Journal of Integer Sequences, Vol. 18 (2015),
Article 15.5.7

A Generalization of the Digital Binomial Theorem

Hieu D. Nguyen
Department of Mathematics
Rowan University
Glassboro, NJ 08028
USA
nguyen@rowan.edu

Abstract

We prove a generalization of the digital binomial theorem by constructing a one-parameter subgroup of generalized Sierpiński matrices. In addition, we derive new formulas for the coefficients of Prouhet-Thue-Morse polynomials and describe group relations satisfied by generating matrices defined in terms of these Sierpiński matrices.

1 Introduction

The classical binomial theorem describes the expansion of $(x+y)^N$ in terms of binomial coefficients. More precisely, for any non-negative integer N, we have

$$(x+y)^N = \sum_{k=0}^{N} \binom{N}{k} x^k y^{N-k}, \tag{1}$$

where the binomial coefficients $\binom{N}{k}$ are defined in terms of factorials:

$$\binom{N}{k} = \frac{N!}{k!(N-k)!}.$$

The author [9] introduced a digital version of this theorem (based on Callan [3]) where the exponents appearing in (1) are viewed as sums of digits. To illustrate this, consider the binomial theorem for $N = 2$:

$$(x+y)^2 = x^2y^0 + x^1y^1 + x^1y^1 + x^0y^2. \tag{2}$$

It is easy to verify that (2) is equivalent to

$$(x+y)^{s(3)} = x^{s(3)}y^{s(0)} + x^{s(2)}y^{s(1)} + x^{s(1)}y^{s(2)} + x^{s(0)}y^{s(3)}, \tag{3}$$

where $s(k)$ denotes the sum of digits of k expressed in binary. For example,

$$s(3) = s(1 \cdot 2^1 + 1 \cdot 2^0) = 2.$$

More generally, we have

Theorem 1 (digital binomial theorem [9])**.** *Let n be a non-negative integer. Then*

$$(x+y)^{s(n)} = \sum_{\substack{0 \le m \le n \\ (m,n-m) \text{ carry-free}}} x^{s(m)}y^{s(n-m)}. \tag{4}$$

Here, a pair of non-negative integers (j,k) is said to be *carry-free* if their addition involves no carries when performed in binary. For example, $(8,2)$ is carry-free since $8+2 = (1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0) + 1 \cdot 2^1 = 10$ involves no carries. It is clear that (j,k) is carry-free if and only if $s(j) + s(k) = s(j+k)$ [2, 9]. Also, observe that if $n = 2^N - 1$, then (4) reduces to (1).

In this paper we generalize Theorem 1 to any base $b \ge 2$. To state this result, we shall need to introduce a *digital dominance* partial order on $\mathbb{N}$ as defined by Ball, Edgar, and Juda [2]. Let

$$n = n_0b^0 + n_1b^1 + \cdots + n_{N-1}b^{N-1}$$

represent the base-b expansion of n and denote $d_{b,i}(n) := n_i$ to be the i-th digit of n in base b. We shall say that m is *digitally* less than or equal to n if $d_{b,i}(m) \le d_{b,i}(n)$ for all $i = 0, 1, \ldots, N-1$. In that case, we shall write $m \preceq_b n$. We are now ready to state our result.

Theorem 2. *Let n be a non-negative integer. Then for any base $b \ge 2$, we have*

$$\prod_{i=0}^{N-1} \binom{x+y+d_{b,i}(n)-1}{d_{b,i}(n)} = \sum_{0 \le m \preceq_b n} \left(\prod_{i=0}^{N-1} \binom{x+d_{b,i}(m)-1}{d_{b,i}(m)} \prod_{i=0}^{N-1} \binom{y+d_{b,i}(n-m)-1}{d_{b,i}(n-m)} \right). \tag{5}$$

Let $\mu_j(n) := \mu_j^{(b)}(n)$ denote the multiplicity of the digit $j > 0$ in the base-b expansion of n, i.e.,

$$\mu_j(n) = |\{i : d_{b,i}(n) = j\}|.$$

As a corollary, we obtain

Corollary 3. *Let n be a non-negative integer. Then for any base $b \geq 2$, we have*

$$\prod_{j=1}^{b-1} \binom{x+y+j-1}{j}^{\mu_j(n)} = \sum_{0 \leq m \preceq_b n} \left(\prod_{j=1}^{b-1} \binom{x+j-1}{j}^{\mu_j(m)} \prod_{j=1}^{b-1} \binom{y+j-1}{j}^{\mu_j(n-m)} \right).$$

Observe that if $b = 2$, then Corollary 3 reduces to Theorem 1.

The source behind Theorem 1 is a one-parameter subgroup of Sierpiński matrices, investigated by Callan [3], which encodes the digital binomial theorem. To illustrate this, define a sequence of lower-triangular matrix functions $S_N(x)$ of dimension $2^N \times 2^N$ recursively by

$$S_1(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \quad S_{N+1}(x) = S_1(x) \otimes S_N(x), \tag{6}$$

where $\otimes$ denotes the Kronecker product of two matrices. For example, $S_2(x)$ and $S_3(x)$ can be computed as follows:

$$S_2(x) = S_1(x) \otimes S_1(x) = \begin{pmatrix} 1 \cdot S_1(x) & 0 \cdot S_1(x) \\ x \cdot S_1(x) & 1 \cdot S_1(x) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 0 & 0 \\ x & 0 & 1 & 0 \\ x^2 & x & x & 1 \end{pmatrix},$$

$$S_3(x) = S_1(x) \otimes S_2(x) = \begin{pmatrix} 1 \cdot S_2(x) & 0 \cdot S_2(x) \\ x \cdot S_2(x) & 1 \cdot S_2(x) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ x & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ x & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ x^2 & x & x & 1 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ x^2 & x & 0 & 0 & x & 1 & 0 & 0 \\ x^2 & 0 & x & 0 & x & 0 & 1 & 0 \\ x^3 & x^2 & x^2 & x & x^2 & x & x & 1 \end{pmatrix}.$$

Observe that when $x = 1$, the infinite matrix $S = \lim_{N \to \infty} S_N(1)$ contains Sierpiński's triangle.

Callan [3] gives a formula for the entries of $S_N(x) = (\alpha_N(j,k,x))$, $0 \leq j,k \leq 2^N - 1$, in terms of the sum-of-digits function:

$$\alpha_N(j,k,x) = \begin{cases} x^{s(j-k)}, & \text{if } 0 \leq k \leq j \leq 2^N - 1 \text{ and } (k, j-k) \text{ are carry-free;} \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Moreover, Callan proved that $S_N(x)$ forms a one-parameter subgroup of $SL(2^N, \mathbb{R})$, i.e., the group of $2^N \times 2^N$ real matrices with determinant one. Namely, we have

$$S_N(x) S_N(y) = S_N(x+y). \tag{8}$$

If we denote the entries of $S_N(x)S_N(y)$ by $t_N(j,k)$, then the equality

$$t_N(j,k) = \sum_{i=0}^{2^N-1} \alpha_N(j,i,x)\alpha_N(i,k,y) = \alpha_N(j,k,x+y)$$

corresponds precisely to Theorem 1 with $j=0$ and $k=0$. For example, if $N=2$, then (8) becomes

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 0 & 0 \\ x & 0 & 1 & 0 \\ x^2 & x & x & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ y & 1 & 0 & 0 \\ y & 0 & 1 & 0 \\ y^2 & y & y & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x+y & 1 & 0 & 0 \\ x+y & 0 & 1 & 0 \\ (x+y)^2 & x+y & x+y & 1 \end{pmatrix}.$$

The rest of this paper is devoted to generalizing Callan's construction of Sierpiński matrices to arbitrary bases and considering two applications of them. In Section 2, we use these generalized Sierpiński matrices to prove Theorem 2. In Section 3, we demonstrate how these matrices arise in the construction of Prouhet-Thue-Morse polynomials defined by the author [10]. In Section 4, we describe a group presentation in terms of generators defined through these matrices and show that these generators satisfy a relation that generalizes the three-strand braid relation found by Ferrand [4]. This relation suggests that Sierpiński matrices encode not only a digital binomial theorem but also an interesting group structure.

2 Sierpiński triangles

To prove Theorem 2, we consider the following generalization of the Sierpiński matrix $S_N(x)$ in terms of binomial coefficients. Define lower-triangular matrices $S_{b,N}(x)$ of dimension $b^N \times b^N$ recursively by

$$S_{b,1}(x) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ \binom{x}{1} & 1 & 0 & \cdots & 0 \\ \binom{x+1}{2} & \binom{x}{1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{x+b-2}{b-1} & \binom{x+b-3}{b-2} & \binom{x+b-4}{b-3} & \cdots & 1 \end{pmatrix} = \begin{cases} \binom{x+j-k-1}{j-k}, & \text{if } 0 \le k \le j \le b-1; \\ 0, & \text{otherwise,} \end{cases}$$

and for $N > 1$,

$$S_{b,N+1}(x) = S_{b,1}(x) \otimes S_{b,N}(x).$$

Example 4. To illustrate our generalized Sierpiński matrices, we calculate $S_{3,1}(x)$ and

$S_{3,2}(x)$:

$$S_{3,1}(x) = \begin{pmatrix} 1 & 0 & 0 \\ \binom{x}{1} & 1 & 0 \\ \binom{x+1}{2} & \binom{x}{1} & 1 \end{pmatrix},$$

$$S_{3,2}(x) = S_{3,1}(x) \otimes S_{3,1}(x)$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \binom{x}{1} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \binom{x+1}{2} & \binom{x}{1} & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \binom{x}{1} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \binom{x}{1}\binom{x}{1} & \binom{x}{1} & 0 & \binom{x}{1} & 1 & 0 & 0 & 0 & 0 \\ \binom{x}{1}\binom{x+1}{2} & \binom{x}{1}\binom{x}{1} & \binom{x}{1} & \binom{x+1}{2} & \binom{x}{1} & 1 & 0 & 0 & 0 \\ \binom{x+1}{2} & 0 & 0 & \binom{x}{1} & 0 & 0 & 1 & 0 & 0 \\ \binom{x+1}{2}\binom{x}{1} & \binom{x+1}{2} & 0 & \binom{x}{1}\binom{x}{1} & \binom{x}{1} & 0 & \binom{x}{1} & 1 & 0 \\ \binom{x+1}{2}\binom{x+1}{2} & \binom{x+1}{2}\binom{x}{1} & \binom{x+1}{2} & \binom{x}{1}\binom{x+1}{2} & \binom{x}{1}\binom{x}{1} & \binom{x}{1} & \binom{x+1}{2} & \binom{x}{1} & 1 \end{pmatrix}.$$

We now generalize Callan's result for $S_N(x)$ by presenting a formula for the entries of $S_{b,N}(x)$; see [7] for a similar generalization but along a different vein.

Theorem 5. *Let $\alpha_N(j,k) := \alpha_N(j,k,x)$ denote the (j,k)-entry of $S_{b,N}(x)$. Then*

$$\alpha_N(j,k) = \begin{cases} \binom{x+d_0-1}{d_0}\binom{x+d_1-1}{d_1}\cdots\binom{x+d_{N-1}-1}{d_{N-1}}, & \text{if } 0 \le k \le j \le b^N - 1 \text{ and } k \preceq_b j; \\ \\ 0, & \text{otherwise,} \end{cases} \tag{9}$$

where $j-k = d_0b^0 + d_1b^1 + \ldots + d_{N-1}b^{N-1}$ is the base-b expansion of $j-k$, assuming $j \ge k$.

Proof. We argue by induction on N. It is clear that (9) holds for $S_{b,1}(x)$. Next, assume that (9) holds for $S_{b,N}(x)$ and let $\alpha_{N+1}(j,k)$ be an arbitrary entry of $S_{b,N+1}(x)$, where $pb^N \le j \le (p+1)b^N - 1$ and $qb^N \le k \le (q+1)b^N - 1$ for some non-negative integers $p, q \in \{0, 1, \ldots, b-1\}$. Set $j' = j - pb^N$ and $k' = k - qb^N$. We consider two cases:

Case 1. $p < q$. Then $j < k$ and $\alpha_{N+1}(j,k) = 0 \cdot \alpha_N(j',k') = 0$.

Case 2. $p \ge q$. Then $j \ge k$ and

$$\alpha_{N+1}(j,k) = \binom{x+p-q-1}{p-q}\alpha_N(j',k'). \tag{10}$$

Let $j-k = d_0b^0 + d_1b^1 + \cdots + d_Nb^N$, where $d_N = p-q$. Then $j'-k' = d_0b^0 + d_1b^1 + \cdots + d_{N-1}b^{N-1}$. By assumption,

$$\alpha_N(j',k') = \begin{cases} \binom{x+d_0-1}{d_0}\binom{x+d_1-1}{d_1}\cdots\binom{x+d_{N-1}-1}{d_{N-1}} & \text{if } 0 \le k' \le j' \le b^N - 1 \text{ and } k' \preceq_b j'; \\ \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

Since $k \preceq_b j$ if and only if $k' \preceq_b j'$, it follows from (10) and (11) that

$$\alpha_{N+1}(j,k) = \begin{cases} \binom{x+d_0-1}{d_0}\binom{x+d_1-1}{d_1}\cdots\binom{x+d_N-1}{d_N} & \text{if } 0 \le k \le j \le b^{N+1}-1 \text{ and } k \preceq_b j; \\ \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

Thus, (9) holds for $S_{b,N+1}$. $\square$

Next, we show that $S_{b,N}(x)$ forms a one-parameter subgroup of $SL(b^N, \mathbb{R})$. To prove this, we shall need the following two lemmas; the first is due to Gould [6] and the second follows easily from the first through an appropriate change of variables.

Lemma 6 (Gould [6])**.**

$$\sum_{k=0}^{n} \binom{x+k}{k}\binom{y+n-k}{n-k} = \binom{x+y+n+1}{n}. \tag{13}$$

Proof. Gould [6] derives (13) as a special case of a generalization of Vandemonde's convolution formula. We shall prove (13) more directly using a combinatorial argument. Let A, B, and $C = \{0, 1, \ldots, n\}$ denote three sets containing x, y, and $n+1$ elements (all distinct), respectively, where n is a positive integer. For any non-negative integer k, define $A_k = A \cup \{0, \ldots, k-1\}$ and $B_k = B \cup \{k+1, \ldots, n\}$. Then given any n-element subset S of $A \cup B \cup C$, there exists a unique integer k_S in $C - S$, called the index of S with respect to A and B, such that $|S \cap A_{k_S}| = k_S$ and $|S \cap B_{k_S}| = n - k_S$. To see this, define $S_A = A \cap S$, $S_B = B \cap S$, and $T = C - S$. We begin by deleting $|S_A|$ consecutive elements from T, in increasing order and beginning with its smallest element, to obtain a subset T'. We then delete $|S_B|$ consecutive elements from T', in decreasing order and beginning with its largest element, to obtain a subset T'', which must now contain a single element denoted by k_S. It is now clear that $|S \cap A_{k_S}| = k_S$ and $|S \cap B_{k_S}| = n - k_S$.

To prove (13), we count the n-element subsets S of $A \cup B \cup C$ in two different ways. On the one hand, since $|A \cup B \cup C| = x+y+n+1$, the number of such subsets is given by $\binom{x+y+n+1}{n}$. On the other hand, we partition all such n-element subsets into equivalence classes according to each subset's index value. Since $|S \cap A_k| = k$ and $|S \cap B_k| = n - k$, it follows that the number of n-element subsets S having the same index k is given by $\binom{x+k}{k}\binom{y+n-k}{n-k}$ and total number of n-element subsets is given by

$$\sum_{k=0}^{n} \binom{x+k}{k}\binom{y+n-k}{n-k}.$$

Lastly, we equate the two answers to obtain (13).

$\square$

Lemma 7. *Let p and q be positive integers with $q \le p$. Then*

$$\sum_{v=q}^{p} \binom{x+p-v-1}{p-v}\binom{y+v-q-1}{v-q} = \binom{x+y+p-q-1}{p-q}. \tag{14}$$

Proof. Set $k = v - q$ and $n = p - q$. Then (14) can be rewritten as

$$\sum_{w=0}^{p-q} \binom{x+p-q-w-1}{p-q-w} \binom{y+w-1}{w} = \binom{x+y+p-q-1}{p-q},$$

which follows from Lemma 6. $\square$

Theorem 8. *For all $N \in \mathbb{N}$,*

$$S_{b,N}(x)S_{b,N}(y) = S_{b,N}(x+y). \tag{15}$$

Proof. We argue by induction on N. Lemma 6 proves that (15) holds for $S_{b,1}(x)$. Next, assume that (15) holds for $S_{b,N}(x)$. Let $t_{N+1}(j,k)$ denote the (j,k)-entry of $S_{b,N+1}(x)S_{b,N+1}(y)$. Then

$$\begin{aligned} t_{N+1}(j,k) &= \sum_{m=0}^{b^{N+1}-1} \alpha_{N+1}(j,m,x)\alpha_{N+1}(m,k,y) \\ &= \sum_{v=0}^{b-1} \sum_{r=0}^{b^N-1} \alpha_{N+1}(j, vb^N + r, x)\alpha_{N+1}(vb^N + r, k, y). \end{aligned}$$

As before, assume $pb^N \le j \le (p+1)b^N - 1$ and $qb^N \le k \le (q+1)b^N - 1$ for some non-negative integers $p, q \in \{0, 1, \ldots, b-1\}$. Set $j' = j - pb^N$ and $k' = k - qb^N$. Again, we consider two cases:

Case 1: $j < k$. Then $\alpha_{N+1}(j,k,x+y) = 0$ by definition. On the other hand, we have

$$\begin{aligned} t_{N+1}(j,k) &= \sum_{m=0}^{j} \alpha_{N+1}(j,m,x)\alpha_{N+1}(m,k,y) + \sum_{m=j+1}^{b^{N+1}-1} \alpha_{N+1}(j,m,x)\alpha_{N+1}(m,k,y) \\ &= \sum_{m=0}^{j} \alpha_{N+1}(j,m,x) \cdot 0 + \sum_{m=j+1}^{b^{N+1}-1} 0 \cdot \alpha_{N+1}(m,k,y) \\ &= 0 \end{aligned}$$

and thus (15) holds.

Case 2: $j \ge k$. Since $S_{b,N+1}(x) = S_{b,1}(x) \otimes S_{b,N}(x)$, we have

$$\alpha_{N+1}(j, vb^N + r, x) = \begin{cases} \binom{x+p-v-1}{p-v}\alpha_N(j', r, x) & \text{if } j \ge vb^N + r; \\ 0 & \text{if } j < vb^N + r. \end{cases}$$

Similarly, we have

$$\alpha_{N+1}(vb^N + r, k, y) = \begin{cases} \binom{y+v-q-1}{v-q}\alpha_N(r, k', y) & \text{if } k \le vb^N + r; \\ 0 & \text{if } k > vb^N + r. \end{cases}$$

It follows that

$$
\begin{aligned}
t_{N+1}(j,k) &= \sum_{v=q}^{p} \sum_{r=0}^{b^N-1} \binom{x+p-v-1}{p-v} \binom{y+v-q-1}{v-q} \alpha_N(j',r,x)\alpha_N(r,k',y) \\
&= \left(\sum_{v=q}^{p} \binom{x+p-v-1}{p-v} \binom{y+v-q-1}{v-q} \right) \sum_{r=0}^{b^N-1} \alpha_N(j',r,x)\alpha_N(r,k',y) \\
&= \binom{x+y+p-q-1}{p-q} \alpha_N(j',k',x+y) \\
&= \alpha_{N+1}(j,k,x+y),
\end{aligned}
$$

where we have made use of the inductive assumption and Lemma 7. This proves that (15) holds. □

As a corollary, we obtain Theorem 2, which we now prove.

Proof of Theorem 2. Let $j = n$ and $k = 0$. Then the identity

$$
\sum_{m=0}^{b^N-1} \alpha_N(j,m,x)\alpha_N(m,k,y) = \alpha_N(j,k,x+y),
$$

which follows from (15), is equivalent to (5). □

We end this section by describing the infinitesimal generator of $S_{b,N}(x)$. Define $X_{b,1}(x) = (\chi_{j,k})$ to be a strictly lower-triangular matrix whose entries $\chi_{j,k}$ are given by

$$
\chi_{j,k} = \begin{cases} x/(j-k), & \text{if } j \geq k+1; \\ 0, & \text{otherwise.} \end{cases} \tag{16}
$$

For $N > 1$, we define matrices

$$
X_{b,N+1}(x) = X_{b,1}(x) \oplus X_{b,N}(x) = X_{b,1}(x) \otimes I_{b^N} + I_b \otimes X_{b,N}(x),
$$

where $\oplus$ denotes the Kronecker sum and I_{b^N} denotes the $b^N \times b^N$ identity matrix. Observe that $X_{b,1}(x)$ has the following matrix form:

$$
X_{b,1}(x) = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 \\
x & 0 & 0 & \cdots & 0 \\
x/2 & x & 0 & \cdots & 0 \\
x/3 & x/2 & x & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
x/(b-1) & x/(b-2) & x/(b-3) & \cdots & 0
\end{pmatrix} \tag{17}
$$

The following lemmas will be needed. The first states a useful identity involving the unsigned Stirling numbers of the first kind, $c(n,k)$, defined by the generating function

$$x(x+1)...(x+n-1)=\sum_{k=0}^{n}c(n,k)x^k.$$

It is well known that $c(n,k)$ counts the number of n-element permutations consisting of k cycles.

Lemma 9. *Let l and n be positive integers with $l\geq n$. Then*

$$\sum_{i=1}^{l-n+1}(i-1)!\binom{l}{i}c(l-i,n-1)=nc(l,n). \tag{18}$$

Proof. We give a combinatorial argument. Let $A=\{1,2,...,l\}$. We count in two different ways the number of permutations $\pi=\sigma_1\sigma_2\cdots\sigma_n$ of A consisting of n cycles where we distinguish one of the cycles σ_j of π. On the one hand, since there are $c(l,n)$ such permutations π and n ways to distinguish a cycle of π, it follows that the answer is given by $nc(l,n)$. On the other hand, we can construct π by first choosing our distinguished cycle σ_1 consisting of i elements. The number of possibilities for σ_1 is $\binom{l}{i}(i-1)!$ since there are $\binom{l}{i}$ ways to choose i elements from A and $(i-1)!$ ways to construct a cycle from these i elements. It remains to construct the remaining cycles $\sigma_2,\dots,\sigma_n$, which we view as a permutation $\pi'=\sigma_2\cdots\sigma_n$ on $l-i$ elements consisting of $n-1$ cycles. Since there are $c(l-i,n-1)$ such possibilities for π', it follows that the number of permutations π with a distinguished cycle is given by

$$\sum_{i=1}^{l-n+1}(i-1)!\binom{l}{i}c(l-i,n-1).$$

Equating the two answers yields (18) as desired. □

Lemma 10. *Let n be a positive integer with $1\leq n\leq b-1$. Then*

$$X_{b,1}^n(x)=(\chi_n(j,k)), \tag{19}$$

where the entries $\chi_n(j,k)$ are given by

$$\chi_n(j,k)=\begin{cases}\frac{n!}{(j-k)!}c(j-k,n)x^n, & \text{if } j\geq k+n;\\ 0, & \text{otherwise.}\end{cases} \tag{20}$$

Proof. We argue by induction on n. It is clear that (20) holds when $n=1$. Suppose $n>1$. If $j<k+n$, then $\chi_n(j,k)=0$ because $X_{b,1}^m$ is a power of strictly lower-triangular matrices.

Therefore, assume $j \geq k+n$. Then

$$\begin{aligned}
\chi_n(j,k) &= \sum_{i=0}^{b-1} \chi_{n-1}(j,i)\chi_1(i,k) = \sum_{i=k+1}^{j-n+1} \chi_{n-1}(j,i)\chi_1(i,k) \\
&= x^n \sum_{i=k+1}^{j-n+1} \frac{(n-1)!}{(j-i)!} c(j-i,n-1)\frac{1}{i-k} \\
&= x^n \sum_{i=k+1}^{l+k-n+1} \frac{(n-1)!}{(l+k-i)!} c(l+k-i,n-1)\frac{1}{i-k} \\
&= \frac{(n-1)!x^n}{l!} \sum_{m=1}^{l-m} \frac{l!}{m(l-m)!} c(l-m,n-1) \\
&= \frac{(n-1)!x^n}{l!} \sum_{m=1}^{l-n+1} (m-1)!\binom{l}{m} c(l-m,n-1),
\end{aligned}$$

where $l = j-k$ and $m = i-k$. It follows from Lemma 9 that

$$\chi_n(j,k) = \frac{(n-1)!x^n}{l!} \cdot nc(l,n) = \frac{n!}{(j-k)!} c(j-k,n)x^n$$

as desired. □

Lemma 11. *We have*

$$\exp(X_{b,1}(x)) = S_{b,1}(x). \tag{21}$$

Proof. Denote the entries of $\exp(X_{b,1}(x))$ by $\xi(j,k)$. It is clear that $\xi(j,k) = 0$ for $j < k$ and $\xi(j,k) = 1$ for $j = k$ since $X_{b,1}$ is strictly lower triangular. Therefore, assume $j \geq k+1$. Since $X_{b,1}^n = 0$ for $n \geq b$, we have

$$\begin{aligned}
\xi(j,k) &= \sum_{n=1}^{b-1} \frac{\chi_n(j,k)}{n!} \\
&= \frac{1}{(j-k)!} \sum_{n=1}^{b-1} c(j-k,n)x^n \\
&= \frac{x(x+1)\cdots(x+j-k-1)}{(j-k)!} \\
&= \binom{x+j-k-1}{j-k} \\
&= \alpha_1(j,k).
\end{aligned}$$

Thus, (21) holds. □

Theorem 12. *Let N be a positive integer. Then*

$$\exp(X_{b,N}(x)) = S_{b,N}(x). \tag{22}$$

Proof. We argue by induction on N. Lemma 11 shows that (22) is true for $N = 1$. Then since $\exp(A \oplus B) = \exp(A) \otimes \exp(B)$ for any two matrices A and B, it follows that

$$\exp(X_{b,N}(x)) = \exp(X_{b,1}(x) \oplus X_{b,N-1}(x)) = S_{b,1}(x) \otimes S_{b,N-1}(x) = S_{b,N}(x),$$

which proves (22). □

3 Prouhet-Thue-Morse polynomials

In this section we demonstrate how the generalized Sierpiński matrices $S_{b,N}(1)$ arise in the study of Prouhet-Thue-Morse polynomials, first investigated by the author [10]. These polynomials were used in the same paper to give a new proof of the well-known Prouhet-Tarry-Escott problem, which seeks $b \geq 2$ sets of non-negative integers S_0, S_1, …, S_{b-1} that have equal sums of like powers up to degree $M \geq 1$, i.e.,

$$\sum_{n \in S_0} n^m = \sum_{n \in S_1} n^m = \cdots = \sum_{n \in S_{b-1}} n^m$$

for all $m = 0, 1, \ldots, M$. In 1851, E. Prouhet [11] gave a solution (but did not publish a proof; see Lehmer [8] for a proof) by partitioning the first b^{M+1} non-negative integers into the sets $S_0, S_1, \ldots, S_{b-1}$ according to the assignment

$$n \in S_{u_b(n)}.$$

Here, $u_b(n)$ is the generalized Prouhet-Thue-Morse sequence A010060, defined as the residue of the sum of digits of n (base b):

$$u_b(n) = \sum_{j=0}^{d} n_j \bmod b,$$

where $n = n_0 d^0 + \cdots + n_d b^d$ is the base-b expansion of n. When $b = 2$, $u(n) := u_2(n)$ generates the classical Prouhet-Thue-Morse sequence: $0, 1, 1, 0, 1, 0, 0, 1, \ldots$.

Let $A = (a_0, a_1, \ldots, a_{b-1})$ be a *zero-sum vector*, i.e., an ordered collection of b arbitrary complex values that sum to zero:

$$a_0 + a_1 + \cdots + a_{b-1} = 0.$$

We define $F_N(x; A)$ to be the *Prouhet-Thue-Morse* (PTM) polynomial of degree $b^N - 1$ whose coefficients belong to A and repeat according to $u_b(n)$, i.e.,

$$F_N(x; A) = \sum_{n=0}^{b^N-1} a_{u_b(n)} x^n. \tag{23}$$

In the case where $b = 2$, $a_0 = 1$, and $a_1 = -1$, we obtain the classic product generating function formula

$$\prod_{m=0}^{N}(1 - x^{2^m}) = \sum_{n=0}^{2^{N+1}-1} (-1)^{u(n)} x^n. \tag{24}$$

Lehmer generalized this formula to the case where $A = (1, \omega, \omega^2, \ldots, \omega^{b-1})$ consists of all b-th roots of unity with $\omega = e^{i2\pi/b}$. The following theorem, proven by the author [10], extends this factorization to $F_N(x; A)$ for arbitrary zero-sum vectors.

Theorem 13 ([10])**.** *Let N be a positive integer and A a zero-sum vector. There exists a polynomial $P_N(x)$ such that*

$$F_N(x; A) = P_N(x) \prod_{m=0}^{N-1}(1 - x^{b^m}). \tag{25}$$

Theorem 13 is useful in that it allows us to establish that the polynomial $F_N(x, A)$ has a zero of order N at $x = 1$, from which Prouhet's solution follows easily by setting $N = M + 1$ and differentiating $F_N(x; A)$ m times [10].

We now derive formulas for the coefficients of $P_N(x)$ in terms of generalized Sierpiński triangles. Towards this end, let

$$P_N(x; \mathbf{c}_N) = \sum_{n=0}^{b^N-1} c_n x^n$$

denote a polynomial whose coefficients are given by the column vector $\mathbf{c}_N = (c_0, ..., c_{b^N-1})^T$. Also, let

$$\mathbf{a}_n = (a_{u_b(0)}, a_{u_b(1)}, \ldots, a_{u_b(b^N-1)})^T$$

be a column vector consisting of elements of A generated by the PTM sequence $u_b(n)$. Next, define a sequence of $b^N \times b^N$ matrices M_N recursively as follows. Set

$$M_1 = (m_{j,k}) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 1 & 0 & \cdots & 0 & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & \cdots & -1 & 1 \end{pmatrix}$$

where

$$m_{j,k} = \begin{cases} 1, & \text{if } j = k; \\ -1, & \text{if } j - k = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Then for $N > 1$, define

$$M_{N+1} = M_1 \otimes M_N = \begin{pmatrix} M_N & 0_N & 0_N & \cdots & 0_N & 0_N \\ -M_N & M_N & 0 & \cdots & 0_N & 0_N \\ & & & \ddots & & \\ 0_N & 0_N & 0_N & \cdots & -M_N & M_N \end{pmatrix}, \tag{26}$$

where $M_1 \otimes M_N$ denotes the Kronecker product. The following theorem establishes a matrix relationship between the vectors $\mathbf{a}_N$ and $\mathbf{c}_N$.

Theorem 14. *Let $A = (a_0, \ldots, a_{b-1})$ be a zero-sum vector. The polynomial equation*

$$F_N(x; A) = P_N(x; \mathbf{c}_N) \prod_{m=0}^{N-1} (1 - x^{b^m}) \tag{27}$$

is equivalent to the matrix equation

$$\mathbf{a}_N = M_N \mathbf{c}_N \tag{28}$$

together with the condition $c_n = 0$ for any n that contains the digit $b-1$ in its base-b expansion, where $0 \leq n \leq b^N - 1$.

To prove Theorem 14, we shall need the following two lemmas, which we state without proof since their results are easy to verify.

Lemma 15. *Let $A = (a_0, a_1, \ldots, a_{b-1})$ and $\mathbf{c}_1 = (c_0, \ldots, c_{b-1})^T$. Then the polynomial equation*

$$\sum_{n=0}^{b-1} a_n x^n = \left(\sum_{n=0}^{b-1} c_n x^n \right) (1 - x)$$

is equivalent to the system of equations

$$\begin{aligned} a_0 &= c_0 \\ a_1 &= -c_0 + c_1 \\ &\vdots \\ a_{b-1} &= -c_{b-2} + c_{b-1} \end{aligned}$$

together with the condition $c_{b-1} = 0$.

Lemma 16. *The system of equations in Lemma 15 can be expressed in matrix form as*

$$\mathbf{a}_1 = M_1 \mathbf{c}_1.$$

Proof of Theorem 14. We argue by induction on N. It is clear that (28) holds for $N = 1$ since the polynomial equation $F_1(x; A) = P_1(x; \mathbf{c}_1)(1-x)$ is equivalent to $\mathbf{a}_1 = M_1\mathbf{c}_1$ because of Lemmas 15 and 16. Next, assume that (28) holds for case N. We shall prove that (28) holds for case $N+1$. Define

$$P_N(x; C_N(p)) = \sum_{n=0}^{b^N-1} c_{n+pb^N} x^{n+pb^N}$$

to be a polynomial whose coefficients are given by the entries of $C_N(p) = (c_{pb^N}, \ldots, c_{(p+1)b^N-1})$, i.e., those elements in $\mathbf{c}_{N+1}$ from position pb^N to position $(p+1)b^N$, so that

$$P_{N+1}(x; \mathbf{c}_{N+1}) = P_{N-1}(x; C_N(0)) + \cdots + P_{N-1}N(x; C_N(b-1)).$$

We then expand the right-hand side of (25) for case $N+1$ as follows:

$$\begin{aligned}
F_{N+1}(x; A) &= (P_N(x; C_N(0)) + \cdots + P_N(x; C_N(b-1))) \left(\prod_{m=0}^{N-1}(1-x^{b^m})\right)(1-x^{b^N}) \\
&= (Q_N(x; C_N(0)) + \cdots + Q_N(x; C_N(b-1)))\,(1-x^{b^N}) \\
&= Q_N(x; C_N(0)) + \Big(Q_N(x; C_N(1)) - x^{b^N} Q_N(x; C_N(0))\Big) + \cdots + \\
&\quad \Big(Q_N(x; C_N(b-1)) - x^{b^N} Q_N(x; C_N(b-2))\Big) - x^{b^N} Q_N(x; C_N(b-1)),
\end{aligned}$$

where we define

$$Q_N(x; C_N(p)) = P_N(x; C_N(p)) \prod_{m=0}^{N-1}(1-x^{b^m}).$$

Next, we equate this result with the definition of $F_{N+1}(x; A)$:

$$F_{N+1}(x; A) = \sum_{n=0}^{b^{N+1}-1} a_{u_b(n)} x^n = F_N(x; A_N(0)) + \cdots + F_N(x; A_N(b-1)),$$

where we define

$$F_N(x; A_N(p)) = \sum_{n=0}^{b^N-1} a_{u(n+pb^N)} x^{n+pb^N}.$$

This leads to the system of polynomial equations

$$\begin{aligned}
F_N(x; A_N(0)) &= Q_N(x; C_N(0)) \\
F_N(x; A_N(1)) &= Q_N(x; C_N(1)) - x^{b^N} Q_N(x; C_N(0)) \\
&\vdots \\
F_N(x; A_N(b-1)) &= Q_N(x; C_N(b-1)) - x^{b^N} Q_N(x; C_N(b-2))
\end{aligned}$$

together with the condition $Q_N(x; C_N(b-1)) = 0$, i.e. $c_n = 0$ for all $(b-1)b^N \leq n \leq b^{N+1}-1$. It follows from Lemmas 15 and 16 that this system is equivalent to the system of matrix equations

$$\begin{aligned}
\mathbf{a}_N(0) &= M_N \mathbf{c}_N(0) \\
\mathbf{a}_N(1) &= -M_N \mathbf{c}_N(0) + M_N \mathbf{c}_N(1) \\
&\vdots \\
\mathbf{a}_N(b-1) &= -M_N \mathbf{c}_N(b-2) + M_N \mathbf{c}_N(b-1),
\end{aligned}$$

where the first matrix equation by assumption satisfies the condition $c_n = 0$ for any $0 \leq n \leq b^N - 1$ that contains the digit $b-1$ in its base-b expansion. This in turn is equivalent to the matrix equation $\mathbf{a}_{N+1} = M_{N+1}\mathbf{c}_{N+1}$ together with the condition that $c_n = 0$ for any $0 \leq n \leq b^{N+1} - 1$ that contains the digit $b-1$ in its base-b expansion. This establishes the theorem for case $N+1$ and completes the proof. □

Lemma 17. *The matrix M_N has inverse $S_N = M_N^{-1}$, where S_N is given recursively by*

$$S_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ & & & \ddots & \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \tag{29}$$

and for $N > 1$,

$$S_{N+1} = S_1 \otimes S_N = \begin{pmatrix} S_N & 0_N & 0_N & \ldots & 0_N \\ S_N & S_N & 0_N & \ldots & 0_N \\ & & & \ddots & \\ S_N & S_N & S_N & \ldots & S_N \end{pmatrix}. \tag{30}$$

Thus, if $\mathbf{a}_N = M_N \mathbf{c}_N$, then

$$\mathbf{c}_N = S_N \mathbf{a}_N. \tag{31}$$

Proof. It is straightforward to verify directly that $S_1 = M_1^{-1}$. Since $S_{N+1} = S_1 \otimes S_N$ and $M_{N+1} = M_1 \otimes M_N$, it follows that $S_N = M_N^{-1}$. □

Observe that $S_N = S_{b,N}(1)$ is the generalized Sierpiński triangle defined in the previous section. We now present a formula for the coefficients c_n in terms of the elements of A.

Theorem 18. *Let $A = (a_0, \ldots, a_{b-1})$ be a zero-sum vector. Then the polynomial equation (27) has solution $P_N(x; C_N)$ whose coefficients c_n, $0 \leq n \leq b^N - 1$, are given by*

$$c_n = \sum_{k \in I_b(n)} a_{u_b(k)}, \tag{32}$$

where $I_b(n) = \{k \in \mathbb{N} : k \preceq_b n\}$. Moreover, $c_n = 0$ for all n whose base-b expansion contains the digit $b-1$.

Proof. From Theorem 5, we know that the non-zero entries in the n-th row of S_N, which are all equal to 1, are located at (n,k) where $k \preceq_b n$. Formula (32) now follows from (31). It remains to show that (32) yields $c_n = 0$ for all n whose base-b expansion contains the digit $b-1$. Let $n = n_0 b^0 + \cdots + n_L b^L + \cdots + n_{N-1} b^{N-1}$ where $n_L = b-1$. Denote $I_b(n;L)$ to be the subset of $I_b(n)$ consisting of integers whose base-b expansion has digit 0 at position L, i.e.,

$$I_b(n;L) = \{k \in \mathbb{N} : k \preceq_b n, k = k_0 b^0 + \cdots + k_N b^N, k_L = 0\}.$$

Then using the fact that A is a zero-sum vector, i.e., $a_0 + \cdots + a_{b-1} = 0$, we have

$$\begin{aligned} c_n &= \sum_{k \in I_b(n;L)} a_{u_b(k)} + \sum_{k \in I_b(n;L)} a_{u_b(k+b^L)} + \cdots + \sum_{k \in I_b(n;L)} a_{u_b(k+(b-1)b^L))} \\ &= \sum_{k \in I_b(n;L)} \left(a_{u_b(k)} + a_{(u_b(k)+1)_b} + \cdots + a_{(u_b(k)+(b-1))_b}\right) \\ &= 0 \end{aligned}$$

as desired. □

Next, we specialize Theorem 18 to base $b = 3$. Define $w(n)$ to be the sum of the digits of n in its base-3 representation modulo 2.

Corollary 19. *Suppose $b = 3$. Let $n \in \mathbb{N}$ be such that its base-3 representation does not contain the digit 2. Then*

$$c_n = (-1)^{w(n)} a_{u_3(2n)}. \tag{33}$$

Proof. Let $n = n_0 3^0 + \cdots + n_{N-1} 3^{N-1}$ be the base-3 representation of n with no digit equal to 2 and leading digit $n_{N-1} = 1$. We argue by induction on N. It is clear that (33) holds when $N = 1$ since from (32) we have

$$c_1 = a_0 + a_1 = -a_2 = (-1)^{w(n)} a_{u_3(2n)}.$$

Next, assume (33) holds for a given N. To prove that (33) holds for $N+1$, we consider two cases by decomposing $n = n' + 3^N$.

Case 1: $n_i = 0$ for all $i = 0, \ldots, N-1$. Then $n = 3^n$ and

$$\begin{aligned} c_n &= \sum_{k \in I_3(n)} a_{u_3(k)} = a_{u_3(0)} + a_{u_3(n)} = a_0 + a_1 = -a_2 \\ &= (-1)^{w(n)} a_{u_3(2n)}. \end{aligned}$$

Case 2: $n_L = 1$ for some $0 \le L \le N-1$. Then set $n'' = n' - 3^L$. It follows that

$$\begin{aligned}
c_n &= \sum_{k\in I_3(n)} a_{u_3(k)} = \sum_{k\in I_3(n,L)} a_{u_3(k)} + \sum_{k\in I_3(n,L)} a_{u_3(k+3^N)} \\
&= \sum_{k\in I_3(n')} a_{u_3(k)} + \sum_{k\in I_3(n')} a_{u_3(k+3^L)} \\
&= \sum_{k\in I_3(n')} a_{u_3(k)} + \sum_{k\in I_3(n',L)} a_{u_3(k+3^L)} + \sum_{k\in I_3(n',L)} a_{u_3(k+2\cdot 3^L)} + \sum_{k\in I_3(n',L)} a_{u_3(k)} - \sum_{k\in I_3(n',L)} a_{u_3(k)} \\
&= \sum_{k\in I_3(n')} a_{u_3(k)} + \sum_{k\in I_3(n',L)} \left(a_{u_3(k)} + a_{(u_3(k)+1)_3} + a_{(u_3(k)+2)_3}\right) - \sum_{k\in I_3(n'')} a_{u_3(k)} \\
&= (-1)^{w(n')} a_{u_3(2n')} - (-1)^{w(n'')} a_{u_3(2n'')} \\
&= (-1)^{w(n')} a_{u_3(2n')} + (-1)^{w(n''+3^L)} a_{u_3(2(n'-3^L))} \\
&= (-1)^{w(n')} \left(a_{u_3(2n')} + a_{(u_3(2n')-2)_3}\right) = (-1)^{w(n')} \left(-a_{(u_3(2n')-1)_3}\right) \\
&= (-1)^{w(n'+3^N)} a_{(u_3(2n')+2)_3))} = (-1)^{w(n)} a_{u_3(2n'+2\cdot 3^L)} \\
&= (-1)^{w(n)} a_{u_3(2n)}.
\end{aligned}$$

Thus, (33) holds for $N+1$. □

4 Group generators and relations

In this section, we reveal further evidence of the rich structure of Sierpiński matrices by describing group generators and relations defined by the matrices S_N and M_N. Recall that S_N and M_N are matrices of dimension $b^N \times b^N$ for a given base b. Define $T_N = M_N^t$ to be the transpose of M_N and $U_N = S_N T_N$, $V_N = T_N S_N$. The following lemma gives a recursive construction of U_N andV_N.

Lemma 20. *We have*

$$\begin{aligned}
U_{N+1} &= U_1 \otimes U_N \\
V_{N+1} &= V_1 \otimes V_N
\end{aligned}$$

Proof. The result follows from the mixed-product property of the Kronecker product. We demonstrate this for U_{N+1}:

$$U_{N+1} = S_{N+1}T_{N+1} = (S_1 \otimes S_N)(T_1 \otimes T_N) = (S_1T_1) \otimes (S_NT_N) = U_1 \otimes U_N.$$

The calculation is the same for V_{N+1}. □

Observe that $U_N = (u_{i,j})$ and $V_N = (v_{i,j})$ are skew-triangular and that V_N is the skew-transpose of U_N, i.e., $v_{i,j} = u_{b-1-j,b-1-i}$ for $i,j = 0,1,\dots,b-1$. Here are some examples of

U_N and V_N when $b = 2$:

$$U_1 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad U_2 = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & 0 & -1 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

$$V_1 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad V_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \\ 0 & -1 & 0 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

The next lemma establishes that the eigenvalues of U_N and V_N are $(b+1)$-th roots of 1 or -1.

Lemma 21. *The set of eigenvalues of U_1 and V_1 are exactly the same and consist of all roots of the polynomial equation*

$$-1 + r - r^2 + \cdots + (-1)^{b+1} r^b = 0.$$

Proof. Let r be a root of $-1 + r - r^2 + \cdots + (-1)^{b+1} r^b = 0$. We claim that r is an eigenvalue of U_1 with eigenvector $\mathbf{v} = (v_1, \ldots, v_b)^T$, where

$$v_k = \sum_{j=1}^{k} (-1)^{j+1} r^j$$

for $k = 1, \ldots, b$. Observe that $v_b = 1$. Denote $\mathbf{w} = (U_1 - rI_b)\mathbf{v} = (w_1, \ldots, w_b)^T$. It suffices to show $\mathbf{w} = 0$. It is straightforward to verify that

$$U_1 = (u_{j,k}) = \begin{cases} 1, & \text{if } k = 1; \\ -1, & \text{if } k = j+1; \\ 0, & \text{otherwise.} \end{cases}$$

We now calculate w_j by considering three cases:

Case 1: $k = 1$. Then

$$w_1 = (u_{1,1} - r)v_1 + u_{1,2}v_2 = (1-r)r - (r - r^2) = 0.$$

Case 2: $1 < k < b$. Then

$$w_k = u_{k,1}v_1 + (u_{k,k} - r)v_k + u_{k,k+1}v_{k+1} = r - r\sum_{j=1}^{k}(-1)^{j+1}r^j - \sum_{j=1}^{k+1}(-1)^{j+1}r^j = 0.$$

Case 3: $k = b$. Then

$$w_b = u_{b,1}v_1 + (u_{b,b} - r)v_b = r - r = 0.$$

Thus, $\mathbf{w} = 0$. It can be shown by a similar argument that the eigenvalues of V_1 are exactly the same as those of U_1. $\square$

Theorem 22. *The matrices U_N and V_N satisfy the relation*

$$U_N^{b+1} = V_N^{b+1} = (-1)^{N(b+1)} I_{b^N}, \tag{34}$$

where I_{b^N} is the $b^N \times b^N$ identity matrix.

Proof. We shall only prove (34) for U_N since the proof for V_N is the same. We argue by induction on N. When $N = 1$, we know from Lemma 21 that all eigenvalues of U_1 are roots of $-1 + r - r^2 + \cdots + (-1)^{b+1} r^b = 0$. It follows that every eigenvalue r satisfies $r^{b+1} = (-1)^{b+1}$; moreover, since they are all distinct, the corresponding eigenvectors are all linearly independent. Thus, $U_1^{b+1} = (-1)^{b+1} I_b$.

Next, assume that (34) holds for U_{N-1}. It follows from the mixed-product property of the Kronecker product that

$$\begin{aligned} U_N^{b+1} &= (U_1 \otimes U_{N-1})^{b+1} = U_1^{b+1} \otimes U_{N-1}^{(N-1)(b+1)} \\ &= (-1)^{b+1} I_b \otimes (-1)^{(N-1)(b+1)} I_{b^{N-1}} \\ &= (-1)^{N(b+1)} I_{b^N}. \end{aligned}$$

Thus, (34) holds for N. $\square$

We note that for $b = 2$, Ferrand [4] proved that the matrices S_N and T_N satisfy the three-strand braid relation

$$S_N T_N S_N = T_N S_N T_N. \tag{35}$$

We give an alternate proof of (35) based on Theorem 22. Define $Q_N = S_N T_N S_N$ and $R_N = T_N S_N T_N$. Then $Q_N R_N = U_N^3 = (-1)^{3N} I_{2^N} = (-1)^N I_{2^N}$ because of (34). Moreover, we claim that $Q_N^2 = R_N^2 = (-1)^N I_{2^N}$. This follows by induction on N, which we demonstrate for Q_N by again using the mixed-product property of the Kronecker product:

$$\begin{aligned} Q_N^2 &= (S_N T_N S_N^2 T_N S_N) \\ &= (S_1 T_1 S_1^2 T_1 S_1) \otimes (S_{N-1} T_{N-1} S_{N-1}^2 T_{N-1} S_{N-1}) \\ &= (-I_2) \otimes ((-1)^{N-1} I_{2^{N-1}}) \\ &= (-1)^N I_{2^N} \end{aligned}$$

Thus, $Q_N R_N = Q_N^2$, which implies the braid relation $Q_N = R_N$. However, we find that the braid relation fails to hold for $b > 2$.

References

[1] J.-P. Allouche and J. Shallit, The ubiquitous Prouhet-Thue-Morse sequence, in C. Ding, T. Helleseth, and H. Niederreiter, eds., *Sequences and Their Applications*, Proc. SETA'98, Springer-Verlag, 1999, pp. 1–16.

[2] T. Ball, T. Edgar, and D. Juda, Dominance orders, generalized binomial coefficients, and Kummer's theorem, *Math. Mag.* **87** (2014), 135–143.

[3] D. Callan, Sierpinski's triangle and the Prouhet-Thue-Morse word, preprint, http://arxiv.org/abs/math/0610932.

[4] E. Ferrand, Pascal and Sierpinski matrices, and the three strand braid group, preprint, http://webusers.imj-prg.fr/~emmanuel.ferrand/publi/PSB.ps.

[5] E. Ferrand, An analogue of the Thue-Morse sequence, *Elect. J. Comb.* **14** (2007), #R30.

[6] H. W. Gould, Some generalizations of Vandermonde's convolution, *Amer. Math. Monthly* **63** (1956), 84–91.

[7] A. Imani and A. R. Moghaddamfar, The inverse of the Pascal lower triangular matrix modulo p, *Acta Math. Univ. Comenianae* **79** (2010), 135–142.

[8] D. H. Lehmer, The Tarry-Escott problem, *Scripta Math.* **13** (1947), 37–41.

[9] H. D. Nguyen, A digital binomial theorem, preprint, http://arxiv.org/abs/1412.3181.

[10] H. D. Nguyen, A new proof of the Prouhet-Tarry-Escott problem, preprint, http://arxiv.org/abs/1411.6168.

[11] E. Prouhet, Mémoire sur quelques relations entre les puissances des nombres, *C. R. Acad. Sci. Paris*, **33** (1851), 225.

2010 *Mathematics Subject Classification*: Primary 11C20; Secondary 05A10.
Keywords: binomial theorem, Sierpiński triangle, Prouhet-Thue-Morse sequence.

(Concerned with sequence A010060.)

Received February 1 2015; revised version received March 30 2015. Published in *Journal of Integer Sequences*, May 26 2015.

Return to Journal of Integer Sequences home page.