

SRT Division Algorithms As Dynamical Systems

Mark McCann* and Nicholas Pippenger†

Department of Computer Science

The University of British Columbia

Vancouver, British Columbia, Canada, V6T 1Z4

mccann@cs.ubc.ca nicholas@cs.ubc.ca

Abstract

SRT division, as it was discovered in the late 1950s represented an important improvement in the speed of division algorithms for computers at the time. A variant of SRT division is still commonly implemented in computers today. Although some bounds on the performance of the original SRT division method were obtained, a great many questions remained unanswered. In this paper, the original version of SRT division is described as a dynamical system. This enables us to bring modern dynamical systems theory, a relatively new development in mathematics, to bear on an older problem. In doing so, we are able to show that SRT division is ergodic, and is even Bernoulli, for all real divisors and dividends. With the Bernoulli property, we are able to use entropy to prove that the natural extensions of SRT division are isomorphic by way of the Kolmogorov-Ornstein Theorem. We demonstrate how our methods and results can be applied to a much larger class of division algorithms.

1 Introduction

Since the discovery of the first radix-2 SRT division algorithm, the use of the term “SRT division” has expanded to include a wide variety of higher radix non-restoring division algorithms that are loosely based on the original. For example, there is the infamous implementation of a radix-4 SRT division algorithm in the first release of the Pentium™ CPU that has become widely known as the “Pentium™ Bug.” One major difference between this implementation of radix-4 SRT division and the original radix-2 SRT division is that the former produces a constant number of quotient bits per step, while the latter produces a variable number. Modern implementations of SRT division use carry-save adders to perform additions and subtractions in constant time. Earlier implementations, however, used carry-propagate adders with delays that grow with the word length. Therefore, the primary goal of the early investigators was to reduce the

number of uses of the costly adder. In the late 1950’s, Sweeney [3], Robertson [16], and Tocher [20] independently made the observation that whenever a partial remainder is in the range $(-\frac{1}{2}, \frac{1}{2})$, there will be one or more leading zeros that can be shifted through in a very short amount of time (usually one cycle) thereby reducing the use of the adder. Although the aforementioned have received most of the credit for the algorithm which is named after them, it can be argued that Nadler described an equivalent algorithm in a 1956 paper [12]. The description of higher-radix SRT division which is the basis for modern SRT division is generally attributed to Atkins [1], but this is not the version of division that we will be concerned with in this paper.

Although what is considered to be “costly” for a division algorithm has changed, it is still interesting and important to understand the behaviour of successive partial remainders on average for a given divisor. Surprisingly, some of the most basic questions that one might have concerning the behaviour of partial remainders for even simple radix-2 SRT division have remained unanswered for over forty years. The difficulty that early investigators experienced in answering such questions was mainly due to a lack of necessary mathematical tools and results. During that past thirty years, the field of “dynamical systems theory” or “ergodic theory” has come into existence in mathematics and has been greatly developed. In this paper we show how to apply some of what is now known in dynamical systems theory to the earliest version of SRT division. In doing so, we are able to prove several previously unknown properties for simple SRT division. The results are quite general and lend themselves to be adapted to other division algorithms. For the remainder of this paper, the term SRT division will refer to the original algorithm unless otherwise stated.

The SRT division algorithms analyzed by Freiman [4] and Shively [19] are the same, but the authors differ in what they take to be a step of the algorithm: Freiman defines a step to be the operations from one use of the adder to the next, while Shively defines it to be the operations from one normalizing shift (of a single place) to the next. The following definitions are consistent with Shively’s:

- (a) n represents the number of iterations performed in the algorithm.
- (b) p_0 is the dividend (or initial partial remainder) normal-

*The work reported here was supported by an NSERC Research Grant.

†The work reported here was supported by an NSERC Research Grant and a Canada Research Chair.

ized so that $p_0 \in [\frac{1}{2}, 1)$.

- (c) $p_i \in (-1, 1)$, $i \in \mathbb{N}$, is the partial remainder after the i th step.
- (d) D is the divisor normalized to $[\frac{1}{2}, 1)$.
- (e) $q_i \in \{-1, 0, 1\}$ ($i \in \{0, \dots, n-1\}$) is the quotient digit generated by the i th step.
- (f) $Q_n = \sum_{i=0}^{n-1} \frac{q_i}{2^i}$ is the “rounded off” quotient generated after n steps of the algorithm.

Given the above definitions, after n steps of the division algorithm, we would like it to be true that

$$p_0 = DQ_n + \varepsilon(n)$$

where $\varepsilon(n)$ is a term that goes to zero as n goes to infinity.

A recurrence relation for the SRT division algorithm can be stated as

$$p_{i+1} = \begin{cases} 2p_i & : |p_i| < \frac{1}{2} \\ 2(p_i - D) & : |p_i| \geq \frac{1}{2} \text{ and } p_i \geq 0 \\ 2(p_i + D) & : |p_i| \geq \frac{1}{2} \text{ and } p_i < 0, \end{cases}$$

and

$$q_i = \begin{cases} 0 & : |p_i| < \frac{1}{2} \\ 1 & : |p_i| \geq \frac{1}{2} \text{ and } p_i \geq 0 \\ -1 & : |p_i| \geq \frac{1}{2} \text{ and } p_i < 0. \end{cases}$$

By observing that

$$p_{i+1} = \begin{cases} 2(p_i - (0)D) & : |p_i| < \frac{1}{2} \\ 2(p_i - (1)D) & : |p_i| \geq \frac{1}{2} \text{ and } p_i \geq 0 \\ 2(p_i - (-1)D) & : |p_i| \geq \frac{1}{2} \text{ and } p_i < 0, \end{cases}$$

we can rewrite the definition of p_{i+1} as

$$p_{i+1} = 2(p_i - q_i D).$$

After n steps have been completed, we have

$$p_n = 2^n p_0 - 2^n q_0 D - 2^{n-1} q_1 D - \dots - 2^1 q_{n-1} D,$$

and then after dividing by 2^n and solving for p_0 we find that

$$\begin{aligned} p_0 &= \frac{p_n}{2^n} + \frac{q_0 D}{2^0} + \frac{q_1 D}{2^1} + \dots + \frac{q_{n-1} D}{2^{n-1}} \\ &= D \sum_{i=0}^{n-1} \frac{q_i}{2^i} + \frac{p_n}{2^n} = DQ_n + \frac{p_n}{2^n}. \end{aligned}$$

Now let $\varepsilon(n) = p_n/2^n$ and let $Q^* = \lim_{n \rightarrow \infty} Q_n$. Since $|p_n| < 1$, in the limit as n goes to infinity

$$p_0 = DQ^*.$$

The quotient bits being generated are not in a standard binary representation, but it is a simple matter to convert

the answer back to standard binary on-the-fly without using any expensive operations.

Table 1 shows an example of using the SRT division algorithm to divide 0.67 by 0.75. The steps that produce non-zero quotient bits have been shown. In this example, after six uses of the adder, the quotient (0.893) has been determined to four digits of precision.

Table 1. SRT division example

$p_0 = 0.67$	$= 0.67$	$Q_0 = 1$
$p_1 = 2(0.67 - D)$	$= -0.16$	$Q_3 = 0.875$
$p_4 = 2(2^2(-0.16) + D)$	$= 0.22$	$Q_6 = 0.890625$
$p_7 = 2(2^2(0.22) - D)$	$= 0.26$	$Q_8 = 0.89453125$
$p_9 = 2(2^1(0.26) - D)$	$= -0.46$	$Q_{10} = 0.893554688$
$p_{11} = 2(2^1(-0.46) + D)$	$= -0.34$	$Q_{12} \doteq 0.893310547$
$p_{13} = 2(2^1(-0.34) + D)$	$= 0.14$	

Now, with this simple system of division in hand, we might want to ask certain questions about its performance. For example, we could ask “How many bits of precision are generated per iteration of the algorithm on average?” To answer this question, we must look at the magnitude of $|Q^* - Q_n| = |p_n/2^n|$. The number of bits of precision on the n th step is then $n - \log_2 p_n$. In the worst case, p_n is close to 1, and therefore we get at least one bit of precision per iteration of the algorithm, regardless of the values of D or p_0 . Of course, a designer of actual floating-point hardware probably wants to know the expected performance based on the expected values of p_n . To answer the many variants of this type of question, it is clear that we must know something about the distribution of partial remainders over time. The remainder of this paper is devoted to extending what is known about the answer to this type of question as it relates to SRT division and its variants.

2 SRT Division as a Dynamical System

The example in table 1 makes it clear that keeping track of the signs of successive partial remainders is irrelevant in determining how many times the adder will be used for a particular calculation. For this reason, we only need to consider the magnitudes of successive partial remainders. We now give a reformulation of SRT division that will allow us to look at division as a dynamical system.

Definition 1 (SRT Division Transformation). For $D \in [\frac{1}{2}, 1)$, we define the function $T_D : [0, 1) \rightarrow [0, 1)$ as

$$T_D(x) = \begin{cases} 2x & : 0 \leq x < \frac{1}{2} \\ 2(D - x) & : \frac{1}{2} \leq x < D \\ 2(x - D) & : D \leq x < 1. \end{cases}$$

This transformation of the unit interval represents the successive partial remainders that arise as SRT division is carried out by a divisor D on a dividend x . D is normalized to $[\frac{1}{2}, 1)$. The dividend x is normalized to $[\frac{1}{2}, 1)$ initially, while each of the successive partial remainders $T_D^n(x)$ ($n \in \mathbb{N}$) subsequently ranges through $[0, 1)$.

By using the characteristic function for a set Δ defined as

$$1_{\Delta}(x) = \begin{cases} 1 & : x \in \Delta \\ 0 & : x \notin \Delta, \end{cases}$$

we can rewrite T_D as

$$T_D(x) = 2x \cdot 1_{[0, \frac{1}{2})}(x) + 2(D - x) \cdot 1_{[\frac{1}{2}, D)}(x) + 2(x - D) \cdot 1_{[D, 1)}(x). \quad (1)$$

If we plot (1) on the unit interval, we obtain a very useful visualization of our transformation. Figure 1 shows the plot of $T_{0.75}(x)$ combined with a plot of the successive partial remainders that arise while dividing 0.67 by 0.75. The heavy solid lines represent the transformation $T_{0.75}$, while the abscissa of the thin vertical lines represent successive partial remainder magnitudes. This is the same system that was presented earlier in table 1. Notice that a vertical line in the interval $[\frac{1}{2}, D)$ corresponds to a subsequent flip in the sign of the next partial remainder.

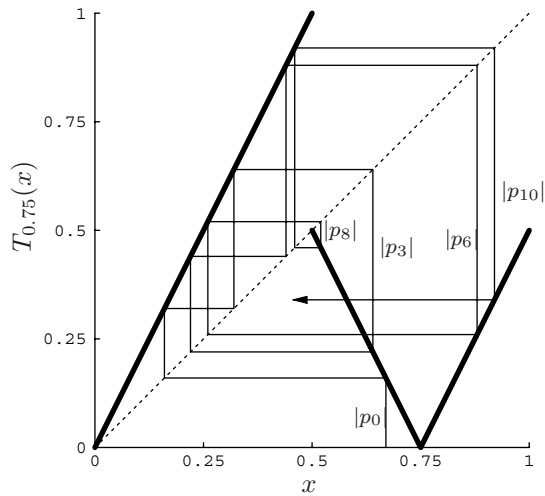


Figure 1. Following partial remainder magnitudes graphically for $D = 0.75$ and $p_0 = 0.67$.

Figure 1 shows an example of following the trajectory of a single partial remainder for a particular divisor. After ten applications of the $T_{0.75}$, there is not any obvious regular pattern, although we expect to see one eventually since the quotient is rational in this case*. Of course, most numbers are not rational and we can deduce that for most numbers, the transformation will never exhibit a repeating pattern. In figures 2 and 3, we see that a very small change in the value of the initial partial remainder quickly produces large differences in the observed behaviour of the subsequent partial remainders. Our system appears to be chaotic (it certainly has sensitive dependence on initial conditions and is topologically transitive), and, if this the case, we will gain little understanding by studying the trajectories of individual partial remainders. The logical next step is to study the behaviour of distributions of points over the whole interval.

*With redundant representations, rational numbers can have aperiodic representations, though we do not expect this to happen.

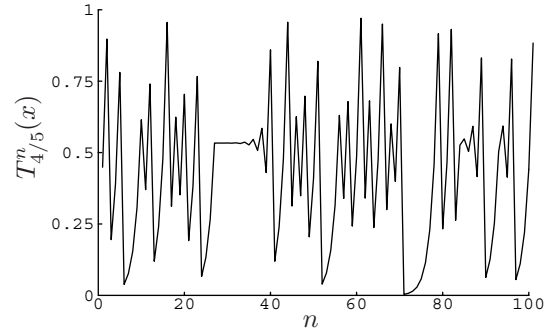


Figure 2. The result of applying $T_{4/5}$ to $x = \frac{\pi}{7}$ one hundred times.

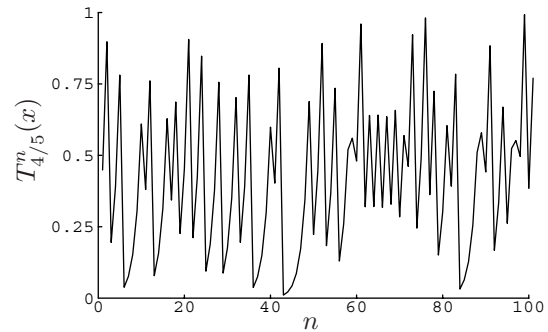


Figure 3. The result of applying $T_{4/5}$ to $x = \frac{\pi}{7} + 0.00001$ one hundred times.

The area of understanding the behaviour of ensembles of points under repeated transformation is the realm of dynamical systems theory. For the remainder of this paper, we assume a certain amount of familiarity with the fundamentals of dynamical systems theory (or ergodic theory), which requires some basic understanding of measure theory. We will include a few helpful background material definitions, but mostly we will provide references. A very good introduction to the study of chaotic systems is Lasota and Mackey's book *Chaos, Fractals, and Noise* [7]. For a more detailed introduction to ergodic theory (along with the necessary measure theory needed to understand this paper), Peter Walters's book *An Introduction to Ergodic Theory* [21] and Karl Petersen's book *Ergodic Theory* [15] are highly recommended.

Definition 2 (Probability Space). If \mathcal{B} is a σ -algebra on subsets of a set X and if m is a measure on \mathcal{B} where $m(X) = 1$, then the triple (X, \mathcal{B}, m) is called a *probability space*. (See [21, pp. 3–9] and [7, pp. 19–31] for a good overview of basic measure theory and Lebesgue integration.)

Definition 3 (Perron-Frobenius operator). For a probability space $(X, \mathcal{B}, m)^\dagger$, the *Perron-Frobenius operator* $P : L^1 \rightarrow L^1$ associated with a non-singular transformation $T : X \rightarrow X$ is defined by

[†]For a probability space (X, \mathcal{B}, m) , the L^1 space of (X, \mathcal{B}, m) is the set of $f : X \rightarrow \mathbb{R}$ satisfying $\int_X |f(x)| dm < \infty$.

$$\int_B Pf(x) dm = \int_{T^{-1}(B)} f(x) dm, \quad \text{for } B \in \mathcal{B}.$$

For a piecewise monotonic $C^{2\ddagger}$ transformation T with n monotonic pieces, we can give an explicit formula for the Perron-Frobenius operator. Let $A = \{A_1, A_2, \dots, A_n\}$ be the partition of X which separates T into n pieces. For $i \in \{1, \dots, n\}$, let $t_i(x)$ represent the natural extension of the i th C^2 function $T(x)|_{A_i}$. The Perron-Frobenius operator for T is then

$$Pf(x) = \sum_{i=1}^n \left| \frac{d}{dx} t_i^{-1}(x) \right| f(t_i^{-1}(x)) \cdot 1_{t_i(A_i)}(x).$$

In particular, for T_D (as in (1)),

$$\begin{aligned} Pf(x) &= \frac{1}{2}f\left(\frac{1}{2}x\right) \cdot 1_{[0,1)}(x) \\ &\quad + \frac{1}{2}f\left(D - \frac{1}{2}x\right) \cdot 1_{(0,2D-1)}(x) \\ &\quad + \frac{1}{2}f\left(D + \frac{1}{2}x\right) \cdot 1_{[0,2-2D)}(x). \end{aligned} \quad (2)$$

With (2) we can show precisely what happens to an initial distribution of points (described by an integrable function) after they are repeatedly transformed under T_D . Figures 4 and 5 show what happens to two different initial distribution of points after five applications of the Perron-Frobenius operator associated with $T_{3/5}(x)$. By the fifth application, the distributions look remarkably similar. One might guess that they are both approaching the same final distribution. This situation is in marked contrast to the chaotic behaviour observed in figures 2 and 3.

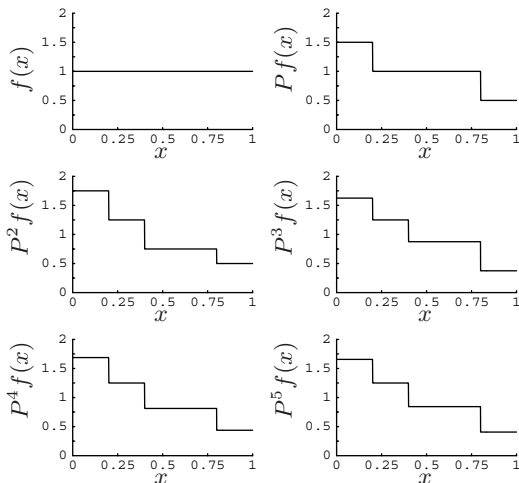


Figure 4. The result of applying the Perron-Frobenius operator P associated with $T_{3/5}$ to $f(x) = 1$ six times.

$\ddagger C^2$ denotes the set of all functions with two continuous derivatives.

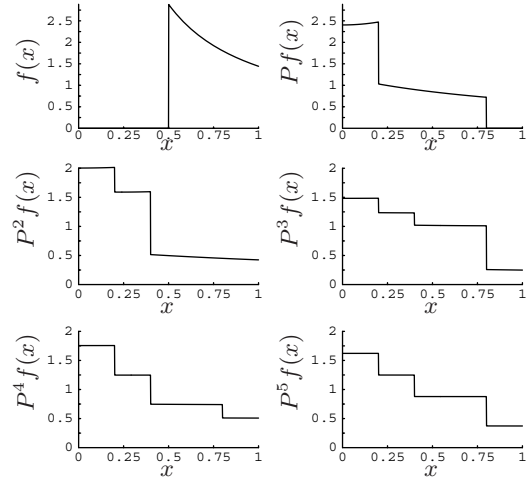


Figure 5. The result of applying the Perron-Frobenius operator P associated with $T_{3/5}$ to

$$f(x) = \frac{1}{\log 2} \int_{1/2}^1 \frac{dx}{x} \text{ six times.}$$

Definition 4 (Stationary Distribution). Let (X, \mathcal{B}, m) be a probability space, let P be the Perron-Frobenius operator associated with a non-singular transformation $T : X \rightarrow X$, and let L^1 denote the L^1 space of (X, \mathcal{B}, m) . If $f \in L^1$ is such that $Pf \stackrel{\circ}{=} f$,[§] then f is called a *stationary distribution* of T .

A practical use of the Perron-Frobenius operator is in deriving and verifying the equations of stationary distributions for given divisors. As an example of this we verify the correctness of a previously known stationary distribution for $D \in [\frac{3}{4}, 1)$. An exact equation for the stationary distribution when $D \in [\frac{3}{4}, 1)$ was first given by Freiman [4] and is restated by Shively [19] as

$$f(x) = \frac{1}{D} 1_{[0,2D-1)}(x) + \frac{1}{2D} 1_{[2D-1,1)}(x). \quad (3)$$

To verify that this is a stationary distribution function, we begin by applying the Perron-Frobenius operator as given in (2) to (3) and verifying that $Pf(x) \stackrel{\circ}{=} f(x)$. So then, applying P to f we get

$$\begin{aligned} Pf(x) &= \frac{1}{2} \left(\frac{1}{D} 1_{[0,2D-1)}\left(\frac{1}{2}x\right) + \right. \\ &\quad \left. \frac{1}{2D} 1_{[2D-1,1)}\left(\frac{1}{2}x\right) \right) 1_{[0,1)}(x) \\ &\quad + \frac{1}{2} \left(\frac{1}{D} 1_{[0,2D-1)}\left(D - \frac{1}{2}x\right) + \right. \\ &\quad \left. \frac{1}{2D} 1_{[2D-1,1)}\left(D - \frac{1}{2}x\right) \right) 1_{(0,2D-1)}(x) \\ &\quad + \frac{1}{2} \left(\frac{1}{D} 1_{[0,2D-1)}\left(D + \frac{1}{2}x\right) + \right. \\ &\quad \left. \frac{1}{2D} 1_{[2D-1,1)}\left(D + \frac{1}{2}x\right) \right) 1_{[0,2-2D)}(x). \end{aligned}$$

Assuming that $D \in [\frac{1}{2}, 1)$, and observing that $x \in [0, 1)$,

[§]The \circ symbol will be used to indicate that a given relation holds except possibly on a set of measure zero.

$$Pf(x) = \frac{1}{2} \left(\frac{1}{D} 1_{[0,4D-2)}(x) + \frac{1}{2D} 1_{[4D-2,1)}(x) \right) 1_{[0,1)}(x) + \frac{1}{2} \left(\frac{1}{D} 1_{(2-2D,1)}(x) + \frac{1}{2D} 1_{(0,2-2D)}(x) \right) 1_{(0,2D-1)}(x) + \frac{1}{2} \left(\frac{1}{2D} 1_{[0,2D-1)}(x) \right) 1_{[0,2-2D)}(x).$$

Finally, assuming that $D \in [\frac{3}{4}, 1)$, we have

$$Pf(x) = \frac{1}{2D} 1_{[0,1)}(x) + \frac{1}{2D} 1_{(2-2D,2D-1)}(x) + \frac{1}{4D} 1_{(0,2-2D)}(x) + \frac{1}{4D} 1_{[0,2-2D)}(x) = \frac{3}{4D} 1_{[0,2-2D)}(x) + \frac{1}{4D} 1_{(0,2-2D)}(x) + \frac{1}{2D} 1_{[2-2D,2D-1)}(x) + \frac{1}{2D} 1_{(2-2D,2D-1)}(x) + \frac{1}{2D} 1_{[2D-1,1)}(x) \doteq \frac{1}{D} 1_{[0,2D-1)}(x) + \frac{1}{2D} 1_{[2D-1,1)}(x) = f(x).$$

In the case of variable quotient-bits-per-cycle algorithms such as the original SRT division, one of the primary uses of a formula for the distribution of partial remainders is for calculating the *shift average* for a given divisor. The shift average is the average number uses of the shift register (single shift or multiplication by two) between uses of the adder. Under the assumption that a register shift is a much faster operation than using the adder, the shift average gives a useful characterization of the expected performance of our algorithm for a given divisor. With (3), we know the fraction of bits that require the use of the adder. To calculate the average number of zero bits generated between non-zero bits (bits requiring use of the adder), we take the reciprocal of the fraction of bits that require the adder. We calculate the shift average for a divisor $D \in [\frac{3}{4}, 1)$ to be

$$s(D) = \left(1 - \frac{1}{2D}\right)^{-1} = \frac{2D}{2D-1}. \quad (4)$$

Unfortunately, since we have not proven that the stationary distributions from SRT division are unique, we have no way of knowing whether or not the shift average calculation in (4) is correct. To prove that all stationary distributions are unique, we need to show that T_D is ergodic for all $D \in [\frac{1}{2}, 1)$. Freiman [4] shows that T_D is ergodic for rational D , but we extend this result to real D . In the next section we give a summary of our results from [10] that let us show that all T_D are Bernoulli. It is known that having the Bernoulli property implies ergodicity. Ergodicity is defined as follows:

Definition 5 (Ergodic [7]). Let (X, \mathcal{B}, m) be a probability space and let a nonsingular transformation $T : X \rightarrow X$ be given. Then T is *ergodic* if for every set $B \in \mathcal{B}$ such that $T^{-1}(B) = B$, either $m(B) = 0$ or $m(X \setminus B) = 0$.

3 Bernoulli Property

Our central result, which we present in this section, is that the class of transformations of the interval that characterizes SRT division for all real divisors D has the property that each transformation T_D is Bernoulli. Although

the basic concept of a Bernoulli shift (the things to which transformations having the Bernoulli property are isomorphic) is not difficult, a complete definition requires enough auxiliary concepts from measure theory (concepts not used anywhere else in this paper) that we chose to refer the interested reader to [14, 15, 18, 21]. Neither an understanding of Bernoulli shifts, nor a formal definition of what it means to be Bernoulli is required to follow our presentation. Having said this, we should mention informally the connection between Bernoulli shifts and transformations having the Bernoulli property.

The transformation T_D is a non-invertible endomorphism of the unit interval. This means that from a given partial remainder we can predict all future partial remainders, but we cannot uniquely predict past partial remainders. There is a natural way (called the natural extension) to make our transformation invertible (an automorphism) to a larger space. Specifically, each non-invertible transformation T_D having the Bernoulli property has an extension to an automorphic transformation, isomorphic to a two-sided Bernoulli shift [15, pp. 13,276]. From the way that entropy for a transformation is defined, the entropy for an automorphic Bernoulli transformation associated with a non-invertible Bernoulli transformation is the same as the entropy for the non-invertible Bernoulli transformation. By proving that all transformations T_D are Bernoulli, and by proving that entropy of each T_D is the same, we will be able to conclude that the natural extensions of SRT division algorithms are isomorphic to each other for all divisors.

Due to space limitations, we are unable to present our proofs in this paper. Instead, we will summarize our results and mention some of the external theorems that were central to our proofs. The omitted proofs and more results can be found in [10].

Our ability to prove that SRT division is Bernoulli, largely depends on the following two theorems of Bowen [2]:

Theorem 1 (of Bowen [2]). *Let T be a piecewise C^2 map of $[0, 1]$, μ be a smooth T -invariant probability measure, and $\lambda = \inf_{0 \leq x \leq 1} |f'(x)| > 1$. If the dynamical system (T, μ) is weak-mixing, then the natural extension of (T, μ) is Bernoulli.*

Theorem 2 (of Bowen [2]). *With T and μ as in Theorem 1, (T, μ) will be weak-mixing if T is expanding.*

With these theorems, we are only left to show that SRT division has the expanding property.

Definition 6 (of Bowen [2], Expanding). We will say that a transformation T on an interval is *expanding* if it has the property that $\sup_{n>0} \mu(T^n U) = 1$ for all open intervals U with $\mu(U) > 0$, where μ is any normalized measure that is absolutely continuous with respect to Lebesgue measure.

The definition for expanding allows us to focus on the behaviour of intervals of points, rather than having to worry about arbitrary sets of points with non-zero measure. In [10], we are able to show that that the following sequence of subsets of intervals is expanding:

$U_1 = U$ and

$$U_{i+1} = \begin{cases} T_D(U_i) & : U_i^\circ \subseteq [0, \frac{1}{2}) \text{ or } U_i^\circ \subseteq [\frac{1}{2}, 1) \\ T_D(U_i \cap [0, \frac{1}{2})) : U_i^\circ \not\subseteq [0, \frac{1}{2}) \text{ and } U_i^\circ \not\subseteq [\frac{1}{2}, 1) \\ \text{and } m(U_i \cap [0, \frac{1}{2})) \geq m(U_i \cap [\frac{1}{2}, 1)) \\ T_D(U_i \cap [\frac{1}{2}, 1)) : U_i^\circ \not\subseteq [0, \frac{1}{2}) \text{ and } U_i^\circ \not\subseteq [\frac{1}{2}, 1) \\ \text{and } m(U_i \cap [0, \frac{1}{2})) < m(U_i \cap [\frac{1}{2}, 1)). \end{cases}$$

$\{U_i\}_{i=1}^\infty$ is constructed by throwing away the smaller piece whenever an interval would be split in two by T_D . Since each $U_i \in \{U_i\}_{i=1}^\infty$ is a subset of the same set of intervals that arise by just repeatedly applying T_D to the same initial U , showing that $\{U_i\}_{i=1}^\infty$ eventually fills the entire interval X implies that T_D is expanding. The sequence $\{U_i\}_{i=1}^\infty$ greatly simplifies the analysis because intervals never become fragmented.

In order to show that T_D satisfies the other requirements of Bowen's theorems, we must show that there exists a measure μ , which is invariant under T_D . We were able to establish that all T_D have invariant measures from the following theorem of Lasota and Yorke [8]:

Theorem 3 (of Lasota and Yorke [8]). *Let (X, \mathcal{B}, m) be a probability space and let $T : X \rightarrow X$ be a piecewise C^2 function such that $\inf |T'| > 1$. If P is the Perron-Frobenius operator associated with T , then for any $f \in L^1$, the sequence $(\frac{1}{n} \sum_{k=0}^{n-1} P^k f)_{n=1}^\infty$ is convergent in norm to a function $f^* \in L^1$. The limit function f^* has the property that $Pf^* = f^*$ and consequently, the measure $d\mu^* = f^* dm$ is invariant under T .*

From the definition of T_D , we see that T_D is C^2 and that $\inf_{0 \leq x \leq 1} |T_D'(x)| = 2 > 1$ since $|T_D'(x)| = 2$ for all x for which the derivative is defined. By Theorem 3 we can conclude that there exists a smooth T_D -invariant probability measure μ . Given that T_D is expanding, we see that Theorem 2 holds. Hence, (T_D, μ) is weak-mixing and, by Theorem 1 (T_D, μ) is Bernoulli.

We mention here that the *natural extensions* of (T, μ) are the associated automorphic transformations that we alluded to at the beginning of this section. See Petersen [15, p. 13] for an exact definition.

Knowing that all T_D are Bernoulli is a very useful property because we can use entropy as a complete invariant to show isomorphism amongst the two-sided Bernoulli shifts associated with T_D that have the same entropy. This comes from the contribution of Ornstein to the Kolmogorov-Ornstein Theorem.

Theorem 4 (of Kolmogorov [5, 6] and Ornstein [13]). *Two Bernoulli shifts are isomorphic if and only if they have the same entropy.*

In general it can be very difficult to calculate the entropy for a class of transformations straight from the definition of entropy (see Walters, [21, pp. 75-87] for a definition of the entropy of a transformation). Even with the many standard formulas that have been derived for calculating entropy, a great number of systems found in practice are not covered. Simple SRT division is one such dynamical system that is

not easy to calculate the entropy for from results found in standard textbooks on ergodic theory. Fortunately, a result by Ledrappier [9] does allow us to calculate the entropy for simple SRT division. With Ledrappier's results, we are able to show that the following formula for entropy holds:

$$h(T_D) = \int \log |T_D'| d\mu = \log 2 \int d\mu = \log 2.$$

This formula was shown by Rohlin [17] to hold for a smaller class of transformations, which does not include the T_D associated with SRT division.

With the above results, we have established isomorphism amongst the automorphic transformations (or natural extensions) associated with simple SRT division transformations by an application of the Kolmogorov-Ornstein Theorem. The key to obtaining this result was being able to show that T_D has Bowen's expanding property. In Section 4, we extend the results of this section to a more general type of SRT division.

4 Multi-Threshold SRT Division

A simple optimization to the original SRT division algorithm, at least with the historical concern of avoiding additions and subtractions in mind, is the inclusion of additional divisors to increase the shift average. In this section, we give a summary of our proof that all such division algorithms with reasonable assumptions on the separation of the divisor multiples have the expanding property. We begin by giving a precise definition of the class of "multi-threshold" SRT transformations.

Definition 7. Let $\alpha \in \mathbb{R}^n$ be such that

- (a) $0 < \alpha_1 < \alpha_2 < \dots < \alpha_n$, and
- (b) For all $x, D \in [\frac{1}{2}, 1)$, there exists $i \in \{1, \dots, n\}$ such that $|\alpha_i D - x| < \frac{1}{2}$.

We define \mathfrak{A}_n to be the set of all $\alpha \in \mathbb{R}^n$, satisfying conditions (a) and (b). Also, $\mathfrak{A} = \bigcup_{n \in \mathbb{N}} \mathfrak{A}_n$.

Definition 8 (Peaks and Valleys). Given an $\alpha \in \mathfrak{A}_{n \geq 2}$, the point of intersection between two lines $f(x) = 2(x - \alpha_i D)$ and $g(x) = 2(\alpha_{i+1} D - x)$ will be called a *peak* and is denoted by $\psi_i = (\frac{1}{2}D(\alpha_{i+1} + \alpha_i), D(\alpha_{i+1} - \alpha_i))$. For convenience, we will refer to the abscissa as $\psi_i^x = \frac{1}{2}D(\alpha_{i+1} + \alpha_i)$, and to the ordinate as $\psi_i^y = D(\alpha_{i+1} - \alpha_i)$. The point of intersection of the two lines $f(x) = 2(\alpha_i D - x)$ and $g(x) = 2(x - \alpha_i D)$ is $(\alpha_i D, 0)$ and will be called a *valley*.

Definition 9. For a $D \in [\frac{1}{2}, 1)$ and $\alpha \in \mathfrak{A}$, define the transformation $T_{D, \alpha}(x) : [0, 1) \rightarrow [0, 1)$. For $\alpha \in \mathfrak{A}_1$, we get the familiar transformation

$$T_{D, \alpha}(x) = \begin{cases} 2x & : 0 \leq x < \frac{1}{2} \\ |2(D - x)| & : \frac{1}{2} \leq x < 1. \end{cases}$$

For $\alpha \in \mathfrak{A}_2$,

$$T_{D,\alpha}(x) = \begin{cases} 2x & : 0 \leq x < \frac{1}{2} \\ |2(\alpha_1 D - x)| & : \frac{1}{2} \leq x < \psi_1^x \\ |2(\alpha_2 D - x)| & : \frac{1}{2} \leq x \text{ and } \psi_1^x \leq x < 1. \end{cases}$$

For $\alpha \in \mathfrak{A}_{n \geq 3}$,

$$T_{D,\alpha}(x) = \begin{cases} 2x & : 0 \leq x < \frac{1}{2} \\ |2(\alpha_1 D - x)| & : \frac{1}{2} \leq x < \psi_1^x \\ |2(\alpha_i D - x)| & : \frac{1}{2} \leq x \text{ and } \psi_i^x \leq x < \psi_{i+1}^x \\ |2(\alpha_n D - x)| & : \frac{1}{2} \leq x \text{ and } \psi_{n-1}^x \leq x < 1. \end{cases}$$

Definition 10. Define $\mathfrak{M}_n = \{T_{D,\alpha} : D \in (\frac{1}{2}, 1], \alpha \in \mathfrak{A}_n\}$ and define $\mathfrak{M} = \bigcup_{n \in \mathbb{N}} \mathfrak{M}_n$. We call \mathfrak{M}_n the set of all n -threshold SRT division transformations and we call \mathfrak{M} the set of multi-threshold SRT division transformations.

Condition (b) in Definition 7 guarantees that the division algorithm generates a new quotient bit every step. In order to restrict the set of \mathfrak{M} begin considered, we make the following definition to place restrictions on the relative distance between divisor multiples:

Definition 11 (Separation). For $\alpha \in \mathfrak{A}_n$, we define the separation in α as

$$\text{separation}(\alpha) = \max_{i \in \{1, \dots, n-1\}} \frac{\alpha_{i+1}}{\alpha_i}.$$

If $\text{separation}(\alpha) = r$, we say that “the divisor multiples in α are separated by at most a factor of r .”

Table 2 shows an example dividing 0.67 by 0.75 using multi-threshold SRT division with $\alpha = (0.75, 1, 1.25)$. This example is performing the same calculation as in table 1, but it has computed the dividend with twice as many digits of precision with the same effective number of uses of the adders. We say “effective” because in multi-threshold SRT division, there are several adders working in parallel. In a real implementation of multi-threshold SRT division, the values for α must be carefully chosen so that not too much overhead is required to select a good partial remainder. There is also a tradeoff between the amount of overhead in choosing a good partial remainder and the precision to which a good partial remainder is selected.

Table 2. Multi-threshold SRT division example

$p_0 = 0.67$	$= 0.67$	$Q_0 = 1$
$p_1 = 2(0.67 - \alpha_2 D)$	$= -0.16$	$Q_3 = 0.90625$
$p_4 = 2(2^2(-0.16) + \alpha_1 D)$	$= -0.155$	$Q_6 = 0.89453125$
$p_7 = 2(2^2(-0.155) + \alpha_1 D)$	$= -0.115$	$Q_{10} \doteq 0.893310547$
$p_{11} = 2(2^3(-0.115) + \alpha_3 D)$	$= 0.035$	$Q_{15} \doteq 0.893333435$
$p_{16} = 2(2^4(0.035) - \alpha_1 D)$	$= -0.005$	$Q_{23} \doteq 0.893333346$
$p_{24} = 2(2^7(0.005) + \alpha_1 D)$	$= -0.155$	

By constructing a sequence of intervals similar to what was done for simple SRT division, we are able to prove that a multi-threshold SRT division transformation $T_{D,\alpha} \in \mathfrak{M}$ is expanding when $\text{separation}(\alpha) \leq \frac{5}{3}$. By making use

of Theorems 1, 2 and 3 from the previous section, it is straightforward to show that $T_{D,\alpha} \in \mathfrak{M}$ is Bernoulli when $\text{separation}(\alpha) \leq \frac{5}{3}$.

The calculation for entropy in multi-threshold SRT division follows the same method used for single divisor SRT division. Ledrappier’s results extend in the same way to multi-threshold SRT division, and we are able to show that the entropy of any $T_{D,\alpha} \in \mathfrak{M}$ with $\text{separation}(\alpha) \leq \frac{5}{3}$ is $\log 2$.

In [10] we proved that for all $T_{D,\alpha} \in \mathfrak{M}$, if $\text{separation}(\alpha) \leq \frac{5}{3}$, then $T_{D,\alpha}$ is Bernoulli. In [10] we prove that for $T_{D,\alpha} \in \mathfrak{M}_{n \geq 4}$, if $\text{separation}(\alpha) > \frac{5}{3}$, then for each $D \in [\frac{1}{2}, 1)$, there exist uncountably many α for which $T_{D,\alpha}$ is not ergodic. We also show that for $T_{D,\alpha} \in \mathfrak{M}_3$, with $\text{separation}(\alpha) \geq \frac{9}{5}$ there are examples of non-ergodic systems and similarly for $T_{D,\alpha} \in \mathfrak{M}_2$, $\text{separation}(\alpha) > 3$ there are non-ergodic systems. We do not provide the proofs here, but instead present figure 6 which demonstrates the existence of a large class of non-ergodic $T_{D,\alpha} \in \mathfrak{M}_{n \geq 4}$ when $\text{separation}(\alpha) > \frac{5}{3}$. In this example, $n = 4$, $D = \frac{11}{16}$, $\alpha = (\frac{37}{66}, \frac{21}{22}, 1, \frac{59}{33})$, and $\text{separation}(\alpha) = \frac{5}{3} + \frac{5}{51}$. The thick lines represent $T_{D,\alpha}$ and the coarse dashed line represents the necessary separation restriction on α to guarantee that $T_{D,\alpha}$ is ergodic. Partial remainders in the set $A = [\frac{11}{48}, \frac{13}{48}] \cup [\frac{22}{48}, \frac{26}{48}] \cup [\frac{44}{48}, 1)$ are mapped back to A by $T_{D,\alpha}$. This means that $T_{D,\alpha}$ is not ergodic, and therefore not Bernoulli.

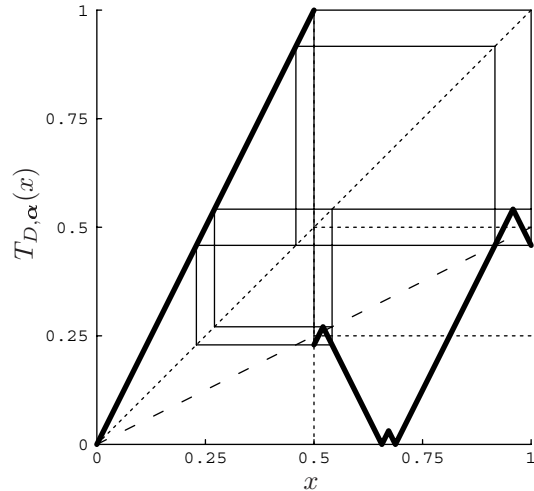


Figure 6. An example of a non-ergodic system for $T_{D,\alpha} \in \mathfrak{M}_{n \geq 4}$.

5 Conclusions

The original question that inspired this paper was “Is simple SRT division ergodic for all real divisors?” In pursuing the answer to this problem, we discovered that not only is simple SRT division ergodic for all divisors, but it is also Bernoulli. Having established a Bernoulli property, and having calculated the entropy for our transformations, we

were able to use the Kolmogorov-Ornstein theorem to conclude that our transformations are equivalent to each other in the sense that their natural extensions are isomorphic. In proving these important properties for simple SRT division, we made extensive use of more general results from dynamical systems theory. Consequently, our results were shown to be easily extensible to more general division systems. In general, it is difficult to prove that a particular class of transformations are ergodic or Bernoulli. Our results have provided an effective means of proving both of these properties for a large class of SRT-like division algorithms.

From the standpoint of understanding an algorithm's expected performance, it is necessary to know that when a stationary distribution is found, it is unique. Having established the uniqueness of stationary distributions, the next step is to find the actual stationary distribution for as wide a class of transformations as possible. In section 3, we verified a known expression for the stationary distribution function for T_D where $D \in [\frac{3}{4}, 1)$. In addition, many of the stationary distribution functions have been classified by Shively and Freiman for $D \in [\frac{3}{5}, \frac{3}{4}]$, although the derivations are not nearly as simple as for $D \in [\frac{3}{4}, 1)$. It turns out that things become very complicated when $D \in [\frac{1}{2}, \frac{3}{5}]$. In his thesis [19], Shively shows many interesting properties for the stationary distribution functions in this region. For example, he shows that there are many different intervals of D where there are an infinite number of different stationary distribution equations. As such, the graph of the shift average for $D \in [\frac{1}{2}, \frac{3}{5}]$ is far from complete and appears to have a complex pattern (from the few points that have been plotted in this region). This is surprising considering the simplicity of the underlying transformation. A better understanding of this final region of simple SRT division would be an interesting goal to pursue.

In the work of Freiman [4], it was first shown that the shift average for $D \in [\frac{3}{5}, \frac{3}{4}]$ is constantly 3, which can be easily shown to be the maximum possible shift average. This property was then used by Metze [11] to obtain a version of SRT division that has an expected shift average of 3 for all divisors. Another area to pursue would be to explore shift averages for multi-threshold SRT division and, if other plateaus are found, they could possibly be used to obtain higher expected shift averages for all possible divisors. Undoubtedly, obtaining a complete understanding of the stationary distribution functions for multi-threshold division would be even more difficult than it is for simple SRT division. It is possible that such results in this area could lead to improvements in modern SRT division. Related to this, it would be interesting to attempt to extend the results of this paper to modern SRT division.

References

- [1] D. E. Atkins. Higher-radix division using estimates of the divisor and partial remainders. *IEEE Trans. on Computers*, C-17(10), Oct. 1968.
- [2] R. Bowen. Bernoulli maps of the interval. *Israel J. Math.*, 28(1-2):161–168, 1977.

- [3] J. Cocke and D. W. Sweeney. High speed arithmetic in a parallel device. Technical report, IBM, February 1957.
- [4] C. V. Freiman. Statistical analysis of certain binary division algorithms. *Proc. IRE*, 49:91–103, 1961.
- [5] A. N. Kolmogorov. A new invariant for transitive dynamical systems. *Dokl. Akad. Nauk SSSR*, 119:861–864, 1958.
- [6] A. N. Kolmogorov. Entropy per unit time as a metric invariant of automorphisms. *Dokl. Akad. Nauk SSSR*, 124:754–755, 1959.
- [7] A. Lasota and M. C. Mackey. *Chaos, fractals, and noise*. Springer-Verlag, New York, second edition, 1994. Stochastic aspects of dynamics.
- [8] A. Lasota and J. A. Yorke. On the existence of invariant measures for piecewise monotonic transformations. *Trans. Amer. Math. Soc.*, 186:481–488 (1974), 1973.
- [9] F. Ledrappier. Some properties of absolutely continuous invariant measures on an interval. *Ergodic Theory Dynamical Systems*, 1(1):77–93, 1981.
- [10] M. McCann. S-R-T division algorithms as dynamical systems. Master's thesis, University of British Columbia, April 2002.
- [11] G. Metze. A class of binary divisions yielding minimally represented quotients. *IRE Trans. on Electronic Computers*, EC-11:761–764, Dec. 1961.
- [12] M. Nadler. A high-speed electronic arithmetic unit for automatic computing machines. *Acta Tech. (Prague)*, (6):464–478, 1956.
- [13] D. S. Ornstein. Bernoulli shifts with the same entropy are isomorphic. *Advances in Math.*, 4:337–352, 1970.
- [14] D. S. Ornstein. *Ergodic theory, randomness, and dynamical systems*. Yale University Press, New Haven, Conn., 1974. James K. Whittemore Lectures in Mathematics given at Yale University, Yale Mathematical Monographs, No. 5.
- [15] K. Petersen. *Ergodic theory*. Cambridge University Press, Cambridge, 1983.
- [16] J. E. Robertson. A new class of digital division methods. *IRE Trans. Electronic Computers*, EC-7:218–222, Sept. 1958.
- [17] V. A. Rohlin. Exact endomorphisms of a Lesbesgue space. *Amer. Math. Soc. Transl.*, 39, 1964.
- [18] P. Shields. *The theory of Bernoulli shifts*. The University of Chicago Press, Chicago, Ill.-London, 1973. Chicago Lectures in Mathematics.
- [19] R. Shively. *Stationary distribution of partial remainders in S-R-T digital division*. PhD thesis, University of Illinois, 1963.
- [20] K. D. Tocher. Techniques of multiplication and division for automatic binary computers. *Quart. J. Mech. Appl. Math.*, 11:364–384, July–September 1958.
- [21] P. Walters. *An introduction to ergodic theory*. Springer-Verlag, New York, 1982.