

HARVARD UNIVERSITY

DOCTORAL THESIS

---

# A Language of Polynomials

---

Author:  
Eric UNG

Supervisor:  
Dr. xxx xxx

*A thesis submitted in fulfillment of the requirements  
for the degree of Doctor of Philosophy  
in the*

Research Group Name  
Department or School Name

June 5, 2024



## Declaration of Authorship

I, Eric UNG, declare that this thesis titled, “A Language of Polynomials” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

---

Date:

---



*“Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism.”*

Dave Barry



HARVARD UNIVERSITY

*Abstract*

Faculty Name  
Department or School Name

Doctor of Philosophy

**A Language of Polynomials**

by Eric UNG

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...





## *Acknowledgements*

The acknowledgments and the people to thank go here, don't forget to include your project advisor...



# Contents

<b>Declaration of Authorship</b>	<b>iii</b>
<b>Abstract</b>	<b>vii</b>
<b>Acknowledgements</b>	<b>ix</b>
<b>1 A Language of Polynomials</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Foundations . . . . .	1
1.3 Monomial of One Variable . . . . .	3
1.4 Addition . . . . .	5
1.5 Product . . . . .	6
1.6 Problem with Matrices . . . . .	7
1.7 Multivariable Monomials . . . . .	7
1.8 Generalized Monomial Deciders . . . . .	9
1.9 Concentric Monomial Deciders . . . . .	10
1.10 Constants . . . . .	11
1.11 Division . . . . .	11
1.12 Multiple Divisions . . . . .	13
1.13 Equivalence . . . . .	14
1.14 Reversing . . . . .	14
1.15 Corollary of Reversing . . . . .	15
1.16 Godel's Theorem . . . . .	16
1.17 Constructing The One Way Function . . . . .	17
<b>2 Analysis of Fibonacci</b>	<b>19</b>
2.1 Euler's Constant . . . . .	19
2.2 Example of a Decider . . . . .	20
2.3 Analysis of the Decider $2x^2$ . . . . .	21
2.4 Representing Monomial Deciders As Code . . . . .	23
2.5 Negative Numbers . . . . .	25
2.6 Pi . . . . .	25
2.7 Fibonacci . . . . .	25
2.8 Analysis Of Parity In Fibonacci . . . . .	26
2.9 Redrawing the Fibonacci Sequence . . . . .	26
2.10 The Fibonacci Decider . . . . .	28
2.11 The Fibonacci Picking Function . . . . .	28
<b>3 Inferrable Languages</b>	<b>29</b>
3.1 Introduction . . . . .	29
3.2 Applying The Fibonacci Decider . . . . .	29
3.3 Fibonacci DOL Decider Left Hand Side . . . . .	30
3.4 Fibonacci DOL Decider Right Hand Side . . . . .	30

3.5	The Law of Commutativity and Noncommutativity . . . . .	30
3.6	Definition Of Support . . . . .	31
3.7	Rationals Of Picking Function . . . . .	31
3.8	Support Of Picking Function . . . . .	31
3.9	Law Of Strings . . . . .	31
3.10	Commutativity Of Addition . . . . .	32
3.11	Commutativity Of Multiplication . . . . .	32
3.12	Additive Identity . . . . .	32
3.13	Multiplicative Identity . . . . .	32
3.14	Additive Inverse . . . . .	32
3.15	Multiplicative Inverse . . . . .	32
3.16	Generalized Operations . . . . .	32
3.17	Generalized Commutativity . . . . .	32
3.18	Associativity Of Addition . . . . .	33
3.19	Associativity Of Multiplication . . . . .	33
3.20	Distributivity . . . . .	33
3.21	Field . . . . .	33
<b>A</b>	<b>Frequently Asked Questions</b>	<b>35</b>
A.1	How do I change the colors of links? . . . . .	35

# List of Figures

1.1	Decider that represents the monomial, $x^3$ .	2
1.2	Top down removal for equivalence of decider and cyclic automata.	3
1.3	Visual example of what $\mathcal{E}_n$ of a rational expression.	4
1.4	Addition of two deciders. The gradient of the circles remain the same after adding the two deciders together as the degree remains the same.	5
1.5	Product of two deciders. The gradient of the circles get denser after adding the two deciders together as the degree increases.	6
1.6	Multivariable monomial deciders can be seen treated as parallel processes running next to each other.	7
1.7	Generalization of a monomial decider.	9
1.8	A concentric monomial decider is a generalized monomial decider with details missing.	10
1.9	A constant represented as monomial decider, $Decider < cx^0 >$ .	11
1.10	$Decider < x^5/x >$ to $Decider < x^5/x^5 >$ .	11
1.11	$Decider < x^5/x/x/x^2 >$	13
1.12	$Decider < x^6/x^2 >$	14
1.13	Two possible representations of $Decider < x^6/x/x >$ .	15
1.14	Path of one representation of $Decider < x^6/x^2 >$ .	16
1.15	Godel's illustrated from $Decider < x^6/x^2 >$ .	17
1.16	Picking a decision function, $d$ , from $Decider < x^6/x^2 >$ .	17
2.1	Decider that represents the constant $e$ .	19
2.2	Decider that represents the monomial, $x^3$ .	21
2.3	Generate function, $2x^2$ .	21
2.4	Analysis of visits to finishing states in, $2Decider < 2x^2 >$ .	22



# List of Tables





*For/Dedicated to/To my...*



## Chapter 1

# A Language of Polynomials

### 1.1 Introduction

This paper is on the construction of the one way function to a matrix multiplication problem - that of multiplying two  $3 \times 3$  matrices to form a  $6 \times 6$  matrix under a locally concatenative property. The matrix multiplication is a type of law of composition that operates on different layers. There may be some higher level mathematics mixed throughout the paper, however, thorough explanation will be attempted, otherwise can be ignored. The reason why it is included is to provide a bridge of multiple directions for the reader to take.

### 1.2 Foundations

There exists a language such that it decides each monomial in the polynomial. In other words, there exists a set of deciders for each monomial in the polynomial where it decides if  $y$  is in the monomial. A decider in this term is not of the definition found originally in textbooks but one that is redefined in the below definition.

Given a polynomial

$$p(x) = ax^2 + bx + c$$

$$p(x) = 3x^2 + 4x + 5$$

$$p(2) = 3(2)^2 + 4(2) + 5$$

$$p(2) = 12 + 8 + 5$$

Let the decider be defined as the following:

Decider is a function  $Decider \langle c \times x^n \rangle \equiv c \times x^n = y$

such that  $x_1 \times x_2 \times \dots \times x_n$  where  $n$  is equal to degree + constant is tested to be equivalent to  $y$  and  $x_1$  is the start and  $x$  degree times is the finish then loop around  $x_1$  to  $x_n$  until it stops

For each state,  $x_i$ ,  $i$  such that it is between 1 to  $n$ ,  $x_i$  contains a subgroup of size  $n$  and for each subgroup,  $s_i$ , there exists another subgroup and so on and so forth such that there are  $n$  layers starting from  $x_i$  to 1. This is the same as saying that it is a rational expression.

### Examples

Decider for  $ax^2$  is  $Decider < 3(2)^2 > \equiv 3(2)^2 = 12$

Decider for  $bx$  is  $Decider < 4(2)^1 > \equiv 4(2)^1 = 8$

Decider for  $c$  is  $Decider < 5(2)^1 > \equiv 5(2)^0 = 5$

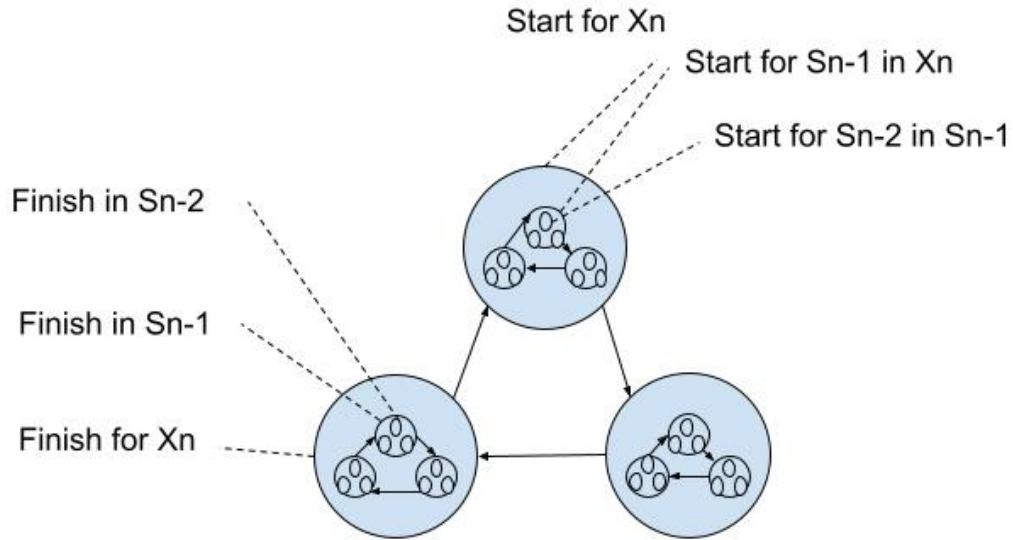


FIGURE 1.1: Decider that represents the monomial,  $x^3$ .

**Theorem:** A Decider is the equivalent to a cyclic automata

*Proof:* Remove the lowest level state,  $S_1$  from the bottom then continue removing  $S_i$  from  $i = 2$  to  $n-1$  until you get only the states that are at  $X_n$ .

Remove the top state down from the  $S_{n-1}$  for each layer  $S_{n-1}$  to  $S(n - n - 1)$ . This preserves the start and finish state for the layer  $x_n$ . This is a cyclic automaton.



FIGURE 1.2: Top down removal for equivalence of decider and cyclic automata.

### 1.3 Monomial of One Variable

Given the definition of a decider:

Decider is a function  $Decider < cx^n > \equiv cx^n = y$

A decider of at least one degree

$Decider < 3x^4 > \equiv 3x^4 = y$

Contains  $Decider < 3x^3 > \equiv 3x^3 = y$

Contains  $Decider < 3x^2 > \equiv 3x^2 = y$

Contains  $Decider < 3x^1 > \equiv 3x^1 = y$

Contains  $Decider < 3x^0 > \equiv 3x^0 = y$

Hence it can be generalized to:

$Decider < cx^n >$  contains the sequence set

There exists a start state and a finish state for each decider.

$\{start, ..., finish\}$

$Decider < cx^n >, Decider < cx^{n-1} >, ..., Decider < cx^0 >$  which has a more formal definition called a rational expression. A rational expression on A over K is a

semiring described as  $\mathcal{E}_n$  such that  $n \geq 0$  where  $A$  is an alphabet (in our case a finite set of integers) and  $K$  is a commutative semiring. This means the following in terms of the decider

$$\begin{aligned} \text{Decider} < cx^n > &= \mathcal{E}_n \\ \text{Contains Decider} < cx^{n-1} > &= \mathcal{E}_{n-1} \\ &\dots \\ \text{Contains Decider} < cx^1 > &= \mathcal{E}_1 \\ \text{Contains Decider} < cx^0 > &= \mathcal{E}_0 \end{aligned}$$

The formal definition of a rational expression is defined below.

**Definition.**  $A_n = A_{n-1} \cup \{E^* | E \in \mathcal{E}_{n-1}, (E, 1) = 0\}$

Here,  $A_n$  is the set of monomials in the polynomial.  $A_{n-1}$  are the monomials of degree  $n-1$  and less of the polynomial and the set  $\{E^* | E \in \mathcal{E}_{n-1}, (E, 1) = 0\}$  is equivalent to  $\text{Decider} < cx^n >$  or equivalently the top of a single state of a decider.

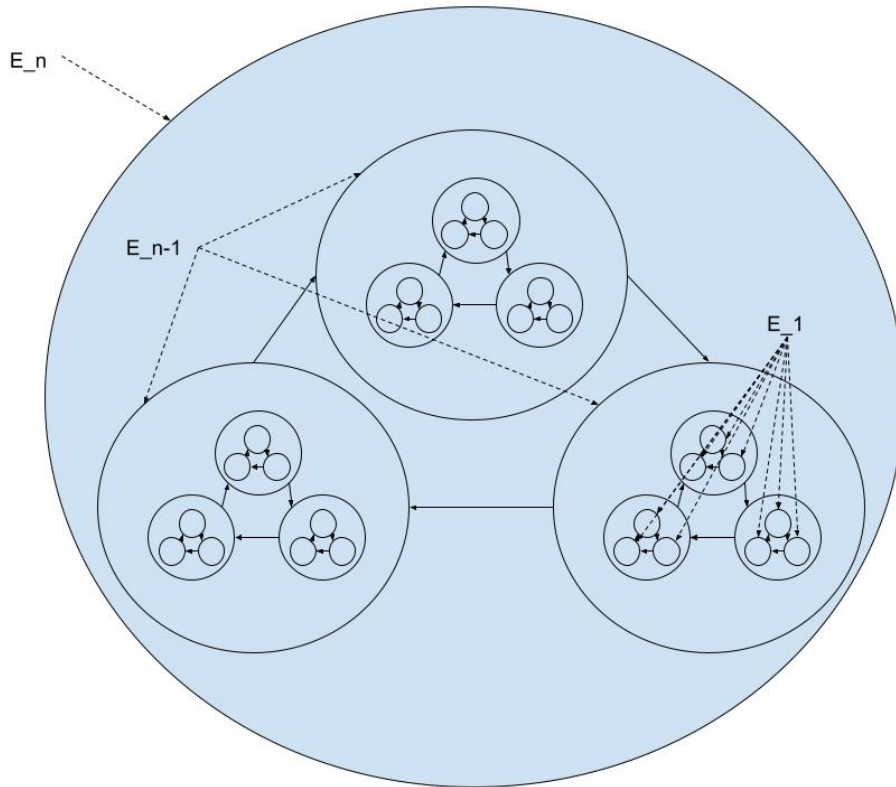


FIGURE 1.3: Visual example of what  $\mathcal{E}_n$  of a rational expression.

Figure 1.3 Visual example of  $\mathcal{E}_n$  of a rational expression.

A rational function is defined as the following:

$K[x]$  and  $K[[x]]$ . Let  $K[[x]]$  describe a set of deciders as a polynomial representation.  $S$  is an element of  $K[[x]]$  meaning  $S$  is a decider.

$$S = \sum_{n \geq 0} a_n x^n$$

## 1.4 Addition



FIGURE 1.4: Addition of two deciders. The gradient of the circles remain the same after adding the two deciders together as the degree remains the same.

Given the first example:

$$\begin{aligned} p(x) &= 3x^2 + 4x + 5 \\ p(2) &= 3(2)^2 + 4(2) + 5 \\ p(2) &= 12 + 8 + 5 \end{aligned}$$

$$m_2 = \text{Decider} \langle 3x^2 \rangle = 3x^2$$

$$m_1 = \text{Decider} \langle 4x^1 \rangle = 4x$$

$$m_0 = \text{Decider} \langle 5x^0 \rangle = 5$$

Generalized to  $m_x$  where  $x$  is the degree

Given polynomial functions,  $p_1$  and  $p_2$ , they are commutative

$$p_1(x) = m_a + \dots + m_0$$

$$p_2(x) = n_b + \dots + n_0$$

$$p_1(x) + p_2(x) = m_a + n_b + (m_{x+1} + n_{y+1}) + \dots + (m_x + n_y) + \dots + (m_0 + n_0) \text{ where } x = y$$

$$\text{Decider} \langle c_x x d_x \rangle + \text{Decider} \langle c_y x d_y \rangle$$

$$= \text{Decider} \langle c_x + c_y, x, d_x \rangle = \text{Deciders} \langle c_x + c_y, x, d_y \rangle$$

$$\implies d_x = d_y$$

## 1.5 Product



FIGURE 1.5: Product of two deciders. The gradient of the circles get denser after adding the two deciders together as the degree increases.

Given two monomials in the language,  $a$  and  $b$ , the product of  $a$  and  $b$  is also in the language.

Given  $\text{Decider} \langle c_x x d_x \rangle$  and  $\text{Decider} \langle c_y x d_y \rangle$  is in language  $L$

Show that the product  $\text{Decider} \langle (c_x + c_y) x d_x \times d_y \rangle$  is in  $L$

$$\text{Decider} \langle c_x x d_x \rangle \times \text{Decider} \langle c_y x d_y \rangle$$

$$= c_x x d_x c_y x d_y$$

$$= c_x x d_x + d_y$$

$$= (c_x + c_y) x (d_x + d_y) \text{ is in } L$$

$$= \text{Decider} \langle (c_x + c_y) x (d_x + d_y) \rangle$$



## 1.6 Problem with Matrices

An important problem arising from deciders is representing them as matrices. The problem can be reformulated as the following: given a polynomial  $p$  of  $x$ , show that the monomial deciders represented in the language can't be contained in a finite matrix after a set number,  $n$ , such that  $x^n$ .

$$[n \times n] [n \times n] = [m \times m] \text{ such that } m \neq n \text{ and } m, n \geq 0 \text{ and } m \leq n$$

The focus of this article pertains to the question of whether or not there exists structures with certain properties that allow law of compositions to handle the above statement. The reason why this seems feasible is because of the following proposition found in Retenaur(66).

*Proposition.* Given a proper square matrix  $M$  over  $\mathcal{E}$ , there exist matrices  $M_1, M_2$  of the same size as  $M$  over  $\mathcal{E}$  such that  $M_1 1 + MM_1$  and  $M_2 1 + M_2M$ . In particular if  $K$  is a ring,  $1 - M$  is an invertible modulo .

## 1.7 Multivariable Monomials

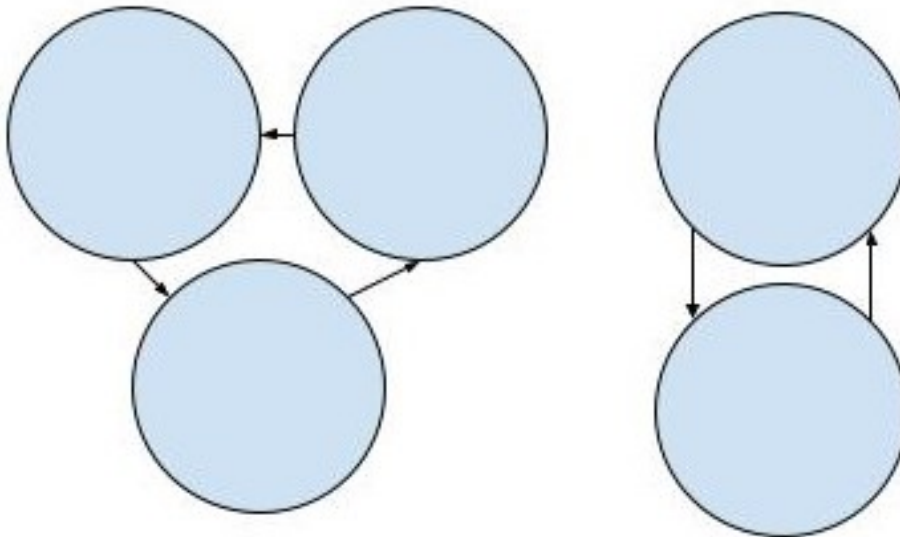


FIGURE 1.6: Multivariable monomial deciders can be seen treated as parallel processes running next to each other.

A monomial with more than one variable can be treated the same way as handling single variables at different degrees.

Addition gives the following:

$$\text{Decider} \langle x^6yz^3 \rangle + \text{Decider} \langle x^6yz^3 \rangle = \text{Decider} \langle 2x^6yz^3 \rangle$$

Multiplication of the decider of the same degree gives the following:

$$\begin{aligned} & \text{Decider} \langle cx^n \rangle \times \text{Decider} \langle cy^n \rangle \times \text{Decider} \langle cz^z \rangle \\ & \equiv \text{Decider} \langle cx^n * cy^n * cz^n \rangle \\ & \equiv \text{Decider} \langle cxyz^{3n} \rangle \end{aligned}$$

where c is some constant

Multiplication of the decider of the different degrees gives the following:

$$\begin{aligned} & \text{Decider} \langle cx^n \rangle \times \text{Decider} \langle cy^m \rangle \times \text{Decider} \langle cz^l \rangle \\ & \equiv \text{Decider} \langle cx^n * cy^m * cz^l \rangle \\ & \equiv \text{Decider} \langle cx^{n+m+l} \rangle \end{aligned}$$

where c is some constant

Given  $\text{Decider} \langle 3xy^2 \rangle$  and  $\text{Decider} \langle 7x^7y^{-1} \rangle$

$$\text{Decider} \langle 3xy^2 \rangle \times \text{Decider} \langle 7x^7y^{-1} \rangle = \text{Decider} \langle 21x^8y \rangle$$

Representing a multivariable monomial of different degrees is a similar line of thought. There are many representations of them, however, this article will choose the simplest and have them separate as seen in figure 1.6. In this manner, multivariable monomials are a set of individual one variable monomials running simultaneously.

## 1.8 Generalized Monomial Deciders

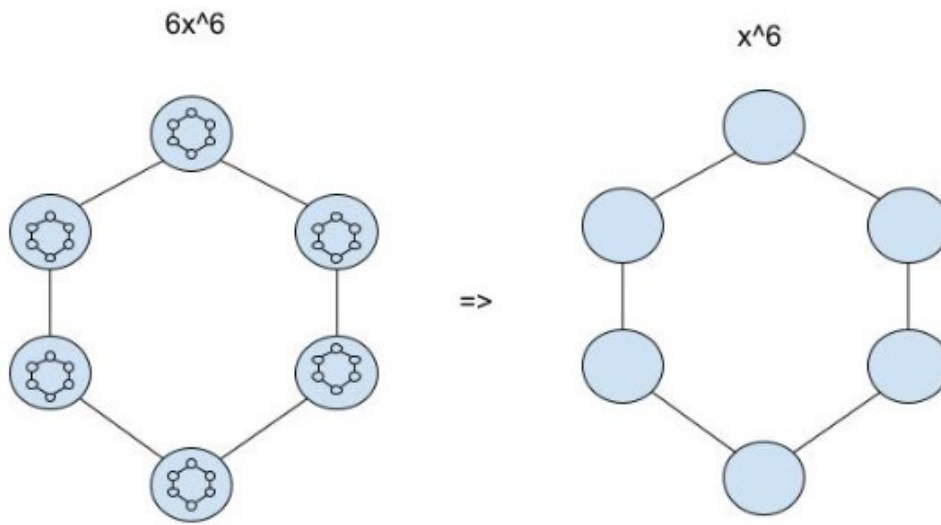


FIGURE 1.7: Generalization of a monomial decider.

A decider can be represented as the top layer only if short hand notation is necessary.

Given a Decider  $\langle m(x) \rangle$  where  $m(x)$  is a monomial, keep the top layer  $S_n$  in  $\mathcal{E}_\setminus$ . This is called the generalized monomial decider.

## 1.9 Concentric Monomial Deciders

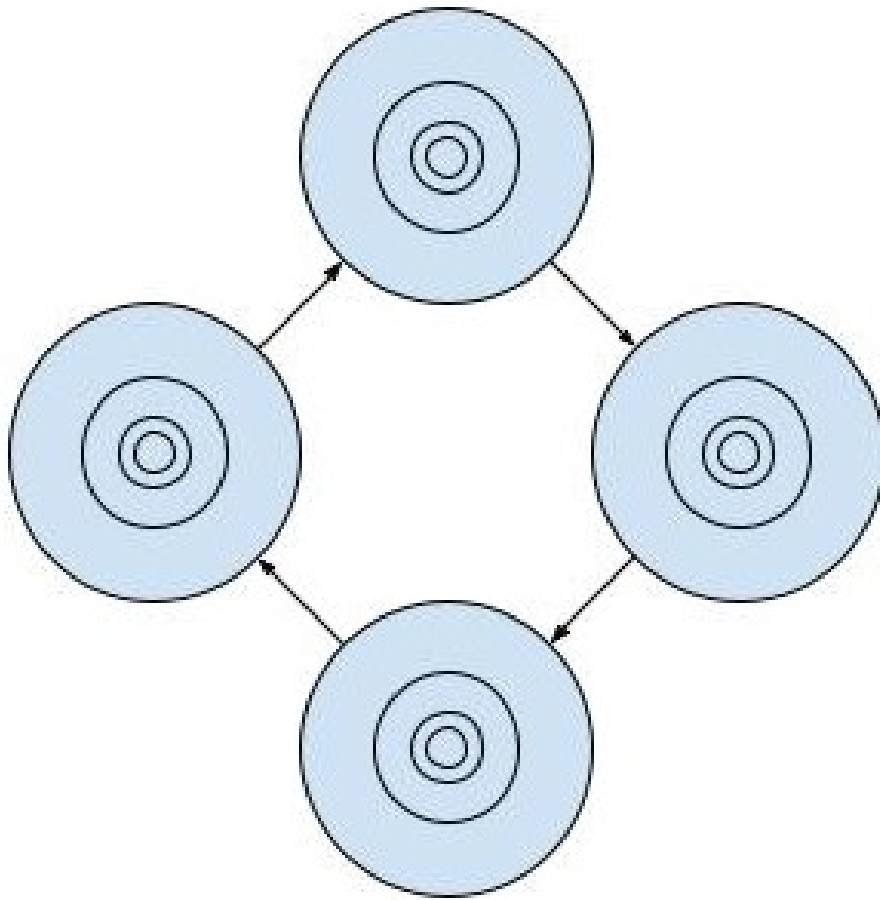


FIGURE 1.8: A concentric monomial decider is a generalized monomial decider with details missing.

Generalization results in an interesting property if monomial decider is required to get in more depth. The top layer that remains from generalization remains the same and still forms a cycle, however, each state has one state and so forth up to  $n-1$  depth.

## 1.10 Constants

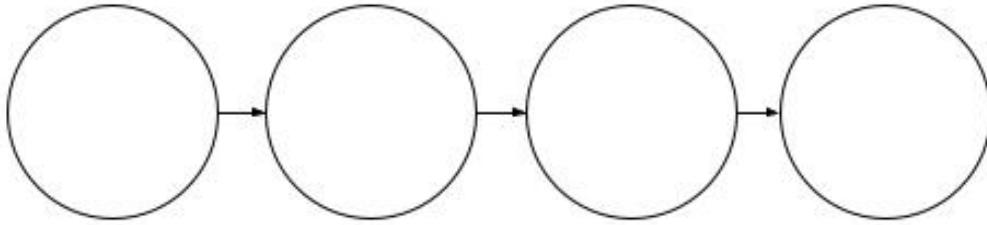


FIGURE 1.9: A constant represented as monomial decider,  $\text{Decider} \langle cx^0 \rangle$ .

Given a constant,  $c$ , of a polynomial:  $f(x) = c$ , Constants are seen as linear directed acyclic graphs.

$$\text{Decider} \langle cx^0 \rangle \equiv c = y$$

Addition gives the following:

$$\text{Decider} \langle c_1x^0 \rangle + \text{Decider} \langle c_2x^0 \rangle \equiv \text{Decider} \langle (c_1 + c_2)x^0 \rangle \equiv \text{Decider} \langle c_1 + c_2 \rangle$$

Multiplication gives the following:

$$\text{Decider} \langle c_1x^0 \rangle \times \text{Decider} \langle c_2x^0 \rangle \equiv \text{Decider} \langle c_1c_2x^0 \rangle \equiv \text{Decider} \langle c_1c_2 \rangle$$

There is no state in the decider where it loops back to the start.

## 1.11 Division

Division of monomial deciders

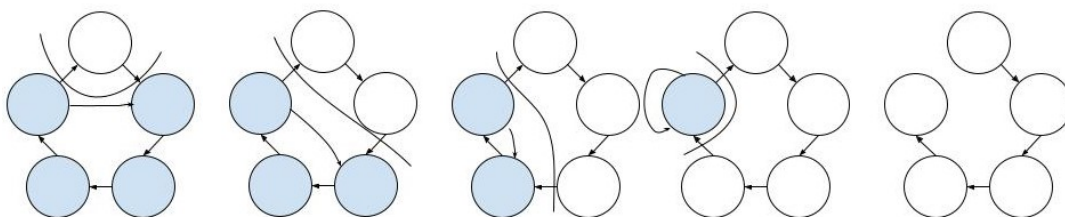


FIGURE 1.10:  $\text{Decider} \langle x^5/x \rangle$  to  $\text{Decider} \langle x^5/x^5 \rangle$ .

$$\text{Decider} \langle x^5/x \rangle \equiv \text{Decider} \langle x^5 \rangle / \text{Decider} \langle x^1 \rangle$$

$$\text{Decider} \langle x^5/x^2 \rangle \equiv \text{Decider} \langle x^5 \rangle / \text{Decider} \langle x^2 \rangle$$

$$\text{Decider} \langle x^5/x^3 \rangle \equiv \text{Decider} \langle x^5 \rangle / \text{Decider} \langle x^3 \rangle$$

$$\text{Decider} \langle x^5/x^4 \rangle \equiv \text{Decider} \langle x^5 \rangle / \text{Decider} \langle x^4 \rangle$$

$$\text{Decider} \langle x^5/x^5 \rangle \equiv \text{Decider} \langle x^5 \rangle / \text{Decider} \langle x^5 \rangle$$

In the following examples,  $x_i \neq x_j$ , meaning  $x_i$  is of a different representation than  $x_j$

$\text{Decider} \langle x^5/x^1 \rangle \equiv$  sequence of permutations of  $x_i, x_j$  such that the count of  $i$  is 4 and  $j$  is 1

$\text{Decider}(\langle x^5/x^2 \rangle \equiv$  sequence of permutations of  $x_i, x_j$  such that the count of  $i$  is 3 and  $j$  is 2

$\text{Decider} \langle x^5/x^3 \rangle \equiv$  sequence of permutations of  $x_i, x_j$  such that the count of  $i$  is 2 and  $j$  is 3

$\text{Decider} \langle x^5/x^4 \rangle \equiv$  sequence of permutations of  $x_i, x_j$  such that the count of  $i$  is 1 and  $j$  is 4

$\text{Decider} \langle x^5/x^5 \rangle \equiv$  sequence of permutations of  $x_i, x_j$  such that the count of  $i$  is 0 and  $j$  is 5

## 1.12 Multiple Divisions

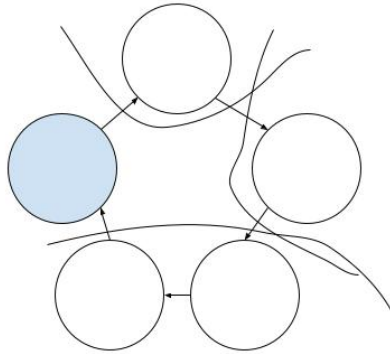


FIGURE 1.11: *Decider*  $\langle x^5/x/x/x^2 \rangle$

Given multiple operations of division, this forms a topological space where the order of operations are ignored.

$$x^5/x^2/x/x = x^5/x^2/x^2.$$

$$\text{Decider} \langle x^5/x^2/x^1/x^1 \rangle \equiv \text{Decider} \langle x^5/x^2/x^2 \rangle$$

### 1.13 Equivalence

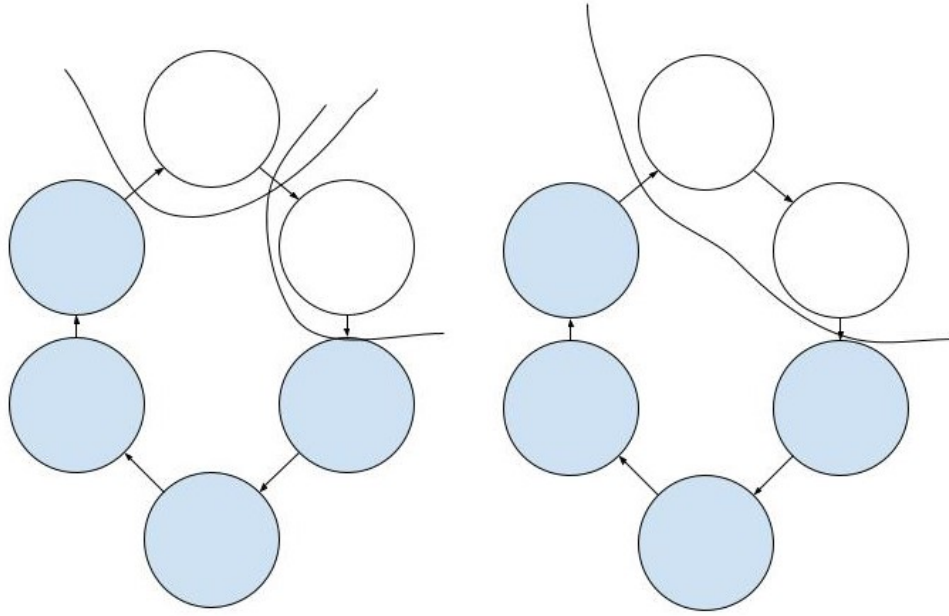


FIGURE 1.12: *Decider*  $\langle x^6/x^2 \rangle$

$$\text{Decider} \langle x^6/x^1/x^1 \rangle \sim \text{Decider} \langle x^6/x^2 \rangle$$

Determining if  $y$  is in  $f(x)$  is easy if we are given any monomial decider in the set of the language of polynomials and their representations has the possibility to give different representations if we consider them as representations of the function  $f$  of  $x$ .

$$\text{Decider} \langle x^6/x^1/x^1 \rangle \sim \text{Decider} \langle x^6/x^2 \rangle \text{ in that they decide if } y \text{ is in } m(x) = x^6/Q$$

**Theorem of Equivalence.** Something on lines of  $\text{Decider} \langle x^6/x^1/x^1 \rangle = \text{Decider} \langle x^6/x^2 \rangle$  such that there is some  $x$  such that the monomial represented by both deciders exists where  $f(x) = y$ .

### 1.14 Reversing

$$\text{Decider} \langle x^6/x^1/x^1 \rangle \equiv \text{sequence of permutations such that it is equal to } \sum_{i=1}^{n-1} i$$

$$\text{Decider} \langle x^6/x^2 \rangle \equiv \text{sequence of permutations of } x_i, x_j \text{ such that it equals } n-1.$$



Is shown that by the permutation of the order of operations that  $Decider < x^6/x^1/x^1 >$  does not have the same number of permutations as  $Decider < x^6/x^2 >$

**Theorem of Reversing.** Given two representations,  $a, b$  in  $Decider < m(x)/Q >$  where  $m(x)$  is monomial and  $Q$  is the division operations such that  $m(x)/Q \geq 1$ ,  $a \neq b$  implies that they don't have the same quotients space.

*Proof.* Proof by construction visually to show  $a \neq b$ .

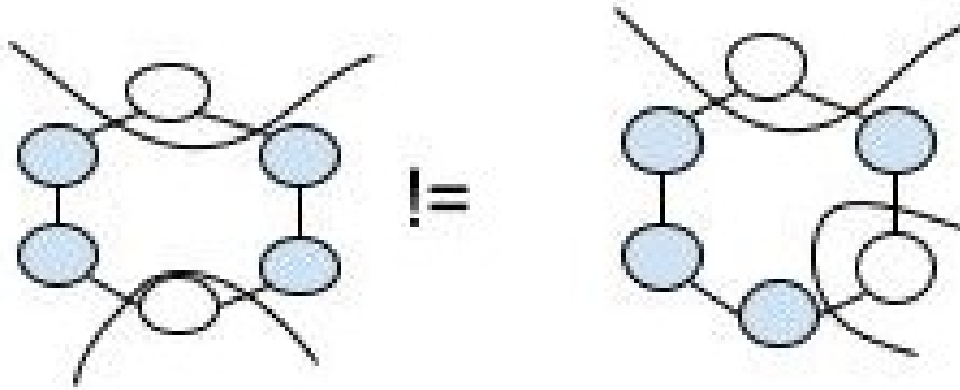


FIGURE 1.13: Two possible representations of  $Decider < x^6/x/x >$ .

The two representations in 1.13 don't have the same quotient space and hence  $a \neq b$ .

## 1.15 Corollary of Reversing

Given a starting point of decider, the path the decider takes to decide if  $y$  is in the monomial,  $m(x)$  is unique to each representation.

**Corollary.** Given a decider,  $d$ , in  $Decider < m(x) >$  then there is path,  $p$ , that exists for  $d$  such that  $p = \text{Path}(d) = s_1, s_2, \dots, s_i, \dots, s_n$  where  $i$  is count of the states in the decider of  $m(x)$ .

*Example.* Choose some  $x$  such that it is in path of  $Decider < x^6/x^2 >$  where  $p = 001111$  then the following graph is what the decider is represented as.

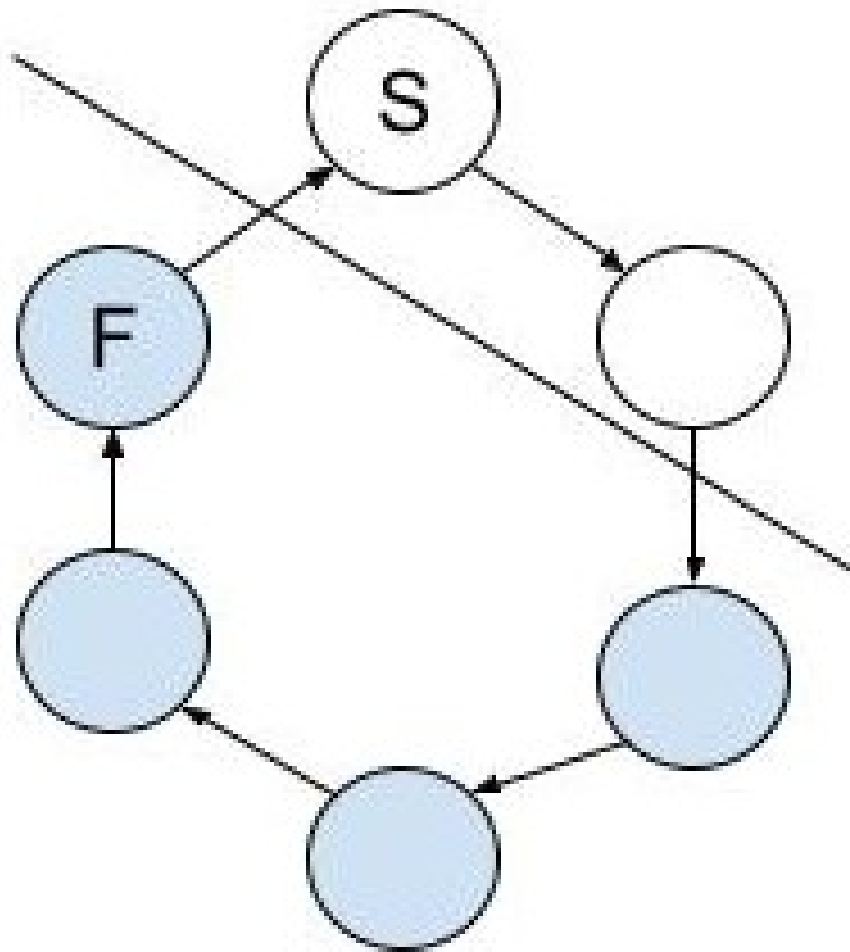


FIGURE 1.14: Path of one representation of  $Decider < x^6/x^2 >$ .

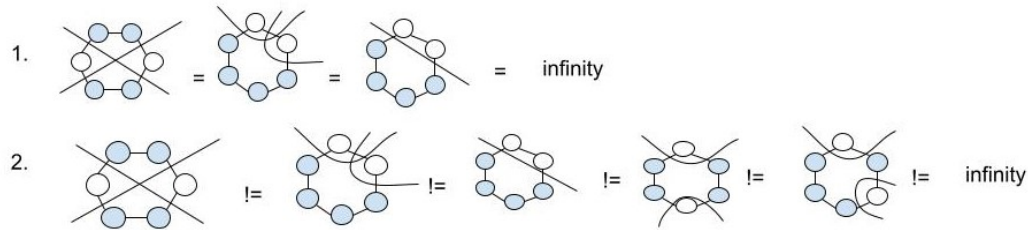
## 1.16 Godel's Theorem

We see that there exists two statements from these theorems

1.  $x = x$  from a theorem of equivalence
2.  $x! = x$  from a theorem of reversal

**Example:** Given some  $d_1, d_2, d_3, \dots, \text{infinity}$  in decision functions in  $Decider < m(x) >$

1.  $d_1 = d_2 = d_3 = \dots = \text{infinity}$
2.  $d_1! = d_2! = d_3 = \dots! = \text{infinity}$

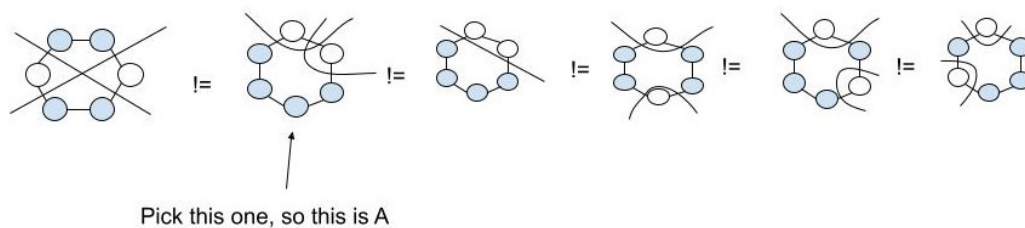
FIGURE 1.15: Godel's illustrated from  $Decider < x^6 / x^2 >$ .

The different representations of a monomial through the language of monomial deciders will give the problem of undecidability. This means that despite many formal definitions of the monomial decider, there is no way to solve the problem of finding a specific representation of a monomial decider without having to guess or apply some sort of probability to it. Relating to the real line, given a real line  $a, b$   $a \leq b$ , there is infinite choices between  $a$  and  $b$ . As long as  $b$  and  $a \geq 0$ , there requires some sort of probability of choosing some specific number that is between  $a$  and  $b$ .

## 1.17 Constructing The One Way Function

A probability exists to find a certain monomial decider in the set of it's variations.  $A/B = \text{Probability}$  where  $A$  is the monomial decider we want and  $B$  is the number of all the variations.

Example:  $d_1, d_2, \dots, d_6$  in  $Decider < x^6 >$  such that  $d_i$  are all distinct.  
 Choose one of the deciders in  $D$  through probability  
 Probability of choosing  $d$  in  $D$  is  $1/6$  so  $0.16666667$

FIGURE 1.16: Picking a decision function,  $d$ , from  $Decider < x^6 / x^2 >$ .

This is called the picking function and every time it is called, the probability is multiplied such that it is  $n^k$ . As an example, if the picking function is called twice using the example above, it is shown that the probability is:

$$1/6 \times 1/6 = 1/6^2 = 1/36 = 0.02777778$$

This is formally known as the one way function.



## Chapter 2

# Analysis of Fibonacci

## 2.1 Euler's Constant

From the the reinterpretation of the theory, Euler's constant is an example of  $P = NP$  because of it's use of calculus. Euler's constant can be defined as

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}$$

To show that it is also in the problem set of  $P \neq NP$ , start by using the picking function going into infinity.

$$e = pf(\sum_{n=0}^{\infty} \frac{1}{n!}) = \sum_{n=0}^{\infty} pf(\frac{1}{n!})$$

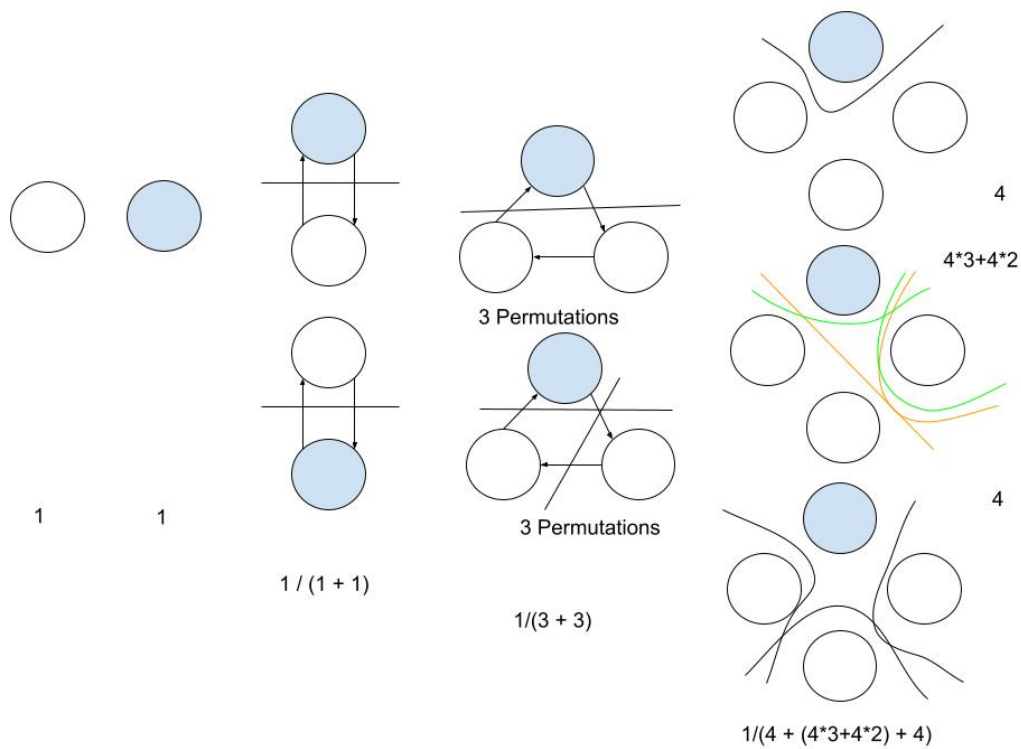


FIGURE 2.1: Decider that represents the constant  $e$ .

The constant  $e$  is the sum of the infinite series of  $\frac{1}{n!}$  and can be represented as a series of monomials representing the Decider< $x$ > using the picking function.

$$e = 1 + 1 + 1/(1 + 1) + 1/(3 + 3) + 1/(4 + (4 * 3 + 4 * 2) + 4) + \dots$$

$$e = pf(Decider < x >) + pf(Decider < x^2/x >) + pf(Decider < x^3/x^2 >) + \dots$$

## 2.2 Example of a Decider

The following is an example of code that roughly sketches a generalized monomial decider, Decider< $2x^2$ >. It tests to see if  $y$  is in the monomial  $m(x) = 2x^2$ . Although approximation and binary search algorithms work, using this method allows for simplicity of technique in representing a decider visually and gives the reader hands-on potential if they want to experiment on the subject further.

```
bool generalizedDecider(int y)
{
    if (y == 0)
    {
        return true;
    }
    var s = y;
    while (s >= 0)
    {
        for (int i = 0; i < 2; i++)
        {
            for (int j = 0; j < 4; j++)
            {
                if (s == 0 && (j == 0 || j == 2) && i == 0)
                {
                    return true;
                }
                else if (s < 0)
                {
                    return false;
                }
                s -= 1;
            }
        }
    }
    return true;
}
```

The above code can be represented visually as follow:

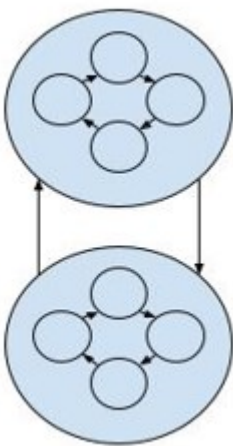


FIGURE 2.2: Decider that represents the monomial,  $x^3$ .

2.3 Analysis of the Decider  $2x^2$

Using the generalizedDecider function above for the Decider $\langle 2x^2 \rangle$  where a sketch of the initial algorithm is created, collecting data to find insight to make a general technique can be found:

Generate	Even Input	Even Output
f(0) = 0	0	1
f(1) = 2	1	1
f(2) = 8	0	1
f(3) = 18	1	1
f(4) = 32	0	1
f(5) = 50	1	1
f(6) = 72	0	1
f(7) = 98	1	1
f(8) = 128	0	1
f(9) = 162	1	1
f(10) = 200	0	1
f(11) = 242	1	1
f(12) = 288	0	1
f(13) = 338	1	1

FIGURE 2.3: Generate function,  $2x^2$ .

**Generate** is  $f(x) = 2x^2 = y$  on the first line and the number of negatives is on the second. There are two finishing and all the even parity outputs end in one state and

all the odd parity outputs end on the other. **Even Input** is the boolean parity of the input being even. **Even Output** is the boolean parity of the output being odd.

Here, it can be seen that there is repeating pattern of even and odd values of the following:

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

From this array, two finishing states are described. When the input and output are both even and one where the input is odd and the output is even. Every time the head of the tape passes a finishing state, the count of the variable, **visit** is increased by one. Counting the number of visits two the finishing states, it can be seen that for every pair, (start,end), there is a difference of three for  $Decider < 2x^2 >$ . The following is a table of the results:

Generate	Visits	Difference
f(0) = 0	0	0
f(1) = 2	1	1
f(2) = 8	4	3
f(3) = 18	9	5
f(4) = 32	16	7
f(5) = 50	25	9
f(6) = 72	37	11
f(7) = 98	50	13

FIGURE 2.4: Analysis of visits to finishing states in,  $2Decider < 2x^2 >$ .

From analysis, the number of times the tape head visits a finishing state is the difference of the previous input plus two. The difference increases by two every time it passes a finishing state. It doesn't pass when the number of visits is even, so it can be deduced that the difference is increased by two every time it passes the odd finishing state. This result allows us to write a program to decide if  $y$  is in  $2x^2$ .

```
bool MonomialDecider2xx(int y)
{
    var totalVisits = 0;
    var currentVisits = 0;
    var diff = 1;
    var s = 0;

    while (s <= y)
    {
        for (int i = 0; i < 2; i++)
        {
            for (int j = 0; j < 2; j++)
```



```

    {
        for (int k = 0; k < 2; k++)
        {
            if ((i == 0) && (j == 0 || j == 1) && (k == 0))
            {
                if (currentVisits == totalVisits)
                {
                    if (s == y)
                    {
                        Console.WriteLine(new String("Deciding on: " +
                            return true;
                    }
                    else if (s > y)
                    {
                        return false;
                    }

                    totalVisits += diff;

                    // If the tape head is on the odd finishing
                    // state increase the diff variable by 2
                    // Do this to represent x^2 in 2x^2
                    if (i == 0 && j == 1 && k == 0)
                    {
                        diff += 2;
                    }
                }

                currentVisits++;
            }
            s++;
        }
    }

    return false;
}

```

## 2.4 Representing Monomial Deciders As Code

With the data above, the requirements on constructing a decider is as follows.

Given the function:

$$f(x) = 2x^2 = \{0, 2, 8, 18, \dots\}$$

The output of  $f(x)$  is of the following.  
 $x$  is even at 0, 8, 32, 72

x is odd at 2,18,50

There are four variables constructed:

Current passes records the number of times path traveled passes a finishing state.

Total number of times traveled on a finishing state needed to reach a valid decision.

Diff is the current number of diff to increment total hits by.

IsEven is if this resets back to even, increment Diff by two.

The following is code generated from our more formal representation of the solution.

```
// After getting some log results , we can construct a decider
bool MonomialDecider(int y)
{
    var isEven = 0;
    var s = 0;

    while (s <= y)
    {
        for (int i = 0; i < 2; i++)
        {
            for (int j = 0; j < 2; j++)
            {
                for (int k = 0; k < 2; k++)
                {
                    if ((i == 0)&&(j == 0 || j == 1)&&(k == 0))
                    {
                        if (hits == total)
                        {
                            if (s == y)
                            {
                                Console.WriteLine(s + ": Hits: " + total);
                                return true;
                            }
                        }
                        else if (s > y)
                        {
                            return false;
                        }

                        total += diff;
                        isEven++;
                        if (isEven % 3 == 2)
                        {
                            isEven = 0;
                            diff += 2;
                        }
                    }
                }
            }
        }
    }
}
```

```

        hits++;
    }
    s++;
}
}
}
return false;
}

```

## 2.5 Negative Numbers

Representing negative numbers can be thought of discretely. Below is a representation of negative numbers.

Cancellation

Addition

Start and Finish:  $2x$

Start and Finish:  $x^2$

Ignoring the rules for commutativity and association for now.

## 2.6 Pi

Representing the constant pi,  $\pi$ , in the language of polynomials using the Leibniz formula  $\pi/4 = 1 - 1/2 + 1/5 - 1/7 + 1/9 + \dots$

## 2.7 Fibonacci

Given the fibonacci sequence, 1, 1, 2, 3, 5, 8, 13, 21,  $\dots$ , representing this sequence as a monomial generator in the language of polynomials can be shown below.

From the circles above, we see that  $f(1) = 1$  and  $f(2) = 2$ . If we add  $f(1)$  and  $f(2)$  together we get  $f(3) = 3$  and so on and so forth.

Notice that on odd inputs,  $E_x$ , there aren't any circles in the circles/states but in even inputs on  $X$ , there are two states. On outputs,  $E_y$ , it is odd twice then even once.

```

int fibonacci(int n)
{
    if (n == 0)
    {
        return 0;
    }

    int y = 1;
    int y1 = 1;
    int y2 = 0;

    for(int i = 1; i < n; i++)
    {
        y = y1 + y2;
        y2 = y1;
        y1 = y;
    }

    return y;
}

```

## 2.8 Analysis Of Parity In Fibonacci

On analyzing the parity of  $E_x$  and  $E_y$  of the fibonacci sequence, we that there are two patterns.

$E_1$	$E_2$	$E_3$
0	1	0
1	0	1
0	1	1

$$\begin{aligned} \text{Det}(E_1, E_2, E_3) &= -1 \\ \text{Det}(E_2, E_1, E_3) &= 1 \end{aligned}$$

$$\begin{aligned} -1 + 1 - 1 &= -1 \\ 1 - 1 + 1 &= 1 \end{aligned}$$

## 2.9 Redrawing the Fibonacci Sequence

From our analysis, it can be seen that there are three states that are a minimum to create a fibonacci sequence. Minimization gives us a monomial generator,  $S_x, S_y, S_z$ . Set the three states to a desired configuration and it will generate the fibonacci sequence. It can shown that it requires three states minimum to generate the fibonacci sequence.

Generator

$$S_x = S_y + S_z$$

$$S_y = S_z + S_x$$

$$S_z = S_x + S_y$$

Using the above, dynamic programming can be modeled as a set of generator functions.

```
int fibonacciGenerator(int n)
{
    int stateX = 0;
    int stateY = 1;
    int stateZ = 1;
    int cycles = 0;

    while (cycles <= n)
    {
        cycles++;

        if (cycles > n)
        {
            return stateX;
        }

        stateX = stateY + stateZ;
        Console.WriteLine("stateX: " + stateX + "\tstateY: " + stateY + "\tstateZ: " + stateZ);

        cycles++;

        if (cycles > n)
        {
            return stateY;
        }

        stateY = stateX + stateZ;
        Console.WriteLine("stateX: " + stateX + "\tstateY: " + stateY + "\tstateZ: " + stateZ);

        cycles++;

        if (cycles > n)
        {
            return stateZ;
        }

        stateZ = stateX + stateY;
        Console.WriteLine("stateX: " + stateX + "\tstateY: " + stateY + "\tstateZ: " + stateZ);
    }

    return stateX;
}
```

## 2.10 The Fibonacci Decider

Given the two monomial deciders we found using the determinant, we know that we must have six numbers in the sequence to decide if they form a Fibonacci sequence. In order to create this decider, we use an addition operator to merge them together because they cancel each other out. All deciders in each set must be true in order for the sequence to be a valid Fibonacci sequence.

## 2.11 The Fibonacci Picking Function

Now, let's apply the picking function,  $pf$ , to the fibonacci decider and show the probability,  $P_r$ , of finding a sequence.  $pf(xyz_1 + xyz_2) = Pr(xyz_1) * Pr(xyz_2) \leq 1/n^k$

Each decider has 3 representations giving  $3^2 = 9$  total for each set. We pick one decider in each set to get the probability.

There are 6 deciders with 6 permutations giving  $6^2 = 36$  permutations.

This shows a concrete example of the picking function which is a type of one way function.

## Chapter 3

# Inferable Languages

### 3.1 Introduction

The concept of statistics and blackboxes has been drawn out extensively in theories and applications for decades but what of languages and knowing what word can be used to generate the next series of words? Everyone guesses what words can come out of someone talking given enough experience. In this article, the idea of inferable languages is presented which are languages that allow the next series of words in the sequence to be inferred given enough samples in the sequence.

### 3.2 Applying The Fibonnaci Decider

Given the definition of the Fibonacci decider and a Lindenmayer system, insight can be derived from to that there exists the commutative and noncommutative properties of the operations.

Fibonacci Decider

*Decider for  $x_1, y_1, z_1$*

$$-x_1 = y_1 - z_1$$

$$y_1 = -x_1 - z_1$$

$$-z_1 = x_1 - y_1$$

*Decider for  $x_2, y_2, z_2$*

$$x_2 = y_2 - z_2$$

$$-y_2 = x_2 - z_2$$

$$z_2 = x_2 - y_2$$

*Fibonacci Decider*

$$x_1 = -y_1 + z_2 - x_2 + y_2 - z_1$$

$$-y_1 = z_2 - x_2 + y_2 - z_1 + x_1$$

$$z_2 = -x_2 + y_2 - z_1 + x_1 - y_1$$

$$-x_2 = y_2 - z_1 + x_1 - y_1 + z_2$$

$$y_2 = -z_1 + x_1 - y_1 + z_2 - x_2$$

$$-z_1 = x_1 - y_1 + z_2 - x_2 + y_2$$

Lindenmayer System

L is the definition of the DOL System

$$L = (V, \omega, P)$$

V are the characters in the language called the alphabet

$\omega$  is the starting string called the start

P are the production rules in the language called the rules

### 3.3 Fibonacci DOL Decider Left Hand Side

Representing the left hand side of the fibonacci sequence as a DOL system alphabet requires an alphabet, rules, and a starting state.

There are two deciders on the right hand side.

### 3.4 Fibonacci DOL Decider Right Hand Side

The law of commutativity and the law of noncommutativity combined gives the law of commutativity and noncommutativity

The Law of Commutativity

$$a + b = b + a$$

$$\text{ex. } 8 + 5 = 5 + 8$$

The Law of Noncommutativity

$$a + b \neq b + a$$

$$\text{ex. } 8 - 5 \neq 5 - 8$$

Each equation in the example on the left has permutations.

From this example, it can be implied that for every variable,  $n$ , in an equation there is  $n^2$  permutations in the sequence.

The first equation is bold and italicized in the set to make a decider.

### 3.5 The Law of Commutativity and Noncommutativity

Operations for the right hand side (RHS) versus the left hand side (LHS) represents different operations of the string in different scenarios.

RHS Evaluation

Right to Left

+ Remove from the back

- Add to the front

$$\text{abaababa} = - \text{abaab} + b - ab + a - \text{aba}$$

$$\text{abaababa} = - \text{abaab} + b - ab - ab$$

$$\text{abaababa} = - \text{abaab} + b - abab$$

$$\text{abaababa} = - \text{abaab} - aba$$

$$\text{abaababa} = - \text{abaababa}$$

LHS Evaluation

Left to Right

+ Remove at the front

- Add to the back

$$\text{abaababa} + \text{abaab} - b + ab - a = -\text{aba}$$

$$\text{aba} - b + ab - a = -\text{aba}$$



$abab + ab - a = -aba$   
 $ab - a = -aba$   
 $aba = -aba$

*Proposition.* The characteristic series of a rational cyclic language is a  $\mathbb{Z}$ -linear combination of characters of finite deterministic automata.

### 3.6 Definition Of Support

A support is defined as the following:

$A^*$  is a word

$S$  is the function

Image by  $S$  of a word  $w$  is denoted by  $(S, w)$  and is the coefficient of  $w$  in  $S$

$\text{Support}(S) = w$  in  $A^*$  such that  $(S, w) \neq 0$

Now we take deciders of a monomial and the picking function to redefine the support of a noncommutative rational language

$R$  is the rational numbers where  $x$  in  $R = a/b$

such that  $a, b$  is in integers and  $b \neq 0$

$Q$  is the quotient space represented in topology such that  $A/$  where are sets and is the divisions of  $A$

$R$ -rational is the representation of  $R$  as the polynomial function

$Q$ -rational is the representation of  $Q$  as a polynomial

### 3.7 Rationals Of Picking Function

Support of the Fibonacci Picking Function of the deciders of a monomial.

$Q$ -rational-deciders are the possible monomial deciders of  $Q$ -rational-string. Use the picking function,  $PF$ , to choose one decision function in  $Q$ -rational-deciders, we see a mapping from  $Q$ -rational  $\Rightarrow$   $R$ -rational.

### 3.8 Support Of Picking Function

The support of an inferrable language is now defined to be:

support of  $PF$  of  $Q$ -rational-deciders =  $\text{support}(PF(Q\text{-rational-deciders}))$

decider in  $Q$ -rational-deciders such that decider is unique  $\equiv \det(\text{decider}) \neq 0$

The decider chosen has an equation that is bold and italicized and there is a set of equations that are distinctly bold and italic that complete this equation to form the decider.

### 3.9 Law Of Strings

Although the law of commutativity and noncommutativity is a theorem, it's helpful to get a big picture view. Let's condense the law of commutativity and noncommutativity down even further to find some laws.

This is operating on variables, strings, and representations of it.

### 3.10 Commutativity Of Addition

Take the length function,  $\text{length}(s) \equiv l(s)$ , and apply to the '=' addition operations and see it's equivalence. Set b to a and reversal is accomplished.

### 3.11 Commutativity Of Multiplication

Commutativity of Multiplication

### 3.12 Additive Identity

The LHS and RHS are equations that test whether or not they are true or false, or in terms of computational complexity theory, it is satisfiable.  $10 = 10$  evaluates to true or 1.  $01 \neq 10$  evaluates to true or 1 too.

### 3.13 Multiplicative Identity

The Identity of Itself on Multiplication

### 3.14 Additive Inverse

The Additive Inverse

General Equivalence

Commutativity under Equivalence

General Reversal

Commutativity under reversal

### 3.15 Multiplicative Inverse

Given a monomial such that it represents a monomial in a polynomial, if we loop around once, we see the identity path.

### 3.16 Generalized Operations

The set of images that describes the operations on monomials can be put together to find a 2x2 matrix that describes them using the laws provided.

### 3.17 Generalized Commutativity

For showing commutativity, have the following images to represent addition and multiplication.

### 3.18 Associativity Of Addition

Associativity of addition is defined as:

$$a + (b + c) = (a + b) + c$$

### 3.19 Associativity Of Multiplication

Associativity of multiplication is defined as:

$$a * (b * c) = (a * b) * c$$

### 3.20 Distributivity

Distributivity is defined as:

$$a * (b + c) = a * b + a * c$$

### 3.21 Field

The Field Axioms are defined as:



## Appendix A

# Frequently Asked Questions

### A.1 How do I change the colors of links?

The color of links can be changed to your liking using:

```
\hypersetup{urlcolor=red}, or  
\hypersetup{citecolor=green}, or  
\hypersetup{allcolor=blue}.
```

If you want to completely hide the links, you can use:

```
\hypersetup{allcolors=.}, or even better:  
\hypersetup{hidelinks}.
```

If you want to have obvious links in the PDF but not the printed text, use:

```
\hypersetup{colorlinks=false}.
```