Fall 2016

Random Walks on Thompson's Group F

Sarah C. Ghandour
Bard College

Random Walks on Thompson's Group F

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Sarah Ghandour

Annandale-on-Hudson, New York
May, 2017

Abstract

In this paper we consider the statistical properties of random walks on Thompson's group F. We use two-way forest diagrams to represent elements of F. First we describe the random walk of F by relating the steps of the walk to the possible interactions between two-way forest diagrams and the elements of $\{x_0, x_1\}$, the finite generating set of F, and their inverses. We then determine the long-term probabilistic and recurrence properties of the walk.

Contents

Dedication

I dedicate this project to my parents.

Acknowledgments

I begin by thanking my advisor, Jim Belk, for his persistence and guidance in helping me complete this project. Thank you for constantly pushing me forward.

My time at Bard would have been a much less rewarding and enjoyable experience had it not been for the friends I made along the way. I have to thank Bridget Bertoldi and Rosemary Nelis for the past five years of friendship, love, support, and laughter. They helped make the Hudson Valley my second home and I could not have survived without them.

Nicole Lang, my roommate, has been a constant source of strength, love, and light. Our four years together as roommates are some of my fondest memories.

I want to thank Gitta Markó for her unwavering love and support. In the moments when I thought I would never finish, she was there to remind me otherwise. Thank you for being patient with me and for loving me no matter what.

A big, massive thanks goes to Eileen Brickner for keeping me sane and always keeping me laughing when the times got tough.

Lastly, I would like to thank my loving parents. My Mom has been my biggest cheerleader and supporter. Thank you for teaching me to work hard, to stand up for myself, and to never give up. Thank you for being my best friend and always just a phone call away. I have to thank my Dad for tirelessly helping me throughout this process. I could not have completed this without him. I will be forever grateful to him for the incredible amount of support and time he gave me.

1
Introduction

Thompson's groups F, T and V were introduced by Richard Thompson in 1965 in connection with his work in logic. He and McKenzie used them to construct finitely-presented groups with unsolvable word problems. This project exclusively considers Thompson's group F.

Thompson's group F appears in many different and diverse areas of mathematics. Obviously, it is prominent in group theory. It also comes up in areas as diverse as cryptography [10] and, less surprisingly, combinatorics.

Thompson's group F is fairly widely researched and is still a very active area in mathematics. There are still some important unanswered questions. Chief among these is whether Thompson's group F is amenable.

Thompson's group F has many different representations which allows for a variety of points of view in studying the properties of the group. in addition to the standard group presentation, there are also piecewise-linear homeomorphisms, rectangle diagrams, rooted binary trees and forest diagrams. Each of these logically equivalent representations provide a different perspective on this group. In this project, we will focus on the forest diagram representation and its relation to the finite-generator presentation of F.

Combinatorially, the finite group presentation of F is

$$F = \langle x_0, x_1 | x_1^{-1} x_2 x_1 = x_3, x_1^{-1} x3 x_1 = x_4 \rangle,$$

where

$$x_2 = x_0^{-1} x_1 x_0, \quad \text{and} \quad x_3 = x_0^{-2} x_1 x_0^2, \quad \text{and} \quad x_4 = x_0^{-3} x_1 x_0^3.$$

Another way of looking at Thompson's group is by way of piecewise linear homeomorphisms. These are homeomorphisms from the interval $[0, 1]$ to $[0, 1]$. The functions satisfy these four conditions:

1. The function is piecewise linear.
2. The function is differentiable except at finitely many points.
3. Each of these points is a dyadic rational number, i.e. a rational number whose denominator is a power of 2.
4. On the intervals of differentiability, the derivatives are powers of 2.

In this case, the elements of the group are simply the homeomorphisms themselves and the operation is the composition of functions. It is fairly easy to see that, since the $f_0(x)$ is always a power of 2, $f(x_i)$ where x_i is a point of non-differentiability, is also a dyadic rational number. Therefore any f^{-1} is well-defined and so every element of this group has an inverse (geometrically, a reflection about the line $y = x$). The identity is simply the line $f(x) = x$. This group is a subgroup of the group of all homeomorphisms from $[0, 1]$ to $[0, 1]$.

Thompson's group may also be interpreted geometrically by way of a rectangle diagram representing $f(x)$. These diagrams simply have the top representing the pre-image of the above functions and the bottom representing the image of the function. [2]

Example 1.0.1. In this paper, we will exclusively consider the two-way forest diagram interpretation of the elements of F [BB]. Forest Diagrams have been created as an alternative representation of F. Belk presents two-way forest diagrams as a way of presenting elements of this group that interact particularly well with the finite generating set $\{x_0, x_1\}$.

A two-way binary forest is a sequence $(\cdots, T_{-1}, T_0, T_1, \cdots)$ of finite binary trees with a pointer at T_0, the Base tree. A trivial tree, one with no branches and a single leaf, is represented as a dot. (Dots represent terminal leaves.) The simplest non-trivial tree is represented as a caret placed on top of two adjacent dots. Starting from the identity, the Base caret is the result of left-multiplication by x_1.

Below is a visual example of a typical Forest Diagram.

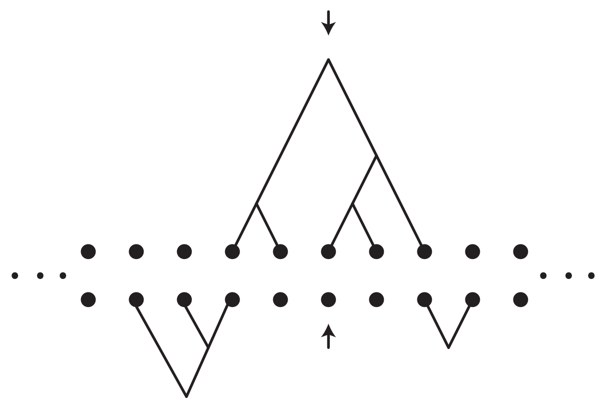

Figure 1.0.1. A typical forest diagram.

$\diamondsuit$

Amenability of Thompson's group F has been investigated through computational explorations which examine the long term behavior of of random walks on Thompson's group F [4]. Results from these explorations remain statistical and speculative, mainly due to computational constraints and because of the unfeasibility of exhaustively sampling random walk trajectories even of modest length. No closed-form expressions of the long term probabilities are presented. Simulation projections and possible lower bounds are presented.

In this paper we specifically investigate the probability that starting from a Base caret, a random walk on F will never delete this caret. We obtain exact solution to this probability. Our approach is two fold:

1. We examine random walks on F whose trajectories are functions of the elements of F, namely the depth of the Base tree, and the position of the top pointer relative to the Base tree.

2. We reformulate these random walk as a gambler's ruin problem, and compute probabilities of winning for a finite goal. The limits of the probabilities as the goal goes to infinity produce the desired results.

2
Simple Random Walk

A simple random walk represents random motion on a lattice, for example $\mathbb{Z}^d$, of a walker that jumps at discrete time steps $t = 1, 2, 3, ...$ to a randomly chosen site on the lattice. A random variable is associated with each step; the distribution of these random variables define the behavior of the walk. A simple symmetric random walk on $\mathbb{Z}^d$ is one where the successive steps are chosen independently. The steps are all of size 1 and are chosen uniformly randomly (with equal probability) out of the $2d$ possible directions on $\mathbb{Z}^d$.

2.1 Probability Definitions

Here we will briefly review definitions from probability.

Definition 2.1.1. An **outcome** is the result of a single trial in an experiment and the **sample space** of an experiment is the set of all possible outcomes of that experiment denoted by S. △

Example 2.1.2. If an experiment were to determine the sex of a newborn child, then the possible outcomes would be a male or female. If the outcome of an experiment is the sex of a newborn child, the sample space would be: $S = \{m, f\}$ where m is the outcome where the child is male and f is the outcome where the child is female. ◊

Definition 2.1.3. An **event** any subset E of the sample space. $\triangle$

In other words, an event is a set consisting of possible outcomes of the experiment. If the outcome of the experiment is contained in E, then we say that E has occurred. Events are very important in probability. Every event E has a probability $P(E)$ of occurring.

Example 2.1.4. If $E = \{f\}$ then E is the event that the child is female. $\Diamond$

Definition 2.1.5. A **random variable** is a function whose domain is a sample space and whose range is some set of real numbers. $\triangle$

If the random variable is denoted by X and has the sample space $S = \{o_1, o_2, ..., o_n\}$ as domain, then we write $X(o_k)$ for the value of X at element o_k. Thus $X(o_k)$ is the real number that the function rule assigns to the element o_k of S. If a random variable has codomain S we call it a random variable on S.

Example 2.1.6. Let $S = \{1, 2, 3, 4, 5, 6\}$ and define X as follows:

$$X(1) = X(2) = X(3) = 1, X(4) = X(5) = X(6) = -1$$

Then X is a random variable whose domain is the sample space S and whose range is the set $\{1, -1\}$. X can be interpreted as the gain of a player in a game in which a die is rolled, the player winning 1 dollar if the outcome is 1 ,2, or 3 and losing 1 dollar if the outcome is 4,5,6. $\Diamond$

Example 2.1.7. Two dice are rolled and we define the familiar sample space

$$S = \{(1, 1), (1, 2), ...(6, 6)\}$$

containing 36 elements. Let X denote the random variable whose value for any element of S is the sum of the numbers on the two dice. Then the range of X is the set containing the 11 values of $X : 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$. Each ordered pair of S has associated with it exactly one element of the range. But, in general, the same value of X arises from many different outcomes. For example $X(o_k) = 5$ is any one of the four elements of the event $\{(1, 4), (2, 3), (3, 2), (4, 1)\}$.

$\diamondsuit$

Definition 2.1.8. A **probability function** is a function f whose value for each real number x is given by $f(x) = P(\{o_k \in S|X(o_k) = x\})$. $f(x)$ is called the probability function of the random variable X. $\triangle$

Example 2.1.9. Consider Example 2.1.6, if the coin is fair, then $f(heads) = P(X = heads) = 0.5$ and $f(tails) = P(X = tails) = 0.5$, and $f(x) = 0$ otherwise. $\diamondsuit$

Example 2.1.10. If both dice in Example 2.1.7 are fair and the rolls are independent, so that each sample point in S has probability $1/36$, then we compute the value of the probability function at $x = 5$ as follows: $f(5) = P(X = 5) = P(\{(1,4),(2,3),(3,2),(4,1)\}) = 4/36$. This is the probability that the sum of the numbers on the dice is 5. We can compute the probabilities $f(2), f(3), ..., f(12)$ in an analogous manner. $\diamondsuit$

Definition 2.1.11. A variable is **identically** and **independently distributed** if each random variable has the same probability distribution as the others and are all mutually independent. $\triangle$

Definition 2.1.12. Independence is when the conditional probability equals the probability. $\triangle$

Definition 2.1.13. The **conditional probability** of an event B is the probability that the event will occur given the knowledge that an event A has already occurred.

This probability is written $P(B|A)$, notation for the probability of B given A. In the case where events A and B are independent (where event A has no effect on the probability of event B), the conditional probability of event B given event A is simply the probability of event B, that is $P(B)$. $\triangle$

Example 2.1.14. In a card game, suppose a player needs to draw two cards of the same suit in order to win. Of the 52 cards, there are 13 cards in each suit. Suppose first the player draws a heart. Now the player wishes to draw a second heart. Since one heart has already been chosen, there are now 12 hearts remaining in a deck of 51 cards. So the conditional probability $P(\text{Draw second heart}|\text{First card a heart}) = 12/51$. ♢

2.2 Definition of a Random Walk

Definition 2.2.1. The discrete random variables $X_1, X_2, \cdots$ on $\mathbb{Z}^d$ are the steps of the **random walk** with the following probability distribution: For all $i \in \mathbb{N} : P(X_i = s) = 1/2d$ if $s \in \mathbb{Z}^d$ and $\|s\| = 1$, and $P(X_i = s) = 0$ otherwise. △

$S_0 = 0 \in \mathbb{Z}^d$. $S_n = X_1 + X_2 + \cdots + X_n$ for $n \in \mathbb{N}$ is the position of the random walk at time n. Description of what $d = 2$ is to be more clear...

Definition 2.2.2. The **trajectory** is the sequence $\{s_1, s_2, s_3, ...\}$ of states that the random walk goes through. △

Example 2.2.3. Below is a graphical representation of the trajectory of a simple random walk in one dimension; on the x-axis are the steps of the walk, and the y-axis is the state. ♢

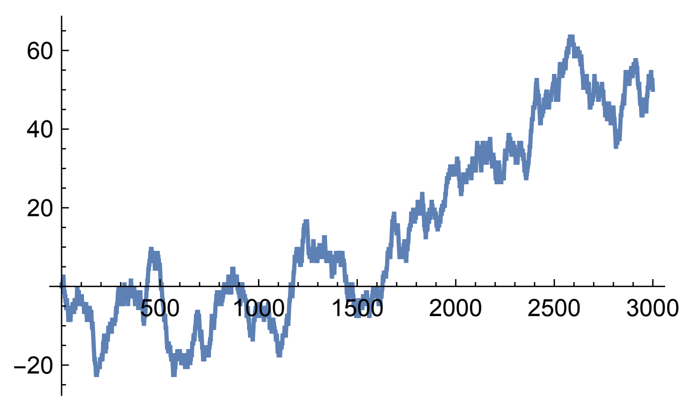

Figure 2.2.1. A random walk in one dimension.

Following are sample paths of a simple random walk in two and three dimensions,. The red dot marks the zero-position, the starting state of the walk.

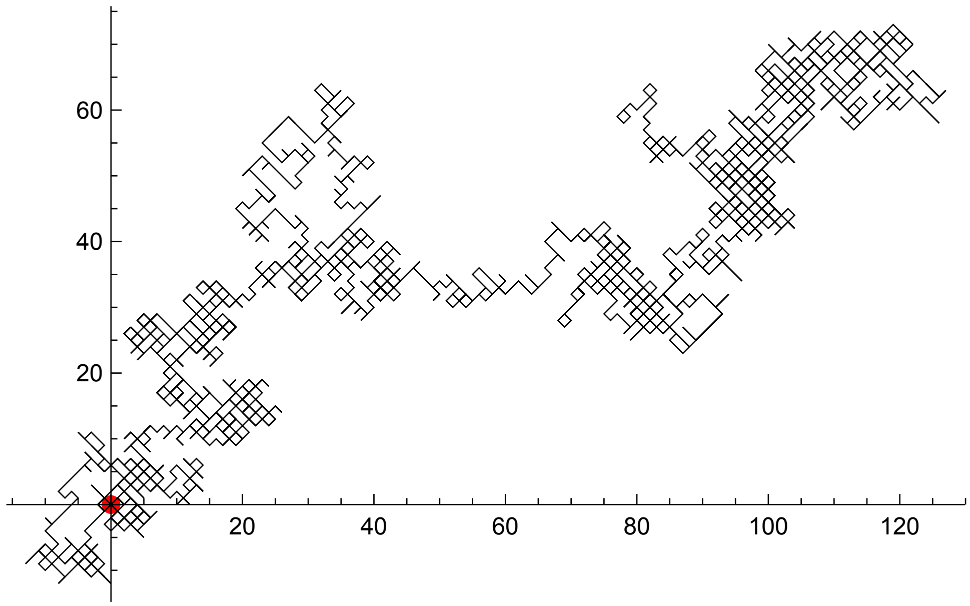

Figure 2.2.2. A random walk in two dimensions.

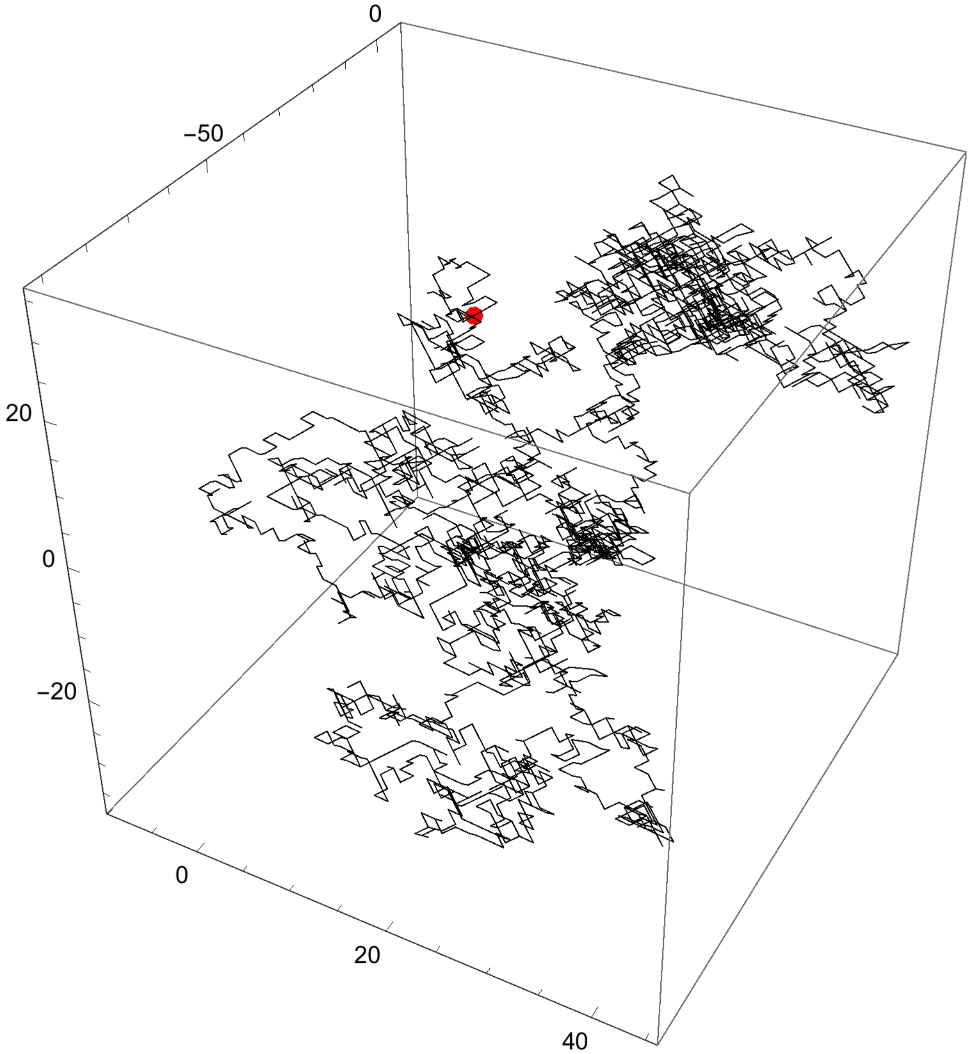

Figure 2.2.3. A random walk in three dimensions.

2.3 Biased Random Walk

Definition 2.3.1. A **Biased Random Walk** on the integers is one where the probability of $+1$ is not equal to the probability of -1. △

Example 2.3.2. Below is an example of a biased random walk. The probability of moving right is 55% and the probability of moving left is 45%. As we can see, the walk quickly moves to the right even with this slight bias.

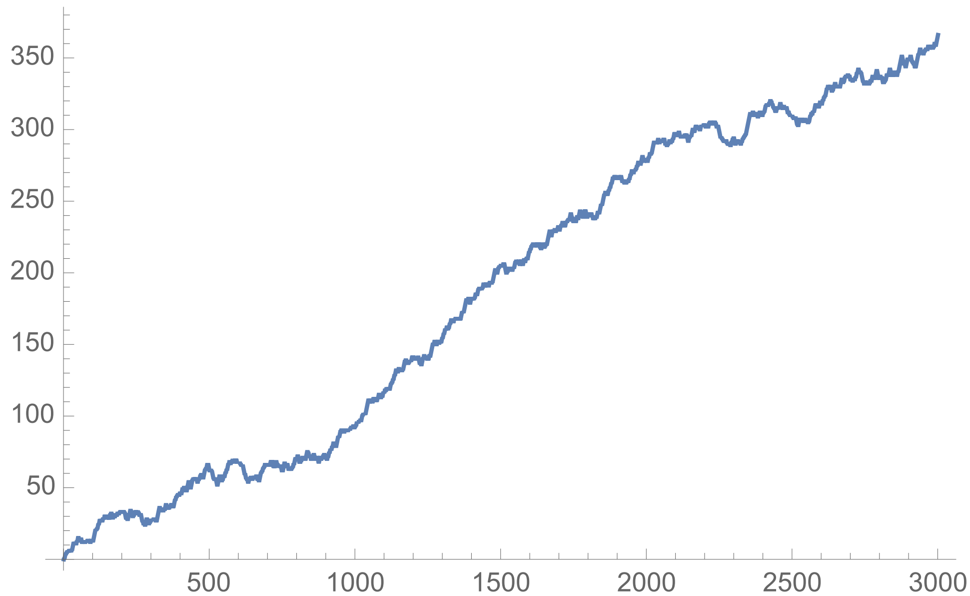

Figure 2.3.1. A biased radom walk.

◊

2.4 Markov Chains

Definition 2.4.1. A **Markov Chain** is collection of random variables X_t (where the index t runs through $0, 1, ...$) having the property that, given the present, the future is conditionally independent of the past. [?\edefn, Papoulis]

In other words,

$$P(X_t = j|X_0 = i_0, X_1 = i_1, ..., X_(t-1) = i_(t-1)) = P(X_t = j|X_(t-1) = i_(t-1)).$$

So if a *Markov sequence* of random variates X_n take the discrete values $a_1, ..., a_N$, then

$$P(x_n = a_(i_n)|x_(n-1) = a_(i_(n-1)), ..., x_1 = a_(i_1)) = P(x_n = a_(i_n)|x_(n-1) = a_(i_(n-1))),$$

and the sequence x_n is called a Markov chain.

We can describe a Markov chain as follows: We have a set of *states*, $S = \{s1, s2, ..., sr\}$. The process starts in one of these states and moves successively from one state to another. Each move is called a step. If the chain is currently in state s_i, then it moves to state s_j

at the next step with a probability denoted by p_{ij}, and this probability does not depend upon which states the chain was in before reaching the current state.

The probabilities p_{ij} are called *transition probabilities*. The process can remain in the state it is in, and this occurs with probability p_{ii}. An initial probability distribution, defined on S, specifies the starting state. In this paper we deterministically specify a particular state as the starting state.

2.5 Markov Chain Representation of Forest Random Walk

The random walk on Thompson's Group F (F) can equivalently be represented as a discrete-time stochastic process with countably-infinite state space composed of the elements of F. We index the elements of the state space, F, by $\mathbb{N}$, such that for $f_i, f_j \in F$, $f_i = f_j$ if and only if $i = j$ for all $i, j \in \mathbb{N}$. We define f_0 as the identity element of F. From here on, we will refer to the elements of F by their index number.

Let $X_t, t \in \mathbb{N}$ be the observed state of the process after t steps. X_0 is the initial state of the process. Without any significant loss of generality, we will consider the case where we start the process from the identity element, that is $X_0 = 0$.

Let P be the infinite-dimensional one-step probability transition matrix of this process with entry $p_{ij} = \mathrm{Pr(X_t = j|X_{t-1} = i)}$ for $t, i, j \in \mathbb{N}$ and $t > 0$. In words, p_{ij} is the probability that the process being in state i after $t-1$ steps transitions to state j in next step, t.

By the specification of this random walk, the process is a discrete-time time-homogeneous countable-state-space Markov Chain (MC).

Definition 2.5.1. The probability of transitioning to the next future state only depends on the present state of the process. Specifically, this one-step transition probability is independent of the past history of the process that culminated in the present state. The **Markov property** is also, more descriptively, called the memoryless property. This property is a direct consequence of the way the random walk is defined, where the step probabilities are the same regardless of the past or the current state. △

The transition probabilities are time-homogeneous, meaning that p_{ij} does not depend on how long the process has been running or, equivalently, at which step in the development of the process the transition takes place.

As a consequence of the Markov property and a countable state space, the process also has the strong Markov property. This means that at each subsequent visit to a specified state i, the process starts anew and behaves as if $X_0 = i$.

So just from the definition of the random walk, we see that it is equivalent to a countable-state MC whose transition probabilities are time-homogeneous.

Here are some more properties of this MC. I state those without proof (We can talk about these.)

The MC is irreducible. This means that for all possible ordered pairs of states $i, j \in \mathbb{N}$, there is a positive probability that, starting in state i the process visits state j in a finite number of steps. In this case we say elements i and j communicate The relation 'communicate' is an equivalence relation.

Showing that this is true requires a definition of a trajectory of the process. Recall that in its finite presentation, F has two generators x_0, and x_1 and each step of the MC corresponds to a left-multiplication of the present state of the MC by one member chosen at random from $\{x_0, x_1, x_0^{-1}, x_1^{-1}\}$, the generators of F and their inverses. So starting with the identity ($X_0 = 0$), each successive state of the MC (an element of F) is the result of iterative left multiplications. The sequence of these iterations is presented as a word from the alphabet set $\{x_0, x_1, x_0^{-1}, x_1^{-1}\}$. For example the one-letter word x_0 corresponds to a MC with $X_1 = x_0$; the two-letter word $x_0 x_1$ corresponds to $X_2 = x_1.x_0$;$x_0 x_1 x_0^{-1}$ corresponds to $X_3 = x_0^{-1}.x_1.x_0$, where . is the group operation of F.

It is clear from this notation that every element in F can be represented by one or more words with finite length. Thus every element of F can be reached can from the identity in a finite number of steps. Conversely, the identity can be reached in a finite number of steps from any element in F: given a finite length word (say of length n) that corresponds to an element in F, the identity can be reached in at most n steps, by a trajectory that is the inverse of the word representing the given element.

Therefore, every element can reach every other element in a finite number of steps via the identity element. Thus the MC is irreducible and F forms a single equivalence class.

The MC is periodic with period $= 2$. Let $p_{ij}^{(n)}$ be the probability that the MC with present state i reaches state j in n steps. The period of state i is defined as the $gcd(n)|p_{ii}^{(}n) > 0$. The MC can only return to its present state in an even number of steps, and gcd of positive even numbers is 2.

The random walk on F is considered in the context of exploring the amenability of F. This is due to the theorem by Kesten:

Theorem 2.5.2. *A group is amenable if and only if* $\lim_{L \longrightarrow \infty} sup\ p(L)^{1/L} = 1$. [7]

Here $p(L)$ is the probability of a random walk, starting from the identity, returning to the identity in L steps. The theorem states that a group is amenable if $p(L)$ decreases more slowly than exponentially with the number of steps, L.

For a specified finite number of steps, L, let m be the number of generators (here, m=2, $x_0, and x_1$).Thus, there are $(2m)^L = 4^L$ non-reduced possible paths (words) of length L. Let $T(L)$ be the set of length-L words which represent the identity. Then $p(L)$ can be directly measured as

$p(L) = \frac{|T(L)|}{4^L}$

This direct approach to obtaining $p(L)$ for F is not computationally feasible even for moderate values of L, since the computational times grow exponentially in L. As an example there are 2,684,354,456 paths (words) of length 14, out of which there are 1,988,452 represent the identity. [4]

In there computational explorations of F, Burillo, Cleary, and Wiest use a Monte Carlo method where they estimate $p(L)$ by taking random samples of paths (words) of a given length.

2.6 Transition Probabilities

Definition 2.6.1. Since the $X_i s$ are identically and independently distributed random variables the future position is only dependent on the current position regardless of the path taken to reach it. Thus the simple random walk is a Markov chain with state space $\mathbb{Z}^d$. $\triangle$

Proposition 2.6.2. *Let $p(l) = P(X_1 = l) = P(S_1 = l)$, the one-step transition probability starting from S_0. $p(l) = 1/2d$ for l a "neighbor" (distance equals 1) of S_0, and 0 otherwise. Also, let $P_n(l) = P(S_n = l)$ be the n-step transition probability, that is the probability the walk is at position l at time n, starting at S_0.*

2.7 Recurrence

Definition 2.7.1. One of the properties of the long term behavior of the random walk is whether the walker returns to S_0. Let S_n be a random walk. Let R be the probability that the walker eventually returns to S_0. If $R = 1$, then S_0 is **recurrent**; if $R < 1$, then S_0 is transient. If S_0 is recurrent, the walk returns to S_0 infinitely many times. If S_0 is **transient**, then there is a positive probability, $1 - R$, that the random walk may never return to S_0. $\triangle$

Let N denote the number of returns to S_0. In the transient case, N, the number of returns to S_0 (returns = failures to escape) before moving away for good (success = escape), follows the geometric distribution with parameter $1-R$, the probability of success. The probability mass function of the distribution, in this case, is

$P(N = k) = (1 - (1 - R))^k(1 - R) = R^k(1 - R)$ for $k = 0, 1, 2, ...$ (The probability of k returns then escape)

Therefore the expected number of returns to a transient S_0 is $\frac{R}{1-R}$, the mean of the geometric distribution.

In a random walk all states communicate, i.e. every position is reachable from every other position. Thus the whole walk is recurrent/transient if S_0 is recurrent/transient.

2.8 Polýa's Theorem

Theorem 2.8.1. *Simple random walks of dimension $d = 1, 2$ are recurrent, and of $d \geq 3$ are transient.*

General criterion for classifying S_0 as recurrent or transient:

Theorem 2.8.2 (Polýa's Theorem)**.** *The state S_0 is transient if and only if $\sum_{n=1}^{\infty} P_n(0) < \infty$.*

Proof. The indicator variable I_t, for $t \in \mathbb{N}$, as $I_t = 1$ if $S_t = 0$, and $I_t = 0$ otherwise. Thus $N = \sum_{t=1}^{\infty} I_t$ is the number of times S_0 is revisited. So the expectation of N is

$$E[N] = E\left[\sum_{t=1}^{\infty} I_t\right] = \sum_{t=1}^{\infty} E[I_t] = \sum_{t=1}^{\infty} P(S_t = 0) = \sum_{t=1}^{\infty} P_t(0).$$

Another expression of $E[N]$ is

$$E[N] = \sum_{k=0}^{\infty}[1 - P(N \leq k)] = \sum_{k=1}^{\infty} P(N \geq k) = \sum_{k=1}^{\infty} R^k$$

The above expression of $E[N]$ is the discrete version of the expectation of an arbitrary random variable, X, where

$$E[X] = \int_0^{\infty} [1 - F_X(x)]dx - \int_{-\infty}^{0} F_X(x)dx,$$

where $F_X(x)$ is the cumulative distribution function of X. The last equality is because each of the N returns to S_0 occurs independently with probability R.

So we have

$$E[N] = \sum_{t=1}^{\infty} P_t(0) = \sum_{k=1}^{\infty} R^k$$

The sum diverges if $R = 1$, that is, if S_0 is recurrent, and converges if $R < 1$, that is, if S_0 is transient.

Computing $\mathbf{P_n(0)}$ *for* $\mathbf{d = 1}$*:*

Any path the random walk takes on a horizontal one-dimensional lattice from S_0 to S_0 must have an even number of steps, with equal number of steps to the left as to the right. Therefore $P_{2n+1}(0) = 0$, (probability of return to S_0 after an odd number of steps = 0) and

$$P_{2n}(0) = \binom{2n}{n}\left(\frac{1}{2}\right)^n\left(\frac{1}{2}\right)^n = \frac{(2n)!}{n!(2n-n)!}\frac{1}{2^{2n}}.$$

(the number of different specific paths of length $2n$ from S_0 to S_0 [n left steps and n right steps] times the probability of any specific path of length $2n$ with independent steps each with probability 1/2.)

Using Stirling's approximation of $n! \approx n^n e^{-n}\sqrt{2\pi n}$ as $n \longrightarrow \infty$, and substituting we get

$$P_{2n}(0) \approx \frac{2^{2n}n^{2n}e^{-2n}\sqrt{4\pi n}}{n^{2n}e^{-2n}2\pi n}\frac{1}{2^{2n}} = \frac{1}{\sqrt{\pi n}} asn \longrightarrow \infty.$$

One-dimensional random walk is recurrent:

In the one-dimensional random walk,

$$\sum_{n=1}^{\infty} P_n(0) = \sum_{n=1}^{\infty} P_{2n}(0) \approx \sum_{n=1}^{\infty}\frac{1}{\sqrt{\pi n}} > \frac{1}{\pi}\sum_{n=1}^{\infty}\frac{1}{n} = \infty.$$

(the first equality is because we can skip over odd number of steps because they have probability 0.)

So the one-dimensional random walk is recurrent. □

Two-dimensional random walk is recurrent:

For a single two-dimensional walk, define two one-dimensional walks as follows:

Let $S_n = (S_n^1, S_n^2)$ be the two-dimensional position after n moves, where S_n^1, S_n^2 are the positions of the component two one-dimensional walks. The steps of a random walk are the differences between successive positions. Here, the two dimensional step, $X_i = (X_i^1, X_i^2)$

can take the values: North = $(+1, +1)$, East = $(+1, -1)$, South = $(-1, -1)$ and West = $(-1, +1)$.

So in this way, any two independent one-dimensional random walks correspond precisely to a single two-dimensional random walk and *vice versa*.

Therefore, for a two-dimensional walk we can write

$$P_{2n}(0) = P(S_{2n} = 0) = P(S_{2n}^1 = 0)P(S_{2n}^2 = 0) \approx (\frac{1}{\sqrt{\pi n}})^2 = \frac{1}{\pi n}$$

and since $P_{2n+1}(0) = 0$, the sum over n gives

$$\sum_{n=1}^{\infty} P_n(0) = \sum_{n=1}^{\infty} P_{2n}(0) \approx \frac{1}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

Thus, as is the one-dimensional random walk, the two-dimensional random walk is recurrent.

Random walk in three or more dimensions is transient:

The general method for proving recurrence or transience of random walks is based on the well-known theorem for Markov chains due to Chapman and Kolmogorov which defines a recurrence relationship to express higher-step transition probabilities in terms of lower step transition probabilities. Discrete Fourier transform can be used to solve the recurrence relation.

A simpler and more directly applicable method for determining the recurrence or transience of a simple random walk is presented in G. F. Lawler and L. N. Coyle *Lectures on Contemporary Probability* [8]

For a random walk in d dimensions, the probability that the random walker, starting at the origin, returns to the origin in $2n$ steps is a costant times $n^{-d/2}$. The reasoning is that, after n steps the walker tends to be a distance about $\sqrt{n}$ from the origin. In $\mathbb{Z}^d$, there are about $n^{d/2}$ points within distance $\sqrt{n}$ from the origin. Thus, the probability of choosing a specific one of these points is of order $n^{-d/2}$.

Proof. Let $Y_j = 1$ if $S_{2j} = 0$ and $Y_j = 0$ otherwise. Then the number of visits to the origin up through time $2n$ is given by the random variable $R_n = Y_0 + \cdots + Y_n$. And the total number of visits is

$$R_\infty = Y_0 + Y_1 \cdots .$$

Then the expected number of returns to the origin in n steps is: $E[R_n] = \sum_{j=0}^{n} P(S_{2j} = 0)$.

For $d \geq 3$,

$$R[R_\infty] = \sum_{j=0}^{\infty} P(S_{2j} = 0)b \leq 1 + constant \sum_{j=1}^{\infty} j^{-d/2} < \infty.$$

Thus, for $d \geq 3$, the expected number of returns to the origin is finite. And the random walk is transient. □ □

3
Random Walks on Groups

Definition 3.0.1. Let G be a group and $S = \{s_1, s_2, s_3, ..., s_n\}$ S is symmetric if $S = S^{-1}$ Every group element can be written as $S_{i_1}^{j_1}, S_{i_2}^{j_2}, S_{i_3}^{j_3}, ..., S_{i_k}^{j_k}$. This is a word in S. △

Definition 3.0.2. Thompson's Group F is defined as the group presentation:

$$F = \langle x_0, x_1 | x_1^{-1} x_2 x_1 = x_3, x_1^{-1} x_3 x_1 = x_4 \rangle,$$

where

$$x_2 = x_0^{-1} x_1 x_0, \quad \text{and} \quad x_3 = x_0^{-2} x_1 x_0^2, \quad \text{and} \quad x_4 = x_0^{-3} x_1 x_0^3.$$

△

Definition 3.0.3. Let G be a group and let S be a random walk on Z. is **non-amenable** if there exist constants $C > 0$ and $0 < r < 1$ so that $P(S_n = e) < Cr^n$ for all n. △

If the limit of the nth root of that probability < 1 then that implies non-amenability.

3.1 Thompson's Group F and Forest diagrams

Thompson's group F (F) was introduced by Richard J. Thompson in the 1960's. Thompson's Group F is usually defined as "the group of piecewise-linear orientation-preserving homeomorphisms of the unit interval, where each homeomorphism has finitely many changes of slope which all are dyadic integers and and whose slopes, when defined, are powers of 2" [BCW].

F presented the first example of a finitely presented infinite simple group. Since then, F has been used in other branches of mathematics, cryptography and computer science. F also is indicated in situations where there are groups actions on binary tree and still stands as the simplest non-trivial examples of a diagram group [6]. Since its discovery, mathematicians have been trying, without success, to solve the amenability problem for F.

Forest Diagrams have been created as an alternative representation of F. Belk presents two-way forest diagrams as a way of presenting elements of this group that interact particularly well with the finite generating set $\{x_0, x_1\}$. A two-way binary forest is a sequence $(\cdots, T_{-1}, T_0, T_1, \cdots)$ of finite binary trees with a pointer at T_0. A trivial tree, one with no branches and a single leaf, is represented as a dot. The simplest non-trivial tree is represented as a caret placed on top of two adjacent dots. [2]

Here is the forest diagram of the identity element of F

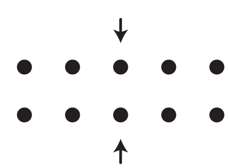

Figure 3.1.1. The forest diagram of the identity element of F.

And here are the two way forest diagrams of x_0 and x_1, the elements of the finite generating set of F.

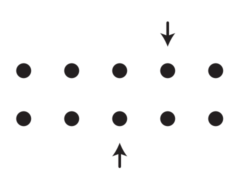

Figure 3.1.2. The first generator, x_0 of F.

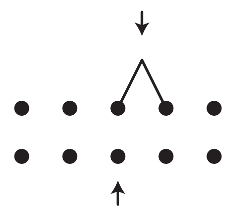

Figure 3.1.3. The second generator, x_1 of F.

And below are the two inverses of the generators of F.

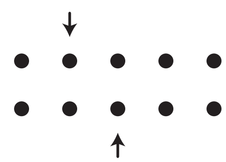

Figure 3.1.4. The inverse of x_0

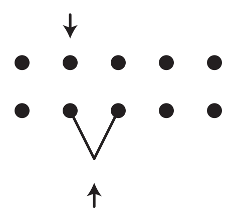

Figure 3.1.5. The inverse of x_1.

Example 3.1.1. There is a third generator of F we call y. This generator is a combination of the steps, x_0 and x_1. Below, is an example of y.

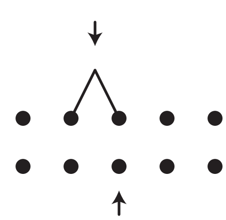

Figure 3.1.6. The generator y or steps x_0^{-1} followed by x_1.

$\diamondsuit$

Example 3.1.2. Below we will give examples of some different combinations of steps on the forest diagram.

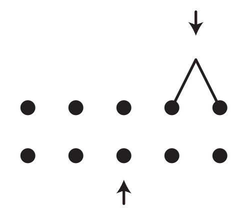

Figure 3.1.7. The steps x_0 then x_1.

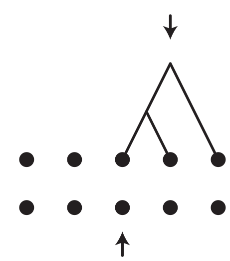

Figure 3.1.8. The steps x_1 then x_1.

$\diamondsuit$

Example 3.1.3. Below are three examples of caret deletion.

In Figure 2.1.8., we start with a top caret. Then, we do the step x_1^{-1}:

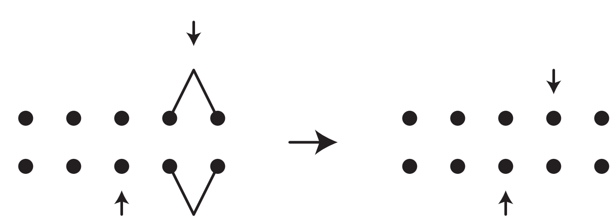

Figure 3.1.9. Example of caret deletion

Below is a second example of caret deletion. We start with a forest diagram with Base caret depth of 2.

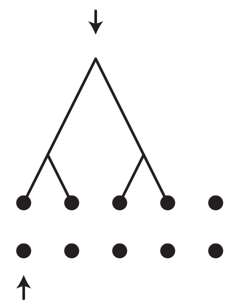

Figure 3.1.10. Step 1 of caret deletion

Then we do the step x_1^{-1}. This step then deletes the top caret and leaves us with Base tree of one caret, or Base tree caret depth of 1:

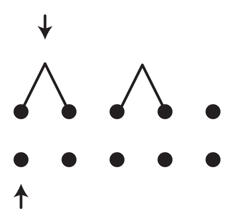

Figure 3.1.11. Step 3 of caret deletion

Below is the third example of caret deletion. We start with a typical forest diagram.

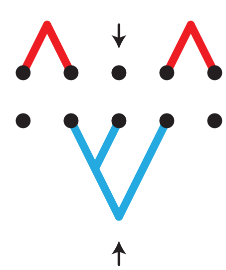

Figure 3.1.12. Step 1.

Then, we do the step x_1^{-1}. As we can see, this action inserts a bottom caret at the leaf pointed to by the top pointer. This action inserts a new leaf and expands the support of the forest diagram..

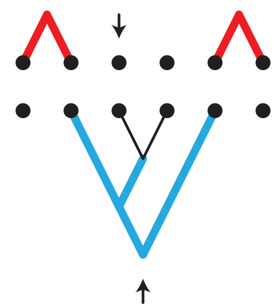

Figure 3.1.13. Step 2.

Of course left-multiplying by x_1 again we return to Figure 3.1.12. $\Diamond$

3.2 Forest Random Walk

Definition 3.2.1. The random walk on F is a series of randomly chosen actions of $\{x_0, x_1\}$ and their inverses. The actions of the generating set and the corresponding inverses are described in Belk Section 3.3 [1]:

Let f be a forest diagram for some $f \in F$. Then:

1. A forest diagram for $x_0 f$ can be obtained by moving the top pointer of f one tree to the right.

2. A forest diagram for $x_1 f$ can be obtained by attaching a caret to the roots of the 0-tree and 1-tree in the top forest of f. Afterwards, the top pointer points to the new, combined tree.

3. A forest diagram for $x_0^{-1} f$ can be obtained by moving the top pointer of f one tree to the left.

4. A forest diagram for $x_1^{-1} f$ can be obtained by 'dropping a negative caret' at the current position of the top pointer. If the current tree is nontrivial, the negative caret cancels with the top caret of the current tree, and the pointer moves to the resulting left child. If the current tree is trivial, the negative caret 'falls through' to the bottom forest, attaching to the specified leaf.

Now we formally define the random walk on F:

Let $\{x_0, x_1, x_0^{-1}, x_1{-}1\}$ be the set of generators of F and their inverses. Let $f_{n-1} \in F$ be the state of the random walk at step $n-1$ for $n = 1, 2, 3 \cdots$. Let $f_0 = e$, the identity of F. Then, f_n, the state of the walk after n steps is determined as

$$f_n = \begin{cases} x_0 f_{n-1} & \textit{with probability } 1/4 \\ x_0^{-1} f_{n-1} & \textit{with probability } 1/4 \\ x_1 f_{n-1} & \textit{with probability } 1/4 \\ x_1^{-1} f_{n-1} & \textit{with probability } 1/4 \end{cases}$$

$\triangle$

4
Immortality of the Base-Tree Caret

In this chapter, we will examine a model of the Gambler's Ruin problem applied to the immortality of the base caret. In evaluating the asymptotic behavior of the random walk on F all other studies to date use simulations and sampling, but do not produce closed-form expressions for these probabilities. In the following chapter, we derive exact probabilities that the base caret is never removed.

4.1 Gambler's Ruin Model

Here we will define some notation for and derive probabilities of winning, or alternatively, ruin.

$\boldsymbol{i}$ is the gambler's initial fortune, in currency units.

$\boldsymbol{X_n}$ is the gambler's fortune in units after n gambles.

$\boldsymbol{T}$ is the number of units that, if accumulated, the game ends and the gambler is a winner.

$\boldsymbol{P_i}$ is the probability that the gambler wins the game given that the initial fortune is i units.

While the game proceeds, $\{X_n : n \geq 0\}$ forms a simple random walk on the nonnegative integers with walk-terminating barriers at 0 and T.

Consider a gambler who starts with an initial fortune of i units and then on each successive gamble either wins one unit with probability p, loses 1 unit with probability q, or it's a draw, (i.e. neither wins nor loses) with probability r, independent of the past. (Of course, $p+q+r=1$.) Let X_n denote the total fortune in units after the n^{th} gamble. The gambler's objective is to reach a total fortune of T units, without first getting ruined (running out of units; $X_n = 0$). If the gambler succeeds, then the gambler is said to win the game. In any case, the gambler stops playing after reaching a fortune of T units or getting ruined, whichever happens first.

Theorem 4.1.1. *The probability that a gambler in the above setup reaches a total fortune of T units, given an initial fortune of i units is*

$$P_i = \begin{cases} \frac{1-(\frac{q}{p})^i}{1-(\frac{q}{p})^T}, & if\ p \neq q \\ \frac{i}{T}, & if\ p = q. \end{cases} \tag{4.1.1}$$

Proof. The current fortune after n gambles is

$$X_n = i + \Delta_1 + \Delta_2 + \cdots \Delta_n, X_0 = i,$$

where $\{\Delta_n\}$ forms an i.i.d. sequence of random variables distributed as $P(\Delta = 1) = p, P(\Delta = -1) = q$, and $P(\Delta = 0) = r$, where $p+q+r=1$, and represents the earnings on the successive gambles.

Since the game stops when either $X_n = 0$ (ruin) or $X_n = T$ (win), let

$$\tau_i = min\{n \geq 0 : X_n \in \{0, T\} | X_0 = i\}$$

denote the time at which the game stops when the initial fortune $X_0 = i$. If $X_{\tau_i} = T$ then the gambler wins, else if $X_{\tau_i} = 0$, then the gambler is ruined.

Let $P_i = P(X_{\tau_i} = T)$ be the probability that the gambler wins when $X_0 = i$. Clearly, $P_0 = 0$ and $P_T = 1$, by definition; so we go on to compute P_i for $1 \leq i \leq T-1$.

By conditioning on the outcome of the first gamble, $\Delta_1 = 1$, $\Delta_1 = -1$ or $\Delta_1 = 0$, we get the following recursion

$$P_i = pP_{i+1} + qP_{i-1} + rP_i \tag{4.1.2}$$

This recursion is derived as follows: If $\Delta_1 = 1$, then the gambler's total fortune increases to $X_1 = i+1$ and by the Markov property the gambler will win with probability P_{i+1}. Alternatively, if $\Delta_1 = -1$, then the gambler's fortune decreases to $X_1 = i-1$ and so by the Markov property the gambler will now win with probability P_{i-1}. Also, if $\Delta_1 = 0$ then the gambler's fortune does not change and so by the Markov Property the gambler will now win with probability P_i. The probabilities corresponding to the three outcomes are p, q and r, respectively, yielding the recursion (3.1.1).

Since $p+q+r = 1$, the recursion (3.1.1) can be re-written as $pP_i + qP_i + rP_i = pP_{i+1} + qP_{i-1} + rP_i$, yielding

$$P_{i+1} - P_i = \frac{q}{p}(P_i - P_{i-1}).$$

In particular, $P_2 - P_1 = (q/p)(P_1 - P_0) = (q/p)P_1$ (since $P_0 = 0$). And $P_3 - P_2 = (q/p)(P_2 - P_1) = (q/p)^2 P_1$. More generally

$$P_{i+1} - P_i = \left(\frac{q}{p}\right)^i P_1, 0 < i < T$$

Thus

$$P_{i+1} - P_1 = \sum_{k=1}^{i}(P_{k+1} - P_k) = \sum_{k=1}^{i}\left(\frac{q}{p}\right)^k P_1,$$

which yields

$$P_{i+1} = P_1 + P_1\sum_{k=1}^{i}(\frac{q}{p})^k = P_1\sum_{k=0}^{i}(\frac{q}{p})^k.$$

$$P_{i+1} = \begin{cases} P_1\frac{1-(\frac{q}{p})^{i+1}}{1-\frac{q}{p}}, & if\ p \neq q \\ P_1(i+1), & if\ p = q. \end{cases} \tag{4.1.3}$$

(Here For $p \neq q$ we use the sum of a geometric series.) Letting $i = T-1$ and using the fact that $P_T = 1$ we get

$$1 = P_T = \begin{cases} P_1\frac{1-(\frac{q}{p})^{T}}{1-\frac{q}{p}} & if\ p \neq q \\ P_1 T, & if\ p = q. \end{cases}$$

Solving for P_1 gives

$$P_1 = \begin{cases} \frac{1-\frac{q}{p}}{1-(\frac{q}{p})^T}, & if\ p \neq q \\ \frac{1}{T}, & if\ p = q. \end{cases}$$

Substituting in (3.1.2) we obtain the solution

$$P_i = \begin{cases} \frac{1-(\frac{q}{p})^i}{1-(\frac{q}{p})^T}, & if\ p \neq q \\ \frac{i}{T}, & if\ p = q. \end{cases} \tag{4.1.4}$$

□

Theorem 4.1.2. *When $p > q$, the probability of a gambler getting infinitely rich (i.e. is never ruined) is $1 - \left(\frac{q}{p})^i\right\rangle 0$.*

Proof. The probability that the gambler never loses is the limit of (3.1.3) as T goes to infinity. In our case $p > q$. Thus $\frac{q}{p} < 1$. Thus

$$P_i^{\infty} = \lim_{T \longrightarrow \infty} P_i = 1 - \left(\frac{q}{p}\right)^i > 0. \tag{4.1.5}$$

□

Theorem 4.1.3. *When $p = q$, the probability that us gambler gets infinitely rich (i.e. is never ruined) is zero.*

Proof. If $P = q$, the limit as T goes to infinity of $\frac{i}{T}$ is

$$P_i^{\infty} = \lim_{T \longrightarrow \infty} P_i = 0. \tag{4.1.6}$$

□

The above two theorems specify the probability of getting infinitely rich, that is having won an infinite number of units under the condition $p > q$ and $p = q$.

4.2 Gambling with Carets

Definition 4.2.1. Define the function $L : F \mapsto \{\cdots, Left2, Left1, Base, Right1, Right2, \cdots\}$ representing the ordinal location of the tree that the top pointer of a particular forest diagram is pointing to. In the following analysis the Base tree is initialized as the original element x_1 and that caret will always be part of the Base tree if and until it is deleted, of course. △

Definition 4.2.2. Define the function $D^l : L \mapsto \mathbb{N}$ as the left distance in trees between the top pointer location and the Base tree. If $L = Base$,then $D^l = 0$; if $L = Left1$, then $D^l = 1$; if $L = Left2$, then $D^l = 2$, and so on. D^l is undefined for $L \in \{Right1, Right2, \cdots\}$. Similarly, define the function $D^r : L \mapsto \mathbb{N}$ as the right distance in trees between the top pointer location and the Base tree. If $L = Base$,then $D^r = 0$; if $L = Right1$, then $D^r = 1$; if $L = Right2$, then $D^r = 2$, and so on. D^r is undefined for $L \in \{Left1, Left2, \cdots\}$. △

Definition 4.2.3. We define the function $C : F \mapsto \mathbb{N}$ as the depth (number of stacked carets) of the base tree. C is a function since once each and every element in F is identified by a unique reduced forest diagram; and for each forest diagram there can be but a single C. Starting from the, identity, $C = 0$, since the base tree is trivial and has no carets. A subsequent left-multiplication by x_1 gives $C = 1$. Then further left multiplying by x_1^{-1} removes the base-tree caret and gives $C = 0$. △

Definition 4.2.4. Instead of the two generators of F, $\{x_0, x_1\}$, here we use an alternative set of generators, namely $\{x_1, y\}$ where $y = x_1x_0^{-1}$. To be clear, for an element $f \in F$, $yf = x_1x_0^{-1}f$. That is f is first left-multiplied by x_0^{-1} and the resultant element is in turn left multiplied by x_1. As in the forest random walk described above, each step of the random walk on F involves a left multiplication of the current element by one of $\{x_1, y, x_1^{-1}, y^{-1}\}$ with equal probability of $1/4$. The choice of y as a generator makes the successive moves more symmetrical, as we shall see below. Formally, the state of the walk after n steps, in terms of the $\{x_0, x_1, x_0^{-1}, x_1^{-1}\}$ generator set is

$$f_n = \begin{cases} x_1 f_{n-1} & \textit{with probability } 1/4 \\ x_1^{-1} f_{n-1} & \textit{with probability } 1/4 \\ x_1 x_0^{-1} f_{n-1} & \textit{with probability } 1/4 \\ x_0^{-1} x_1^{-1} f_{n-1} & \textit{with probability } 1/4 \end{cases}$$

△

In what follows, we investigate the probability that the above random walk random walk on F, but whose trajectory records values of the function C, starting with $f_0 = x_1$ (that is $C = 1$) will never return to $C = 0$. In other words, what is the probability that once a caret is added to the trivial base tree, that caret is never removed? (Note that $C = 0$ can result from multiple elements of F, among them the identity.)

Starting from $f_0 = x_1$ having $C = 1$ left multiplication by either x_1, or y increases C by 1 (giving $C = 2$) while left multiplication by either x_1^{-1}, or y^{-1} decreases C by 1 (giving $C = 0$). Thus with probability 1/2, C increases from from 1 to 2 and with the same probability decreases from 1 to 0.

Once the random walk transitions from $C = 1$ to $C = 2$, the probability structure of the walk changes. Not every step will result in a change of C. Conditional on the top pointer being on Base, Left1 or Right1 (that is the vicinity of Base tree) and $C \geq 2$ the probability of an increase of one caret in C is 1/2 and that of a decrease in C of one caret is 1/4, and the probability of no change in C is 1/4. Note that changes in C can only take place if the top pointer of the forest diagram is in the vicinity of the Base tree (That is on the Base tree, one tree to the left of the base tree (Left1), or one tree to the right (Right1)).

Starting with the $C = 2$ this random walk is a variant of the gambler's ruin problem which we will address below. We also show that the gambler's ruin model can also be applied to random walks on F whose trajectories are the values of the functions D^l and D^r. The gambler's ruin models of the random walks provide a convenient tool for calculating the desired probabilities. These are the probability that once a caret is added to the trivial base tree, that caret is never removed, and the probability that starting from the vicinity of the Base tree, the top pointer eventually returns to the Base tree.

Example 4.2.5. Below is an example of the base tree caret and carets stacked on the base tree caret.

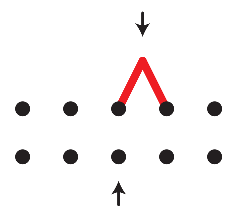

Figure 4.2.1. Base tree caret.

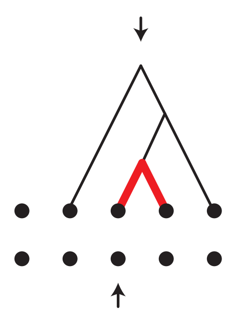

Figure 4.2.2. Carets stacked on the base tree caret. Base caret depth = 3.

◊

Below is a Markov Chain representation of the transition probabilities for moving left and right of the Base tree. We can see that in the immediate vicinity of the Base tree (that is the three trees: Left1, Base, and Right) the transition probabilities define a biased random walk where there is greater probability that the walker on either the Left1 or Right1 tree moves onto the Base tree than the walker who is on the the Base tree moves onto either the Left1 or Right1 trees. Elsewhere, the walk is balanced in terms of the top pointer moving right or left.

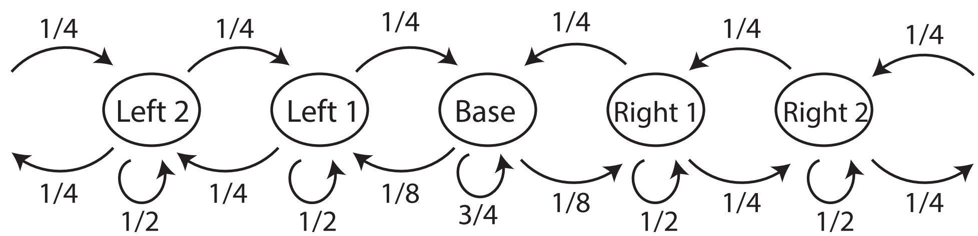

Figure 4.2.3. Transition probabilities for moving left and right of the base caret.

Below, is the same Markov Chain representation as figure 4.2.3, but with removing the probabilities that you stay on the current position.

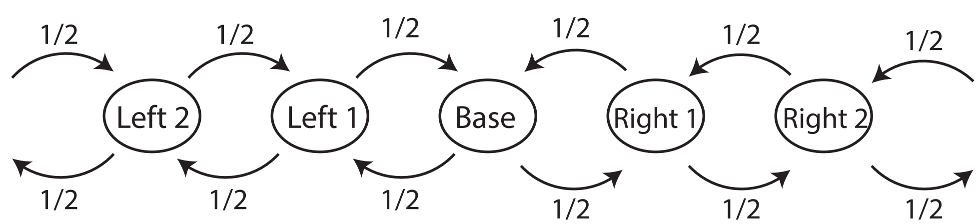

Figure 4.2.4. Conditional transition probabilities for moving left and right of the base caret.

Below, we use a Markov Chain representation to illustrate the transition probabilities for the depth of the base tree. In other words, this shows the probability one deletes the base tree, builds on the base tree, or moves left or right of the base tree.

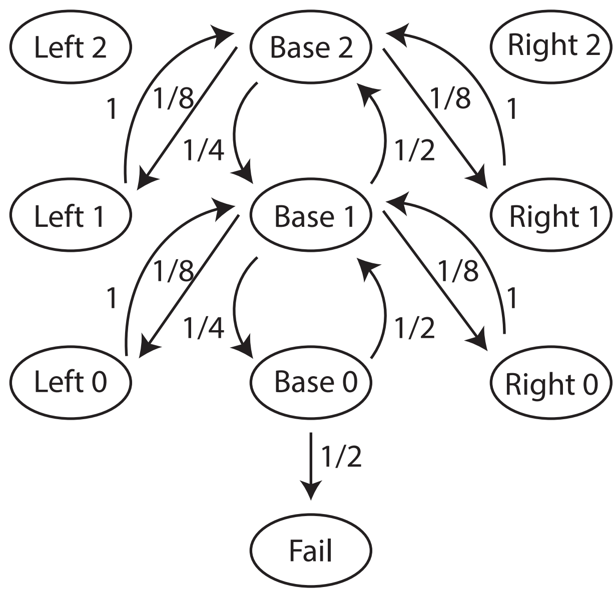

Figure 4.2.5. Transition probabilities for chain of depth of base tree.

In our case the random walk takes place in two phases: Phase one and starting with one caret on the base tree, then with equal probability of 1/2, the caret gambler either fails ($C = 0$) or gets to phase 2, to enter into a game with a beginning fortune of 2 carets and where the probability of winning a caret ($C \longrightarrow C + 1$) is $p = 1/2$ and probability of losing a caret ($C \longrightarrow C - 1$) is $q = 1/4$.

The probability that starting with two carets ($i = 2$) the gambler gets infinitely rich is

$$P_2^\infty = 1 - \left(\frac{(1/4)}{(1/2)}\right)^2 = \frac{3}{4}.$$

So under this scenario, starting with one caret on the Base tree, the probability that this caret is never destroyed, is the probability of moving from 1 caret to 2 carets (1/2) times the probability that starting with two carets ($i = 2$) the gambler gets infinitely rich (3/4):

$$\frac{P_2^\infty}{2} = \frac{3}{8}.$$

But this probability is based on the transition probabilities conditional on the top pointer being in the vicinity of the Base tree. So the next step is to compute the probability that starting in the vicinity of the Base tree, the top pointer returns to the Base tree.

To do this we random walks on F whose trajectories are the values of the functions D^l and D^r, described above: We consider first D^l and by symmetry we apply the results to D^r. The gambler's ruin model for D^l uses as currency the trees to the left of the Base. Starting with Left1 tree, the probability of moving to Left2 is $p = 1/4$ (this is the transition probability of $D^l = 1$ to $D^l = 2$ (winning a tree). Also, $q = 1/4$, the probability of moving from Left1 ($D^l = 1$) to the Base tree ($D^l = 0$). As we move the left of Left1 tree, these single step transition probabilities are unchanged. Thus the D^r random walk starting at Left1 tree can be reformulated as a gambler's ruin problem with initial fortune of 1 tree and $p = q$. But from (4.1.5) we know that the probability of winning an infinite number of trees is

$$P_i^\infty = \lim_{T \longrightarrow \infty} P_i = 0,$$

Since there can be only two outcomes of the game, the probability of returning to the Base tree is

$$1 - P_i^\infty = 1.$$

Thus with certainty the D^l random walk returns to the Base tree.

A symmetric argument for D^r random walk gives the same result for the right-hand gambler's ruin starting at Right1 tree.

Thus either starting from either Left1 or Right1, with with probability 1 the distance random walks return to the vicinity of the Base tree.

What about starting from the Base tree? The probability of returning to the base tree is

$$\frac{3}{4} + \frac{1}{8}(1 - P_i^\infty) + \frac{1}{8}(1 - P_i^\infty) = 1.$$

Thus starting in the vicinity of the Base tree the random walk returns with certainty, probability of 1.

Therefore, the unconditional probability that the Base caret is never removed is exactly the same probability conditional on the top pointer being in the vicinity of the base tree $= 3/8$.

Bibliography

[1] Jim Belk, *Thompson's group F*, arXiv preprint arXiv:0708.3609 (2007).

[2] James M and Brown Belk Kenneth S, *Forest diagrams for elements of Thompson's group F*, International Journal of Algebra and Computation **15** (2005), 815–850.

[3] Dimitri P. and Tsitsiklis Bertsekas John N., *Introduction to Probability*, M.I.T., Massachusetts, 2000.

[4] Josep and Cleary Burillo Puig Sean and Wiest, *Computational explorations in Thompson's group F* (2005).

[5] Persi Diaconis, *Random walks on groups: characters and geometry*, Groups St Andrews 2001 in Oxford **1** (2002), 120–142.

[6] Victor S and Sapir Guba Mark V, *Diagram groups*, Memoirs of the Amer. Math. Soc **130** (1996), 1–117.

[7] Harry Kesten, *Symmetric random walks on groups*, Transactions of the American Mathematical Society **92** (1959), 336–354.

[8] Gregory F and Coyle Lawler Lester Noel, *Lectures on Contemporary Probability*, Vol. 2, American Mathematical Soc., 1999.

[9] Athanasios Papoulis, *Brownian Movement and Markoff Processes*, McGraw-Hill, New York, 1984.

[10] Vladimir and Ushakov Shpilrain Alexander, *Thompson?s group and public key cryptography*, International Conference on Applied Cryptography and Network Security **v1** (2005), 151–163.