MAXIMAL ENTRIES OF ELEMENTS IN CERTAIN MATRIX MONOIDS

SANDIE HAN, ARIANE M. MASUDA, SATYANAND SINGH, AND JOHANN THIEL

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 determined the depth \( n \) matrices containing the maximal entry for each \( n \geq 1 \). By using ideas from our previous work on \((u, v)\)-Calkin-Wilf trees, 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 hashing functions based on \( L_u \) and \( R_v \).

1. Introduction

For fixed integers \( u, v \geq 1 \), let \( L_u := \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix} \) and \( R_v := \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix} \). The monoid generated by \( L_u \) and \( R_v \) is free. That is, every 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 1 of \( M \). For example, if \( M = L_u^3 R_v^2 L_u^2 \), then the depth of \( M \) is 34.

In [2, 3], Bromberg and Bromberg et al. determine the depth \( n \) matrix containing the largest entry in the case where \( u = v = 2 \) and \( u = v = 3 \) for each \( n \geq 1 \). The proof is by induction. They show that if \( M \) is the depth \( n \) matrix containing the largest entry, then either \( L_u M \) or \( R_v M \), depending on the parity of \( n \), must be the depth \( n + 1 \) matrix containing the largest entry.

The focus of this paper is to answer some open questions appearing in [2, 3] by expanding the above result to the general case \( u, v \geq 1 \). In the case where \( u, v \geq 2 \), our method uses a similar induction argument as above. In the case where either \( u = 1 \) or \( v = 1 \), the situation is more complicated, requiring a modified approach.

To reduce some of our calculations and to better organize and present our work, we use a generalization of the Calkin-Wilf tree [4] for positive linear fractional transformations (PLFTs) due to Nathanson [10]. In particular, we will use the matrix version 2 of this tree (see [4] for a more thorough history of this material).

We construct an infinite binary tree where every vertex is labeled by a matrix in \( GL_2(\mathbb{N}_0) \) according to the following 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 $\begin{bmatrix} a + vc & b + vd \\ c & d \end{bmatrix}$.

Such a tree is referred to as a PLFT $(u, v)$-Calkin-Wilf tree and is denoted by $T^{(u,v)}(M)$ (see Figure 1). We denote by $T^{(u,v)}(M; n)$ the (finite) set of matrices of depth $n$ in $T^{(u,v)}(M)$ where $n \geq 0$.

\[
I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

\[
R_v = \begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix}
\]

\[
L_u = \begin{bmatrix} 1 & 0 \\ 2u & 1 \end{bmatrix}
\]

\[
R_vL_u = \begin{bmatrix} 1 + uv & v \\ u & 1 \end{bmatrix}
\]

\[
L_uR_v = \begin{bmatrix} 1 & v \\ u & 1 + uv \end{bmatrix}
\]

\[
R_vL_u = \begin{bmatrix} 1 & v \\ u & 1 + uv \end{bmatrix}
\]

\[
L_u = \begin{bmatrix} 1 & 0 \\ 2u & 1 \end{bmatrix}
\]

Figure 1. The first three rows of the tree $T^{(u,v)}(I_2)$.

It is easy to see that the PLFT $(u, v)$-Calkin-Wilf tree organizes the elements in the monoid generated by $L_u$ and $R_v$ by depth. In fact, this organization is highly symmetric, a property which will be used later.

The remainder of this paper is divided into three sections. Section 2 contains our main result. Section 3 is a lengthy section devoted to proving the main result. The proof involves a careful analysis of various cases using different techniques. Finally, in Section 4, we show how our result solves a question regarding the collision resistance of some hashing functions based on $L_u$ and $R_v$ [2, 3].

2. Main theorem

We begin by setting some notation so that we may state the main theorem.

**Notation 1.** We define $\mu : GL_2(\mathbb{N}_0) \to \mathbb{N}$ by $\mu \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \max\{a, b, c, d\}$. For a finite subset $S$ of $GL_2(\mathbb{N}_0)$, we extend the definition of $\mu$ to $S$ by $\mu(S) = \max\{\mu(M) : M \in S\}$.

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

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

and

(2) $\mu(T^{(u,v)}(I_2; 2n + 2)) = \begin{cases} \frac{\pm s_{u, v} \sqrt{t_{u, v}} \left( p_{u, v}^+(q_{u, v}^-)^{n+1} + p_{u, v}^-(q_{u, v}^+)^{n+1} \right)}{2^{n+2} \sqrt{s_{u, v}(4 + uv)}} & \text{if } s_{u, v} > 1, \\
\frac{\pm s_{u, v} \sqrt{t_{u, v}}(q_{u, v}^+)^{n+1} + (q_{u, v}^-)^{n+1}}{2^{n+2} \sqrt{(4 + uv)}} & \text{otherwise.} \end{cases}$
Furthermore, the value given by (1) is attained by the (2,1) entry of the matrix $(L_uR_v)^nL_u$ when $u \geq v$ and by the (1,2) entry of the matrix $(R_vL_u)^nR_v$ when $v \geq u$. Similarly, the value given by (2) is attained by the (1,1) entry of the matrix $(R_vL_u)^n$ when $u \geq v > 1$, by the (1,1) entry of the matrix $L_u(L_uR_v)^{n-1}L_u$ when $u \geq v = 1$, by the (2,2) entry of the matrix $(L_uR_v)^n$ when $v \geq u > 1$, and by the (2,2) entry of the matrix $R_v(R_vL_u)^{n-1}R_v$ when $v \geq u = 1$.

This result is similar to a theorem on the largest values of the Stern sequence by Lucas and expanded upon by Paulin [8, 11].

In the proof of Theorem 1 we first show (1) is true when $u \geq v$ for $v \geq 2$ and then for $v = 1$ using a different method. We then use the symmetrical nature of the PLFT $(u,v)$-Calkin-Wilf tree in two ways: to extend (1) to the case where $v > u$ and to show that (2) holds (see Table 1 and Table 2 for examples of Theorem 1).

We define a sequence $F_n^{(u,v)}$ recursively by $F_0^{(u,v)} = 0$, $F_1^{(u,v)} = 1$, and for $n > 1$

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

Note that $F_n^{(1,1)} = F_n$ where $F_n$ is the $n^{\text{th}}$ Fibonacci number. Theorem 1 shows that $F_n^{(u,v)} = \mu(T(u,v)(I_2; n))$ when $u, v > 1$ or $u = v = 1$. Furthermore, when $u = v$, $F_n^{(u,u)}$ is a Lucas sequence.

| $v$ | 1 | 2 | 3 |
|-----|---|---|---|
| 1   | $\frac{(3+\sqrt{5})^{n+1}-(3-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$ | $\frac{(2+\sqrt{3})^{n+1}-(2-\sqrt{3})^{n+1}}{\sqrt{3}}$ | $\frac{3((5+\sqrt{21})^{n+1}-(5-\sqrt{21})^{n+1})}{2^{n+1}\sqrt{21}}$ |
| 2   | $\frac{(2+\sqrt{3})^{n+1}-(3-\sqrt{3})^{n+1}}{\sqrt{2}}$ | $\frac{(3+2\sqrt{2})^{n+1}-(3-2\sqrt{2})^{n+1}}{2\sqrt{2}}$ | $\frac{3((4+\sqrt{15})^{n+1}-(4-\sqrt{15})^{n+1})}{2\sqrt{15}}$ |
| 3   | $\frac{3(5+\sqrt{21})^{n+1}-(5-\sqrt{21})^{n+1}}{2^{n+1}\sqrt{21}}$ | $\frac{3(4+\sqrt{15})^{n+1}-(4-\sqrt{15})^{n+1}}{2\sqrt{15}}$ | $\frac{(1+3\sqrt{13})^{n+1}-(1-3\sqrt{13})^{n+1}}{2^{n+1}\sqrt{13}}$ |

**Table 1.** The value of $\mu(T(u,v)(I_2; n))$ for various choices of $u$ and $v$.

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

**Table 2.** The value of $\mu(T(u,v)(I_2; n+2))$ for various choices of $u$ and $v$.

---

3 We omit larger values of $u$ and $v$ in Table 2 case due to space considerations.
3. Proof of the Main Theorem

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

In Theorem 1, the claim is that, when $u \geq v$, $(L_u R_v)^n L_u$ has the largest 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 $p_{u,v}^+ = \pm v\sqrt{u} + \sqrt{v(4 + uv)}$ and $q_{u,v}^+ = 2 + uv \pm \sqrt{uv(4 + uv)}$.

**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 $\vec{v}_1 = \begin{bmatrix} \frac{\sqrt{v(4+uv)} - v\sqrt{u}}{2v\sqrt{u}} \\ 1 \end{bmatrix}$ and $\vec{v}_2 = \begin{bmatrix} \frac{-\sqrt{v(4+uv)} - v\sqrt{u}}{2v\sqrt{u}} \\ 1 \end{bmatrix}$, 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
\[
\begin{bmatrix}
\alpha_n \\
\gamma_n
\end{bmatrix} = \begin{bmatrix}
1 & v \\
u & 1 + uv
\end{bmatrix}^n \begin{bmatrix}
\alpha_0 \\
\gamma_0
\end{bmatrix}
\]
\[
= \begin{bmatrix}
1 & v \\
u & 1 + uv
\end{bmatrix}^n (c_1\tilde{v}_1 + c_2\tilde{v}_2)
\]
\[
= c_1\lambda_1^n\tilde{v}_1 + c_2\lambda_2^n\tilde{v}_2.
\]
So \(\gamma_n = c_1\lambda_1^n + c_2\lambda_2^n\), which gives the desired result after the appropriate substitutions. \(\square\)

**Proposition 1.** 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
\[
(L_uR_v)^n L_u M = \begin{bmatrix}A_n & * \\ C_n & * \end{bmatrix}.
\]
Then \(A_n = \alpha_n\) and \(C_n = \gamma_n\) where \(\alpha_n\) and \(\gamma_n\) are as defined in Lemma 1.

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

Note that a result similar to Proposition 1 could easily be found for the right column of \((L_uR_v)^n L_u M\). 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 1 applied to \(I_2\), we can compute the entries in the left column of a specific family of matrices, namely matrices of the form \((L_uR_v)^n L_u\). 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 \((v\text{-}UD)\) 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. \(\square\)

**Lemma 3.** Suppose that \(M \in SL_2(\mathbb{N}_0)\) and let \(M' \in T^{(u,v)}(M; n)\) for some \(n > 0\). Then \(M'\) is either \(u\)-LD or \(v\)-UD.
Proof. If \( M' \in T^{(u,v)}(M;n) \), then either \( M' = L_u M'' \) or \( M' = R_v M'' \) for some \( M'' \in T^{(u,v)}(M;n-1) \). By Lemma 2, the result follows.

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 \( u \geq 1 \). The proof of the first case is fairly straightforward and mimics many of the parts in the Bromberg et al. proof \[3\] in the case \( u = v \geq 2 \). The second case is more involved and requires a somewhat different approach.

**Proposition 2.** 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 \( M' \in T^{(u,v)}(M;2n+1) \) and \( a \geq c \). 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 7.

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 \( T^{(u,v)}(M;1) \). 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 \( M' \in T^{(u,v)}(M;2k+3) \). Then \( M' \in T^{(u,v)}(M'',2) \) for some \( M'' \in T^{(u,v)}(M,2k+1) \) 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,

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

and

\[
a' + c' = \begin{cases} 
(1 + 2u)a'' + c'' & \text{if } M' = L_u^2 M'', \\
(1 + u)a'' + (1 + uv + v)c'' & \text{if } M' = L_u R_v M'', \\
(1 + uv + u)a'' + (1 + v)c'' & \text{if } M' = R_v L_u M'', \\
a'' + (1 + 2v)c'' & \text{if } M' = R_v^2 M''.
\end{cases}
\]

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

\[
2ua'' + c'' = ua'' + ua'' + c'' 
\leq ua'' + 2c''
\]
\[ \leq ua'' + (1 + uv)c''. \]

We have that
\[ (1 + uv)a'' + vc'' = a'' + uva'' + vc'' \leq a'' + 2vc''. \]

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

Using similar arguments as above, we also have that
\[ (1 + 2u)a'' + c'' = (1 + u)a'' + ua'' + c'' \leq (1 + u)a'' + 2c'' \leq (1 + u)a'' + (1 + uv + v)c'', \]

as well as
\[ (1 + uv + u)a'' + (1 + v)c'' = (1 + u)a'' + uva'' + (1 + v)c'' \leq (1 + u)a'' + (1 + 2v)c'' \leq (1 + u)a'' + (1 + uv + v)c''. \]

So \( a' + c' \leq (1 + u)a'' + (1 + uv + v)c'' \).

Since, by assumption, \( c'' \leq C_k \) and \( a'' + c'' \leq A_k + C_k \), it follows that
\[ \begin{align*}
ua'' + (1 + uv)c'' &= u(a'' + c'') + (1 + u(v - 1))c'' \\
&\leq u(A_k + C_k) + (1 + u(v - 1))C_k \\
&= uA_k + (1 + uv)C_k \\
&= C_{k+1}
\end{align*} \]

and
\[ \begin{align*}
(1 + u)a'' + (1 + uv + v)c'' &= (1 + u)(a'' + c'') + (u(v - 1) + v)c'' \\
&\leq (1 + u)(A_k + C_k) + (u(v - 1) + v)C_k \\
&= (1 + u)A_k + (1 + uv + v)C_k \\
&= A_{k+1} + C_{k+1},
\end{align*} \]

as desired. If \( M'' \) is \( v \)-UD, then one can show that \( c' < a' \leq (1 + uv)a'' + vc'' \) and \( a' + c' \leq (1 + uv + u)a'' + (1 + v)c'' \) using a very similar set of arguments as above. The needed inequalities follow from the fact that \( c'' \leq a'' \) and \( v \leq u \) in this case. \( \square \)

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 \( \sum_{k \geq N} b_k \geq \sum_{k \geq N} a_k \) for every nonnegative integer \( N \), then we say that \( f(x) \succ g(x) \). 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 \( \succeq \) is a partial order.
(2) If \( f(x) \succeq g(x) \), then \( \deg(f) \geq \deg(g) \).
(3) If \( f_1(x) \succeq g_1(x) \) and \( f_2(x) \succeq g_2(x) \), then \( f_1(x) + f_2(x) \succeq g_1(x) + g_2(x) \).
(4) If \( f(x) \succeq g(x) \) and \( g(x) \succeq h(x) \), then \( f(x) \succeq h(x) \).
(5) If \( f(x) = g(x) + h(x) \) for some polynomial \( h(x) \) over \( \mathbb{N}_0 \), then \( f(x) \succeq g(x) \).
(6) We have that \( x^i f(x) \succeq x^j f(x) \) 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 \( \sum_{i=0}^{n} a_i x^i \succeq \sum_{i=0}^{m} b_i x^i \).

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 \( f(x) \succeq g(x) \), 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 \( f_{m_0}(x) = \sum_{i=0}^{m_0} c_i x^i \) 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 \( f_{m_0}(x) \succeq g(x) \) and that \( b_i \leq c_i \) for all \( i \geq m_0 \). Furthermore,

\[
f(r) = \sum_{i=0}^{n} a_i r^i \\
= \sum_{i=m_0+1}^{n} (a_i - \epsilon_i) r^i + a_{m_0} r^{m_0} + \sum_{i=0}^{m_0} a_i r^i \\
\geq \sum_{i=m_0+1}^{n} (a_i - \epsilon_i) r^i + \left( a_{m_0} + \sum_{i=m_0+1}^{n} \epsilon_i \right) r^{m_0} + \sum_{i=0}^{m_0} a_i r^i \\
= f_{m_0}(r).
\]

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 \( f(x) \succeq g(x) \).

In order to apply Lemma 4 to our current case, we first show that the left column entries of matrices appearing in \( T^{(u,1)}/I_2 \) 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 $M' \in T^{(u,1)}(M;n)$ 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 $M' \in T^{(u,1)}(M;k+1)$. It follows that $M' = L_1M''$ or $M' = R_1M''$ for some $M'' \in T^{(u,1)}(M;k)$.

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 $L_1M'' = \begin{bmatrix} uf(u) & * \\ uf(u) + g(u) & * \end{bmatrix}$ and $R_1M'' = \begin{bmatrix} f(u) + g(u) & * \\ g(u) & * \end{bmatrix}$. In either case, it is obvious that the statement holds for $M'$, which gives the result by induction. \qed

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. 

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

\qed

Lemma 7. For any $n \geq 0$, let $F_n(x)$ and $G_n(x)$ be the polynomials over $\mathbb{N}_0$ such that $(L_1R_1)^n L_u = \begin{bmatrix} F_n(u) & * \\ G_n(u) & * \end{bmatrix}$. 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 1, $F_{n+1}(x) = F_n(x) + G_n(x)$ 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

$$F_{k+1}(x) = F_k(x) + G_k(x)$$

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

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

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

Also,

$$G_{k+1}(x) = G_k(x) + xF_{k+1}(x)$$

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

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

The result follows by induction. □

Note that $F_n(x^2) = F_{2n-1}(x)$ where $F_n(x)$ is the $n$th Fibonacci polynomial [1].

**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

$I_{k+1}(x) = xH_k(x) + I_k(x)$
Lemma 8 above. The failure of the inequality (2) means that we must consider two sets of families of matrices as candidates for the largest left column entry of $H_k$. To complete the proof of (a), it is enough to show that

$$H_{k+1}(x) = H_k(x) + I_{k+1}(x)$$

and

$$H_{k+1}(x) = H_k(x) + I_{k+1}(x)$$

The result follows by induction. □

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 2 means that we must consider two sets of families of matrices as candidates for the largest 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 $\lfloor f \rfloor_n$ denote the coefficient of $x^i$ associated with $x^n$. If $\deg(f) > n$, then $\lfloor f \rfloor_n = 0$.

**Proposition 3.** For any $n \geq 1$, we have that:

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

(b) $H_n(x) + I_n(x) \subseteq F_u(x) + G_n(x)$.

*Proof.* Since, for any $n \geq 1$, $(R_1L_u)^nL_u$ is $v$-UD, it follows that $I_n(x) \subseteq H_n(x)$. 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,

$$\sum_{i \geq k} [G_n]_i = \sum_{i = 0}^{n-k+1} \binom{2n+1-i}{i} = \sum_{i = 0}^{n-k} \binom{2n+1-i}{i} + \binom{n+k}{n-k+1}.$$
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 4.** For any $n \geq 1$, we have that:

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

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

(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

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

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

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

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

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

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

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

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

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

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

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

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

which gives (b).

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

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

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

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

\[ \square \]

**Proposition 5.** Suppose that $M \in T^{(u,1)}(I_2, 2n+1)$ 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 1.

**Proof.** By Lemma 3 we have that, for any $n$, $a = f(u)$ and $c = g(u)$ for some polynomials $f(x)$ and $g(x)$ over $N_0$. By Lemma 4 and Proposition 3 to prove the proposition, it is enough to show that $f(x) \preceq F_n(x)$ and $g(x) \preceq G_n(x)$ if $M$ is $u$-LD and $g(x) \preceq I_n(x)$ and $f(x) \preceq H_n(x)$ if $M$ is 1-UD.

As in the proof of Proposition 2, 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 $M \in T^{(u,v)}(I_2, 2k+3)$. Then $M \in T^{(u,v)}(M', 2)$ for some $M' \in T^{(u,v)}(I_2, 2k+1)$ with $M' = \begin{bmatrix} f(u) & * \\ g(u) & * \end{bmatrix}$.
for some polynomials \( \overline{f}(x) \) and \( \overline{g}(x) \) over \( \mathbb{N}_0 \). It follows that

\[
M = \left\{ \begin{array}{ll}
\begin{bmatrix}
\overline{f}(u) \\
2u \overline{f}(u) + \overline{g}(u)
\end{bmatrix} & \text{if } M = L_u^2 M', \\
\begin{bmatrix}
\overline{f}(u) + \overline{g}(u) \\
u \overline{f}(u) + (1 + u) \overline{g}(u)
\end{bmatrix} & \text{if } M = L_u R_1 M', \\
\begin{bmatrix}
(1 + u) \overline{f}(u) + \overline{g}(u) \\
u \overline{f}(u) + \overline{g}(u)
\end{bmatrix} & \text{if } M = R_1 L_u M', \\
\begin{bmatrix}
\overline{f}(u) + 2 \overline{g}(u) \\
\overline{g}(u)
\end{bmatrix} & \text{if } M = R_1^2 M'.
\end{array} \right.
\]

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

\[
\overline{f}(x) \preceq \overline{f}(x) + \overline{g}(x) \\
\preceq F_k(x) + G_k(x) \\
= F_{k+1}(x)
\]

and

\[
2x \overline{f}(x) + \overline{g}(x) = x \overline{f}(x) + x \overline{f}(x) + \overline{g}(x) \\
\preceq x \overline{f}(x) + \overline{g}(x) + \overline{g}(x) \\
\preceq x \overline{f}(x) + (1 + x) \overline{g}(x) \\
\preceq x F_k(x) + (1 + x) G_k(x) \\
= G_{k+1}(x).
\]

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

By assumption and Proposition 4 part (b) and (c), we have that

\[
(1 + x) \overline{f}(x) + \overline{g}(x) \preceq \overline{f}(x) + 2 \overline{g}(x) \\
\preceq F_k(x) + 2 G_k(x) \\
\preceq H_{k+1}(x)
\]

and

\[
\overline{g}(x) \preceq x \overline{f}(x) + \overline{g}(x) \\
\preceq x F_k(x) + G_k(x) \\
= I_{k+1}(x).
\]

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

If \( M' \) is 1-UD, then \( \overline{f}(x) \preceq \overline{g}(x) \). Furthermore, by assumption, Proposition 3 parts (a) and (b), and Proposition 4 part (a), we have that

\[
\overline{f}(x) \preceq \overline{f}(x) + \overline{g}(x) \\
\preceq H_k(x) + I_k(x)
\]
\[ F_k(x) + G_k(x) = F_{k+1}(x), \]

\[ 2x\overline{f}(x) + \overline{g}(x) \leq 2xH_k(x) + I_k(x) \leq G_{k+1}(x), \]

and

\[ x\overline{f}(x) + (1 + x)f(x) + (1 + x)g(x) \leq xH_k(x) + (1 + x)I_k(x) \leq G_{k+1}(x). \]

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

Finally,

\[ \overline{f}(x) + 2\overline{g}(x) \leq (1 + x)f(x) + (1 + x)g(x) \leq (1 + x)H_k(x) + I_k(x) = H_{k+1}(x), \]

and

\[ \overline{g}(x) \leq x\overline{f}(x) + \overline{g}(x) \leq xH_k(x) + I_k(x) = I_{k+1}(x). \]

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

Proposition 2 and Proposition 5 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 \((L_uR_v)^nL_u\). 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 1). In fact, the same argument generalizes in the following way.

Lemma 9. Let \( \mathcal{L}(u,v) \) and \( \mathcal{R}(u,v) \) be the collections of all matrices that are descendants of \( L_u \) and \( R_v \) in \( \mathcal{T}(u,v) \), respectively, and \( M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \). If \( M \in \mathcal{L}(u,v) \) \((M \in \mathcal{R}(u,v))\), then \( \mu(M) = \max\{a,c\} \) \((\mu(M) = \max\{b,d\})\).

It remains to prove (B).

Proposition 6. Let \( M \in \mathcal{T}(u,v)(I_2; n) \). Then

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

\[
\begin{align*}
    f_1(X, Y) &= \sum_i a_i X^{\alpha_i} Y^{\alpha_i}, \\
    f_2(X, Y) &= Y \sum_i b_i X^{\beta_i} Y^{\beta_i}, \\
    f_3(X, Y) &= X \sum_i c_i X^{\gamma_i} Y^{\gamma_i}, \text{ and} \\
    f_4(X, Y) &= \sum_i d_i X^{\delta_i} Y^{\delta_i}.
\end{align*}
\]

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

Suppose that the statement holds for all matrices in \( T(u,v)(I_2; k) \) for some \( k \geq 0 \). Let \( M \in T(u,v)(I_2; k+1) \). Then \( M \in \{L_u M', R_v M'\} \) for some \( M' \in T(u,v)(I_2; k) \). In particular, by assumption, we have that \( M' = \begin{bmatrix} f_1'(u,v) & f_2'(u,v) \\ f_3'(u,v) & f_4'(u,v) \end{bmatrix} \) where \( f_i'(X,Y) \in N_0[X,Y] \) and \( \deg(f_i') \leq k \) for \( i = 1, 2, 3, 4 \). It now follows that

\[
M = \begin{cases} 
    \begin{bmatrix} f_1'(u,v) & f_2'(u,v) \\ uf_1'(u,v) + f_2'(u,v) & uf_2'(u,v) + f_4'(u,v) \end{bmatrix} & \text{if } M = L_u M', \\
    \begin{bmatrix} f_1'(u,v) + vf_3'(u,v) & f_2'(u,v) + vf_4'(u,v) \\ f_3'(u,v) & f_4'(u,v) \end{bmatrix} & \text{if } M = R_v M'.
\end{cases}
\]

Using (3), it follows that

\[
\begin{align*}
    f_1(X, Y) &= \sum_i a_i X^{\alpha_i} Y^{\alpha_i}, \\
    f_2(X, Y) &= Y \sum_i b_i X^{\beta_i} Y^{\beta_i}, \\
    f_3(X, Y) &= X \sum_i c_i X^{\gamma_i} Y^{\gamma_i}, \text{ and} \\
    f_4(X, Y) &= \sum_i d_i X^{\delta_i} Y^{\delta_i}.
\end{align*}
\]

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

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

\[
\begin{align*}
    f_1'(X, Y) &= \sum_i a_i X^{\alpha_i} Y^{\alpha_i}, \\
    f_2'(X, Y) &= Y \sum_i b_i X^{\beta_i} Y^{\beta_i}, \\
    f_3'(X, Y) &= X \sum_i c_i X^{\gamma_i} Y^{\gamma_i}, \text{ and} \\
    f_4'(X, Y) &= \sum_i d_i X^{\delta_i} Y^{\delta_i}.
\end{align*}
\]

Using (3), it follows that

\[
\begin{align*}
    f_1(X, Y) &= f_1'(X, Y) \\
    &= \sum_i a_i X^{\alpha_i} Y^{\alpha_i},
\end{align*}
\]
\[ f_2(X,Y) = f'_2(X,Y) \]
\[ = Y \sum_i b_i X^{\beta_i} Y^{\gamma_i}, \]
\[ f_3(X,Y) = X f'_2(X,Y) + f'_3(X,Y) \]
\[ = X \sum_i a_i X^{\alpha_i} Y^{\alpha_i} + X \sum_i c_i X^{\gamma_i} Y^{\gamma_i}, \text{ and} \]
\[ f_4(X,Y) = X f'_3(X,Y) + f'_4(X,Y) \]
\[ = X Y \sum_i b_i X^{\beta_i} Y^{\gamma_i} + \sum_i \delta_i X^{\delta_i} Y^{\delta_i} \]
\[ = \sum_i b_i X^{\beta_i+1} Y^{\gamma_i+1} + \sum_i \delta_i X^{\delta_i} Y^{\delta_i}. \]

A similar argument applies in the case when \( M = R_n M' \). Having exhausted all possibilities, the statement holds for \( M \) and therefore the result follows by induction.

\[ \square \]

We denote by \( c_{I_2}^{(u,v)}(n,i) \) the \( i \)-th element (from left to right) of the \( n \)-th row in \( T^{(u,v)}(I_2) \). The following proposition serves two purposes. It addresses the case \( v > u \) by showing that \( \mu(T^{(u,v)}(I_2;n)) = \mu(T^{(v,u)}(I_2;n)) \) and it is needed for the proof of (B).

**Proposition 7.** 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 \( k \)-th 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
\[ c_{I_2}^{(u,v)}(k+1,i) = L_u \cdot c_{I_2}^{(u,v)}(k,(i+1)/2) = \begin{bmatrix} a' & b' \\ ua' + c' & ub' + d' \end{bmatrix} \]
and
\[ c_{I_2}^{(v,u)}(k+1,2^{k+1}+1-i) = R_u \cdot c_{I_2}^{(v,u)}(k,(2^{k+1}+1-i)/2) = R_u \cdot \begin{bmatrix} d' & c' \\ b' & a' \end{bmatrix} = \begin{bmatrix} ub' + d' & ud' + c' \\ b' & a' \end{bmatrix}, \]

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 $M \in \mathcal{R}^{(u,v)}$. By Proposition 7 there is a matrix $M' \in \mathcal{L}^{(v,u)}$ 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 $u$ and $v$, 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 1 makes the above relationship precise (see Figure 2).

**Corollary 1.** Let $n \geq 1$ and $i \in \{1, \ldots, 2^n\}$. If $c_{I_2}^{(u,v)}(n,i) = \left[\begin{array}{c} f_1(u,v) \\ f_2(u,v) \end{array} \right]$, then $c_{I_2}^{(u,v)}(n,2^n+1-i) = \left[\begin{array}{c} f_4(v,u) \\ f_3(v,u) \end{array} \right]$.

\[
\begin{array}{c}
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix} \\
\begin{bmatrix}
1 & u \\
u & 1
\end{bmatrix}
\end{array}
\quad
\begin{array}{c}
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix} \\
\begin{bmatrix}
1 & u \\
u & 1
\end{bmatrix}
\end{array}
\]

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

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

**Figure 2.** A side-by-side comparison of the first three rows of $\mathcal{T}^{(u,v)}(I_2)$ and $\mathcal{T}^{(v,u)}(I_2)$.

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

**Proposition 8.** Let $M = c_{I_2}^{(u,v)}(n,i)$ for some $1 \leq i \leq 2^{n/2}$ and $M' = c_{I_2}^{(u,v)}(n,2^n+1-i)$. Then $\mu(M') \leq \mu(M)$.

**Proof.** We have that $M = \left[\begin{array}{c} f_1(u,v) \\ f_2(u,v) \end{array} \right]$ where $f_i(X,Y) \in \mathbb{N}_0[X,Y]$ for $i = 1, 2, 3, 4$ satisfy the conclusion of Proposition 8. By Corollary 1, $M' = \left[\begin{array}{c} f_4(v,u) \\ f_3(v,u) \end{array} \right]$. By Lemma 8, $\mu(M) = \max\{f_1(u,v), f_3(v,u)\}$ and $\mu(M') = \max\{f_1(v,u), f_3(v,u)\}$.

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

\[
\mu(M') = f_3(v,u) = v \sum_i c_i v^{\gamma_i} u^{\gamma_i} \leq u \sum_i c_i u^{\gamma_i} v^{\gamma_i} = f_3(u,v).
\]

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

\[
\mu(M') = f_1(v,u) = \sum_i a_i v^{\alpha_i} u^{\alpha_i}.
\]
Proof of Theorem 1. The proofs of (A) and (B) using Lemma 9 and Proposition 8, respectively, complete the proof of (1) for all \( u \) and \( v \).

Applying Proposition 2 to the matrix \( R_v = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \), we get that, for \( n \geq 0 \),

\[
\mu(T^{(u,v)}(R_v; 2n + 1)) = \mu(L_u R_v)^n L_u R_v = \mu((L_u R_v)^{n+1})
\]

since right multiplication by \( \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \) simply exchanges the columns of a matrix. Note that, by Proposition 8, \( \mu((R_v L_u)^{n+1}) = \mu((L_u R_v)^{n+1}) \).

Suppose that there exists an \( M \in T^{(u,v)}(I_2; 2n + 2) \) with \( \mu(M) > \mu((R_v L_u)^{n+1}) \). The above computation shows that \( M \in L^{(u,v)} \), so there is an \( 1 \leq i \leq 2^{n+1} \) such that \( M = c_{i_2}^{(u,v)}(2n + 2, i) \). Let \( M' = c_{i_2}^{(u,v)}(2n + 2, 2^n + 1 - i) \). (Note that \( M' \in R^{(u,v)} \).) By Proposition 8 we obtain a contradiction if \( M \) is \( v \)-UD. Furthermore, with Proposition 6 part (b), we have that

\[
\mu(M) = u \sum_i c_i u^i v^i
\]

\[
\mu(M') = v \sum_i c_i u^i v^i, \text{ and}
\]

\[
\mu((R_v L_u)^{n+1}) = \sum_i b_i u^\beta_i v^\beta_i.
\]

By assumption, \( u \sum_i c_i u^i v^i > \sum_i b_i u^\beta_i v^\beta_i \), which implies that

\[
\mu(M') > \sum_i b_i u^\beta_i v^\beta_i = \mu((R_v L_u)^{n+1}),
\]

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 5 and Proposition 4 part (c) since, for \( n \geq 0 \),

\[
\mu(T^{(u,1)}(I_2; 2n + 2)) \leq u F_n(u) + G_n(u) = \mu(L_u (L_u R_1)^n L_u).
\]

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

A hashing 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 \( f : \mathbb{N} \rightarrow [0, m) \) 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 hashing function satisfy some basic requirements (as seen in [3]):

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 [3], Bromberg et al. define a hashing function, which we refer to as the BSV hash\(^4\) for binary strings in the following way. Let \( p \) be a large prime. For fixed integers \( u, v \geq 1 \) and a binary string \( w = a_0a_1 \cdots a_n \) 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 \( \lambda \), 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 \[
\begin{bmatrix}
0 & 1 \\
4 & 3
\end{bmatrix}.
\]

Clearly, we have that collisions in the output of a BSV hash cannot occur for pairs of distinct binary strings whose associated matrices (prior to reduction modulo \( p \)), in the monoid generated by \( L_u \) and \( R_v \), have entries are smaller than \( p \). Theorem 1 immediately gives a upper bound on the binary string length that guarantees collision resistance, answering some open questions in [3]. This is indirectly related to the girth of the Cayley graph of the group generated by \( L_u \) and \( R_v \)\(^7\).

**Corollary 2.** Let \( u, v \geq 1 \) and \( n_0 := n_0(u, v) \) be the largest integer such that \( \mu(T^{(u,v)}(I_2; n_0)) < p \). Then there are no collisions between distinct bit strings of length \( \leq n_0 \) in the BSV hash.

**References**

[1] Benjamin, A.T. and Quinn, J.J., *Proofs that Really Count*, MAA (2003), p. 141
[2] Bromberg, L., *Some applications of noncommutative groups and semigroups to information security* (2015). CUNY Academic Works
[3] Bromberg, L., Shpilrain, V. and Vdovina, A., *Navigating in the Cayley graph of \( SL_2(\mathbb{F}_p) \) and applications to hashing*, Semigroup Forum (2017) 94: 314.
[4] Calkin, N. and Wilf, H.S., *Recounting the rationals*, Amer. Math. Monthly 107 (2000), no. 4, 360-363.
[5] Han, S., Masuda, A.M., Singh, S., and Thiel, J., *Orphans in forests of linear fractional transformations*, Electron. J. Combin. 23 (2016), no. 3, Paper 3.6, 24pp.
[6] Han, S., Masuda, A.M., Singh, S., and Thiel, J., *The \( (u,v) \)-Calkin-Wilf forest*, Int. J. Number Theory 12 (2016), no. 5, 1311-1328.
[7] Helfgott, H.A., *Growth and generation in \( SL_2(\mathbb{Z}/p\mathbb{Z}) \)*, Ann. of Math. (2) 167 (2008), no. 2, 601-623.
[8] Lucas, E., *Sur les suites de Farey*, Bull. Soc. Math. France, 6 (1878), 118119.
[9] Nathanson., M.B., *Pairs of matrices in \( GL_2(\mathbb{R}_{\geq 0}) \) that freely generate*, Amer. Math. Monthly 122 (2015), no. 8, 790-792.
[10] Nathanson., M.B., *A forest of linear fractional transformations*, Int. J. Number Theory 11 (2015), no. 4, 1275-1299.

\(^4\)The BSV hash is a generalization of a hash function defined by Zémor [13].
[11] Paulin, R., *Largest values of the Stern sequence, alternating binary expansions and continuants*, J. Integer Seq., 20 (2017), Article 17.2.8.

[12] Sanov, I.N., *A property of a representation of a free group* (Russian), Doklady Akad. Nauk SSSR (N. S.) 57 (1947), 657-659.

[13] Zémor, G., *Hash functions and graphs with large girths*, EUROCRYPT 91, Lecture Notes Comp. Sci. 547 (1991), 508-511.

Department of Mathematics, New York City College of Technology (CUNY), 300 Jay Street, Brooklyn, New York 11201

*E-mail address*: {shan,amasuda,ssingh,jthiel}@citytech.cuny.edu