A Calculational Approach to Path-Based Properties of the Eisenstein-Stern and Stern-Brocot Trees via Matrix Algebra

João F. Ferreira[a,b], Alexandra Mendes[a]

[a] *School of Computing, Teesside University, UK*
[b] *HASLab / INESC TEC, Universidade do Minho, Portugal*

Abstract

This paper proposes a calculational approach to prove properties of two well-known binary trees used to enumerate the rational numbers: the Stern-Brocot tree and the Eisenstein-Stern tree (also known as Calkin-Wilf tree). The calculational style of reasoning is enabled by a matrix formulation that is well-suited to naturally formulate path-based properties, since it provides a natural way to refer to paths in the trees.

Three new properties are presented. First, we show that nodes with palindromic paths contain the same rational in both the Stern-Brocot and Eisenstein-Stern trees. Second, we show how certain numerators and denominators in these trees can be written as the sum of two squares x^2 and y^2, with the rational $\frac{x}{y}$ appearing in specific paths. Finally, we show how we can construct Sierpiński's triangle from these trees of rationals.

Keywords: Stern-Brocot tree, Eisenstein-Stern tree (aka Calkin-Wilf tree), number theory, calculational method, palindromic paths, Euclid's algorithm, invariant, rational number, sum of two squares, Sierpiński's triangle, Lucas's theorem

Why do people look for compact notations? A compact notation leads to shorter documents (less lines of code in programming) in which patterns are easier to identify and to reason about. Properties can be stated in clear-cut, one-line long equations which are easy to memorize. — José N. Oliveira [1]

1. Introduction

Vigorous reasoning is concise. As stated in the opening quote by José N. Oliveira, conciseness facilitates reasoning and the identification of patterns. Indeed, Oliveira's work in pointfree calculational techniques and algebraic methods in programming [2, 3, 4] is an excellent example of how conciseness leads to shorter documents and elegant theories. As Oliveira writes in [3]:

> *Theories "refactored" via the PF-transform [pointfree transform] become more general, more structured and simpler. Elegant expressions replace lengthy formulae and easy-to-follow calculations replace pointwise proofs with lots of "..." notation, case analyses and natural language explanations for "obvious" steps.*
>
> *(...)*
>
> *Thanks to the PF-transform, opportunities for creativity steps are easier to spot and carry out with less symbol trading.*

In the same spirit as José N. Oliveira's work on the application of calculational techniques, this paper proposes a calculational approach to prove properties of two well-known binary trees used to enumerate

Email addresses: joao@joaoff.com (João F. Ferreira), alexandra@archimendes.com (Alexandra Mendes)

the rational numbers: the Stern-Brocot tree and the Eisenstein-Stern tree (also known as Calkin-Wilf tree). The approach described in this paper is based on the matrix formulation first presented in [5]. In Section 2, we discuss this matrix formulation in more detail, together with some background on the Stern-Brocot and Eisenstein-Stern trees of rationals.

As we hope to demonstrate, besides allowing a calculational style of reasoning, the matrix formulation has other advantages. First, because both Stern-Brocot and Eisenstein-Stern trees can be obtained from a single tree of matrices, it becomes easier to establish relationships between the two trees of rationals. Second, the matrix formulation is well-suited to formulate and reason about *path-based* properties, for it provides a natural way to refer to paths in the trees. In Section 3, for instance, we show how we can use the algebra of matrices to prove properties that relate the Stern-Brocot and Eisenstein-Stern trees. An example is the previously unknown property (as far as we know) that nodes with palindromic paths contain the same rational in both trees of rationals. The way in which this new property was found is an example of the *"opportunities for creative steps"* provided by the calculational method.

A third advantage is that, because a 2×2 matrix contains more information than a single rational, it becomes easier to find properties that are not at all obvious when considering only the trees of rationals. In Sections 4 and 5, we show how the extra information provided by matrices can be used to find new path-based properties. More specifically, in Section 4 we show how certain numerators and denominators in the Stern-Brocot and Eisenstein-Stern trees can be written as the sum of two squares x^2 and y^2, with the rational $\frac{x}{y}$ appearing in specific positions of these trees. In Section 5, we show how this extra information can be used to establish a relationship between Sierpiński's triangle and the Stern-Brocot and Eisenstein-Stern trees. Incidentally, the first time that the authors of this paper studied and generated Sierpiński's triangle computationally was in one of José N. Oliveira's modules on program calculation [1] (the goal was to write a "Sierpiński's triangle generator" as a catamorphism).

We conclude the paper in Section 6, where we also give an account of current and future work.

2. Preliminaries

A standard theorem of mathematics is that the rationals are "denumerable", i.e. they can be put in one-to-one correspondence with the natural numbers. Another way of saying this is that it is possible to enumerate the rationals so that each appears exactly once. Two of the most well-studied sequences used to enumerate the rationals are known as *Stern-Brocot sequence* and *Calkin-Wilf sequence*.

These sequences give rise to complete binary trees, commonly known as *Stern-Brocot tree* and *Calkin-Wilf tree*. For reasons of historical accuracy, we deviate from common practice and use a different name for what is commonly know as Calkin-Wilf tree. As pointed out in [6], Stern [7] had already documented essentially the same structural characterisation of the rationals almost 150 years earlier than Calkin and Wilf. Stern attributes the structure to Eisenstein, so henceforth we refer to the "Eisenstein-Stern" tree of rationals where recent publications would refer to the "Calkin-Wilf" tree of rationals. For more details on Stern's characterisation, see the appendix in [6]. For a comprehensive account of properties of the Stern-Brocot tree, including further relationships with Euclid's algorithm, see [8, pp. 116–118]. For more details about the Eisenstein-Stern tree, we refer the reader to [9].

The first four levels of the Stern-Brocot tree and of the Eisenstein-Stern tree are shown in Figures 1 and 2, respectively.

There has been a spate of interest in the construction of bijections between the natural numbers and the (positive) rationals (see [5, 10, 11, 9] and [12, pp. 94–97]). In [11], it is shown that the rationals can be efficiently enumerated[1] by "deforesting" the Eisenstein-Stern tree of rationals [9] (the algorithm is credited to Moshe Newman). Motivated by the remark in [10] that it is "not at all obvious" how to "deforest" the Stern-Brocot tree of rationals, the authors of [5] developed an efficient algorithm for enumerating the rationals according to both orderings. The algorithm is based on a bijection between the rationals and

[1] By an *efficient enumeration* we mean a method of generating each rational without duplication with constant cost per rational in terms of arbitrary-precision simple arithmetic operations.

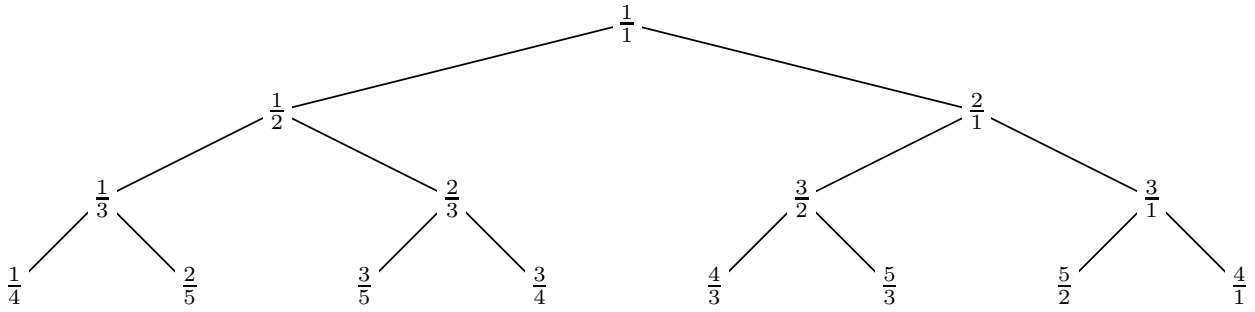


Figure 1: Stern-Brocot tree of rationals

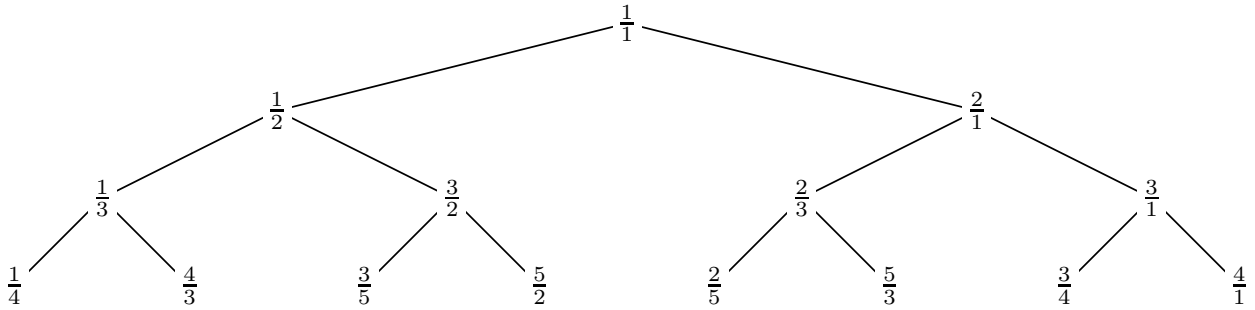


Figure 2: Eisenstein-Stern tree of rationals (also known as Calkin-Wilf tree)

invertible 2×2 matrices. The key to the algorithm's derivation is the reformulation of Euclid's algorithm in terms of matrices. The enumeration is efficient in the sense that it has the same time and space complexity as the algorithm credited to Moshe Newman in [11], albeit with a constant-fold increase in the number of variables and number of arithmetic operations needed at each iteration. The enumeration presented in [5] gives rise to a full binary tree of finite products of the matrices $\mathbf{L}$ and $\mathbf{R}$ defined as

$$\mathbf{L} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{R} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

The root of the tree is the identity matrix $\mathbf{I}$ (the empty product). The tree can be displayed with "L" labelling a left branch (post-multiplication by $\mathbf{L}$) and "R" labelling a right branch (post-multiplication by $\mathbf{R}$). Figure 3 displays the first four levels of the tree.

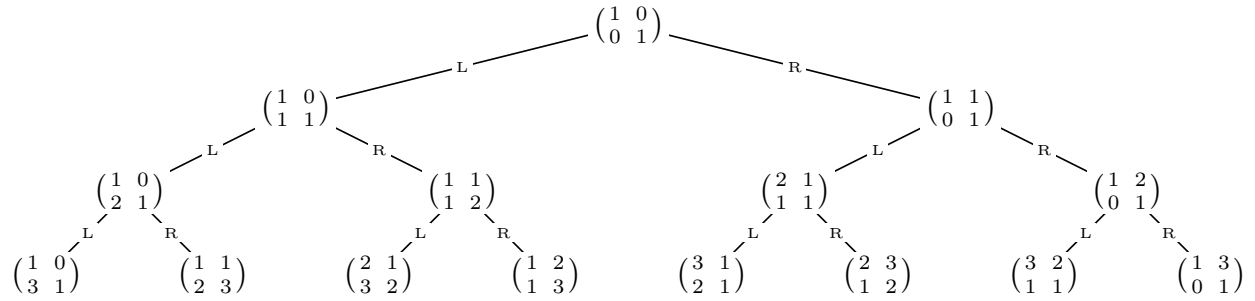


Figure 3: Tree of products of $\mathbf{L}$ and $\mathbf{R}$

By pre-multiplying each matrix in the tree by $(1 \;\; 1)$, we get a tree of rationals. (Premultiplying by $(1 \;\; 1)$ is accomplished by adding the elements in each column.) The resulting tree is the Eisenstein-Stern tree (where the vector $(x \;\; y)$ corresponds to the rational $\frac{y}{x}$).

By post-multiplying each matrix in the tree by $\binom{1}{1}$, we also get a tree of rationals. (Postmultiplying by $\binom{1}{1}$ is accomplished by adding the elements in each row.) The resulting tree is the Stern-Brocot tree (where the vector $\binom{x}{y}$ corresponds to the rational $\frac{x}{y}$).

The key observation in [5] is that the problem of enumerating the rationals can be transformed into the problem of enumerating all finite products of the matrices $\mathbf{L}$ and $\mathbf{R}$. This is achieved by transforming each matrix $\mathbf{M}$ into its successor $\mathsf{next}(\mathbf{M})$, defined as:

$$\mathsf{next}(\mathbf{M}) = \begin{cases} \mathbf{L}^{n+1} & \text{if } \mathbf{M} = \mathbf{R}^n \\ \mathbf{M} \times \begin{pmatrix} 2j+1 & 1 \\ -1 & 0 \end{pmatrix} & \text{if } \mathbf{M} \neq \mathbf{R}^n \end{cases}$$

where for $\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have $j = \lfloor \frac{b+d-1}{a+c} \rfloor$. The first case (when $\mathbf{M} = \mathbf{R}^n$) states that the matrix that follows the rightmost matrix of level n is the first matrix of level $n{+}1$ (i.e. $\mathbf{L}^{n+1}$). To understand the second case, note that the matrix immediately following a matrix $\mathbf{M}$ (that is not the last, i.e. $\mathbf{M} \neq \mathbf{R}^n$) is found by identifying the rightmost $\mathbf{L}$ in the decomposition of $\mathbf{M}$ as a product of the matrices $\mathbf{L}$ and $\mathbf{R}$. Supposing $\mathbf{M}$ is the product $\mathbf{M}'\mathbf{L}\mathbf{R}^j$, its successor is $\mathbf{M}'\mathbf{R}\mathbf{L}^j$; so, to find the successor matrix, we post-multiply $\mathbf{M}'\mathbf{L}\mathbf{R}^j$ by $\mathbf{R}^{-j}\mathbf{L}^{-1}\mathbf{R}\mathbf{L}^j$, which is the same as $\begin{pmatrix} 2j+1 & 1 \\ -1 & 0 \end{pmatrix}$. For the full details, we refer the reader to [5, 6].

As discussed in the introduction, the matrix formulation has several advantages. First, because both Stern-Brocot and Eisenstein-Stern trees can be obtained from the tree of matrices, it becomes easier to establish relationships between the two trees of rationals. Second, because a $2{\times}2$ matrix contains more information than a single rational, it becomes easier to find properties that are not at all obvious when considering only the trees of rationals. In Sections 4 and 5, we show how the extra information provided by matrices can be used to find new properties. Finally, the matrix formulation is well-suited to formulate and reason about *path-based* properties, for it provides a natural way to refer to paths in the trees. For example, if we want to consider the rationals with path LRR, we can study the matrix product $\mathbf{LRR}$. In the remainder of this paper, we use paths and matrix products interchangeably. We will use expressions like "the rational with path $\mathbf{LRR}$" or "the node with path $\mathbf{LRR}$" to refer to the rational obtained from the matrix $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$ (i.e. it either refers to the rational $\frac{3}{4}$ in the Stern-Brocot tree or to the rational $\frac{5}{2}$ in the Eisenstein-Stern tree). We also use matrix terminology with paths. An example is the use of the expression "*transpose paths*"; we use expressions such as "the transpose of the path $\mathbf{LRR}$ is the path $\mathbf{LLR}$" (note that the transpose of the product is the product of the transposes in reverse order; also $\mathbf{L}^T = \mathbf{R}$ and $\mathbf{R}^T = \mathbf{L}$).

As a first example of what we call a *path-based property*, let us show that for all paths $\mathbf{M}$ that are equal to their own transpose (e.g. the path $\mathbf{LR}$), the rational with path $\mathbf{M}$ in the Stern-Brocot tree is the reciprocal of the rational with path $\mathbf{M}$ in the Eisenstein-Stern tree. This can easily be proved as:

$$\begin{array}{ll} & \frac{m}{n} \text{ has path } \mathbf{M} \text{ in the Stern-Brocot tree} \\ = & \quad \{ \text{ matrix formulation } \} \\ & \binom{m}{n} = \mathbf{M} \times \binom{1}{1} \\ = & \quad \{ \mathbf{M} = \mathbf{M}^T \} \\ & \binom{m}{n} = \mathbf{M}^T \times \binom{1}{1} \\ = & \quad \{ \text{ transpose of the product } \} \\ & (m \;\; n) = (1 \;\; 1) \times \mathbf{M} \\ = & \quad \{ \text{ matrix formulation } \} \\ & \frac{n}{m} \text{ has path } \mathbf{M} \text{ in the Eisenstein-Stern tree} \end{array}$$

All the matrices used in the remainder of the paper are finite products of $\mathbf{L}$s and $\mathbf{R}$s, unless stated otherwise.

3. Calculating with matrices

In this section, we show how we can prove existing and discover new properties of the Stern-Brocot and Eisenstein-Stern trees using the algebra of matrices. We start with a well-known property of the Eisenstein-

Stern tree: the denominator of each fraction in the tree is the numerator of the next fraction in the tree.

Theorem 1. *In the Eisenstein-Stern tree, the denominator of each fraction in the tree is the numerator of the next fraction in the tree. Formally:*

$$(1 \;\; 1) \times \mathbf{M} \times \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;\; = \;\; (1 \;\; 1) \times \mathsf{next}(\mathbf{M}) \times \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Proof. The definition of $\mathsf{next}(\mathbf{M})$ induces two cases. The first case is when $\mathbf{M} \neq \mathbf{R}^n$, so we have $\mathsf{next}(\mathbf{M}) = \mathbf{M} \times \left(\begin{smallmatrix} 2j+1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ for some j:

$$\begin{array}{ll} & (1 \;\; 1) \times \mathsf{next}(\mathbf{M}) \times \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \; \mathbf{M} \neq \mathbf{R}^n \; \} \\ & (1 \;\; 1) \times \mathbf{M} \times \left(\begin{smallmatrix} 2j+1 & 1 \\ -1 & 0 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \text{ arithmetic } \} \\ & (1 \;\; 1) \times \mathbf{M} \times \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \end{array}$$

The second case is when $\mathbf{M} = \mathbf{R}^n$, so we have $\mathsf{next}(\mathbf{M}) = \mathbf{L}^{n+1}$. We calculate:

$$\begin{array}{ll} & (1 \;\; 1) \times \mathbf{R}^n \times \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = (1 \;\; 1) \times \mathbf{L}^{n+1} \times \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \text{ arithmetic } \} \\ & (1 \;\; 1) \times \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = (1 \;\; 1) \times \left(\begin{smallmatrix} 1 & 0 \\ n+1 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \text{ arithmetic } \} \\ & (1 \;\; n+1) \times \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = (n+2 \;\; 1) \times \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \text{ arithmetic } \} \\ & 1 = 1 \\ = & \quad \{ \text{ reflexivity } \} \\ & \mathit{true} \end{array}$$

□

This theorem appears in [9], where it is proved in three cases and by contradiction. In fact, as described in [6], this property is known since at least 1858, since it is obviously present in Stern's paper [7]. An inductive proof can be found in [12] and an alternative proof based in branching can be found in [13]; both proofs are decomposed into three cases.

It can be said that the matrix formulation of Theorem 1 and its proof do not offer great advantages, other than reducing the number of cases that need to be analysed. In fact, it could be argued that our proof is slightly more complicated, since it uses the properties $\mathbf{L}^n = \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$ and $\mathbf{R}^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ without proving them (they can easily be proved by induction). Nevertheless, and although the proof is not pointfree, the style of reasoning used naturally supports pointfree reasoning. We now prove this claim by showing a pointfree proof that the jth node in level n of the Eisenstein-Stern tree is the reciprocal of the jth node from the end of level n. For example, we can see in Figure 2 that the third node in level 3 (the rational $\frac{3}{5}$) is the reciprocal of the third node from the end of level 3 (the rational $\frac{5}{3}$).

We start by introducing the notion of *bit reversal* for finite products of $\mathbf{L}$s and $\mathbf{R}$s.

Definition 1. *Let* $\mathbf{M}$ *be a finite product of* $\mathbf{L}$*s and* $\mathbf{R}$*s. The bit reversal of* $\mathbf{M}$*, denoted as* $\mathsf{br}(\mathbf{M})$*, is the product obtained by replacing in* $\mathbf{M}$ *all the* $\mathbf{L}$*s by* $\mathbf{R}$*s and all the* $\mathbf{R}$*s by* $\mathbf{L}$*s. Formally, it can be defined recursively as:*

$$\begin{array}{l} \mathsf{br}(\mathbf{I}) = \mathbf{I} \\ \mathsf{br}(\mathbf{L}) = \mathbf{R} \\ \mathsf{br}(\mathbf{R}) = \mathbf{L} \\ \mathsf{br}(\mathbf{L} \times \mathbf{M}) = \mathbf{R} \times \mathsf{br}(\mathbf{M}) \\ \mathsf{br}(\mathbf{R} \times \mathbf{M}) = \mathbf{L} \times \mathsf{br}(\mathbf{M}) \end{array}$$

This definition induces the use of case analysis, which, in general, we want to avoid. So, we introduce the following lemma that allows us to express the bit reversal of a matrix as a product of matrices. We write $\mathbf{S}$ to denote the *exchange matrix* of size 2, that is, $\mathbf{S} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. The exchange matrix, also known as reversal matrix or backward identity, can be used to exchange rows and columns: to exchange the rows of a matrix $\mathbf{M}$, we pre-multiply[2] $\mathbf{M}$ by $\mathbf{S}$; to exchange the columns, we post-multiply by $\mathbf{S}$. We also have $\mathbf{S} = \mathbf{S}^{-1} = \mathbf{S}^T$ and $\mathbf{S}^2 = \mathbf{I}$. Moreover, $(1 \;\; 1) \times \mathbf{S} = (1 \;\; 1)$ and $\mathbf{S} \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$.

Lemma 1. *The bit reversal of a matrix* $\mathbf{M}$ *can be defined as:*

$$\mathsf{br}(\mathbf{M}) = \mathbf{S} \times \mathbf{M} \times \mathbf{S}$$

Proof. Proof in Appendix A. □

In the remaining of the paper, we always use this definition of br. Now that we have the notion of *bit reversal* defined we can state the theorem on reciprocals:

Theorem 2. *The* j*th node in level* n *of the Eisenstein-Stern tree is the reciprocal of the* j*th node from the end of level* n*. Formally:*

$$(1 \;\; 1) \times \mathbf{M} \;=\; (1 \;\; 1) \times \mathsf{br}(\mathbf{M}) \times \mathbf{S}$$

Proof.

$$\begin{array}{ll} & (1 \;\; 1) \times \mathsf{br}(\mathbf{M}) \times \mathbf{S} \\ = & \quad \{ \text{ definition of } \mathsf{br} \text{ and arithmetic } \} \\ & (1 \;\; 1) \times \mathbf{S} \times \mathbf{M} \times \mathbf{S}^2 \\ = & \quad \{ \; \mathbf{S}^2 = \mathbf{I} \; \} \\ & (1 \;\; 1) \times \mathbf{S} \times \mathbf{M} \\ = & \quad \{ \; (1 \;\; 1) \times \mathbf{S} = (1 \;\; 1) \; \} \\ & (1 \;\; 1) \times \mathbf{M} \end{array}$$

□

This theorem is proved in [13] by induction on the levels of the tree and case analysis. We believe that our proof is a good alternative: it is simpler, shorter, and completely pointfree! Moreover, we can follow similar steps to prove the same property for the Stern-Brocot tree.

Theorem 3. *The* j*th node in level* n *of the Stern-Brocot tree is the reciprocal of the* j*th node from the end of level* n*. Formally:*

$$\mathbf{M} \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} \;=\; \mathbf{S} \times \mathsf{br}(\mathbf{M}) \times \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Proof.

$$\begin{array}{ll} & \mathbf{S} \times \mathsf{br}(\mathbf{M}) \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \text{ definition of } \mathsf{br} \text{ and arithmetic } \} \\ & \mathbf{S}^2 \times \mathbf{M} \times \mathbf{S} \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \; \mathbf{S}^2 = \mathbf{I} \; \} \\ & \mathbf{M} \times \mathbf{S} \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \\ = & \quad \{ \; \mathbf{S} \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \; \} \\ & \mathbf{M} \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \end{array}$$

□

We can also obtain Theorem 3 as a consequence of Theorem 2 by transposing the matrices and using the equality $\mathsf{br}(\mathbf{M})^T = \mathsf{br}(\mathbf{M}^T)$. The proof is left to the reader.

[2]Note that if $\mathbf{M}$ is a finite product of $\mathbf{L}$s and $\mathbf{R}$s, the matrix $\mathbf{MS}$ may not be a finite product of $\mathbf{L}$s and $\mathbf{R}$s (e.g. $\mathbf{LS}$).

3.1. Characterisation of node invariance

So far, we have only verified known properties of the Stern-Brocot and Eisenstein-Stern trees. However, the calculational approach is well-suited to investigate and discover new properties. In this section, we show how we can characterise the paths of the nodes that represent the same rational in both the Stern-Brocot and Eisenstein-Stern trees. For example, the path **L** represents the same rational in both trees ($\frac{1}{2}$); the same applies to the path **LRL** ($\frac{3}{5}$). We say that the nodes with paths **L** and **LRL** are invariant. In general, when a node represents the same rational in both Stern-Brocot and Eisenstein-Stern trees, we say that the node is invariant. We seek to characterise all the paths that have this property.

Recall that the rational with path **M** in the Stern-Brocot tree is given by $\mathbf{M} \times \binom{1}{1}$; the resulting vector $\binom{x}{y}$ represents the rational $\frac{x}{y}$. Similarly, the rational with path **M** in the Eisenstein-Stern tree is given by $(1 \;\; 1) \times \mathbf{M}$; the resulting vector $(x \;\; y)$ represents the rational $\frac{y}{x}$. As a result, a way of formulating that a node with path **M** is invariant is:

$$\mathbf{M} \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \mathbf{S} \times ((1 \;\; 1) \times \mathbf{M})^T$$

Note that on the right-hand side the transpose transforms the row vector into a column vector and the pre-multiplication by **S** swaps its rows. Moreover, by transposing the product, this formula can be rewritten into the more symmetric:

$$\mathbf{M} \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \mathbf{S} \times \mathbf{M}^T \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{1}$$

Because we want to characterise the paths **M**, it would be good to get rid of the column vector $\binom{1}{1}$. We do not have a general cancellation property that allows us to remove the column vector from both sides, but the following lemma shows that we can do it for *transpose paths*.

Lemma 2. *Let* **M** *be an arbitrary* 2×2 *matrix. We have:*

$$\mathbf{M} \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \mathbf{M}^T \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \equiv \quad \mathbf{M} = \mathbf{M}^T$$

Proof. Proof in Appendix A. □

Using this lemma, we can simplify (1) as follows:

$$\begin{array}{ll} & \mathbf{M} \times \binom{1}{1} = \mathbf{S} \times \mathbf{M}^T \times \binom{1}{1} \\ = & \quad \{\ S \times \binom{1}{1} = \binom{1}{1}\ \} \\ & \mathbf{M} \times \mathbf{S} \times \binom{1}{1} = \mathbf{S} \times \mathbf{M}^T \times \binom{1}{1} \\ = & \quad \{\ \text{transpose of the product and } \mathbf{S}^T = \mathbf{S}\ \} \\ & \mathbf{M} \times \mathbf{S} \times \binom{1}{1} = (\mathbf{M} \times \mathbf{S})^T \times \binom{1}{1} \\ = & \quad \{\ \text{Lemma 2}\ \} \\ & \mathbf{M} \times \mathbf{S} = (\mathbf{M} \times \mathbf{S})^T \end{array}$$

Now that we got rid of the vector $\binom{1}{1}$, we can further simplify and obtain a characterisation of **M**:

$$\begin{array}{ll} & \mathbf{M} \times \mathbf{S} = (\mathbf{M} \times \mathbf{S})^T \\ = & \quad \{\ \text{transpose of the product}\ \} \\ & \mathbf{M} \times \mathbf{S} = \mathbf{S} \times \mathbf{M}^T \\ = & \quad \{\ \mathbf{S} = \mathbf{S}^{-1}\ \} \\ & \mathbf{M} = \mathbf{S} \times \mathbf{M}^T \times \mathbf{S} \\ = & \quad \{\ \text{definition of } \mathsf{br}\ \} \\ & \mathbf{M} = \mathsf{br}(\mathbf{M}^T) \end{array}$$

So, we have just proved that a node with path $\mathbf{M}$ is invariant if and only if $\mathbf{M} = \mathsf{br}(\mathbf{M}^T)$. But since $\mathbf{L}^T = \mathbf{R}$ and $\mathbf{R}^T = \mathbf{L}$, we have that $\mathsf{br}(\mathbf{M}^T)$ is the same product as $\mathbf{M}$ but in reverse order! We can thus write:

$$\begin{array}{ll} & \mathbf{M} = \mathsf{br}(\mathbf{M}^T) \\ = & \quad \{ \text{ definition } \} \\ & \mathbf{M} \text{ is a palindromic path} \end{array}$$

In conclusion, we have just proved the following theorem.

Theorem 4. *A node with path* $\mathbf{M}$ *is invariant if and only if* $\mathbf{M}$ *is a palindromic path. Formally, we have:*

$$\mathbf{M} \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \mathbf{S} \times \mathbf{M}^T \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \equiv \quad \mathbf{M} = \mathsf{br}(\mathbf{M}^T)$$

As far as we know, this theorem was never explicitly stated before. Although invariance is defined and identified in [13, Theorem 28], there is no connection with the nature of the paths. On the other hand, although the authors of [10] did not consider node invariance and did not explicitly state this property, they did point out that each level of the Eisenstein-Stern tree is the bit-reversal permutation of the corresponding level of the Stern-Brocot tree. It is not difficult to prove Theorem 4 using their observation.

4. On the sums of two squares

As the previous section demonstrates, the use of matrices is particularly well-suited to formulate and reason about path-based properties. Another advantage of using the matrix formulation is that they have more information than rationals, since 2×2 matrices consist of 4 integers. This allows us to discover relationships that are not at all obvious when considering only the trees of rationals.

In this section, we make use of this extra information to extend previous work and show how certain numerators and denominators in the Eisenstein-Stern and Stern-Brocot trees can be written as the sum of two squares x^2 and y^2, with the rational $\frac{x}{y}$ appearing in specific positions of these trees. For example, using the properties that are about to be presented, we are able to conclude that we can write the denominator of the rational with path **LRL** in the Eisenstein-Stern tree (Figure 2) as the sum of the squares of the numerator and denominator of the rational with the path **L** in the same tree (i.e. 5 can be written as $1^2 + 2^2$).

We use the results presented in [14] as a starting point. In that paper, an extended version of Euclid's algorithm is inverted to investigate when a number can be written as the sum of two squares. Euclid's algorithm is expressed in matrix terms[3] and computes a matrix $\mathbf{D}$ that is a product of **L**s and **R**s. The main theorem of [14] states that a number m at least 2 can be written as the sum of two squares if there is a number n such that $0<n<m$ and $n^2 \cong -1 \pmod{m}$. Moreover, when the inputs to the algorithm satisfy these conditions, the final value of $\mathbf{D}$ is of the form $\mathbf{M} \times \mathbf{L}$ with $\mathbf{M} = \mathbf{M}^T$. Although the matrices are key to establish the result in [14], no connection was established with the Stern-Brocot and Eisenstein-Stern trees. We investigate the connection in this section.

First, we present a lemma showing that when a matrix $\mathbf{M}$ can be decomposed as the product of another matrix by its transpose, we have $\mathbf{M} = \mathbf{M}^T$.

Lemma 3. *Let* $\mathbf{M}$ *be an arbitrary* 2×2 *matrix.*

$$\langle \forall \mathbf{P} : \mathbf{M} = \mathbf{P}\mathbf{P}^T : \mathbf{M} = \mathbf{M}^T \rangle$$

where $\mathbf{P}$ *ranges over all* 2×2 *matrices.*

[3] More precisely, a vector $(x \;\; y)$ is iteratively post-multiplied by either $\mathbf{L}^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$ or $\mathbf{R}^{-1} = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$. This corresponds to the assignments $x, y := x-y, y$ and $x, y := x, y-x$, respectively. In addition to computing the greatest common divisor, the extended algorithm also computes a matrix $\mathbf{C}$ that is a product of the matrices $\mathbf{L}^{-1}$ and $\mathbf{R}^{-1}$. The matrix $\mathbf{D}$ mentioned in the body text is the inverse of $\mathbf{C}$.

Proof. Proof in Appendix A. □

This lemma is relevant because it gives us a new path-based property of the Eisenstein-Stern tree: the denominator of rationals with path of the form $\mathbf{PP}^T\mathbf{L}$ can be written as the sum of two squares. Let $\frac{n}{m}$ be the rational with path $\mathbf{PP}^T\mathbf{L}$; then

$$(m \;\; n) = (1 \;\; 1) \times \mathbf{PP}^T\mathbf{L}$$

If we let $\mathbf{P} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have:

$$(m \;\; n) = (1 \;\; 1) \times \mathbf{PP}^T\mathbf{L} = ((a+c)^2 + (b+d)^2 \;\; c(a+c) + d(b+d)) \tag{2}$$

meaning that m can be written as the sum of two squares: $(a+c)^2 + (b+d)^2$. Now, let the rational with path $\mathbf{P}$ be $\frac{x}{y}$. Given the above definition of $\mathbf{P}$, it is the same as $\frac{b+d}{a+c}$. From (2), we can conclude that the denominator of the rational with path $\mathbf{PP}^T\mathbf{L}$ can be written as $x^2 + y^2$. Moreover, using Theorem 1, we can immediately conclude that the numerator of the rational with path $\mathbf{PP}^T\mathbf{R}$ can be written as $x^2 + y^2$. We can thus formulate the following theorem.

Theorem 5. *Let $\frac{x}{y}$ be the rational in the Eisenstein-Stern tree with path $\mathbf{P}$. Then,*

a) the denominator of the rational with path $\mathbf{PP}^T\mathbf{L}$ is $x^2 + y^2$

b) the numerator of the rational with path $\mathbf{PP}^T\mathbf{R}$ is $x^2 + y^2$

Example 1 (Paths in the Eisenstein-Stern tree)**.** *At the beginning of the section we gave the example of the path $\mathbf{LRL}$, which gives $5^2 = 2^2 + 1^2$. We now give another example: if starting from the root we follow a path $\mathbf{P}$ where*

$$\mathbf{P} = \mathbf{LLRRLRLLR}$$

we get the node with the rational $\frac{61}{44}$. If from that node we follow the transpose path $\mathbf{P}^T$, i.e.

$$\mathbf{P}^T = \mathbf{LRRLRLLRR}$$

and then go left, we get to the node $\mathbf{PP}^T\mathbf{L}$ with the rational $\frac{3987}{5657}$. We have $5657 = 61^2 + 44^2$. Figure 4(a) illustrates the shapes of the paths that can be taken in the Eisenstein-Stern tree.

By transposing all the matrices in (2), we get a similar theorem associated with the Stern-Brocot tree:

Theorem 6. *Let $\frac{x}{y}$ be the rational in the Stern-Brocot tree with path $\mathbf{P}^T$. Then,*

a) the denominator of the rational with path $\mathbf{LPP}^T$ is $x^2 + y^2$

b) the numerator of the rational with path $\mathbf{RPP}^T$ is $x^2 + y^2$

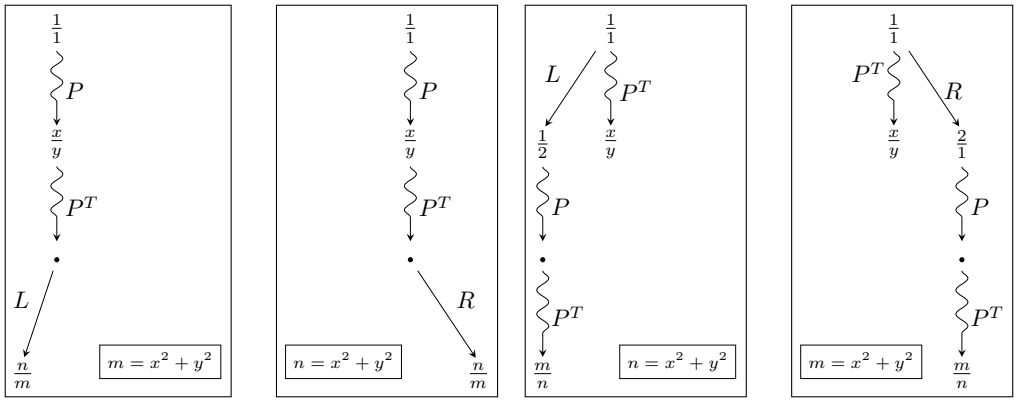
Example 2 (Paths in the Stern-Brocot tree)**.** *If starting from the root we go left and then we follow a path $\mathbf{P}$ where*

$$\mathbf{P} = \mathbf{LLRRLRLLR}$$

we get the node with path $\mathbf{LP}$. If from that node we follow the transpose path $\mathbf{P}^T$, i.e.

$$\mathbf{P}^T = \mathbf{LRRLRLLRR}$$

we get to the node $\mathbf{LPP}^T$ with the rational $\frac{1670}{5657}$. If starting from the root we follow the path $\mathbf{P}^T$, we reach the node with rational $\frac{61}{44}$. We have $5657 = 61^2 + 44^2$. Figure 4(b) illustrates the shapes of the paths that can be taken in the Stern-Brocot tree.



(a) Paths in the Eisenstein-Stern tree (b) Paths in the Stern-Brocot tree

Figure 4: Certain numerators and denominators in the Eisenstein-Stern and Stern-Brocot trees can be written as sums of two squares

5. Uncovering Sierpiński's triangle

In the previous section, we used the extra information provided by matrices to establish a relationship between nodes that would be more difficult to identify if we had only used the rationals. In this section, we show how this extra information makes it easier to establish a relationship between Sierpiński's triangle and the Eisenstein-Stern and Stern-Brocot trees.

5.1. Intermezzo: on Pascal's and Sierpiński's triangles

Pascal's triangle is a triangular array of numbers whose left and right border are all 1's, and where each number is the sum of the two numbers immediately above it. The nth row and kth column of Pascal's triangle contains the binomial coefficient $C(n, k)$. The first 16 levels of Pascal are shown in Figure 5(a). Now, if we take Pascal's triangle and colour the even numbers white and the odd numbers black, we get the startling property that the resulting triangle is an approximation to Sierpiński's triangle! Sierpiński's triangle is a famous fractal structure with the overall shape of a triangle, subdivided recursively into smaller triangles (see Figure 5(b)).

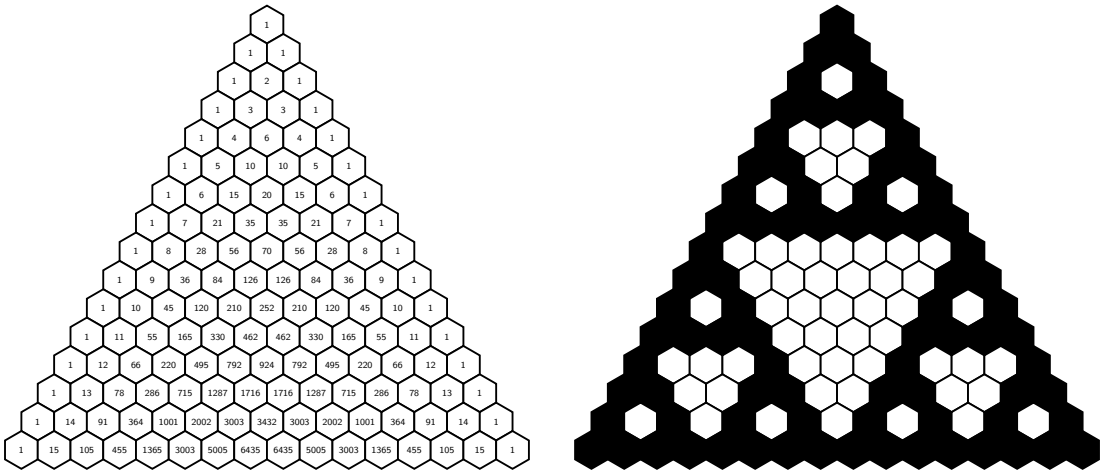
As explained in Ian Stewart's essay *Pascal's Fractals* [15], the theorem that justifies this connection is stated in [16] and was originally proved by the great French recreational mathematician Édouard Lucas. The theorem lets us predict whether a cell will be black or white, without calculating the corresponding binomial coefficient. It can be stated as:

$$\begin{array}{lcl} odd(C(n,k)) & \Leftarrow & n \leftharpoondown k \\ even(C(n,k)) & \Leftarrow & n \not\leftharpoondown k \end{array}$$

where $n \leftharpoondown k$ is true when every binary digit in k is at most the corresponding digit in n. For example, we have $7 \leftharpoondown 3$, since these in binary are respectively 111 and 011 and no digit in 3 is greater than the corresponding digit in 7. This means that $C(7, 3)$ is odd. On the other hand, we have $2 \not\leftharpoondown 1$, since these in binary are respectively 10 and 01, and the least significant digit in 1 is greater than the corresponding digit in 2. This means that $C(2, 1)$ is even. As pointed out in [17], we can define $n \leftharpoondown k$ as

$$n \leftharpoondown k \quad \equiv \quad n \,\&\, k \;=\; k$$

where & is the *bitwise and* operator.



(a) First 16 rows of Pascal's triangle

(b) Sierpiński's triangle (level 4)

Figure 5: Pascal's and Sierpiński's triangles

5.2. Sierpiński's triangle in the Eisenstein-Stern and Stern-Brocot trees

The question that we propose to address here is: can we construct Sierpiński's triangle from the Eisenstein-Stern tree or from the Stern-Brocot tree? The challenge is to decide how to colour a given node based solely on the rational that the node contains.

The first step we need to take is to identify suitable triangular shapes within the trees. The two obvious choices are to consider only the nodes with paths $\mathbf{L}^n\mathbf{R}^k$ or the nodes with paths $\mathbf{R}^n\mathbf{L}^k$, both with $k<n$. The triangles obtained from these nodes are illustrated in Figure 6. Focusing first on the triangle made of nodes with paths $\mathbf{L}^n\mathbf{R}^k$, we note that

$$\mathbf{L}^n\mathbf{R}^k = \begin{pmatrix} 1 & k \\ n & nk+1 \end{pmatrix}$$

Because we have the values of n and k in the antidiagonal of these matrices, we can immediately use Lucas's theorem to obtain Sierpiński's triangle from the tree of matrices[4]:

$$\begin{array}{rcl} \mathit{black}(\left(\begin{smallmatrix} 1 & k \\ n & nk+1 \end{smallmatrix}\right)) & \Leftarrow & n \leftharpoondown k \\ \mathit{white}(\left(\begin{smallmatrix} 1 & k \\ n & nk+1 \end{smallmatrix}\right)) & \Leftarrow & n \not\leftharpoondown k \end{array}$$

The predicate $\mathit{black}(x)$ (respectively, $\mathit{white}(x)$) can be defined as "the colour of node x is black" (respectively, white), where x is either a matrix or a rational. Moreover, since $\mathbf{L}^n\mathbf{R}^k$ corresponds to the rational $\frac{k(n+1)+1}{n+1}$ in the Eisenstein-Stern tree we can easily decide when to colour a rational black or white:

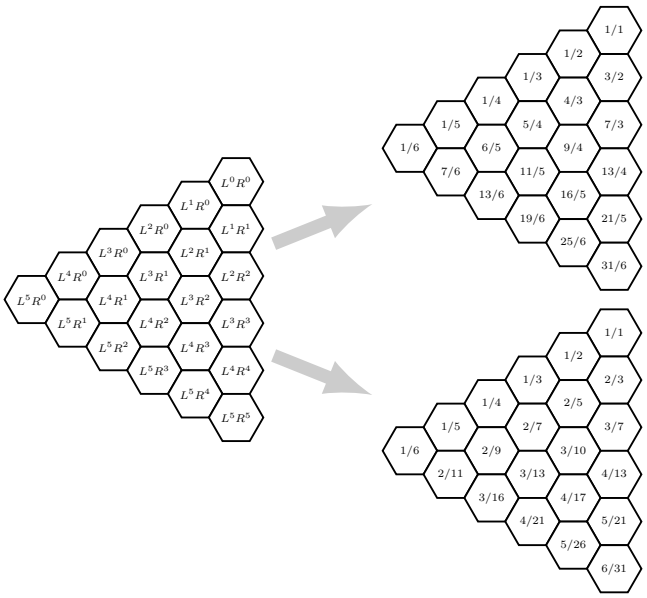
$$\begin{array}{rcl} \mathit{black}(\frac{x}{y}) & \Leftarrow & y{-}1 \leftharpoondown (x{-}1)/y \\ \mathit{white}(\frac{x}{y}) & \Leftarrow & y{-}1 \not\leftharpoondown (x{-}1)/y \end{array}$$

Similarly, we have the following for the Stern-Brocot tree:

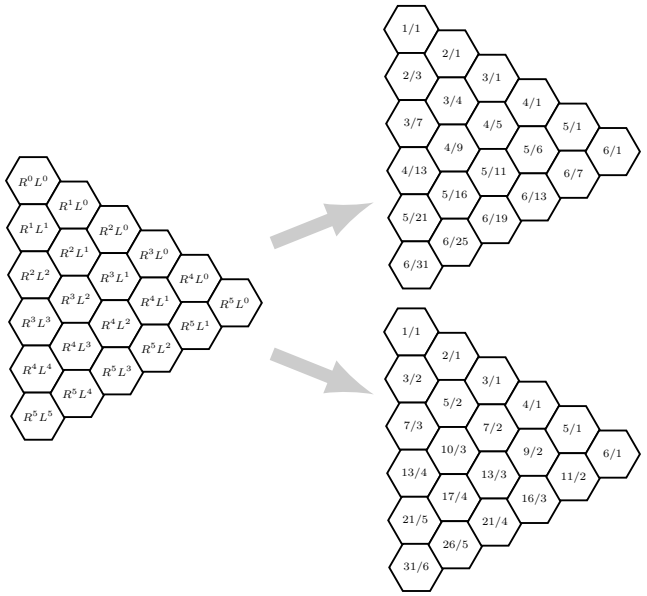
$$\begin{array}{rcl} \mathit{black}(\frac{x}{y}) & \Leftarrow & (y{-}1)/x \leftharpoondown x{-}1 \\ \mathit{white}(\frac{x}{y}) & \Leftarrow & (y{-}1)/x \not\leftharpoondown x{-}1 \end{array}$$

Figure 7 shows the result of applying the two rules above. We have similar results for the triangle made of

[4]Note that in Lucas's theorem the definition of $C(n,k)$ is irrelevant: the colouring is only dependent on the arguments n and k. That is why we can immediately apply the theorem to $\mathbf{L}^n\mathbf{R}^k$.



(a) Triangle with nodes of the shape $\mathbf{L}^n\mathbf{R}^k$ (left) and correspondent nodes in the Eisenstein-Stern (top right) and Stern-Brocot (bottom right) trees



(b) Triangle with nodes of the shape $\mathbf{R}^n\mathbf{L}^k$ (left) and correspondent nodes in the Eisenstein-Stern (top right) and Stern-Brocot (bottom right) tree

Figure 6: Possible triangles within the Eisenstein-Stern and Stern-Brocot trees

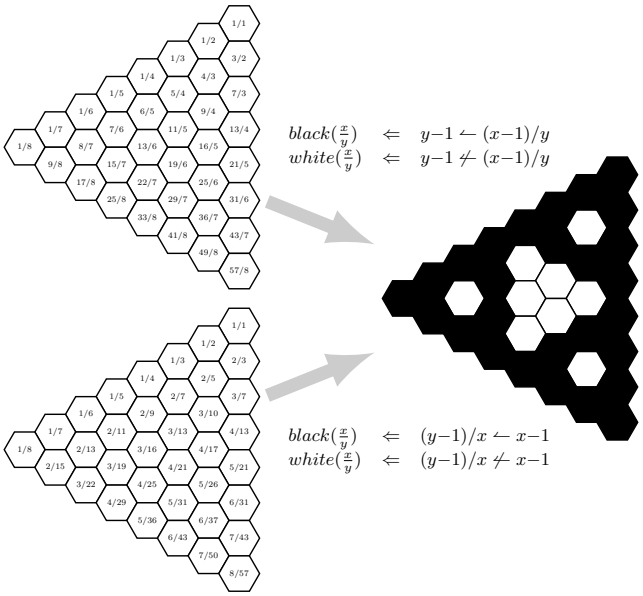


Figure 7: Linking nodes of the form $\mathbf{L}^n\mathbf{R}^k$ in the Eisenstein-Stern (top left) and Stern-Brocot (bottom left) trees with an approximation to Sierpiński's triangle

nodes with paths $\mathbf{R}^n\mathbf{L}^k$. The details are left as an exercise for the reader.

To conclude this section, we invite the reader to derive the results above using only the rationals of the Eisenstein-Stern and Stern-Brocot trees shown in Figure 7. For the authors, it is not obvious how to do it, since Lucas's theorem can not be directly applied. On the other hand, the extra information provided by the matrices makes a solution obvious!

6. Conclusion

We hope to have demonstrated that the calculational approach followed in this paper makes proofs more structured and simpler to follow (particularly, in the context of handwritten proofs). Together with the matrix formulation, the approach proposed certainly provides "*opportunities for creativity steps*": for example, from a simple definition of node invariance, we were able to calculate a new property of palindromic paths linking the Stern-Brocot and Eisenstein-Stern trees, with no guessing involved!

The natural interpretation of matrix products as paths and the extra information provided by matrices were key to formulate the new properties shown in Sections 4 and 5. We find appealing the idea of encoding more information into a concise structure that can be syntactically manipulated. It would be interesting to see whether we can use the approach presented here to prove other known properties of these trees and to discover new connections between them. For example, it would be good to investigate whether we could write a calculational proof of the properties relating the Eisenstein-Stern tree and the hyperbinary sequence [9]. Another interesting direction is to use the approach presented in this paper to prove properties about the Bird Tree [18]. Given a tree of matrices where left branching corresponds to post-multiplication by **LS** and right branching corresponds to post-multiplication by **RS**, the Bird tree can be obtained by post-multiplying each matrix by the vector $\binom{1}{1}$. Note that since Lemma 1 is still valid, Theorem 3 and its proof also apply to the Bird Tree! However, since $(\mathbf{LS})^T \neq \mathbf{RS}$, we do not have the same node invariance results. We leave this investigation as future work.

Another idea that deserves further investigation is the formulation of alternative criteria to colour the trees of rationals so that we obtain an approximation to Sierpiński triangle (e.g. criteria based on parity as in the example given for Pascal's triangle).

This paper is part of an endeavour which aims at reinvigorating mathematical content by adopting a calculational style of reasoning [6, 19, 14, 20, 21]. As suggested by the results shown in [22], the calculational method can indeed have a positive impact on mathematics education. However, in our view, the combination of practicality with mathematical elegance that arises from an adequate focus on calculational techniques can enrich and improve, not only mathematics education, but also the process of constructing computer programs. We plan to continue this effort not only by trying to find more properties of the Stern-Brocot, Eisenstein-Stern, and Bird trees, but also by investigating whether other areas of mathematics can be made more calculational. We are also building software tools that can help us write calculational proofs in a more reliable way; as an example, we are currently extending the structure editor described in [23] to support automated verification of handwritten calculational proofs.

Acknowledgements

Thanks to José Nuno Oliveira for inspiring us and for instilling into us the ability to appreciate the beauty of Mathematics and Computer Science. His contagious enthusiasm and passion continue to shape the work we do and will certainly have a great impact in the rest of our careers.

We would also like to thank Roland Backhouse, Jeremy Gibbons, and the anonymous referees for their helpful comments.

The LaTeX code used to produce the figures in Section 5 is based on code originally written by Paul Gaborit.

Appendix A. Omitted Proofs

Proof of Lemma 1 (page 6). We show that by using the equality

$$\mathsf{br}(\mathbf{M}) = \mathbf{S} \times \mathbf{M} \times \mathbf{S} \tag{A.1}$$

we have the same five cases as shown in Definition 1.

1. $\mathsf{br}(\mathbf{I})$
   $=$ { (A.1) }
   $\mathbf{S} \times \mathbf{I} \times \mathbf{S}$
   $=$ { arithmetic }
   $\mathbf{S}^2$
   $=$ { $\mathbf{S}^2 = \mathbf{I}$ }
   I

2. $\mathsf{br}(\mathbf{L})$
   $=$ { (A.1) and definition of $\mathbf{L}$ }
   $\mathbf{S} \times \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \times \mathbf{S}$
   $=$ { arithmetic }
   $\mathbf{S} \times \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$
   $=$ { arithmetic }
   $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$
   $=$ { definition of $\mathbf{R}$ }
   $\mathbf{R}$

3. $\mathsf{br}(\mathbf{R})$
   $=$ { (A.1) and definition of $\mathbf{R}$ }

$$
\begin{array}{ll}
 & \mathbf{S} \times \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \times \mathbf{S} \\
= & \quad \{ \text{ arithmetic } \} \\
 & \mathbf{S} \times \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \\
= & \quad \{ \text{ arithmetic } \} \\
 & \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \\
= & \quad \{ \text{ definition of } \mathbf{L} \ \} \\
 & \mathbf{L}
\end{array}
$$

For the two remaining cases, we assume that $\mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

4.
$$
\begin{array}{ll}
 & \mathsf{br}(\mathbf{L} \times \mathbf{M}) \\
= & \quad \{ \text{ arithmetic } \} \\
 & \mathsf{br}(\left(\begin{smallmatrix} a & b \\ a+c & b+d \end{smallmatrix}\right)) \\
= & \quad \{ \text{ (A.1) and arithmetic } \} \\
 & \left(\begin{smallmatrix} b+d & a+c \\ b & a \end{smallmatrix}\right) \\
= & \quad \{ \text{ arithmetic } \} \\
 & \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} d & c \\ b & a \end{smallmatrix}\right) \\
= & \quad \{ \text{ definition of } \mathbf{R} \text{ and arithmetic } \} \\
 & \mathbf{R} \times \mathbf{S} \times \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \times \mathbf{S} \\
= & \quad \{ \text{ (A.1) } \} \\
 & \mathbf{R} \times \mathsf{br}(\mathbf{M})
\end{array}
$$

5.
$$
\begin{array}{ll}
 & \mathsf{br}(\mathbf{R} \times \mathbf{M}) \\
= & \quad \{ \text{ arithmetic } \} \\
 & \mathsf{br}(\left(\begin{smallmatrix} a+c & b+d \\ c & d \end{smallmatrix}\right)) \\
= & \quad \{ \text{ (A.1) and arithmetic } \} \\
 & \left(\begin{smallmatrix} d & c \\ b+d & a+c \end{smallmatrix}\right) \\
= & \quad \{ \text{ arithmetic } \} \\
 & \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} d & c \\ b & a \end{smallmatrix}\right) \\
= & \quad \{ \text{ definition of } \mathbf{L} \text{ and arithmetic } \} \\
 & \mathbf{L} \times \mathbf{S} \times \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \times \mathbf{S} \\
= & \quad \{ \text{ (A.1) } \} \\
 & \mathbf{L} \times \mathsf{br}(\mathbf{M})
\end{array}
$$

□

The following lemma is used in the proof of Lemma 2.

Lemma 4. *Let* $\mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. *Then:*

$$\mathbf{M} = \mathbf{M}^T \ \equiv \ b = c$$

Proof of Lemma 4.

$$
\begin{array}{ll}
 & \mathbf{M} = \mathbf{M}^T \\
= & \quad \{ \text{ definition of } \mathbf{M} \text{ and } \mathbf{M}^T \ \}
\end{array}
$$

$$
\begin{array}{ll}
& \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \\
= & \quad \{ \text{ arithmetic } \} \\
& a = a \ \wedge \ b = c \ \wedge \ c = b \ \wedge \ d = d \\
= & \quad \{ \text{ reflexivity and symmetry of equality; idempotence of conjunction } \} \\
& b = c
\end{array}
$$

□

Proof of Lemma 2 (page 7). Let $\mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then:

$$
\begin{array}{ll}
& \mathbf{M} \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \mathbf{M}^T \times \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \\
= & \quad \{ \ \mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) ; \text{ arithmetic } \} \\
& \left(\begin{smallmatrix} a+b \\ c+d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+c \\ b+d \end{smallmatrix}\right) \\
= & \quad \{ \text{ arithmetic } \} \\
& a + b = a + c \quad \wedge \quad c + d = b + d \\
= & \quad \{ \text{ arithmetic } \} \\
& b = c \ \wedge \ c = b \\
= & \quad \{ \text{ symmetry of equality and idempotence of conjunction } \} \\
& b = c \\
= & \quad \{ \text{ Lemma 4 } \} \\
& \mathbf{M} = \mathbf{M}^T
\end{array}
$$

□

Proof of Lemma 3 (page 8). Let $\mathbf{P} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then:

$$
\begin{array}{ll}
& \mathbf{M} = \mathbf{P} \times \mathbf{P}^T \\
= & \quad \{ \ \mathbf{P} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \ \} \\
& \mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \times \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \\
= & \quad \{ \text{ arithmetic } \} \\
& \mathbf{M} = \left(\begin{smallmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{smallmatrix}\right) \\
\Rightarrow & \quad \{ \text{ definition of transpose } \} \\
& \mathbf{M} = \mathbf{M}^T
\end{array}
$$

□

References

[1] J. N. Oliveira, An introduction to pointfree programming, chapter of book in preparation (1999).
URL http://www4.di.uminho.pt/~jno/html/jnopub.html

[2] J. N. Oliveira, C. J. Rodrigues, Pointfree factorization of operation refinement, in: J. Misra, T. Nipkow, E. Sekerinski (Eds.), FM 2006: Formal Methods, 14th International Symposium on Formal Methods, Hamilton, Canada, August 21-27, 2006, Proceedings, Vol. 4085 of Lecture Notes in Computer Science, Springer, 2006, pp. 236–251. doi:10.1007/11813040_17.
URL http://dx.doi.org/10.1007/11813040_17

[3] J. N. Oliveira, Transforming data by calculation, in: R. Lämmel, J. Visser, J. Saraiva (Eds.), Generative and Transformational Techniques in Software Engineering II, International Summer School, GTTSE 2007, Braga, Portugal, July 2-7, 2007. Revised Papers, Vol. 5235 of Lecture Notes in Computer Science, Springer, 2007, pp. 134–195. doi:10.1007/978-3-540-88643-3_4.
URL http://dx.doi.org/10.1007/978-3-540-88643-3_4

[4] J. N. Oliveira, A relation-algebraic approach to the "Hoare logic" of functional dependencies, J. Log. Algebr. Meth. Program. 83 (2) (2014) 249–262. doi:10.1016/j.jlap.2014.02.013.
URL http://dx.doi.org/10.1016/j.jlap.2014.02.013

[5] R. Backhouse, J. F. Ferreira, Recounting the rationals: Twice!, in: Mathematics of Program Construction, Vol. 5133 of LNCS, Springer-Verlag, 2008, pp. 79–91.
URL http://joaoff.com/publications/2008/rationals
[6] R. Backhouse, J. F. Ferreira, On Euclid's algorithm and elementary number theory, Sci. Comput. Program. 76 (3) (2011) 160–180. doi:10.1016/j.scico.2010.05.006.
URL http://joaoff.com/publications/2010/euclid-alg
[7] M. A. Stern, Über eine zahlentheoretische Funktion, Journal für die reine und angewandte Mathematik 55 (1858) 193–220.
[8] R. L. Graham, D. E. Knuth, O. Patashnik, Concrete Mathematics: a Foundation for Computer Science, 2nd Edition, Addison-Wesley Publishing Company, 1994.
[9] N. Calkin, H. S. Wilf, Recounting the rationals, The American Mathematical Monthly 107 (4) (2000) 360–363.
[10] J. Gibbons, D. Lester, R. Bird, Enumerating the rationals, Journal of Functional Programming 16 (3) (2006) 281–291.
[11] D. E. Knuth, C. Rupert, A. Smith, R. Stong, Recounting the rationals, continued, American Mathematical Monthly 110 (7) (2003) 642–643.
[12] M. Aigner, G. Ziegler, Proofs From The Book, 3rd Edition, Springer-Verlag, 2004.
[13] B. Bates, M. Bunder, K. Tognetti, Linking the Calkin-Wilf and Stern-Brocot trees, European Journal of Combinatorics 31 (7) (2010) 1637 – 1661. doi:http://dx.doi.org/10.1016/j.ejc.2010.04.002.
URL http://www.sciencedirect.com/science/article/pii/S019566981000048X
[14] J. F. Ferreira, Designing an algorithmic proof of the two-squares theorem, in: C. Bolduc, J. Desharnais, B. Ktari (Eds.), Mathematics of Program Construction, Vol. 6120 of LNCS, Springer-Verlag, 2010, pp. 140–156.
URL http://joaoff.com/publications/2010/sum-two-squares
[15] I. Stewart, Game, Set and Math. Enigmas and Conundrums., Penguin Books, 1991.
[16] G. J. Chaitin, Algorithmic Information Theory, Cambridge University Press, New York, NY, USA, 1987.
[17] D. E. Knuth, The Art of Computer Programming, Vol. 4a: Combinatorial Algorithms (Part 1), Addison-Wesley, 2011.
[18] R. Hinze, The Bird tree, J. Funct. Program. 19 (5) (2009) 491–508. doi:10.1017/S0956796809990116.
URL http://dx.doi.org/10.1017/S0956796809990116
[19] J. F. Ferreira, A. Mendes, R. Backhouse, L. S. Barbosa, Which mathematics for the information society?, in: Teaching Formal Methods, Vol. 5846 of LNCS, Springer-Verlag, 2009, pp. 39–56.
URL http://joaoff.com/publications/2009/which-mathis
[20] J. F. Ferreira, Principles and applications of algorithmic problem solving, Ph.D. thesis, School of Computer Science, University of Nottingham (2010).
[21] J. F. Ferreira, A. Mendes, A. Cunha, C. Baquero, P. F. Silva, L. S. Barbosa, J. N. Oliveira, Logic training through algorithmic problem solving, in: P. Blackburn, H. van Ditmarsch, M. Manzano, F. Soler-Toscano (Eds.), Tools for Teaching Logic - Third International Congress, TICTTL 2011, Salamanca, Spain, June 1-4, 2011. Proceedings, Vol. 6680 of Lecture Notes in Computer Science, Springer, 2011, pp. 62–69. doi:10.1007/978-3-642-21350-2_8.
URL http://dx.doi.org/10.1007/978-3-642-21350-2_8
[22] J. F. Ferreira, A. Mendes, Students' feedback on teaching mathematics through the calculational method, in: 39th IEEE Frontiers in Education Conference, 2009. FIE '09., 2009, pp. 1–6.
URL http://joaoff.com/publications/2009/feedback-calculational
[23] A. Mendes, R. C. Backhouse, J. F. Ferreira, Structure editing of handwritten mathematics: Improving the computer support for the calculational method, in: R. Dachselt, T. C. N. Graham, K. Hornbæk, M. A. Nacenta (Eds.), Proceedings of the Ninth ACM International Conference on Interactive Tabletops and Surfaces, ITS 2014, Dresden, Germany, November 16 - 19, 2014, ACM, 2014, pp. 139–148. doi:10.1145/2669485.2669495.
URL http://doi.acm.org/10.1145/2669485.2669495