MAXIMAL ENTRIES OF ELEMENTS IN CERTAIN MATRIX MONOIDS

Sandie Han

Department of Mathematics, New York City College of Technology, The City University of New York (CUNY, New York
shan@citytech.cuny.edu

Ariane M. Masuda[1]

Department of Mathematics, New York City College of Technology, The City University of New York (CUNY), New York
amasuda@citytech.cuny.edu

Satyanand Singh

Department of Mathematics, New York City College of Technology, The City University of New York (CUNY), New York
ssingh@citytech.cuny.edu

Johann Thiel

Department of Mathematics, New York City College of Technology, The City University of New York (CUNY), New York
jthiel@citytech.cuny.edu

Abstract

Let $L_u = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$ and $R_v = \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}$ be matrices in $SL_2(\mathbb{Z})$ with $u, v \geq 1$. Since the monoid generated by L_u and R_v is free, we can associate a depth to each element based on its product representation. In the cases where $u = v = 2$ and $u = v = 3$, Bromberg, Shpilrain, and Vdovina found a depth n matrix containing the maximal entry for each $n \geq 1$. By using ideas from our previous work on positive linear fractional transformation (u, v)-Calkin-Wilf trees and a polynomial partial ordering, we extend their results for any $u, v \geq 1$ and in the process we recover the Fibonacci and some Lucas sequences. As a consequence we obtain bounds which guarantee collision resistance on a family of Cayley hash functions based on L_u and R_v.

1. Introduction

Let $L_u := \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$ and $R_v := \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}$ where u and v are fixed positive integers. These matrices have been considered in the study of growth and expansion in groups, expander graphs, and in connection with the girth of certain Cayley graphs in $SL_2(\mathbb{F}_p)$ (p a prime) in important works by Bourgain and Gamburd [4], and Helfgott [11]. We are interested in the monoid generated by L_u and R_v. Nathanson [13] provided a simple proof that this monoid is free. That is, every non-identity element M in the monoid generated by L_u and R_v can be written as an alternating product of positive powers of L_u and R_v in a unique way. We refer to the sum of these powers as the depth[2] of M. For example, if $M = L_u^3 R_v^{24} L_u^7$, then the depth of M is 34. We define the depth of the identity matrix as zero.

In 2017, Bromberg, Shpilrain, and Vdovina [6] proposed a Cayley hash function[3] based on L_u and R_v in $SL_2(\mathbb{F}_p)$. Bromberg [5] and Bromberg, Shpilrain, and Vdovina [6] measured the collision resistance of these Cayley hash functions by finding a depth n matrix containing the maximal entry in the cases where $u = v = 2$ and $u = v = 3$ for each $n \geq 1$. The proof is by induction. They show that if M is a depth n matrix containing the maximal entry and maximal column sum, then either $L_u M$ or $R_v M$, depending on the parity of n, must be a depth $n+1$ matrix containing the maximal entry and maximal column sum.

The goal of this paper is to answer and expand upon some open questions[4] appearing in [5, 6]. Our main contribution is to extend the above result to the general case $u, v \geq 1$ (Theorem 1). In the case where $u, v \geq 2$, our method uses a similar induction argument as above. When either $u = 1$ or $v = 1$, this induction argument fails. We indicate at the end of Proposition 3 exactly where the problem occurs. In this case the situation is more complicated, requiring a different strategy. The novelty of our approach lies in the framework of the Calkin-Wilf tree. This tree provides a rich, highly symmetric structure that allows us to organize the elements of the monoid in an intuitive way. Together with a partial ordering for polynomials, this yields a proof for the more intricate case.

The Calkin-Wilf tree is a rooted tree whose vertices are labeled by positive rational numbers. Starting from the root 1, each vertex a/b has two children: the left one is $a/(a + b)$ and the right one is $(a + b)/b$ (see Figure 1). A nice feature of this tree is that every positive rational number appears in the tree exactly once and in reduced form. In past decades, the Calkin-Wilf tree has received a lot of attention due to its many remarkable properties; see [7, 14] for a more thorough history of this material.

---

[2]Some readers may prefer the term length, but our choice of the word depth will be made clear shortly.

[3]The term Cayley hash function comes from the connection to Cayley graphs [10] mentioned in the previous paragraph.

[4]The original questions in [5, 6] only ask about the case $u = 1$ and $v = 2$ (or vice versa).
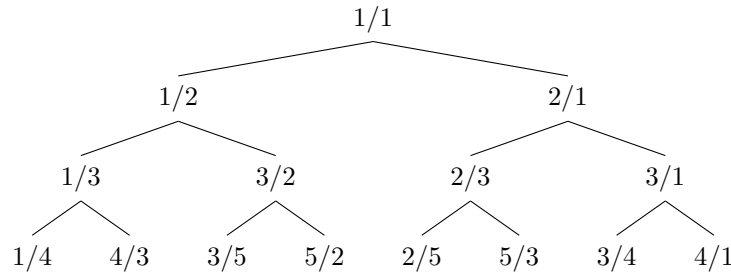
Figure 1: The first four rows of the Calkin-Wilf tree.

For a generalization of the Calkin-Wilf tree, one can consider a modified genera-
tion rule for each vertex a/b: its left child is defined by $a/(ua+b)$ and its right child
by $(a+vb)/b$. Such a tree is called the (u,v)-*Calkin-Wilf tree* and its vertices are
a subset of the vertices of the Calkin-Wilf tree. In fact, given $uv > 1$, the positive
rationals can be partitioned in pairwise disjoint (u,v)-Calkin-Wilf trees with roots
coming from a special "orphan" set [8, 9, 14].

Another generalization of the Calkin-Wilf tree can be made for rooted trees
whose vertices are matrices in $GL_2(\mathbb{N}_0)$ with a generation rule based on matrix
multiplication with a pair of fixed matrices L and R. Nathanson refers to such trees
as generalized Calkin-Wilf trees for positive linear transformations[5] (PLTFs) [14].
In the case where $L = L_u$ and $R = R_v$, we construct the *PLFT (u,v)-Calkin-Wilf
tree*, denoted by $\mathcal{T}^{(u,v)}(M)$, according to the following generation rules:

1. the root is labeled M,

2. the left child of a vertex $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is labeled $\begin{bmatrix} a & b \\ ua+c & ub+d \end{bmatrix}$, and

3. the right child of a vertex $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is labeled $\begin{bmatrix} a+vc & b+vd \\ c & d \end{bmatrix}$.

In Figure 5 in the Appendix we illustrate the $\mathcal{T}^{(1,1)}(I_2)$ tree. By associating a
reduced rational number a/b to the vector $\begin{bmatrix} a \\ b \end{bmatrix}$ and considering the column vectors
of each matrix, it can be seen that $\mathcal{T}^{(1,1)}(I_2)$ is essentially running two Calkin-Wilf
trees in parallel that are independent of each other.

This PLFT (u,v)-Calkin-Wilf tree perspective helps us understand the monoid
generated by L_u and R_v, because the left child and the right child of a vertex M
are obtained precisely by multiplying M (on the left) by L_u and R_v, respectively.

---

[5]We also use the term PLFT here since there is a clear isomorphism between the monoid of
PLFTs (under function composition) and $GL_2(\mathbb{N}_0)$. For a proof of this fact, see [14] and [9].
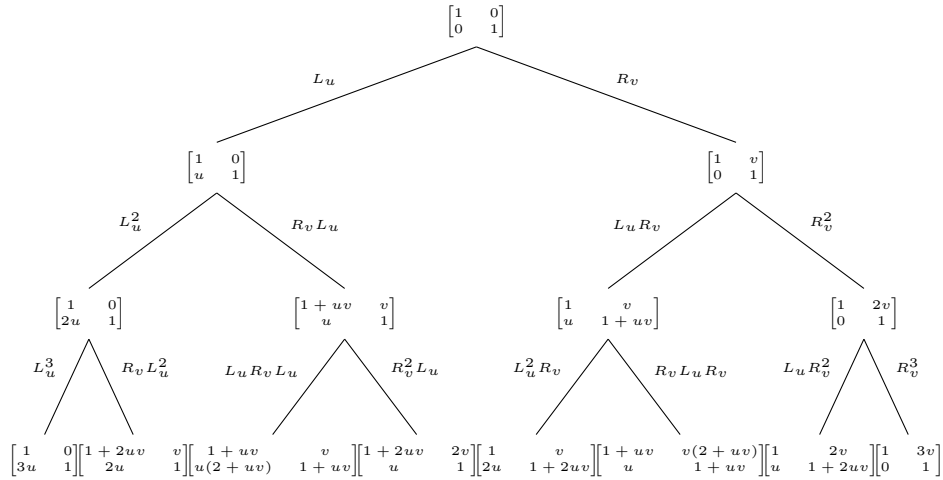
Figure 2: The first four rows of the $\mathcal{T}^{(u,v)}(I_2)$ tree.

Furthermore, the PLFT (u, v)-Calkin-Wilf tree organizes the elements in the monoid generated by L_u and R_v by depth n (see Figure 2). This organization is highly symmetric, a property which is exploited in this paper. A visual inspection of the forms of the entries in terms of u and v in Figure 2 suggests our results. To highlight our key ideas and make them more clear, we provide several examples and a concise summary of our arguments. See Figures 5-8 in the Appendix for an illustration of the first five rows of the $\mathcal{T}^{(1,1)}(I_2)$, $\mathcal{T}^{(5,2)}(I_2)$, $\mathcal{T}^{(2,5)}(I_2)$, and $\mathcal{T}^{(5,1)}(I_2)$ trees.

1.1. Examples

We begin with a few different examples illustrating various cases. Let $M_{i,j}$ denote the (i, j)-entry of M.

- In the case of the $\mathcal{T}^{(1,1)}(I_2)$ tree (see Figure 5), the numerical values of the maximal entries and their corresponding positions in depth n are:

$$
\begin{array}{ccccccccc}
1 & \to & 1 & \to & 2 & \to & 3 & \to & \cdots, \\
I_{1,1} & \to & (L_1)_{2,1} & \to & (R_1 L_1)_{1,1} & \to & (L_1 R_1 L_1)_{2,1} & \to & \cdots.
\end{array}
$$

We observe that the first five maximal entries coincide with the first five terms of the Fibonacci sequence. We also observe that a path of maximal entries exhibits an alternating L_u and R_v pattern. A close examination of the $\mathcal{T}^{(1,1)}(I_2)$ tree reveals that the path given above is not unique since

$$
I_{1,1} \to (R_1)_{1,2} \to (L_1 R_1)_{2,2} \to (R_1 L_1 R_1)_{1,2} \to \cdots
$$

provides another path to obtain the maximal entries. It is also interesting to see that this path is the symmetric image of the previous path.

- In the case of the $\mathcal{T}^{(5,2)}(I_2)$ tree (see Figure 6), the numerical values of the maximal entries and their corresponding positions in depth n are:

$$\begin{array}{ccccccccc}
1 & \rightarrow & 5 & \rightarrow & 11 & \rightarrow & 60 & \rightarrow & \cdots, \\
I_{1,1} & \rightarrow & (L_5)_{2,1} & \rightarrow & (R_2 L_5)_{1,1} & \rightarrow & (L_5 R_2 L_5)_{2,1} & \rightarrow & \cdots.
\end{array}$$

We observe the generalized Fibonacci relations $11 = 5 \cdot v + 1$, $60 = 11 \cdot u + 5$ and $131 = 60 \cdot v + 11$, and the path exhibits the same alternating L_u and R_v pattern as before. Furthermore, a close examination of $\mathcal{T}^{(5,2)}(I_2)$ reveals that for odd depth, the maximal entry appears to occur uniquely in one position, whereas, for even depth, the same is not true.

- In the case of the $\mathcal{T}^{(2,5)}(I_2)$ tree (see Figure 7), the numerical value of the maximal entries and their corresponding positions at depth n are:

$$\begin{array}{ccccccccc}
1 & \rightarrow & 5 & \rightarrow & 11 & \rightarrow & 60 & \rightarrow & \cdots, \\
I_{2,2} & \rightarrow & (R_5)_{1,2} & \rightarrow & (L_2 R_5)_{2,2} & \rightarrow & (R_5 L_2 R_5)_{1,2} & \rightarrow & \cdots.
\end{array}$$

Note that the maximal values of the $\mathcal{T}^{(2,5)}(I_2)$ tree are exactly the same as those of $\mathcal{T}^{(5,2)}(I_2)$ tree, and the path of the maximal entries is the symmetric counterpart of the path in $\mathcal{T}^{(5,2)}(I_2)$.

- In the case of the $\mathcal{T}^{(5,1)}(I_2)$ tree (see Figure 8), the numerical values of the maximal entries and their corresponding positions at depth n are:

$$\begin{array}{ccccccccc}
1 & \rightarrow & 5 & \rightarrow & 10 & \rightarrow & 35 & \rightarrow & \cdots, \\
I_{2,2} & \rightarrow & (L_5)_{2,1} & \rightarrow & (L_5)_{2,1}^2 & \rightarrow & (L_5 R_1 L_5)_{2,1} & \rightarrow & \cdots.
\end{array}$$

Note that this path does not exhibit the nice alternating L_u and R_v pattern and the generalized Fibonacci relation fails here. Although the first two terms of the sequence follow the Fibonacci relation, $10 = 5 + 1 \cdot u$ and $35 = 10 + 5 \cdot u$, the third term does not since $65 \neq 35 + 10 \cdot u$.

1.2. The Maximal Entry in $\mathcal{T}^{(u,v)}(I_2; n)$

We denote by $\mathcal{T}^{(u,v)}(M; n)$ the (finite) set of matrices of depth n in $\mathcal{T}^{(u,v)}(M)$, where $n \geq 0$. We often refer to $\mathcal{T}^{(u,v)}(M; n)$ as the nth row of the tree. In our search for the maximal entry among all matrices of $\mathcal{T}^{(u,v)}(M; n)$, not only do we observe Fibonacci-like sequence relations among the maximal entries, we are also able to provide an explicit formula for the maximal entry at each depth.

We define the function $\mu : GL_2(\mathbb{N}_0) \to \mathbb{N}$ by $\mu\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \max\{a, b, c, d\}$, which computes the maximal entry of a matrix $M \in GL_2(\mathbb{N}_0)$. For a finite subset S of $GL_2(\mathbb{N}_0)$, we extend the definition of μ to S by $\mu(S) = \max\{\mu(M) : M \in S\}$. So $\mu(\mathcal{T}^{(u,v)}(M; n))$ is the maximal entry among all matrices of depth n in the $\mathcal{T}^{(u,v)}(M)$ tree. In our main theorem (Theorem 1) we show that for $n \geq 0$ and fixed $u \geq v \geq 1$:

$$\mu(\mathcal{T}^{(u,v)}(I_2; n)) = \begin{cases} ((L_u R_v)^{(n-1)/2} L_u)_{2,1} & \text{when } n \text{ is odd,} \\ (L_u (L_u R_v)^{n/2} L_u)_{2,1} & \text{when } n \text{ is even and } u > v = 1, \\ ((R_v L_u)^{n/2})_{1,1} & \text{otherwise.} \end{cases}$$

Similarly, by symmetry, for $n \geq 0$ and fixed $v \geq u \geq 1$:

$$\mu(\mathcal{T}^{(u,v)}(I_2; n)) = \begin{cases} ((R_v L_u)^{(n-1)/2} R_v)_{1,2} & \text{when } n \text{ is odd,} \\ (R_v (R_v L_u)^{n/2} R_v)_{1,2} & \text{when } n \text{ is even, and } v > u = 1, \\ ((L_u R_v)^{n/2})_{2,2} & \text{otherwise.} \end{cases}$$

Theorem 1 provides an explicit formula in terms of u, v and n for computing $\mu(\mathcal{T}^{(u,v)}(I_2; n))$. We define a recursive sequence $F_n^{(u,v)}$ by $F_0^{(u,v)} = 1$, $F_1^{(u,v)} = \max\{u, v\}$, and for $n > 1$

$$F_n^{(u,v)} = \begin{cases} \max\{u, v\} \cdot F_{n-1}^{(u,v)} + F_{n-2}^{(u,v)} & \text{for } n \text{ odd,} \\ \min\{u, v\} \cdot F_{n-1}^{(u,v)} + F_{n-2}^{(u,v)} & \text{for } n \text{ even.} \end{cases}$$

Theorem 1 also shows that when $u, v > 1$ or $u = v = 1$, $\mu(\mathcal{T}^{(u,v)}(I_2; n)) = F_n^{(u,v)}$, that is, the maximal entries coincide with the terms of the above generalized Fibonacci sequence. In particular, $\mu(\mathcal{T}^{(1,1)}(I_2; n)) = F_n^{(1,1)}$ gives precisely the nth Fibonacci number. When $u = v$, $F_n^{(u,u)}$ is a Lucas sequence. This result is analogous to a theorem on the largest values of the Stern sequence by Lucas expanded upon by Paulin [12, 15] and is reminiscent of the work Bates, Bunder, and Tognetti [1, 2] in locating specific rationals within the Calkin-Wilf and Stern-Brocot trees.

Our approach in the proof of Theorem 1 is to consider the entries of each matrix as polynomials in one variable following the (u, v)-Calkin-Wilf tree generation rule (see Figures 2 and 3). The difficulty lies in the determination of the different rates of growth of the polynomial functions in Proposition 8 as the result of the generation rule, that is, whether the left child (multiplication by u) has a larger entry than the right child (multiplication by v) or vice versa. Another challenge is the case $u > v = 1$, which requires special treatment using a polynomial partial ordering;

the difficulty is due to a "misalignment". Namely, the maximal entry in an odd row does not belong to a matrix that is the child of a matrix containing the maximal entry in the previous (even) row.
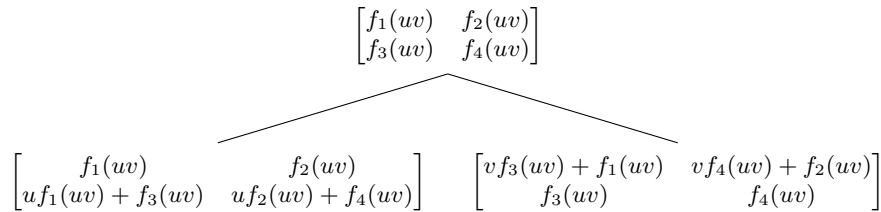
$$\begin{bmatrix} f_1(uv) & f_2(uv) \\ f_3(uv) & f_4(uv) \end{bmatrix}$$

$$\begin{bmatrix} f_1(uv) & f_2(uv) \\ uf_1(uv) + f_3(uv) & uf_2(uv) + f_4(uv) \end{bmatrix} \qquad \begin{bmatrix} vf_3(uv) + f_1(uv) & vf_4(uv) + f_2(uv) \\ f_3(uv) & f_4(uv) \end{bmatrix}$$

Figure 3: Entries in the tree in terms of u and v.

1.3. Certain Symmetric Properties of PLFT (u, v)-Calkin-Wilf Trees

The symmetric features of $\mathcal{T}^{(u,v)}(I_2)$ have greatly aided our proof by simplifying the computations and reducing the number of cases that need to be considered. Let $n \geq 1$ and $i \in \{1, \ldots, 2^n\}$. We denote by $c_{I_2}^{(u,v)}(n, i)$ the ith element from left to right and $c_{I_2}^{(u,v)}(n, 2^n + 1 - i)$ the ith element from right to left of depth n in $\mathcal{T}^{(u,v)}(I_2)$. The elements $c_{I_2}^{(u,v)}(n, i)$ and $c_{I_2}^{(u',v')}(n, 2^n + 1 - i)$ are said to be in *symmetric positions*[6]. Let $\mathcal{L}^{(u,v)} = \mathcal{T}^{(u,v)}(L_u)$ and $\mathcal{R}^{(u,v)} = \mathcal{T}^{(u,v)}(R_v)$ represent the "left side" and "right side" of $\mathcal{T}^{(u,v)}(I_2)$.

The following properties are instrumental in our proof:

- Note that if $1 \leq i \leq 2^{n-1}$, then $c_{I_2}^{(u,v)}(n, i)$ is a vertex in $\mathcal{L}^{(u,v)}$ and $c_{I_2}^{(u,v)}(n, 2^n + 1 - i)$ is a vertex in $\mathcal{R}^{(u,v)}$. It is easy to see that if

$$c_{I_2}^{(u,v)}(n, i) = \cdots R_v^{\alpha_4} L_u^{\alpha_3} R_v^{\alpha_2} L_u^{\alpha_1},$$

  then

$$c_{I_2}^{(u',v')}(n, 2^n + 1 - i) = \cdots L_{u'}^{\alpha_4} R_{v'}^{\alpha_3} L_{u'}^{\alpha_2} R_{v'}^{\alpha_1}$$

  when $1 \leq i \leq 2^{n-1}$.

- If $c_{I_2}^{(u,v)}(n, i) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $c_{I_2}^{(v,u)}(n, 2^n + 1 - i) = \begin{bmatrix} d & c \\ b & a \end{bmatrix}$ (Proposition 9).
  Hence, we may assume $u \geq v$ since, from the above symmetry, it follows that $\mu(\mathcal{T}^{(u,v)}(I_2; n)) = \mu(\mathcal{T}^{(v,u)}(I_2; n))$. That is, the maximal entry among matrices of depth n of $\mathcal{T}^{(u,v)}(I_2)$ is the same as that of $\mathcal{T}^{(v,u)}(I_2)$.

---

[6]Note that pairs of matrices in symmetric positions do not have to be vertices of the same tree.

- If $c_{I_2}^{(u,v)}(n, i) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $c_{I_2}^{(u,v)}(n, 2^n + 1 - i) = \begin{bmatrix} d & \frac{cv}{u} \\ \frac{bu}{v} & a \end{bmatrix}$ (Proposition 8 and [9, Theorem 1]). This symmetric property together with Proposition 10 and the assumption that $u \geq v$ leads to the conclusion that the maximal entry occurs in a matrix on the left side of the tree.

- Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a matrix in $\mathcal{T}^{(u,v)}(I_2)$. Then Lemma 9 shows that the maximal entry on the left side of the tree must appear in the first column of the matrix, that is, $\mu(M) = \max\{a, c\}$. Likewise the maximal entry on the right side of the tree must appear in the second column of the matrix, that is, $\mu(M) = \max\{b, d\}$. Given the assumption $u \geq v$, we focus our work on the first columns of the left side of the tree.

Proposition 3 provides an expression for the maximal entry for odd rows. Let $(L_u R_v)^n L_u = \begin{bmatrix} A_n & * \\ C_n & * \end{bmatrix} \in \mathcal{T}^{(u,v)}(I_2; 2n + 1)$. If $M = \begin{bmatrix} a & * \\ c & * \end{bmatrix} \in \mathcal{T}^{(u,v)}(I_2; 2n + 1)$, then by induction on n, we are able to show that $a, c \leq C_n$. Moreover, we provide an explicit formula for C_n by solving a discrete dynamical system (Lemma 1 and Proposition 2).

For the even rows, we use a convenient argument that reduces the problem to the odd row case. Namely, we consider the maximal entry of $\mathcal{T}^{(u,v)}(R_v; 2n + 1)$. The maximal entry has the form $\mu(\mathcal{T}^{(u,v)}(R_v; 2n + 1)) = \mu((R_v L_u)^{n+1})$ by Proposition 10. We then show that $\mu(\mathcal{T}^{(u,v)}(I_2; 2n + 2)) = \mu(\mathcal{T}^{(u,v)}(R_v; 2n + 1))$.

1.4. An Interesting Application in Cryptography

Another goal of this paper is to address a question raised in [5, 6] related to Cayley hash functions. We provide an answer as an application of Theorem 1.

A hash function is a function that accepts data of arbitrary size as an input and produces an output of a fixed size. For example, the function $f : \mathbb{N} \to [0, m)$ given by $f(n) = n \pmod{m}$ always outputs a nonnegative integer that is no larger than $m - 1$, regardless of the size of the input. This can be a useful tool in storing data (such as online passwords). This leads one to demand that a desirable hash function satisfy some basic requirements (as seen in [6]):

1. It should be computationally difficult to determine an input that hashes to a given output.

2. It should be computationally difficult to determine a second input that hashes to the same output as another given input.

3. It should be computationally difficult to determine two inputs that hash to the same output (referred to as collision resistance).

In [6], Bromberg, Shpilrain, and Vdovina define a Cayley hash function, which we refer to as the BSV hash[7], for binary strings in the following way. Let p be a large prime. For fixed integers $u, v \geq 1$ and a binary string $w = a_0 a_1 \cdots a_n$ where $a_i \in \{0, 1\}$ for $i = 0, \ldots, n$, let $M = \prod_{i=0}^{n} f(a_i)$ where $f(0) = L_u$ and $f(1) = R_v$. (For the empty string λ, define $f(\lambda) = I_2$.) The hashed output, a matrix in $SL_2(\mathbb{F}_p)$, is obtained by reducing the entries of M modulo p. For example, when $u = 2$, $v = 3$ and $p = 5$, the hashed output of the string 01100 is given by $\begin{bmatrix} 0 & 1 \\ 4 & 3 \end{bmatrix}$.

There is a natural one-to-one correspondence between matrices in $\mathcal{T}^{(u,v)}(M; n)$ and bit strings of length n. As such, if one can show that $\mu(\mathcal{T}^{(u,v)}(M; n))$ is bounded above by some monotonically increasing function $f_{(u,v)}(n)$ for all n, then the conclusion is that, in the BSV hash, all bit strings of length at most $n_0 := n_0(u, v)$ have distinct hashed values (i.e., there are no collisions for pairs of "short" strings) where n_0 is the largest integer such that $f_{(u,v)}(n_0) < p$. In [6], this is precisely what is done in the cases $u = v = 2$ and $u = v = 3$.

Proposition 1 (Bromberg, Shpilrain, and Vdovina [6]). *In the BSV hash there are no collisions between outputs of length less than*

$$
\begin{cases}
\log_{\sqrt{3 + \sqrt{8}}} p & \text{when } u = v = 2 \text{ and} \\
\log_{\sqrt{\frac{11 + \sqrt{117}}{2}}} p & \text{when } u = v = 3.
\end{cases}
$$

Corollary 1, a consequence of Theorem 1, immediately allows us to extend this result to any $u, v \geq 1$. In particular, in the case where $u = 2$ and $v = 1$, we get that in the BSV hash there are no collisions between outputs of length less than $\log_{\sqrt{2 + \sqrt{3}}} p$ where $\sqrt{2 + \sqrt{3}} \approx 1.9$, answering a question posed in [6, Problem 3].

The remainder of this paper is organized in the following way. Section 2 contains our main result. Section 3 is devoted to giving a thorough proof of the main result. The proof involves a careful analysis of various cases using a series of different techniques.

2. Main Results

We now state our main results. First, we provide a monotonic closed formula for the maximal entry of any matrix of depth n for any $u, v \geq 1$, denoted by $\mu(\mathcal{T}^{(u,v)}(I_2; n))$, depending on the parity of n. We also determine a matrix and position entry that contain the maximal value for every depth n. As a consequence, we obtain an upper bound on the binary string length that guarantees collision resistance on the BSV Cayley hash function for any $u, v \geq 1$.

---

[7]The BSV hash is a generalization of a hash function defined by Zémor [16].

Theorem 1. *For $n \geq 0$ and positive integers u and v, let $s_{u,v} = \min\{u,v\}$, $t_{u,v} = \max\{u,v\}$, $p_{u,v}^{\pm} = \pm s_{u,v}\sqrt{t_{u,v}} + \sqrt{s_{u,v}(4+uv)}$ and $q_{u,v}^{\pm} = 2 + uv \pm \sqrt{uv(4+uv)}$. Then*

$$\mu(\mathcal{T}^{(u,v)}(I_2; 2n+1)) = \frac{\sqrt{t_{u,v}}\left((q_{u,v}^{+})^{n+1} - (q_{u,v}^{-})^{n+1}\right)}{2^{n+1}\sqrt{s_{u,v}(4+uv)}} \tag{1}$$

and

$$\mu(\mathcal{T}^{(u,v)}(I_2; 2n+2))$$
$$= \begin{cases} \frac{p_{u,v}^{+}(q_{u,v}^{+})^{n+1} + p_{u,v}^{-}(q_{u,v}^{-})^{n+1}}{2^{n+2}\sqrt{s_{u,v}(4+uv)}} & \text{if } s_{u,v} > 1, \\ \frac{\sqrt{t_{u,v}}\left((\sqrt{t_{u,v}}p_{u,v}^{-} + 2)(q_{u,v}^{+})^{n+1} + (\sqrt{t_{u,v}}p_{u,v}^{+} - 2)(q_{u,v}^{-})^{n+1}\right)}{2^{n+2}\sqrt{(4+uv)}} & \text{otherwise.} \end{cases} \tag{2}$$

Furthermore, the value given by (1) is attained by the $(2,1)$ entry of the matrix $(L_u R_v)^n L_u$ when $u \geq v$ and by the $(1,2)$ entry of the matrix $(R_v L_u)^n R_v$ when $v \geq u$. Similarly, the value given by (2) is attained by the $(1,1)$ entry of the matrix $(R_v L_u)^n$ when $u \geq v > 1$, by the $(2,1)$ entry of the matrix $L_u(L_u R_v)^{n-1} L_u$ when $u \geq v = 1$, by the $(2,2)$ entry of the matrix $(L_u R_v)^n$ when $v \geq u > 1$, and by the $(1,2)$ entry of the matrix $R_v(R_v L_u)^{n-1} R_v$ when $v \geq u = 1$.

For concrete examples of Theorem 1, see Tables 1 and 2.

u \ v	1	2
1	$\frac{(3+\sqrt{5})^{n+1} - (3-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$	$\frac{(2+\sqrt{3})^{n+1} - (2-\sqrt{3})^{n+1}}{\sqrt{3}}$
2	$\frac{(2+\sqrt{3})^{n+1} - (2-\sqrt{3})^{n+1}}{\sqrt{3}}$	$\frac{(3+2\sqrt{2})^{n+1} - (3-2\sqrt{2})^{n+1}}{2\sqrt{2}}$
3	$\frac{3((5+\sqrt{21})^{n+1} - (5-\sqrt{21})^{n+1})}{2^{n+1}\sqrt{21}}$	$\frac{3((4+\sqrt{15})^{n+1} - (4-\sqrt{15})^{n+1})}{2\sqrt{15}}$

Table 1: The value of $\mu(\mathcal{T}^{(u,v)}(I_2; 2n+1))$ for various choices of u and v.

u \ v	1
1	$\frac{(\sqrt{5}+1)(3+\sqrt{5})^{n+1} + (\sqrt{5}-1)(3-\sqrt{5})^{n+1}}{2^{n+2}\sqrt{5}}$
2	$(2+\sqrt{3})^{n+1} + (2-\sqrt{3})^{n+1}$
3	$\frac{3((\sqrt{21}-1)(5+\sqrt{21})^{n+1} + (\sqrt{21}+1)(5-\sqrt{21})^{n+1})}{2^{n+2}\sqrt{21}}$

Table 2: The value of $\mu(\mathcal{T}^{(u,v)}(I_2; 2n+2))$ for various choices[8] of u and v.

The discussion in the introduction, together with Theorem 1, immediately gives the following result.

---

[8]We restrict the number of entries in this table due to space considerations.

Corollary 1. *Let $u, v \geq 1$ and $n_0 := n_0(u, v)$ be the largest integer such that $\mu(\mathcal{T}^{(u,v)}(I_2; n_0)) < p$. Then there are no collisions between distinct bit strings of length at most n_0 in the BSV hash.*

When $u = v \in \{2, 3\}$, our results in Theorem 1 and Corollary 1 coincide with the ones obtained by Bromberg, Shpilrain, and Vdovina in [6].

3. Proof of Theorem 1

For the remainder of the paper, since we are concentrating on a proof of Theorem 1, which involves the $\mathcal{T}^{(u,v)}(I_2)$ tree, we will focus our attention only on matrices in $SL_2(\mathbb{N}_0)$.

In Theorem 1, the claim is that, when $u \geq v$, $(L_u R_v)^n L_u$ has the maximal entry among all other matrices in $\mathcal{T}^{(u,v)}(I_2; 2n + 1)$. We first show that the left column entries of matrices of this form can be easily computed using a discrete dynamical system.

Lemma 1. *Let $u, v \in \mathbb{N}$ and $a, c \in \mathbb{N}_0$ (not both zero). Define $\alpha_n := \alpha_n^{(u,v)}(a, c)$ and $\gamma_n := \gamma_n^{(u,v)}(a, c)$ recursively by*

$$\alpha_n = \begin{cases} a & \text{for } n = 0, \\ \alpha_{n-1} + v\gamma_{n-1} & \text{otherwise} \end{cases}$$

and

$$\gamma_n = \begin{cases} ua + c & \text{for } n = 0, \\ u\alpha_{n-1} + (1 + uv)\gamma_{n-1} & \text{otherwise.} \end{cases}$$

Then $\gamma_n \geq \alpha_n$,

$$\gamma_n = \frac{(cp_{u,v}^+ + aq_{u,v}^+\sqrt{u})(q_{u,v}^+)^n + (cp_{u,v}^- - aq_{u,v}^-\sqrt{u})(q_{u,v}^-)^n}{2^{n+1}\sqrt{v(4 + uv)}},$$

and

$$\alpha_n = \frac{(cp_{u,v}^+ + aq_{u,v}^+\sqrt{u})(q_{u,v}^+)^n p_{u,v}^- - (cp_{u,v}^- - aq_{u,v}^-\sqrt{u})(q_{u,v}^-)^n p_{u,v}^+}{2^{n+2}\sqrt{uv(4 + uv)}}$$

where $p_{u,v}^{\pm} = \pm v\sqrt{u} + \sqrt{v(4 + uv)}$ and $q_{u,v}^{\pm} = 2 + uv \pm \sqrt{uv(4 + uv)}$.

Proof. It is clear that $\gamma_0 \geq \alpha_0$. The fact that $\gamma_n \geq \alpha_n$ for $n \geq 1$ follows from noticing that $\gamma_n = u\alpha_n + \gamma_{n-1}$.

As a matrix equation, we have that, for $n \geq 1$,

$$\begin{bmatrix} \alpha_n \\ \gamma_n \end{bmatrix} = \begin{bmatrix} 1 & v \\ u & 1+uv \end{bmatrix} \begin{bmatrix} \alpha_{n-1} \\ \gamma_{n-1} \end{bmatrix}.$$

The eigenvalues of the matrix $\begin{bmatrix} 1 & v \\ u & 1+uv \end{bmatrix}$ are

$$\lambda_1 = \frac{1}{2}\left(2 + uv + \sqrt{uv(4+uv)}\right) \quad \text{and} \quad \lambda_2 = \frac{1}{2}\left(2 + uv - \sqrt{uv(4+uv)}\right)$$

with associated eigenvectors $\vec{v}_1 = \begin{bmatrix} \frac{\sqrt{v(4+uv)} - v\sqrt{u}}{2\sqrt{u}} \\ 1 \end{bmatrix}$ and $\vec{v}_2 = \begin{bmatrix} \frac{-\sqrt{v(4+uv)} - v\sqrt{u}}{2\sqrt{u}} \\ 1 \end{bmatrix}$,

respectively. Solving the vector equation

$$\begin{bmatrix} \alpha_0 \\ \gamma_0 \end{bmatrix} = c_1 \vec{v}_1 + c_2 \vec{v}_2$$

gives that

$$c_1 = \frac{c(v\sqrt{u} + \sqrt{v(4+uv)}) + a\sqrt{u}(2+uv+\sqrt{uv(4+uv)})}{2\sqrt{v(4+uv)}}$$

and

$$c_2 = \frac{c(-v\sqrt{u} + \sqrt{v(4+uv)}) - a\sqrt{u}(2+uv-\sqrt{uv(4+uv)})}{2\sqrt{v(4+uv)}}.$$

It follows that

$$\begin{aligned} \begin{bmatrix} \alpha_n \\ \gamma_n \end{bmatrix} &= \begin{bmatrix} 1 & v \\ u & 1+uv \end{bmatrix}^n \begin{bmatrix} \alpha_0 \\ \gamma_0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & v \\ u & 1+uv \end{bmatrix}^n (c_1\vec{v}_1 + c_2\vec{v}_2) \\ &= c_1\lambda_1^n \vec{v}_1 + c_2\lambda_2^n \vec{v}_2. \end{aligned}$$

So $\gamma_n = c_1\lambda_1^n + c_2\lambda_2^n$, which gives the desired result after the appropriate substitutions. $\qquad\square$

Proposition 2. *Suppose that $M \in SL_2(\mathbb{N}_0)$ is given by $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. For any $n \geq 0$, let*

$$(L_u R_v)^n L_u M = \begin{bmatrix} A_n & * \\ C_n & * \end{bmatrix}.$$

Then $A_n = \alpha_n$ and $C_n = \gamma_n$ where α_n and γ_n are as defined in Lemma 1.

Proof. The result follows by noting the relationship between the left columns of $(L_u R_v)^n L_u M$ and $(L_u R_v)^{n+1} L_u M$. $\qquad\qquad\square$

Note that a result similar to Proposition 2 could easily be found for the right column of $(L_u R_v)^n L_u M$. However, as we will see later on, this is not necessary. The symmetries associated with PLFT (u, v)-Calkin-Wilf trees will allow us to reduce the number of cases to be analyzed.

With Proposition 2 applied to I_2, we can compute the entries in the left column of a specific family of matrices, namely matrices of the form $(L_u R_v)^n L_u$. The next step will be to show that the left column entries of any matrix of depth $2n + 1$ are no larger than C_n.

Definition 1. *Let $M \in SL_2(\mathbb{N}_0)$ be given by $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. We say that M is u-lower dominant (u-LD) if $c \geq ua$ and $d \geq ub$ and we say that M is v-upper dominant (v-UD) if $a \geq vc$ and $b \geq vd$.*

We get the following immediate consequences of the definitions of u-LD and v-UD.

Lemma 2. *A matrix in $SL_2(\mathbb{N}_0)$ is u-LD (v-UD) if and only if it is of the form $L_u M$ ($R_v M$) for some $M \in SL_2(\mathbb{N}_0)$.*

Proof. Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. We have that $L_u M = \begin{bmatrix} a & b \\ ua + c & ub + d \end{bmatrix}$. Clearly we have that $ua + c \geq ua$ and $ub + d \geq ub$, which give the needed inequalities. The remaining part of the proof is similar. $\qquad\qquad\square$

Lemma 3. *Suppose that $M \in SL_2(\mathbb{N}_0)$ and let $M' \in \mathcal{T}^{(u,v)}(M; n)$ for some $n > 0$. Then M' is either u-LD or v-UD.*

Proof. If $M' \in \mathcal{T}^{(u,v)}(M; n)$, then either $M' = L_u M''$ or $M' = R_v M''$ for some $M'' \in \mathcal{T}^{(u,v)}(M; n - 1)$. By Lemma 2, the result follows. $\qquad\quad\square$

At this time we consider two separate cases. In the first case we assume that $u \geq v \geq 2$ and in the second that $u \geq v = 1$. The proof of the first case is fairly straightforward and mimics many of the parts in the Bromberg, Shpilrain, and Vdovina proof [6]. The second case is more involved and requires a somewhat different approach.

Proposition 3. *Let $u \geq v \geq 2$. Suppose that $M, M' \in SL_2(\mathbb{N}_0)$, given by $M = \begin{bmatrix} a & * \\ c & * \end{bmatrix}$ and $M' = \begin{bmatrix} a' & * \\ c' & * \end{bmatrix}$, are such $M' \in \mathcal{T}^{(u,v)}(M, 2n + 1)$ and $a \geq c$. Then $\min\{a', c'\} \leq A_n$ and $\max\{a', c'\} \leq C_n$, where A_n and C_n are as defined in Proposition 2. Furthermore, when M' is v-UD, $a' \leq \frac{v}{u} C_n$.*

Proof. For $n = 0$, notice that $L_u M = \begin{bmatrix} a & * \\ ua + c & * \end{bmatrix}$ and $R_v M = \begin{bmatrix} a + vc & * \\ c & * \end{bmatrix}$ are the only two matrices in $\mathcal{T}^{(u,v)}(M; 1)$. Since $(v-1)c \leq (u-1)a$, the result holds in this case.

Suppose that the statement is true for all matrices of depth $2k + 1$, for some $k \geq 0$. Let $M' \in \mathcal{T}^{(u,v)}(M, 2k + 3)$. Then $M' \in \mathcal{T}^{(u,v)}(M'', 2)$ for some $M'' \in \mathcal{T}^{(u,v)}(M, 2k + 1)$ given by $M'' = \begin{bmatrix} a'' & * \\ c'' & * \end{bmatrix}$. It must be the case that

$$M' \in \{L_u^2 M'', L_u R_v M'', R_v L_u M'', R_v^2 M''\}.$$

In particular,

$$M' = \begin{cases} \begin{bmatrix} a'' & * \\ 2ua'' + c'' & * \end{bmatrix} & \text{if } M' = L_u^2 M'', \\[2ex] \begin{bmatrix} a'' + vc'' & * \\ ua'' + (1 + uv)c'' & * \end{bmatrix} & \text{if } M' = L_u R_v M'', \\[2ex] \begin{bmatrix} (1 + uv)a'' + vc'' & * \\ ua'' + c'' & * \end{bmatrix} & \text{if } M' = R_v L_u M'', \\[2ex] \begin{bmatrix} a'' + 2vc'' & * \\ c'' & * \end{bmatrix} & \text{if } M' = R_v^2 M''. \end{cases}$$

If M'' is u-LD, then $ua'' \leq c''$, so

$$\begin{aligned} 2ua'' + c'' = ua'' + ua'' + c'' \\ \leq ua'' + 2c'' \\ \leq ua'' + (1 + uv)c''. \end{aligned}$$

We have that

$$\begin{aligned} (1 + uv)a'' + vc'' = a'' + uva'' + vc'' \\ \leq a'' + 2vc''. \end{aligned}$$

Finally, it follows that $2v \leq 1 + uv$ since $u \geq 2$, so $a'' + 2vc'' \leq ua'' + (1 + uv)c''$. These inequalities show that $\max\{a', c'\} \leq ua'' + (1 + uv)c''$.

It is easy to see that $\min\{a', c'\}$ is at most either $a'' + vc''$ or $ua'' + c''$.

Since, by assumption, $a'' \leq A_k$ and $c'' \leq C_k$, it follows that

$$\begin{aligned} ua'' + (1 + uv)c'' \leq uA_k + (1 + uv)C_k \\ = C_{k+1}, \end{aligned}$$

$$a'' + vc'' \leq A_k + vC_k$$
$$= A_{k+1},$$

and

$$ua'' + c'' \leq 2c''$$
$$\leq A_k + vC_k$$
$$= A_{k+1},$$

since $v \geq 2$, as desired.

If M'' is v-UD, then one can show that $\max\{a', c'\} \leq (1 + uv)a'' + vc''$ using a very similar set of arguments as above. The needed inequalities follow from the fact that $vc'' \leq a''$ and $u \geq v \geq 2$ in this case. This completes the proof that $\min\{a', c'\} \leq A_n$ and $\max\{a', c'\} \leq C_n$.

For the remainder of the proof, we assume that M' is v-UD. If M'' is u-LD, then

$$u((1 + uv)a'' + vc'') = u(a'' + uva'' + vc'')$$
$$\leq u(a'' + 2vc'')$$
$$\leq ua'' + uv^2c''$$
$$\leq v(uA_k + (1 + uv)C_k)$$
$$= vC_{k+1}.$$

Similarly, M'' is v-UD, then

$$u(a'' + 2vc'') \leq u(2a'' + vc'')$$
$$\leq u((1 + uv)a'' + vc'')$$
$$\leq u\left((1 + uv)\frac{v}{u}C_k + vA_k\right)$$
$$= v(uA_k + (1 + uv)C_k)$$
$$= vC_{k+1}$$

where the third inequality follows by the induction hypothesis. Having exhausted all possibilities, we obtain that $a' \leq \frac{v}{u}C_n$.

$\square$

A careful reading of the proof above will show that the assumption that $u \geq v \geq 2$ was needed to ensure that the inequalities $2v \leq 1 + uv$ and $2u \leq 1 + uv$ both hold true. If $v = 1$, then the second inequality does not hold in general. We begin our alternate approach with a critical definition.

Definition 2. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ be polynomials over $\mathbb{N}_0$. If $\sum_{k \geq N} a_k \geq \sum_{k \geq N} b_k$ for every nonnegative integer N, then we say that $f(x) \succcurlyeq g(x)$. Here we assume that $a_i = 0$ for $i > n$ and $b_j = 0$ for $j > m$.

Note some properties of the above definition.

1. The relation is a partial order.

2. If $f(x) \succcurlyeq g(x)$, then $\deg(f) \geq \deg(g)$.

3. If $f_1(x) \succcurlyeq g_1(x)$ and $f_2(x) \succcurlyeq g_2(x)$, then $f_1(x) + f_2(x) \succcurlyeq g_1(x) + g_2(x)$.

4. If $f(x) \succcurlyeq g(x)$ and $g(x) \succcurlyeq h(x)$, then $f(x) \succcurlyeq h(x)$.

5. If $f(x) = g(x) + h(x)$ for some polynomial $h(x)$ over $\mathbb{N}_0$, then $f(x) \succcurlyeq g(x)$.

6. We have that $x^i f(x) \succcurlyeq x^j f(x)$ for $i \geq j \geq 0$. (This is due to a simple shift in the coefficients of the polynomial $f(x)$.)

7. If $a_i \geq b_i$ for each i then $\sum_{i=0}^n a_i x^i \succcurlyeq \sum_{i=0}^m b_i x^i$.

The importance of Definition 2 appears in the following lemma. It is a straightforward property that can be used to determine if one polynomial is greater than or equal to another when evaluated over positive integers.

Lemma 4. *If $f(x) \succcurlyeq g(x)$, then $f(r) \geq g(r)$ for every positive integer r.*

Proof. Suppose $f(x) = \sum_{i=0}^n a_i x^i$ and $g(x) = \sum_{i=0}^m b_i x^i$ where $a_n, b_m \neq 0$. By hypothesis, we must have $n \geq m$.

Suppose that b_{m_0} is such that $b_{m_0} > a_{m_0}$ and $b_i \leq a_i$ for all $i > m_0$. Let $\epsilon_i = a_i - b_i$ for $i > m_0$ and define a new polynomial $f_{m_0}(x) = \sum_{i=0}^n c_i x^i$ by

$$f_{m_0}(x) = \sum_{i=m_0+1}^n (a_i - \epsilon_i)x^i + \left(a_{m_0} + \sum_{i=m_0+1}^n \epsilon_i\right) x^{m_0} + \sum_{i=0}^{m_0} a_i x^i.$$

It follows that $f_{m_0}(x) \succcurlyeq g(x)$ and that $b_i \leq c_i$ for all $i \geq m_0$. Furthermore,

$$f(r) = \sum_{i=0}^n a_i r^i$$

$$= \sum_{i=m_0+1}^n (a_i - \epsilon_i + \epsilon_i)r^i + a_{m_0} r^{m_0} + \sum_{i=0}^{m_0} a_i r^i$$

$$\geq \sum_{i=m_0+1}^n (a_i - \epsilon_i)r^i + \left(a_{m_0} + \sum_{i=m_0+1}^n \epsilon_i\right) r^{m_0} + \sum_{i=0}^{m_0} a_i r^i$$

$$= f_{m_0}(r).$$

Iterating this procedure will generate a finite list of polynomials $f_{m_0}(x), f_{m_1}(x), \ldots,$ $f_{m_k}(x)$ with $f(r) \geq f_{m_0}(r) \geq \cdots \geq f_{m_k}(r)$ and $f_{m_k}(x) = \sum_{i=0}^n d_i x^i$ such that $d_i \geq b_i$ for all $1 \leq i \leq n$. Clearly $f_{m_k}(r) \geq g(r)$, which gives the desired result. $\square$

Note that the converse of Lemma 4 is not true. If $f(x) = x^3 + 1$ and $g(x) = x^2 + x$, then $f(r) \geq g(r)$ for every positive integer r, but it is **not** true that $f(x) \succcurlyeq g(x)$.

In order to apply Lemma 4 to our current case, we first show that the left column entries of matrices appearing in $\mathcal{T}^{(u,1)}(I_2)$ can all be expressed as polynomials evaluated at u. We also explicitly compute such polynomials for certain families of matrices, namely matrices of the form $(L_u R_1)^n L_u$ and $(R_1 L_u)^n L_u$.

Lemma 5. *Let $M' \in \mathcal{T}^{(u,1)}(M; n)$ be given by $M' = \begin{bmatrix} a' & * \\ c' & * \end{bmatrix}$. Then $a' = f(u)$ and $c' = g(u)$ where $f(x)$ and $g(x)$ are polynomials over $\mathbb{N}_0$ with $f(0) = 1$ and $g(0) = 0$.*

Proof. Clearly the statement is true for $n = 0$.

Suppose that the statement holds for all matrices of depth k for some $k \geq 0$. Let $M' \in \mathcal{T}^{(u,1)}(M; k+1)$. It follows that $M' = L_u M''$ or $M' = R_1 M''$ for some $M'' \in \mathcal{T}^{(u,1)}(M; k)$. By assumption, $M'' = \begin{bmatrix} f(u) & * \\ g(u) & * \end{bmatrix}$ for some polynomials $f(x)$ and $g(x)$ over $\mathbb{N}_0$. It follows that $L_u M'' = \begin{bmatrix} f(u) & * \\ uf(u) + g(u) & * \end{bmatrix}$ and $R_1 M'' = \begin{bmatrix} f(u) + g(u) & * \\ g(u) & * \end{bmatrix}$. In either case, it is obvious that the statement holds for M', which gives the result by induction. $\qquad\square$

Note that the polynomials in Lemma 5 depend on M, but not on the value of u.

We will make extensive use of the following result based on Pascal's rule that $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$ for $1 \leq k \leq n$.

Lemma 6. *We have that*

$$\sum_{i=0}^{a-1} \binom{b-i}{i} x^{a-i} + \sum_{i=0}^{a} \binom{b+1-i}{i} x^{a+1-i} = \sum_{i=0}^{a} \binom{b+2-i}{i} x^{a+1-i}.$$

Proof.

$$\sum_{i=0}^{a-1} \binom{b-i}{i} x^{a-i} + \sum_{i=0}^{a} \binom{b+1-i}{i} x^{a+1-i}$$

$$= \sum_{i=1}^{a} \binom{b+1-i}{i-1} x^{a+1-i} + \sum_{i=0}^{a} \binom{b+1-i}{i} x^{a+1-i}$$

$$= \sum_{i=1}^{a} \left[\binom{b+1-i}{i-1} + \binom{b+1-i}{i} \right] x^{a+1-i} + x^{a+1}$$

$$= \sum_{i=0}^{a} \binom{b+2-i}{i} x^{a+1-i}$$

$$\square$$

Lemma 6 contains an identity involving binomial coefficients that we apply multiple times with different parameters in Lemma 7, Lemma 8, Proposition 4, and Proposition 5. We elected to carefully document our use of the lemma and the partial ordering of polynomials for clarity. The reader may choose to skip to Proposition 6 after reading Lemma 7.

Lemma 7. *For any $n \geq 0$, let $F_n(x)$ and $G_n(x)$ be the polynomials over $\mathbb{N}_0$ such that $(L_u R_1)^n L_u = \begin{bmatrix} F_n(u) & * \\ G_n(u) & * \end{bmatrix}$. Then*

$$F_n(x) = \sum_{i=0}^{n} \binom{2n-i}{i} x^{n-i}$$

and

$$G_n(x) = \sum_{i=0}^{n} \binom{2n+1-i}{i} x^{n+1-i}.$$

Proof. Since $L_u = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$, it is clear that $F_0(x) = 1$ and $G_0(x) = x$, which satisfy the desired conclusion in the case $n = 0$. For $n \geq 0$, note that, by Proposition 2, $F_{n+1}(x) = F_n(x) + G_n(x)$ and $G_{n+1}(x) = xF_n(x) + (1+x)G_n(x) = xF_{n+1}(x) + G_n(x)$. In particular, if we assume that the conclusion holds for some $k \geq 0$, then by Lemma 6 we obtain that

$$\begin{aligned}
F_{k+1}(x) &= F_k(x) + G_k(x) \\
&= \sum_{i=0}^{k} \binom{2k-i}{i} x^{k-i} + \sum_{i=0}^{k} \binom{2k+1-i}{i} x^{k+1-i} \\
&= \sum_{i=0}^{k} \binom{2k+2-i}{i} x^{k+1-i} + 1 \\
&= \sum_{i=0}^{k+1} \binom{2k+2-i}{i} x^{k+1-i}.
\end{aligned}$$

Also,

$$\begin{aligned}
G_{k+1}(x) &= G_k(x) + xF_{k+1}(x) \\
&= \sum_{i=0}^{k} \binom{2k+1-i}{i} x^{k+1-i} + \sum_{i=0}^{k+1} \binom{2k+2-i}{i} x^{k+2-i} \\
&= \sum_{i=0}^{k+1} \binom{2k+3-i}{i} x^{k+2-i}.
\end{aligned}$$

The result follows by induction. $\square$

Note that $F_n(x^2) = \mathcal{F}_{2n-1}(x)$ where $\mathcal{F}_m(x)$ is the mth Fibonacci polynomial [3].

Lemma 8. *For any $n \geq 1$, let $H_n(x)$ and $I_n(x)$ be the polynomials over $\mathbb{N}_0$ such that $(R_1 L_u)^n L_u = \begin{bmatrix} H_n(u) & * \\ I_n(u) & * \end{bmatrix}$. Then*

$$H_n(x) = \sum_{i=0}^{n} \left(\binom{2n-i}{i} + \binom{2n-1-i}{i} \right) x^{n-i}$$

and

$$I_n(x) = \sum_{i=0}^{n-1} \left(\binom{2n-1-i}{i} + \binom{2n-2-i}{i} \right) x^{n-i}.$$

Proof. As in Lemma 7, the case $n = 1$ follows trivially. Note that $H_{n+1}(x) = (1+x)H_n(x) + I_n(x)$ and $I_{n+1}(x) = xH_n(x) + I_n(x)$. If we assume that the conclusion holds for some $k \geq 0$, then by Lemma 6 we get that

$$
\begin{aligned}
I_{k+1}(x) &= xH_k(x) + I_k(x) \\
&= \sum_{i=0}^{k} \binom{2k-i}{i} x^{k+1-i} + \sum_{i=0}^{k-1} \binom{2k-1-i}{i} x^{k-i} + \sum_{i=0}^{k} \binom{2k-1-i}{i} x^{k+1-i} \\
&\quad + \sum_{i=0}^{k-1} \binom{2k-2-i}{i} x^{k-i} \\
&= \sum_{i=0}^{k} \left(\binom{2k+1-i}{i} + \binom{2k-i}{i} \right) x^{k+1-i}
\end{aligned}
$$

and

$$
\begin{aligned}
H_{k+1}(x) &= H_k(x) + I_{k+1}(x) \\
&= \sum_{i=0}^{k} \left(\binom{2k-i}{i} x^{k-i} + \binom{2k+1-i}{i} x^{k+1-i} \right) \\
&\quad + \sum_{i=0}^{k} \left(\binom{2k-1-i}{i} x^{k-i} + \binom{2k-i}{i} x^{k+1-i} \right) \\
&= 1 + \sum_{i=0}^{k} \binom{2k+2-i}{i} x^{k+1-i} + \sum_{i=0}^{k} \binom{2k+1-i}{i} x^{k+1-i} \\
&= \sum_{i=0}^{k+1} \left(\binom{2k+2-i}{i} + \binom{2k+1-i}{i} \right) x^{k+1-i}.
\end{aligned}
$$

The result follows by induction. $\square$

The main difference between the cases $u \geq v \geq 2$ and (the current) $u \geq v = 1$ is expressed by Lemma 8 above. The failure of the inequality $2v \leq 1 + uv$ in the proof of Proposition 3 means that we must consider two sets of families of matrices as candidates for the maximal left column entry of odd depth. While a little more work is involved, we obtain the desired result with the propositions that follow.

Definition 3. *If $f(x)$ is a polynomial over $\mathbb{N}_0$, we let $[f]_n$ denote the coefficient of f associated with x^n. If $n > \deg(f)$, then $[f]_n = 0$.*

Proposition 4. *For any $n \geq 1$, we have that:*

(a) $I_n(x) \preccurlyeq H_n(x) \preccurlyeq G_n(x)$,

(b) $H_n(x) + I_n(x) \preccurlyeq F_n(x) + G_n(x)$.

Proof. Since, for any $n \geq 1$, $(R_1 L_u)^n L_u$ is v-UD, it follows that $I_n(x) \preccurlyeq H_n(x)$. Let $0 \leq k \leq n$. By Lemma 8 and Lemma 6 with $x = 1$,

$$\sum_{i \geq k} [H_n]_i = \sum_{i=0}^{n-k} \left(\binom{2n-i}{i} + \binom{2n-1-i}{i} \right) = \sum_{i=0}^{n-k} \binom{2n+1-i}{i} + \binom{n+k-1}{n-k}$$

and, by Lemma 7,

$$\sum_{i \geq k} [G_n]_i = \sum_{i=0}^{n-k+1} \binom{2n+1-i}{i} = \sum_{i=0}^{n-k} \binom{2n+1-i}{i} + \binom{n+k}{n-k+1}.$$

To complete the proof of (a), it is enough to show that $\binom{n+k-1}{n-k} \leq \binom{n+k}{n-k+1}$. Note that, for $k = 0$, we have that the desired inequality holds trivially. For $k \geq 1$, since $n - k + 1 \leq n + k$,

$$\binom{n+k-1}{n-k} \leq \binom{n+k-1}{n-k} \cdot \frac{n+k}{n-k+1} = \binom{n+k}{n-k+1},$$

as desired.

By Lemma 6 with $x = 1$ and Lemma 8,

$$\sum_{i \geq k} [H_n + I_n]_i = \sum_{i=0}^{n-k} \left(\binom{2n-i}{i} + \binom{2n-1-i}{i} + \binom{2n-1-i}{i} + \binom{2n-2-i}{i} \right)$$

$$= \sum_{i=0}^{n-k} \left(\binom{2n-i}{i} + \binom{2n+1-i}{i} \right) + \binom{n+k-2}{n-k} + \binom{n+k-1}{n-k}.$$

As in the proof of (a), it can be shown that $\binom{n+k-2}{n-k} \leq \binom{n+k-1}{n-k+1}$ for $0 \leq k \leq n$. This is enough to obtain (b) since, by Lemma 7,

$$\sum_{i \geq k}[F_n + G_n]_i = \sum_{i=0}^{n-k}\left(\binom{2n-i}{i} + \binom{2n+1-i}{i}\right) + \binom{n+k}{n-k+1}.$$

$\square$

Proposition 5. *For any $n \geq 1$, we have that:*

(a) $2xH_n(x) + I_n(x) \preccurlyeq G_{n+1}(x)$,

(b) $F_n(x) + 2G_n(x) \preccurlyeq H_{n+1}(x)$,

(c) $xF_n(x) + G_n(x) = I_{n+1}(x)$.

Proof. By Lemma 6 with $x = 1$, Lemma 7 and Lemma 8, for $0 \leq k \leq n$, we have that

$$\sum_{i \geq k}[2xH_n + I_n]_i = \sum_{i \geq k}[xH_n + I_{n+1}]_i$$

$$= \sum_{i=0}^{n-k}\left(\binom{2n-1-i}{i} + 2\binom{2n-i}{i} + \binom{2n+1-i}{i}\right)$$

$$= \sum_{i=0}^{n-k+1}\left(\binom{2n+1-i}{i} + \binom{2n+2-i}{i}\right)$$

$$\quad - \binom{n+k-1}{n-k+1} - \binom{n+k}{n-k+1}$$

$$= \sum_{i=0}^{n-k+2}\binom{2n+3-i}{i} - \binom{n+k-1}{n-k+1}$$

$$\quad - \binom{n+k}{n-k+1} - \binom{n+k}{n-k+2}$$

$$= \sum_{i=0}^{n-k+2}\binom{2n+3-i}{i} - \binom{n+k-1}{n-k+1} - \binom{n+k+1}{n-k+2}$$

$$\leq \sum_{i=0}^{n-k+2}\binom{2n+3-i}{i}$$

$$= \sum_{i \geq k}[G_{n+1}]_i,$$

proving (a).

By Lemma 6 with $x = 1$, Lemma 7 and Lemma 8, for $0 \leq k \leq n$, we have that

$$
\begin{aligned}
\sum_{i \geq k} [F_n + 2G_n]_i &= \sum_{i=0}^{n-k} \left(\binom{2n-i}{i} + 2\binom{2n+1-i}{i} \right) + 2\binom{n+k}{n-k+1} \\
&= \sum_{i=0}^{n-k} \left(\binom{2n+2-i}{i} + \binom{2n+1-i}{i} \right) + \binom{n+k}{n-k} \\
&\quad + 2\binom{n+k}{n-k+1} \\
&= \sum_{i=0}^{n-k} \left(\binom{2n+2-i}{i} + \binom{2n+1-i}{i} \right) + \binom{n+k+1}{n-k+1} \\
&\quad + \binom{n+k}{n-k+1} \\
&= \sum_{i=0}^{n-k+1} \left(\binom{2n+2-i}{i} + \binom{2n+1-i}{i} \right) \\
&= \sum_{i \geq k} [H_{n+1}]_i,
\end{aligned}
$$

which gives (b).

Part (c) follows quickly from Lemma 7 and Lemma 8:

$$
\begin{aligned}
xF_n(x) + G_n(x) &= \sum_{i=0}^{n} \binom{2n-i}{i} x^{n+1-i} + \sum_{i=0}^{n} \binom{2n+1-i}{i} x^{n+1-i} \\
&= \sum_{i=0}^{n} \left(\binom{2n+1-i}{i} + \binom{2n-i}{i} \right) x^{n+1-i} \\
&= I_{n+1}(x).
\end{aligned}
$$

$\square$

Proposition 6. *Suppose that $M \in \mathcal{T}^{(u,1)}(I_2, 2n+1)$ is given by $M = \begin{bmatrix} a & * \\ c & * \end{bmatrix}$. Then $\max\{a, c\} \leq C_n$ and $a' + c' \leq A_n + C_n$, where A_n and C_n are as defined in Proposition 2.*

Proof. By Lemma 5 we have that, for any n, $a = f(u)$ and $c = g(u)$ for some polynomials $f(x)$ and $g(x)$ over $\mathbb{N}_0$. By Lemma 4 and Proposition 4, to prove the proposition, it is enough to show that $f(x) \preccurlyeq F_n(x)$ and $g(x) \preccurlyeq G_n(x)$ if M is u-LD and $g(x) \preccurlyeq I_n(x)$ and $f(x) \preccurlyeq H_n(x)$ if M is 1-UD.

As in the proof of Proposition 3, the above claim is trivially true for $n = 0$.

Suppose that the statement is true for all matrices of depth $2k+1$, for some $k \geq 0$. Let $M \in \mathcal{T}^{(u,v)}(I_2, 2k+3)$. Then $M \in \mathcal{T}^{(u,v)}(M', 2)$ for some $M' \in \mathcal{T}^{(u,v)}(I_2, 2k+1)$ with $M' = \begin{bmatrix} \overline{f}(u) & * \\ \overline{g}(u) & * \end{bmatrix}$ for some polynomials $\overline{f}(x)$ and $\overline{g}(x)$ over $\mathbb{N}_0$. It follows that

$$M = \begin{cases} \begin{bmatrix} \overline{f}(u) & * \\ 2u\overline{f}(u) + \overline{g}(u) & * \end{bmatrix} & \text{if } M = L_u^2 M', \\[2ex] \begin{bmatrix} \overline{f}(u) + \overline{g}(u) & * \\ u\overline{f}(u) + (1+u)\overline{g}(u) & * \end{bmatrix} & \text{if } M = L_u R_1 M', \\[2ex] \begin{bmatrix} (1+u)\overline{f}(u) + \overline{g}(u) & * \\ u\overline{f}(u) + \overline{g}(u) & * \end{bmatrix} & \text{if } M = R_1 L_u M', \\[2ex] \begin{bmatrix} \overline{f}(u) + 2\overline{g}(u) & * \\ \overline{g}(u) & * \end{bmatrix} & \text{if } M = R_1^2 M'. \end{cases}$$

If M' is u-LD, then $\overline{g}(x) \succcurlyeq x\overline{f}(x)$. Furthermore, by assumption, it follows that

$$\begin{aligned} \overline{f}(x) &\preccurlyeq \overline{f}(x) + \overline{g}(x) \\ &\preccurlyeq F_k(x) + G_k(x) \\ &= F_{k+1}(x) \end{aligned}$$

and

$$\begin{aligned} 2x\overline{f}(x) + \overline{g}(x) &= x\overline{f}(x) + x\overline{f}(x) + \overline{g}(x) \\ &\preccurlyeq x\overline{f}(x) + \overline{g}(x) + \overline{g}(x) \\ &\preccurlyeq x\overline{f}(x) + (1+x)\overline{g}(x) \\ &\preccurlyeq xF_k(x) + (1+x)G_k(x) \\ &= G_{k+1}(x). \end{aligned}$$

This shows that our claim holds if M is u-LD in this case.

By assumption and Proposition 5 part (b) and (c), we have that

$$\begin{aligned} (1+x)\overline{f}(x) + \overline{g}(x) &\preccurlyeq \overline{f}(x) + 2\overline{g}(x) \\ &\preccurlyeq F_k(x) + 2G_k(x) \\ &\preccurlyeq H_{k+1}(x) \end{aligned}$$

and

$$\begin{aligned} \overline{g}(x) &\preccurlyeq x\overline{f}(x) + \overline{g}(x) \\ &\preccurlyeq xF_k(x) + G_k(x) \\ &= I_{k+1}(x). \end{aligned}$$

This shows that our claim also holds if M is 1-UD in this case.

If M' is 1-UD, then $\overline{f}(x) \succcurlyeq \overline{g}(x)$. Furthermore, by assumption, Proposition 4 parts (a) and (b), and Proposition 5 part (a), we have that

$$\begin{aligned}
\overline{f}(x) &\preccurlyeq \overline{f}(x) + \overline{g}(x) \\
&\preccurlyeq H_k(x) + I_k(x) \\
&\preccurlyeq F_k(x) + G_k(x) \\
&= F_{k+1}(x),
\end{aligned}$$

$$\begin{aligned}
2x\overline{f}(x) + \overline{g}(x) &\preccurlyeq 2xH_k(x) + I_k(x) \\
&\preccurlyeq G_{k+1}(x),
\end{aligned}$$

and

$$\begin{aligned}
x\overline{f}(x) + (1+x)\overline{g}(x) &\preccurlyeq xH_k(x) + (1+x)I_k(x) \\
&\preccurlyeq G_{k+1}(x).
\end{aligned}$$

This shows that our claim holds if M is u-LD in this case.

Finally,

$$\begin{aligned}
\overline{f}(x) + 2\overline{g}(x) &\preccurlyeq (1+x)\overline{f}(x) + \overline{g}(x) \\
&\preccurlyeq (1+x)H_k(x) + I_k(x) \\
&= H_{k+1}(x)
\end{aligned}$$

and

$$\begin{aligned}
\overline{g}(x) &\preccurlyeq x\overline{f}(x) + \overline{g}(x) \\
&\preccurlyeq xH_k(x) + I_k(x) \\
&= I_{k+1}(x).
\end{aligned}$$

This shows that our claim also holds if M is 1-UD in this case. $\qquad\square$

Proposition 3 and Proposition 6 show that, for $u \geq v$, the left column entries of any descendant of L_u of depth $2n + 1$ are bounded above by C_n. Furthermore, the propositions show that the upper bound is achieved by the $(2, 1)$ entry of $(L_u R_v)^n L_u$. To complete the proof of (1) we must show that:

(A) the right column entries of any descendant of L_u of depth $2n + 1$ and

(B) all entries of any descendant of R_v of depth $2n + 1$

are bounded above by C_n.

A proof by induction of (A) follows quickly by noticing that the right column entries of any descendant M of L_u (including L_u itself) are bounded above by the corresponding left column entries of M (see Figure 2). In fact, the same argument generalizes in the following way.

Lemma 9. *Let* $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. *If* M *is a vertex in* $\mathcal{L}^{(u,v)}$ (M *is a vertex in* $\mathcal{R}^{(u,v)}$), *then* $\mu(M) = \max\{a, c\}$ ($\mu(M) = \max\{b, d\}$).

In the case where $M = (R_v L_u)^n$ or $M = (L_u R_v)^n L_u$ for some $n \geq 0$, we can deduce Lemma 9 directly by noting the following relationship between the entries in the first column with the entries in the second column.

Proposition 7. *Let* $n \geq 0$. *If* $M = (R_v L_u)^n$, *then* $M = \begin{bmatrix} bu + d & b \\ \frac{bu}{v} & d \end{bmatrix}$ *for some integers* b *and* d. *If* $M = (L_u R_v)^n L_u$, *then* $M = \begin{bmatrix} d & b \\ \frac{u}{v}(b + vd) & d \end{bmatrix}$ *for some integers* b *and* d.

Proof. Suppose $M = (R_v L_u)^n$. The result is true for $n = 0$. Suppose that $n = k$ and $M = \begin{bmatrix} bu + d & b \\ \frac{bu}{v} & d \end{bmatrix}$. Then

$$
\begin{aligned}
(R_v L_u)^{k+1} &= R_v L_u M \\
&= \begin{bmatrix} 1 + uv & v \\ u & 1 \end{bmatrix} \begin{bmatrix} bu + d & b \\ \frac{bu}{v} & d \end{bmatrix} \\
&= \begin{bmatrix} (1 + uv)(bu + d) + bu & b(1 + uv) + vd \\ u(bu + d) + \frac{bu}{v} & bu + d \end{bmatrix}.
\end{aligned}
$$

It is easy to see that this matrix has the desired form, proving the first part of the proposition.

Suppose $M = (L_u R_v)^n L_u$. The result is true for $n = 0$, where $M = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$. Suppose that $n = k$ and $M = \begin{bmatrix} d & b \\ \frac{u}{v}(b + vd) & d \end{bmatrix}$, then

$$
\begin{aligned}
(L_u R_v)^{k+1} L_u &= L_u R_v M \\
&= \begin{bmatrix} 1 & v \\ u & 1 + uv \end{bmatrix} \begin{bmatrix} d & b \\ \frac{u}{v}(b + vd) & d \end{bmatrix} \\
&= \begin{bmatrix} d + u(b + vd) & b + vd \\ du + \frac{u}{v}(1 + uv)(b + vd) & bu + d(1 + uv) \end{bmatrix}.
\end{aligned}
$$

It is easy to see that this matrix has the desired form, proving the second part of the proposition. $\square$

Given Proposition 7 and Corollary 2 below, we can also show that $(L_u R_v)^n = \begin{bmatrix} d & b \\ \frac{bu}{v} & bu + d \end{bmatrix}$ and $(R_v L_u)^n R_v = \begin{bmatrix} d & b + vd \\ \frac{bu}{v} & d \end{bmatrix}$ for some integers b and d.

It remains to prove (B).

Proposition 8. *Let* $M \in \mathcal{T}^{(u,v)}(I_2; n)$. *Then*

(a) $M = \begin{bmatrix} f_1(uv) & f_2(uv) \\ f_3(uv) & f_4(uv) \end{bmatrix}$ *where* $f_i(X) \in \mathbb{N}_0[X]$ *and* $\deg(f_i) \leq n$ *for* $i = 1, 2, 3, 4.$

(b) *Futhermore,*

$$f_1(X) = \sum_i a_i X^{\alpha_i},$$

$$f_2(X) = v \sum_i b_i X^{\beta_i},$$

$$f_3(X) = u \sum_i c_i X^{\gamma_i}, \; and$$

$$f_4(X) = \sum_i d_i X^{\delta_i}.$$

Proof. (a) The statement is clearly true in the case where $M = I_2$.

Suppose that the statement holds for all matrices in $\mathcal{T}^{(u,v)}(I_2; k)$ for some $k \geq 0$. Let $M \in \mathcal{T}^{(u,v)}(I_2; k+1)$. Then $M \in \{L_u M', R_v M'\}$ for some $M' \in \mathcal{T}^{(u,v)}(I_2; k)$. In particular, by assumption, we have that

$$M' = \begin{bmatrix} f_1'(uv) & f_2'(uv) \\ f_3'(uv) & f_4'(uv) \end{bmatrix}$$

where $f_i'(X) \in \mathbb{N}_0[X]$ and $\deg(f_i') \leq k$ for $i = 1, 2, 3, 4$. It now follows that

$$M = \begin{cases} \begin{bmatrix} f_1'(uv) & f_2'(uv) \\ u f_1'(uv) + f_3'(uv) & u f_2'(uv) + f_4'(uv) \end{bmatrix} & \text{if } M = L_u M', \\[2em] \begin{bmatrix} f_1'(uv) + v f_3'(uv) & f_2'(uv) + v f_4'(uv) \\ f_3'(uv) & f_4'(uv) \end{bmatrix} & \text{if } M = R_v M'. \end{cases} \tag{3}$$

It is clear that, in either case, the statement holds for M and therefore the result follows by induction.

(b) The statement is clearly true in the case where $M = I_2$.

Suppose that the statement holds for all matrices in $\mathcal{T}^{(u,v)}(I_2; k)$ for some $k \geq 0$. Let $M \in \mathcal{T}^{(u,v)}(I_2; k+1)$. Then $M \in \{L_u M', R_v M'\}$ for some

$M' \in \mathcal{T}^{(u,v)}(I_2; k)$. Suppose $M = L_u M'$. By assumption, we have that

$$f_1'(X) = \sum_i a_i X^{\alpha_i},$$

$$f_2'(X) = v \sum_i b_i X^{\beta_i},$$

$$f_3'(X) = u \sum_i c_i X^{\gamma_i}, \text{ and}$$

$$f_4'(X) = \sum_i d_i X^{\delta_i}.$$

Using (3), it follows that

$$f_1(X) = f_1'(X)$$
$$= \sum_i a_i X^{\alpha_i},$$
$$f_2(X) = f_2'(X)$$
$$= v \sum_i b_i X^{\beta_i},$$
$$f_3(X) = u f_1'(X) + f_3'(X)$$
$$= u \sum_i a_i X^{\alpha_i} + u \sum_i c_i X^{\gamma_i}, \text{ and}$$

$$u f_2'(X) + f_4'(X) = uv \sum_i b_i X^{\beta_i} + \sum_i d_i X^{\delta_i}.$$

Note that since

$$u f_2'(uv) + f_4'(uv) = uv \sum_i b_i (uv)^{\beta_i} + \sum_i d_i (uv)^{\delta_i}$$
$$= \sum_i b_i (uv)^{\beta_i + 1} + \sum_i d_i (uv)^{\delta_i},$$

the statement holds with $f_4(X) = \sum_i b_i X^{\beta_i + 1} + \sum_i d_i X^{\delta_i}$.

A similar argument applies in the case when $M = R_v M'$.

Having exhausted all possibilities, the statement holds for M and therefore the result follows by induction.

$\square$

The following proposition serves two purposes. It addresses the case $v > u$ by showing that $\mu(\mathcal{T}^{(u,v)}(I_2; n)) = \mu(\mathcal{T}^{(v,u)}(I_2; n))$ and it is needed for the proof of (B).

Proposition 9. *Let* $n \geq 1$ *and* $i \in \{1, \ldots, 2^n\}$. *If* $c_{I_2}^{(u,v)}(n,i) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, *then*

$$c_{I_2}^{(v,u)}(n, 2^n + 1 - i) = \begin{bmatrix} d & c \\ b & a \end{bmatrix}.$$

Proof. We have that

$$c_{I_2}^{(u,v)}(1,1) = L_u = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}, \quad c_{I_2}^{(v,u)}(1,2) = R_u = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix},$$

$$c_{I_2}^{(u,v)}(1,2) = R_v = \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}, \quad c_{I_2}^{(v,u)}(1,1) = L_v = \begin{bmatrix} 1 & 0 \\ v & 1 \end{bmatrix}.$$

This shows that the result is true when $n = 1$. Suppose that it is also true for all matrices in the kth row. Take an odd i in $\{1, \ldots, 2^{k+1}\}$. Assume that $c_{I_2}^{(u,v)}(k, (i+1)/2) = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$. Then

$$\begin{aligned} c_{I_2}^{(u,v)}(k+1,i) &= L_u \cdot c_{I_2}^{(u,v)}(k, (i+1)/2) \\ &= \begin{bmatrix} a' & b' \\ ua' + c' & ub' + d' \end{bmatrix} \end{aligned}$$

and

$$\begin{aligned} c_{I_2}^{(v,u)}(k+1, 2^{k+1}+1-i) &= R_u \cdot c_{I_2}^{(v,u)}(k, (2^{k+1}+1-i)/2) \\ &= R_u \cdot \begin{bmatrix} d' & c' \\ b' & a' \end{bmatrix} \\ &= \begin{bmatrix} ub' + d' & ua' + c' \\ b' & a' \end{bmatrix}, \end{aligned}$$
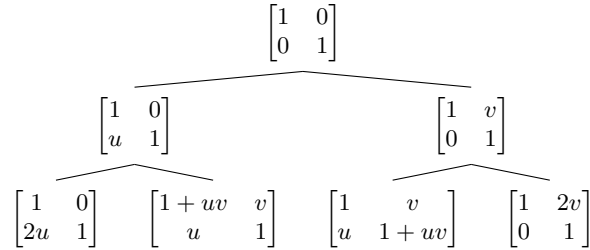
since $2^{k+1} + 1 - i$ is even and $(2^{k+1} + 1 - i)/2 = 2^k + 1 - (i+1)/2$. When i is even, the proof follows in a similar way. The result follows by induction. $\square$

Let M be a vertex in $\mathcal{R}^{(u,v)}$. By Proposition 9, there is a matrix M' that is a vertex in $\mathcal{L}^{(v,u)}$ whose entries and depth are the same as M. By Proposition 8 part (a), the entries of M' are polynomials in u and v. Interchanging uv, we immediately obtain a relationship between the entries of matrices in $\mathcal{L}^{(u,v)}$ and $\mathcal{R}^{(u,v)}$ of the same depth. Corollary 2 makes the above relationship precise (see Figure 4).
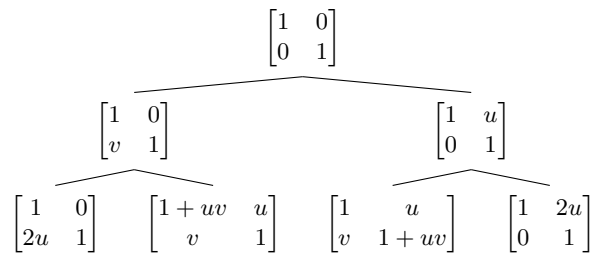
Corollary 2. *Let* $n \geq 1$ *and* $i \in \{1, \ldots, 2^n\}$. *If* $c_{I_2}^{(u,v)}(n,i) = \begin{bmatrix} f_1(uv) & f_2(uv) \\ f_3(uv) & f_4(uv) \end{bmatrix}$, *then* $c_{I_2}^{(u,v)}(n, 2^n + 1 - i) = \begin{bmatrix} f_4(uv) & \frac{v f_3(uv)}{u} \\ \frac{u f_2(uv)}{v} & f_1(uv) \end{bmatrix}$.

We are now in a position to prove (B).

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 2u & 1 \end{bmatrix} \quad \begin{bmatrix} 1+uv & v \\ u & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & v \\ u & 1+uv \end{bmatrix} \quad \begin{bmatrix} 1 & 2v \\ 0 & 1 \end{bmatrix}$$

(a) The first three rows of $\mathcal{T}^{(u,v)}(I_2)$.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ v & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 2u & 1 \end{bmatrix} \quad \begin{bmatrix} 1+uv & u \\ v & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & u \\ v & 1+uv \end{bmatrix} \quad \begin{bmatrix} 1 & 2u \\ 0 & 1 \end{bmatrix}$$

(b) The first three rows of $\mathcal{T}^{(v,u)}(I_2)$.

Figure 4: A side-by-side comparison of the first three rows of $\mathcal{T}^{(u,v)}(I_2)$ and $\mathcal{T}^{(v,u)}(I_2)$.

Proposition 10. *Let $M = c_{I_2}^{(u,v)}(n, i)$ for some $1 \le i \le 2^{n-1}$ and $M' = c_{I_2}^{(u,v)}(n, 2^n + 1 - i)$ with $u \ge v$. Then $\mu(M') \le \mu(M)$.*

Proof. We have that $M = \begin{bmatrix} f_1(uv) & f_2(uv) \\ f_3(uv) & f_4(uv) \end{bmatrix}$ where $f_i(X) \in \mathbb{N}_0[X]$ for $i = 1, 2, 3, 4$ satisfy the conclusion of Proposition 8. By Corollary 2, $M' = \begin{bmatrix} f_4(uv) & \frac{v f_3(uv)}{u} \\ \frac{u f_2(uv)}{v} & f_1(uv) \end{bmatrix}$.

By Lemma 9, $\mu(M) = \max\{f_1(uv), f_3(uv)\}$ and $\mu(M') = \max\{f_1(uv), \frac{v f_3(uv)}{u}\}$.

If M is u-LD, then M' is v-UD. In particular,

$$\begin{aligned}
\mu(M') &= \frac{v f_3(uv)}{u} \\
&= \frac{v}{u} \cdot u \sum_i c_i(uv)^{\gamma_i} \\
&\le u \sum_i c_i(uv)^{\gamma_i} \\
&= f_3(uv) \\
&= \mu(M).
\end{aligned}$$

If M is v-UD, then M' is u-LD. In particular,

$$\mu(M') = f_1(uv)$$
$$= \mu(M).$$

$\square$

Proof of Theorem 1. The proofs of (A) and (B) using Lemma 9 and Proposition 10, respectively, complete the proof of (1) for all u and v.

Applying Proposition 3 to the matrix $\overline{R}_v = R_v \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, we get that, for $n \geq 0$,

$$\mu(\mathcal{T}^{(u,v)}(R_v; 2n+1)) = \mu(\mathcal{T}^{u,v}(\overline{R}_v; 2n+1))$$
$$= \mu((L_u R_v)^n L_u \overline{R}_v)$$
$$= \mu((L_u R_v)^{n+1})$$

since right multiplication by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ simply exchanges the columns of a matrix. Note that, by Proposition 10, $\mu((R_v L_u)^{n+1}) = \mu((L_u R_v)^{n+1})$.

Suppose that there exists an $M \in \mathcal{T}^{(u,v)}(I_2; 2n+2)$ with $\mu(M) > \mu((R_v L_u)^{n+1})$. Proposition 10 shows that we can assume that M is a vertex in $\mathcal{L}^{(u,v)}$, so there is an i such that $1 \leq i \leq 2^{2n+1}$ and $M = c_{I_2}^{(u,v)}(2n+2, i)$. Let $M' = c_{I_2}^{(u,v)}(2n+2, 2^{2n+2} + 1 - i)$. (Note that M' is a vertex in $\mathcal{R}^{(u,v)}$.) By Corollary 2 and Proposition 10, we obtain a contradiction if M is v-UD. Assuming that M is u-LD, $M = \begin{bmatrix} a & * \\ ua + c & * \end{bmatrix}$ where $\begin{bmatrix} a & * \\ c & * \end{bmatrix}$, the parent of M, is some matrix satisfying the result of Proposition 3. That is, either $a \leq A_n$ and $c \leq C_n$ (with $ua \leq c$) or $a \leq \frac{v}{u} C_n$ and $c \leq A_n$. In either case it follows that

$$\mu(M) = ua + c$$
$$\leq A_n + vC_n$$
$$= \mu((R_v L_u)^{n+1}),$$

a clear contradiction. Therefore, no such M exists, completing the proof of (2) when $u \geq v > 1$.

For $u \geq v = 1$, (2) follows from Proposition 6 and Proposition 4 part (c) since, for $n \geq 0$,

$$\mu(\mathcal{T}^{(u,1)}(I_2; 2n+2)) \leq uF_n(u) + G_n(u)$$
$$= \mu(L_u (L_u R_1)^n L_u).$$

Finally, (2) follows for $v > u$ using a similar argument to (A) and (B). $\square$

References

[1] B. Bates, M. Bunder, and K. Tognetti, Locating terms in the Stern-Brocot tree, *European J. Combin.* **31** (2010), no. 7, 1020-1033.

[2] B. Bates, M. Bunder, and K. Tognetti, Linking the Calkin-Wilf and Stern-Brocot trees, *European J. Combin.* **31** (2010), no. 7, 1637-1661.

[3] A.T. Benjamin and J.J. Quinn, *Proofs that Really Count: The Art of Combinatorial Proof*, The Dolciani Mathematical Expositions, **27**. Mathematical Association of America, Washington, DC, 2003. xiv+194 pp.

[4] J. Bourgain and A. Gamburd, Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$, *Ann. of Math. (2)* **167** (2008), no. 2, 625-642.

[5] L. Bromberg, *Some applications of noncommutative groups and semigroups to information security*, Thesis (Ph.D.), City University of New York, 2015. 77 pp.

[6] L. Bromberg, V. Shpilrain, and A. Vdovina, Navigating in the Cayley graph of $SL_2(\mathbb{F}_p)$ and applications to hashing, *Semigroup Forum* **94** (2017), no.2, 314-324.

[7] N. Calkin and H.S. Wilf, Recounting the rationals, *Amer. Math. Monthly* **107** (2000), no. 4, 360-363.

[8] S. Han, A.M. Masuda, S. Singh, and J. Thiel, Orphans in forests of linear fractional transformations, *Electron. J. Combin.* **23** (2016), no. 3, Paper 3.6, 24pp.

[9] S. Han, A.M. Masuda, S. Singh, and J. Thiel, The (u,v)-Calkin-Wilf forest, *Int. J. Number Theory* **12** (2016), no. 5, 1311-1328.

[10] H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math. (2)* **167** (2008), no. 2, 601-623.

[11] H.A. Helfgott, Growth in groups: ideas and perspectives, *Bull. Amer. Math. Soc. (N.S.)* **52** (2015), no. 3, 357-413.

[12] E. Lucas, Sur les suites de Farey, *Bull. Soc. Math. France* **6** (1878), 118-119.

[13] M.B. Nathanson, Pairs of matrices in $GL_2(\mathbb{R}_{\geq 0})$ that freely generate, *Amer. Math. Monthly* **122** (2015), no. 8, 790-792.

[14] M.B. Nathanson, A forest of linear fractional transformations, *Int. J. Number Theory* **11** (2015), no. 4, 1275-1299.

[15] R. Paulin, Largest values of the Stern sequence, alternating binary expansions and continuants, *J. Integer Seq.* **20** (2017), Article 17.2.8.

[16] G. Zémor, Hash functions and graphs with large girths, EUROCRYPT 91, Lecture Notes Comp. Sci. **547** (1991), 508-511.
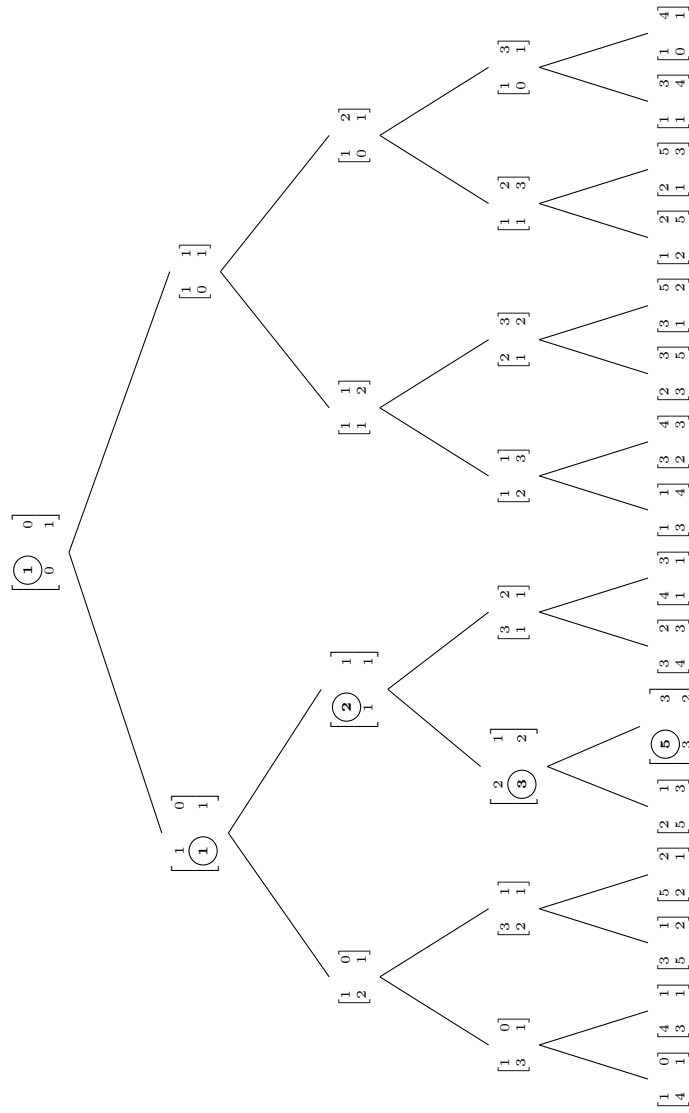
Appendix - Examples of PLFT (u, v)-Calkin-Wilf Trees

Figure 5: The first five rows of the $\mathcal{T}^{(1,1)}(I_2)$ tree.

Figure 6: The first five rows of the $\mathcal{T}^{(5,2)}(I_2)$ tree.

Figure 7: The first five rows of the $\mathcal{T}^{(2,5)}(I_2)$ tree.

Figure 8: The first five rows of the $\mathcal{T}^{(5,1)}(I_2)$ tree.