_N}$ is a binary factorization for every positive integer N.*
(2) *Fixing a positive integer N such that X^N is a term of $f_i\left(X\right)$ for some $i\in I$, the following are equivalent.*
   (a) *X^N is a term of some $\Psi_{a_j}\left(X^{b_j}\right)$, where $\left(\Psi_{a_j}\left(X^{b_j}\right)\right)_{0\leq j<L}$ is the unique Ψ-sequence that has nonconsecutive products $\left\{f_i\left(X\right)\right\}_{i\in I}$.*
   (b) *$\left\{f_i^{<N}\left(X\right)\right\}_{i\in I_N}$ is a binary factorization of size N.*
   (c) *$\left\{f_i^{<N}\left(X\right)\right\}_{i\in I_N}$ is a binary factorization.*
   (d) *$\prod_{i\in I_N} f_i^{<N}\left(X\right)$ is a polynomial of degree less than N.*

Theorem (Capping the dice of a fair sack)**.** *Suppose we have a fair sack of dice $\{\mathbf{d}_i\}_{i\in I}$. For a positive integer N and $i\in I$, let $\mathbf{d}_i^{<N}$ be the unbiased die whose faces are those faces of $\mathbf{d}_i$ that are less than N, and let $I_N=\left\{i\in I\colon \mathbf{d}_i^{<N}\text{ has more than one face}\right\}$.*

(1) *We can order the $\mathbf{d}_i$ so that they form a factorization sack if and only if $\left\{\mathbf{d}_i^{<N}\right\}_{i\in I_N}$ is a fair sack of dice for every positive integer N.*
(2) *Fixing a positive integer N such that N is a face on $\mathbf{d}_i$ for some $i\in I$, the following are equivalent.*
   (a) *N is a face that appears on a die of the unique factorization sack which forms $\{\mathbf{d}_i\}_{i\in I}$ by using an interval free partition.*
   (b) *$\left\{\mathbf{d}_i^{<N}\right\}_{i\in I}$ is a fair sack of dice of total N.*
   (c) *$\left\{\mathbf{d}_i^{<N}\right\}_{i\in I}$ is a fair sack of dice.*
   (d) *$\sum_{i\in I_N}\max\mathbf{d}_i^{<N}$ is less than N, where $\max\mathbf{d}_i^{<N}$ is the largest face on the die $\mathbf{d}_i^{<N}$.*

6. Conclusion

By way of Theorem 5 and Theorem 7, we have shown that additive systems, sacks of fair dice, and binary factorizations are the same, roughly speaking. Any additional results on these topics can be translated to the other topics, and we hope that others will do this.

We caution readers, however, to be aware of imperfections in the correspondences among a set of positive integers, a power series, and a die. For example, let $f_1(X) = \sum_{n=0}^{\infty} \frac{1}{2^n} X^n$. This does not correspond to a set of positive integers because it has coefficients that are not 0 or 1. It also does not correspond to a die, because there are infinitely many nonzero terms.

Since $f_1(1) = \sum_{n=0}^{\infty} \frac{1}{2^n} = 2$, perhaps $f_1(X)$ should represent a die, except with infinitely many faces, with face n having a probability of $\frac{1}{2^{n+1}}$. For our purposes, however, this seems to have limited applicability. Indeed, defining $f_2(X) = \frac{1}{2} + \frac{1}{2}\Psi_\infty(X)$, the reader can verify that $f_1(X) f_2(X) = \Psi_\infty(X)$. One might then anticipate that the dice represented by $f_1(X)$ and $f_2(X)$ should make a fair sack. However, $f_2(X)$ does not represent a die in the way $f_1(X)$ does since $f_2(1) = \infty$.

Thinking instead about additive systems, could $f_1(X)$ and $f_2(X)$ correspond to "weighted sets" of positive integers, where each coefficient gives a weight of the corresponding positive integer? In this way $f_1(X) f_2(X) = \Psi_\infty(X)$ might tell us that the weighted sets form a sort of weighted additive system. We will leave it to others to determine if this is a productive path to pursue.

References

[1] W. I. Gasarch, C. P. Kruskal, When can one load a set of dice so that the sum is uniformly distributed?, *Math. Mag.* **72:2** (1999) 133–138 https://doi.org/10.1080/0025570X.1999.11996715.

[2] M. Maltenfort, Characterizing additive systems, *Amer. Math. Monthly* **124:2** (2017) 132–158 https://dx.doi.org/10.4169/amer.math.monthly.124.2.132.

[3] I. Morrison, Sacks of dice with fair totals, *Amer. Math. Monthly* **125:7** (2018) 579–592 https://doi.org/10.1080/00029890.2018.1473699.

[4] A. O. Munagi, k-Complementing Subsets of Nonnegative Integers, *Int. J. Math. Math. Sci.* **2005:2** (2005) 215–224, https://dx.doi.org/10.1155/IJMMS.2005.215.