

# A proof that HT is more likely to outnumber HH than vice versa in a sequence of $n$ coin flips

Simon Segert

## 1 Abstract

Consider the following probability puzzle: A fair coin is flipped  $n$  times. For each  $HT$  in the resulting sequence, Bob gets a point, and for each  $HH$  Alice gets a point. Who is more likely to win? We provide a proof that Bob wins more often for *every*  $n \geq 3$ . As a byproduct, we derive the asymptotic form of the difference in win probabilities, and obtain an efficient algorithm for their calculation.

## 2 Introduction

The puzzle described in the abstract was posed in [Lit24]. It is subtle because even though both players have the same expected score, it turns out that their win probabilities are not equal. It is possible to algorithmically compute the win probabilities and thereby rigorously determine the winner for a specific value of  $n$  [EZ24]. However to our knowledge a proof that Bob wins for every value of  $n$  has not been given. **We provide here a formal proof that Bob wins more often for every  $n$ .**

The proof uses generating function technology, which allows us to derive several interesting and unexpected results as a byproduct. To state these, let  $P_n(Bob)$  denote the probability of the event that Bob has more points after  $n$  flips, and similarly for Alice. Let  $\Delta_n = P_n(Bob) - P_n(Alice)$  be the difference in win probabilities. We show that **the asymptotic expansion of the differences is**  $\Delta_n = \frac{1}{2\sqrt{n\pi}} + O(n^{-3/2})$  and moreover that  **$\Delta_n$  can be computed in  $O(n)$  time**. Note that similar results had also been obtained by [EZ24], using somewhat different techniques than here.

There are two major steps of the proof: the first consists of establishing the following explicit formula for the generating function:

$$f(t) := \sum_{n \geq 0} \Delta_n (2t)^n = \frac{1}{2} \frac{1}{\sqrt{(1-t)(1-2t)(2t^2+t+1)}} - \frac{1}{2} \frac{1}{1-t}, \quad (1)$$

and the second consists of showing that the coefficients are positive. We actually provide two independent arguments for the positivity of the coefficients, so in

a sense we provide 1.5 proofs that Bob wins more often. The first argument uses closure properties of the class of absolutely monotonic functions, and the second relates  $f(t)$  to the generating function of a certain manifestly positive combinatorial sequence.

### 3 Proof of Main Result

We will now prove that  $\Delta_n > 0$  for  $n \geq 3$ . We will split up the argument into three subsections. In Section 3.1, we prove the claimed form of the generating function. We then give two independent arguments for the positivity of the coefficients of the generating function, in Sections 3.2 and 3.3.

#### 3.1 Derivation of generating function

The objective of this section is to prove the following theorem:

**Theorem 3.1.** *The generating function  $f(t) = \sum_n \Delta_n (2t)^n$  is given by*

$$f(t) = \frac{1}{2} \frac{1}{\sqrt{(1-t)(1-2t)(2t^2+t+1)}} - \frac{1}{2} \frac{1}{1-t} \quad (2)$$

As a first step, we will derive an expression for  $\Delta_n$  in terms of a complex integral<sup>1</sup>.

**Lemma 3.1.** *For any  $n > 0$ , we have*

$$\Delta_n = 2^{-n} \int_C \mathbf{1}^t \frac{A(z)^{n-1} - A(1/z)^{n-1}}{1-z} \mathbf{1} dz \quad (3)$$

where  $A(z) = \begin{pmatrix} 1 & 1/z \\ 1 & z \end{pmatrix}$ ,  $\mathbf{1}$  is the vector of ones, and  $C$  is any simple contour in the complex plane that encloses the origin.

*Proof.* Define the random variable  $X_n$  to be the outcome of the  $n$ th flip (i.e. H or T), and define the random variable  $Y_n$  to be Alice's score minus Bob's score after  $n$  flips. Finally, consider the values

$$p_{n,k,T} = P(Y_n = k | X_n = T) \quad (4)$$

with  $p_{n,k,H}$  defined analogously. By the chain rule of probability:

$$p_{n,k,T} = \frac{1}{2} P(Y_n = k | X_{n-1} = T, X_n = T) + \frac{1}{2} P(Y_n = k | X_{n-1} = H, X_n = T) \quad (5)$$

For the first term, we know that neither player can get a point for a subsequence that starts with  $T$ . Thus if the last two flips are  $TT$  and the cumulative

---

<sup>1</sup>Note that, by convention, we will assume that all complex integrals are multiplied by a factor of  $\frac{1}{2\pi i}$ , which we do not explicitly write out

score is  $k$ , then the cumulative score must already have been  $k$  after only  $n-1$  flips. So the first term is  $P(Y_n = k | X_{n-1} = T, X_n = T) = P(Y_{n-1} = k | n-1 = T, X_n = T) = p_{n-1,k,T}$  (since  $Y_{n-1}$  is independent of  $X_n$ ). As for the second term, if the last two flips are  $HT$ , then this gives 1 point for Bob, and therefore the score difference after the first  $n-1$  flips must have been  $k+1$ . So this is  $p_{n-1,k+1,H}$ . Thus we obtain the recurrence

$$p_{n,k,T} = \frac{1}{2}p_{n-1,k,T} + \frac{1}{2}p_{n-1,k+1,H} \quad (6)$$

Similarly, we can derive the recurrence

$$p_{n,k,H} = \frac{1}{2}p_{n-1,k,T} + \frac{1}{2}p_{n-1,k-1,H} \quad (7)$$

Next, consider the probability generating function  $\phi_{n,T}(z) = \sum_n p_{n,k,T} z^k$ , with  $\phi_{n,H}$  defined analogously.

By multiplying each of the two recurrences above by  $z^k$  and summing over  $k$ , we obtain the matrix equation:

$$\begin{pmatrix} \phi_{n,T}(z) \\ \phi_{n,H}(z) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & z^{-1} \\ 1 & z \end{pmatrix} \begin{pmatrix} \phi_{n-1,T}(z) \\ \phi_{n-1,H}(z) \end{pmatrix} \quad (8)$$

and by induction:

$$\begin{pmatrix} \phi_{n,T}(z) \\ \phi_{n,H}(z) \end{pmatrix} = \frac{1}{2^{n-1}} \begin{pmatrix} 1 & z^{-1} \\ 1 & z \end{pmatrix}^{n-1} \begin{pmatrix} \phi_{1,T}(z) \\ \phi_{1,H}(z) \end{pmatrix} \quad (9)$$

$$= \frac{1}{2^{n-1}} \begin{pmatrix} 1 & z^{-1} \\ 1 & z \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (10)$$

Letting  $\phi_n(z) = \sum_n P(Y_n = k) z^k$  be the probability generating function for  $Y_n$ , we evidently have the relation  $\phi_n(z) = \frac{1}{2}\phi_{n,T}(z) + \frac{1}{2}\phi_{n,H}(z)$ . Thus:

$$\phi_n(z) = 2^{-n} \begin{pmatrix} 1 & 1 \end{pmatrix}^T \begin{pmatrix} 1 & z^{-1} \\ 1 & z \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (11)$$

Now, note that  $Y_n$  can only take finitely many values (since neither player can get more than  $n-1$  points after  $n$  flips). In particular,  $\phi_n(z)$  is a meromorphic function, so by the residue formula:

$$P(Y_n = k) = \int_C z^{-1-k} \phi(z) dz \quad (12)$$

for any simple closed contour  $C$  which contains the origin. If we take  $C$  to lie

completely within the (open) unit disc  $|z| < 1$ , then we have

$$P_n(\text{Bob wins}) = \sum_{k < 0} P(Y_n = k) \quad (13)$$

$$= \sum_{k < 0} \int_C z^{-1-k} \phi(z) dz \quad (14)$$

$$= \sum_{k \geq 0} \int_C z^k \phi_n(z) dz \quad (15)$$

$$= \int_C \frac{\phi_n(z)}{1-z} dz \quad (16)$$

where the geometric sum converges by assumption on  $C$ . By a symmetric argument,

$$P_n(\text{Alice wins}) = \int_{C'} \frac{\phi_n(z)}{1-1/z} \frac{dz}{z^2} \quad (17)$$

where now  $C'$  lies in the *complement* of the (closed) unit disc  $|z| \leq 1$ . In particular, we can take  $C'$  to be the “inverse” of  $C$ :  $C' = \{1/z : z \in C\}$ . Making the change of variable  $z \mapsto 1/z$  we see that

$$P_n(\text{Alice wins}) = \int_C \frac{\phi_n(1/z)}{1-z} dz \quad (18)$$

Note that there is a negative sign that arises from the fact that the function  $1/z$  reverses the orientation along the curve. Therefore

$$\Delta_n = \int_C \frac{\phi_n(z) - \phi_n(1/z)}{1-z} dz \quad (19)$$

where  $C$  lies in the interior of the unit disc. Note that the integrand has a removable singularity at  $z = 1$  and no other singularities except for  $z = 0$ ; this implies that the above formula for  $\Delta_n$  is valid for any  $C$  that encloses the origin (i.e. we can drop the condition that  $C$  lies in the unit disc).  $\square$

*Proof.* (of Theorem 3.1)

Starting with the complex integral formula, we see that, for  $t$  in a sufficiently small neighborhood of the origin, we have

$$f(t) = t \mathbf{1}^t \int_C \frac{(I - tA(z))^{-1} - (I - tA(1/z))^{-1}}{1-z} \mathbf{1} dz \quad (20)$$

Doing a bit of algebra (cf. Section 5.1), the integral becomes

$$f(t) = t^3 \int_C \frac{z^3 - z^2 - z + 1}{(t^2 z^2 + (t-1)z + (t-t^2))((t^2 - t)z^2 + (1-t)z - t^2)} dz \quad (21)$$

Interestingly, both quadratic equations in the denominator have the same discriminant  $\Delta(t) = 4t^4 - 4t^3 + t^2 - 2t + 1$ . By the quadratic formula, we see the integral has four poles located at:

$$\frac{-t+1 \pm \sqrt{\Delta(t)}}{2t^2} \quad (22)$$

$$\frac{t-1 \pm \sqrt{\Delta(t)}}{2t^2 - 2t} \quad (23)$$

Now, for small  $t$ , we have  $\sqrt{\Delta(t)} = 1 - t + O(t^3)$ . Thus as  $t \rightarrow 0$  the pole  $\frac{-t+1+\sqrt{\Delta(t)}}{2t^2}$  tends to infinity, while the complementary one tends to zero. Similarly for the other pair of poles, the "+" sign one tends to zero while the other one tends to infinity. Since  $C$  is fixed, we see in particular that for sufficiently small  $t$  that  $\frac{-t+1-\sqrt{\Delta(t)}}{2t^2}$  and  $\frac{t-1+\sqrt{\Delta(t)}}{2t^2-2t}$  will lie in  $C$  while the other two will lie outside of it. Therefore, the expression for  $f(t)$  reduces to computing the residues at these two poles. Since all four poles are simple, we can directly read off the residue at one of the poles  $r_i$  as

$$\text{Res}_{r_i} = P(r_i)/Q'(r_i) \quad (24)$$

where  $P$  and  $Q$  are respectively the numerator and denominator of the expression in the integral and the prime denotes the derivative with respect to  $z$ . At this point, we can verify the claimed form of  $f$  through mechanical calculation (or computer algebra system, cf. Section 5.2). □

## 3.2 First proof of positivity

Our goal is to show that  $f^{(k)}(0) > 0$  for each  $k \geq 3$ . This is similar to the notion of *absolute monotonicity*, but differs in that we only care about the derivatives at a single point, and moreover we want a strict inequality. It will therefore be useful at this point to study this class of functions in more detail.

**Definition 3.1.1.** *Let  $g$  be a function with a convergent power series expansion in a neighborhood of 0. We say that  $g$  is **strictly absolutely monotonic at the origin** (or "**samo**" for short) if  $g^{(i)}(0) > 0$  for every  $i \geq 0$ . More generally, we say that  $g$  is **k-samo** if  $g^{(i)}(0) \geq 0$  for  $i < k$  and  $g^{(i)}(0) > 0$  for  $i \geq k$ .<sup>2</sup>*

We can rephrase our goal as showing that  $f$  is 3-samo. We now state a few simple but useful facts which mirror the corresponding results for absolutely monotonic functions:

**Proposition 3.1.1.** *The sum of two k-samo functions is k-samo. Moreover, a positive scalar multiple of a k-samo function is k-samo.*

<sup>2</sup>Note that 0-samo is synonymous with samo

*Proof.* Clear. □

**Proposition 3.1.2.** *Let  $f$  be  $k$ -samo. Then  $f - f(0)$  is  $\max(k, 1)$ -samo.*

*Proof.* Clear. □

**Proposition 3.1.3.** *Let  $f$  be  $k_1$ -samo and  $g$  be  $k_2$ -samo. Then  $fg$  is  $k_1 + k_2$ -samo.*

*Proof.* By the iterated product rule, the  $k$ th derivative of the product is a positive linear combination of terms of the form  $f^{(i)}(0)g^{(k-i)}(0)$  for  $i = 0, \dots, k$ . We consider two cases, the first being  $k < k_1 + k_2$ . In this case we must have either  $i < k_1$  or  $k - i < k_2$ , and therefore one of the terms in the product  $f^{(i)}(0)g^{(k-i)}(0)$  is equal to zero.

Now consider the second case  $k \geq k_1 + k_2$ . The derivative is clearly a sum of non-negative terms, so we just need to show that at least one of them is strictly positive. Setting  $i = k_1$  we have  $f^{(k_1)}(0)g^{(k-k_1)}(0)$ . The first factor is clearly positive by assumption on  $f$ , and the second term is similarly positive because  $k - k_1 \geq k_2$ . □

**Proposition 3.1.4.** *If  $\log f$  is  $k$ -samo, then so is  $f$ .*

*Proof.* Expand the derivatives of  $e^{\log f}$  using Faa di Bruno's formula. □

**Proposition 3.1.5.** *If  $f$  is  $k$ -samo then  $\int_0^x f(t)dt$  is  $k + 1$ -samo.*

*Proof.* Clear. □

We can use the above properties of samo functions to reduce our problem to the following simpler one:

**Proposition 3.1.6.** *Let  $h(t)$  be defined by*

$$h(t) = \frac{t+2}{2t^2+t+1} + \frac{1}{1-2t} \quad (25)$$

*If  $h(t)$  is samo, then the generating function  $f(t)$  is 3-samo.*

*Proof.* We can see by direct computation (cf. Section 5.3) that

$$\frac{2t^2}{1-t}h(t) = \frac{d}{dt} \log \frac{\sqrt{1-t}}{\sqrt{(1-2t)(2t^2+t+1)}} \quad (26)$$

Assume  $h$  is samo. The function  $\frac{2t^2}{1-t}$  is clearly 2-samo, so by assumption on  $h$  and Proposition 3.1.3, we conclude that RHS is 2-samo. By Proposition 3.1.5, we conclude that  $\log \frac{\sqrt{1-t}}{\sqrt{(1-2t)(2t^2+t+1)}}$  is 3-samo, and by Proposition 3.1.4, we see that  $\frac{\sqrt{1-t}}{\sqrt{(1-2t)(2t^2+t+1)}}$  is 3-samo. By Proposition 3.1.2, we have  $\frac{\sqrt{1-t}}{\sqrt{(1-2t)(2t^2+t+1)}} - 1$  is 3-samo. Finally, because  $\frac{1}{1-t}$  is samo, we conclude by Proposition 3.1.3 that

$$f(t) = \frac{1}{2(1-t)} \left( \frac{\sqrt{1-t}}{\sqrt{(1-2t)(2t^2+t+1)}} - 1 \right) \quad (27)$$

is 3-samo as desired.  $\square$

At this point, the natural thing is to analyze  $h$ .

**Proposition 3.1.7.** *The coefficients of the function  $h(t)$  defined in Proposition 3.1.6 are given by*

$$h(t)[t^n] = 2\operatorname{Re}(\phi^n) + 2^n \quad (28)$$

where  $\phi = \frac{-1+\sqrt{-7}}{2}$  and  $n \geq 0$ .

*Proof.* It suffices to show that  $\frac{t+2}{2t^2+t+1} = \sum_n 2\operatorname{Re}(\phi^n)t^n$ . To wit, we have for sufficiently small  $t$  that

$$\sum_n 2\operatorname{Re}(\phi^n)t^n = 2\operatorname{Re}\left(\frac{1}{1-t\phi}\right) \quad (29)$$

$$= \frac{1}{1-t\phi} + \frac{1}{1-t\bar{\phi}} \quad (30)$$

$$= \frac{1-t\bar{\phi}+1-t\phi}{|1-t\phi|^2} \quad (31)$$

$$= \frac{2+t}{(1+t/2)^2+7t^2/4} \quad (32)$$

$$= \frac{2+t}{1+t+2t^2} \quad (33)$$

$\square$

As a simple corollary:

**Proposition 3.1.8.** *The function  $h(t)$  is samo.*

*Proof.* By Proposition 3.1.7, we need to show that  $2^n + 2\operatorname{Re}(\phi^n) > 0$  for every  $n$ . We have

$$\operatorname{Re}(\phi^n) \geq -|\phi|^n = -2^{n/2} \quad (34)$$

and therefore the coefficients are strictly positive provided that  $n \geq 3$ . The cases  $n = 0, 1, 2$  are easily verified directly.  $\square$

Combining Propositions 3.1.6, 3.1.7 and 3.1.8, we have proven the following:

**Theorem 3.2.** *The coefficients  $f(t)[t^n]$  of the generating function are strictly positive for all  $n \geq 3$ . In particular, Bob is more likely to win the game than Alice for any  $n \geq 3$ .*

### 3.3 Second proof of positivity

We now provide an alternative argument for the positivity of  $\Delta_n$ , by relating it to combinatorial sequence which is manifestly positive. This proof uses the explicit form of the generating function  $f(t)$  but is otherwise completely independent from the argument given in Section 3.2.

**Definition 3.2.1.** Let  $S \subset \mathbb{Z}_{\geq 0}^2 - \{(0,0)\}$  be a finite subset of the non-negative plane lattice. Assume that there is an associated positive integer  $c_s \geq 1$  for each  $s \in S$ ; we denote the collection of all by  $C = \{c_s\}_{s \in S}$ . A **colored lattice path** is a finite sequence  $\{(s_i, x_i)\}_i$  such that  $s_i \in S$  and  $x_i \in \{1, \dots, c_{s_i}\}$  for each  $i$  (the path may be empty). The **endpoint** of the path is defined to be  $\sum_i s_i \in \mathbb{Z}^2$ .

Note that the values  $c_s$  have an obvious interpretation as a collection of possible colors for each type of edge.

**Definition 3.2.2.** Let  $S, C$  be as above, and let  $(a, b) \in \mathbb{Z}^2$ . The number of colored lattice paths with endpoint  $(a, b)$  is denoted by  $N_{S,C}(a, b)$ .

We can now state the main result of this section.

**Theorem 3.3.** The sequence  $\Delta_n$  can be expressed in terms of a count of colored lattice paths:

$$\Delta_n = \frac{N_{S,C}(n, n) - 1}{2^{n+1}} \quad (35)$$

where  $S = \{(6, 5), (0, 1), (1, 1), (3, 3)\}$ ,  $c_{(3,3)} = 2$ , and  $c_{(i,j)} = 1$  for  $(i, j) \in S - \{(3, 3)\}$ . In particular  $\Delta_n > 0$  for  $n \geq 3$ .

The proof will follow easily from two simple lemmas:

**Lemma 3.2.** The bivariate generating function  $G_{S,C}(x, y) = \sum_{(a,b) \in \mathbb{Z}_{\geq 0}^2} N_{S,C}(a, b) x^a y^b$  is given by

$$G_{S,C}(x, y) = \frac{1}{1 - \sum_{(i,j) \in S} c_{(i,j)} x^i y^j} \quad (36)$$

*Proof.* By considering the last segment in a path we obtain the relation:

$$N_{S,C}(a, b) = \delta_a \delta_b + \sum_{(i,j) \in S} c_{(i,j)} N_{S,C}(a - i, b - j) \quad (37)$$

where  $N_{S,C}(a, b) = 0$  if  $\min(a, b) < 0$  and where the  $\delta$  term corresponds to the empty path. Multiplying both sides by  $x^a y^b$  and summing over  $a$  and  $b$  gives the result.  $\square$

**Lemma 3.3.** (Stanley) Let  $f, g, h$  be univariate polynomials with  $h(0) = 0$ . Consider the bivariate function  $G(x, y) = \frac{1}{1 - xf(xy) - yg(xy) - h(xy)}$ . Then the Diagonal  $D(t) := \sum_{n \geq 0} G(x, y)[x^n y^n] t^n$  is given by

$$D(t) = \frac{1}{\sqrt{(1 - h(t))^2 - 4tf(t)g(t)}} \quad (38)$$



*Proof.* This is Exercise 6.15 in [Sta23], and a solution is also provided therein.  $\square$

We now prove Theorem 3.3 from the two lemmas. Taking the  $S$  and  $C$  defined in the statement of the Theorem, we see from Lemma 3.2 that

$$G_{S,C}(x, y) = \frac{1}{1 - x^6 y^5 - y - xy - 2x^3 y^3} \quad (39)$$

$$= \frac{1}{1 - x(x^5 y^5) - y(1) - (2x^3 y^3 + xy)} \quad (40)$$

$$= \frac{1}{1 - xf(xy) - yg(xy) - h(xy)} \quad (41)$$

$$(42)$$

where

$$f(t) := t^5 \quad (43)$$

$$g(t) := 1 \quad (44)$$

$$h(t) := 2t^3 + t \quad (45)$$

Therefore by Lemma 3.3 the diagonal  $D_{S,C}(t) := \sum_n N_{S,C}(n, n)t^n$  satisfies

$$D_{S,C}(t) = \frac{1}{\sqrt{(1 - h(t))^2 - 4tf(t)g(t)}} \quad (46)$$

$$= \frac{1}{\sqrt{(1 - t - 2t^3)^2 - 4t^6}} \quad (47)$$

$$= \frac{1}{\sqrt{4t^4 - 4t^3 + t^2 - 2t + 1}} \quad (48)$$

$$= 2f(t) + \frac{1}{1 - t} \quad (49)$$

where  $f(t) = \sum_n \Delta_n (2t)^n$  and we have used Theorem 3.1 in the last line. Theorem 3.3 follows immediately.

## 4 Consequences of the Proof

### 4.1 Asymptotic Analysis

It is easy to see that  $\Delta_n \rightarrow 0$ , but a natural and non-obvious follow up question is how fast is the convergence? Using the explicit form of the generating function, this can be answered with a simple application of the famous Darboux formula (cf. [Wil93]).

Notation-wise, we define  $d_n := 2^n \Delta_n + 1/2$ , which are the coefficients of the function  $\tilde{f}(t) = \frac{1}{2} \frac{1}{\sqrt{(1-t)(1-2t)(2t^2+t+1)}}$ . Observe that  $\tilde{f}(t)\sqrt{1/2 - t}$  can be extended to a holomorphic function in the disc  $|z| < 1/2 + \epsilon$ . Darboux's formula then implies the following asymptotic form:

$$2^{-n}d_n = \frac{1}{2} \binom{n-1/2}{n} + O(n^{-3/2}) = \frac{1}{2\sqrt{\pi}} \frac{\Gamma(n+1/2)}{\Gamma(n+1)} + O(n^{-3/2}) \quad (50)$$

By Stirling's formula, we in particular obtain:

$$\Delta_n = \frac{1}{2\sqrt{n\pi}} + O(n^{-3/2}) \quad (51)$$

The same result was also obtained in [EZ24] through different means.

## 4.2 Recurrence Relation

Here we provide an algorithm to compute  $\Delta_n$  in  $O(n)$  time. To do so, we will use the reparametrization  $d_n = 2^n \Delta_n + 1/2$  from above and compute  $d_n$ . The main observation is that the generating function  $\tilde{f}(t)$  for  $d_n$  is an inverse square root of a rational function. In particular, it satisfies an algebraic relation of the form  $p(t)\tilde{f}(t) + q(t)\tilde{f}'(t) = 0$  for some polynomials  $p$  and  $q$ . By equating the terms to zero, we see that the coefficients of  $\tilde{f}$  satisfy a linear recurrence relation. Crucially, the number of terms in the recurrence relation does not depend on  $n$  (i.e. it is bounded by the degrees of  $p$  and  $q$ ). Therefore, directly iterating the recurrence allows us to compute the  $n$ th term in  $O(n)$  time.

To give the details, we obtain by direct computation:

$$(\log \tilde{f})'(t) = \frac{-8t^3 + 6t^2 - t + 1}{(1-x)(1-2t)(2t^2 + t + 1)} \quad (52)$$

In particular, we get an equation:

$$(4t^4 - 4t^3 + t^2 - 2t + 1)\tilde{f}'(t) + (8t^3 - 6t^2 + t - 1)\tilde{f}(t) = 0 \quad (53)$$

Setting the coefficients of the LHS to zero gives the recurrence:

$$(-8/n + 4)d_{n-4} - (-6/n + 4)d_{n-3} + (-1/n + 1)d_{n-2} - (-1/n + 2)d_{n-1} + d_n = 0 \quad (54)$$

We can also plug in  $d_n = 2^n \Delta_n + 1/2$  to obtain a recurrence directly for  $\Delta_n$ :

$$\Delta_n = \frac{1}{n2^n} + \left(\frac{1}{2n} - \frac{1}{4}\right) \Delta_{n-4} + \left(-\frac{3}{4n} + \frac{1}{2}\right) \Delta_{n-3} + \left(\frac{1}{4n} - \frac{1}{4}\right) \Delta_{n-2} + \left(-\frac{1}{2n} + 1\right) \Delta_{n-1}$$

A similar recurrence relation had been obtained by [EZ24] using a different argument.

An obvious consequence is that this algorithm not only computes  $\Delta_n$  in  $O(n)$  time, but can in fact generate the entire sequence  $\Delta_1, \dots, \Delta_n$  in  $O(n)$  time.

## 5 Appendix-symbolic calculations

We provide code to verify the omitted calculations in the main text using the Python package Sympy.

### 5.1 Equation 21

```
from sympy import *
z, t = symbols('z t')
P = t**3*(z**3 - z**2 - z + 1)
Q = (t**2*z**2 + (t - 1)*z + (t - t**2))*((t**2 - t)*z**2 + (1 - t)*z - t**2)
A = Matrix([[1, 1/z], [1, z]])
A2 = A.subs(z, 1/z)
I = Matrix([[1, 0], [0, 1]])
integral = t*sum((I - t*A).inv() - (I - t*A2).inv())/(1 - z)
simplify(integral - P/Q) # returns 0
```

### 5.2 Residue calculation (Theorem 3.1)

```
from sympy import *
z, t = symbols('z t')
P = t**3*(z**3 - z**2 - z + 1)
Q = (t**2*z**2 + (t - 1)*z + (t - t**2))*((t**2 - t)*z**2 + (1 - t)*z - t**2)
delta = 4*t**4 - 4*t**3 + t**2 - 2*t + 1
r1 = (-t + 1 - sqrt(delta))/(2*t*t)
r2 = (t - 1 + sqrt(delta))/(2*t*t - 2*t)
R = P/diff(Q, z)
gf = R.subs(z, r1) + R.subs(z, r2)
gf2 = (1/sqrt(delta) - 1/(1 - t))/2
simplify(gf - gf2) # returns 0
```

### 5.3 Logarithmic derivative (Proposition 3.1.6)

```
h = (t + 2)/(2*t*t + t + 1) + 1/(1 - 2*t)
Q = (1 - t)/((1 - 2*t)*(2*t*t + t + 1))
simplify(diff(log(sqrt(Q)) - 2*t*t*h/(1 - t))) # returns 0
```

## 6 Generalization to Markov Chains

Much of the above analysis goes through in the following much more general setting:

## 6.1 Setup

**Definition 6.0.1.** Let  $T$  be a  $K \times K$  row-stochastic matrix. A **Stationary Markovian Random Walk** is a random sequence  $x_1, x_2, \dots$  where  $P(x_{i+1} = a | x_i = b) = T(b, a)$  for  $i > 1, a, b \in \{1, 2, \dots, K\}$  and  $P(x_1 = a) = (\pi_T)_a$ , where  $\pi_T$  is the stationary distribution of  $T$  (assumed to exist and be unique).

**Definition 6.0.2.** A **Value Function** is an integer matrix  $V \in \mathbb{Z}^{K \times K}$ . If  $\{x_i\}_i$  is an smrw with kernel  $T$ , the  **$n$ -step value**  $Y_n^{T,V}$  is the random variable:

$$Y_n^{T,V} = \sum_{i=1}^{n-1} V_{x_i, x_{i+1}} \quad (55)$$

We also write  $Y_n$  when  $T$  and  $V$  are clear from the context.

Basically we will be interested in the distribution of the rv  $Y_n$ , where  $T$  and  $V$  are as above but otherwise (almost) arbitrary. We will regard  $T$  as being fixed, and  $V$  as potentially variable. The only hypothesis we will put on  $T$  is that it is *irreducible*. This means that for any  $a, b$ , there exists some  $k = k_{a,b}$  such that  $(T^k)_{a,b}$  is strictly positive. In particular, the Perron-Frobenius theorem then implies that a unique stationary distribution  $\pi_T$  exists; i.e.  $\pi_T^T T = \pi_T$  and  $\pi_T$  is the only distribution with this property.

The following related matrices will play a key role in the theory.

**Definition 6.0.3.** Let  $T, V$  be as above. The  **$M$ -matrix** is defined as the following polynomial matrix:

$$M_{T,V}(z)_{a,b} = T_{a,b} z^{V(a,b)} \quad (56)$$

and the  **$F$ -matrix** is defined as

$$F_{T,V}(t) = M_{T,V}(e^t) \quad (57)$$

The basic upshot is that the behavior of the function  $\rho(F_{T,V}(t))$  near the origin provides precise control over the asymptotics of  $Y_n$ . Here  $\rho$  denotes the (complex-valued) spectral radius of a matrix. We will flesh this out in what follows.

Moreover, most of the key arguments from section 3.1 now carry over basically unchanged.

**Proposition 6.0.1.** Let  $T, V$  be as above. The probability generating function  $\phi_n^{T,V}(z) := \mathbb{E} z^{Y_n^{T,V}}$  is given by

$$\phi_n^{T,V}(z) = \pi_T^T M_{T,V}(z)^{n-1} \mathbf{1} \quad (58)$$

and the characteristic function  $c_n^{T,V}(t) := \mathbb{E} e^{it Y_n^{T,V}}$  is given by

$$c_n^{T,V}(t) = \pi_T^T F_{T,V}(it)^{n-1} \mathbf{1} \quad (59)$$

*Proof.* The claim about the characteristic function follows from the form of the pgf. The argument for the pgf, in turn, is basically identical to the derivation of equation 11. To wit, defining  $q_{n,y,k} := P(Y_n = y, x_n = k)$  we have the following recurrence:

$$q_{n,y,k} = \sum_{k'} q_{n-1,y-V_{k',k},k'} T(k',k) \quad (60)$$

So the “partial generating functions”  $\phi_{n,k}(z) := \sum_y z^y P(Y_n = y, x_n = k)$  satisfy

$$\phi_{n,k}(z) = \sum_{k'} T_{k',k} z^{V_{k',k}} \phi_{n-1,k'}(z) \quad (61)$$

Or in matrix form:

$$\phi_{n,\cdot}(z)^T = \phi_{n-1,\cdot}^T M(z) \quad (62)$$

By induction

$$\phi_{n,\cdot}(z)^T = \phi_{1,\cdot}^T M^{n-1}(z) \quad (63)$$

On the other hand, since  $Y_1 = 0$  a.s. we have  $\phi_{1,k}(z) = \sum_y z^y P(Y_1 = y, x_1 = k) = P(Y_1 = 0, x_1 = k) = \pi_k$ , so

$$\phi_{n,\cdot}(z) = \pi^t M^{n-1}(z) \quad (64)$$

while clearly  $\phi_n(z) = \sum_k \phi_{n,k}(z)$

□

For convenience, we state a slight generalization of this which handles the case of joint distributions of multiple value functions defined over the same underlying random walk.

**Proposition 6.0.2.** *Let  $T, K, \pi$  be as above, and let  $V_1$  and  $V_2$  be value functions with associated  $n$ -step values  $Y_n^1$  and  $Y_n^2$ . The joint distribution  $(Y_n^1, Y_n^2)$  has probability generating function  $\phi_n^{V_1, V_2}(x, y)$  given by*

$$\phi_n^{T, V_1, V_2}(x, y) = \pi_T^T M_{T, V_1, V_2}(x, y)^{n-1} \mathbf{1} \quad (65)$$

and characteristic function  $c_n^{V_1, V_2}(s, t)$

$$c_n^{T, V_1, V_2}(s, t) = \pi_T^T F_{T, V_1, V_2}(is, it)^{n-1} \mathbf{1} \quad (66)$$

where the bivariate  $M$  and  $F$  matrices are defined by

$$M_{T, V_1, V_2}(x, y)_{a,b} := T(a, b) x^{V_1(a,b)} y^{V_2(a,b)} \quad (67)$$

$$F_{T, V_1, V_2}(s, t) := M_{T, V_1, V_2}(e^s, e^t) \quad (68)$$

Note that this generalizes to the joint distribution of any finite number of value functions in the obvious way.

It is fairly easy to see that for large  $n$ , the value of the characteristic function will be dominated by the contribution of the largest eigenvalue:  $\phi_n(t) =$

$\rho(F_{T,V}(it))^n(1+O(1/n))$ . Thus, we can basically carry over the standard arguments for the setting of sums of independent random variables. In particular, one can prove a central limit theorem (even in the vector-valued case) in basically the same way as in the iid case. Analogously to the iid case, one finds that the asymptotic distribution is controlled by the derivatives of  $\rho(F_{T,V}(it))$  at the origin. It turns out there are explicit linear-algebraic formulas for these derivatives, which we turn to next.

## 7 Evaluating derivatives of the spectral radius

We now derive explicit algebraic expressions for the first few derivatives of  $\rho(F_{T,V}(t))$  at  $t = 0$ .

Introduce the notation  $Q := (I - T)^g$  for the indicated group inverse<sup>3</sup>. Moreover, we use  $\circ$  to denote the Hadamard (pointwise) product of two matrices.

We make use of the paper [HR92] in particular Theorem 4.1 therein, which gives the following (real) power series expansion:

$$\rho(T + \epsilon E) = 1 + \rho_1(E)\epsilon + \rho_2(E)\epsilon^2 + O(\epsilon^3)$$

where  $\rho_1(E) = \pi^t E \mathbf{1}$  and  $\rho_2(E) = \pi^t E Q E \mathbf{1}$ .

Since  $F_{T,V}(\epsilon) = T + \epsilon(T \circ V) + O(\epsilon^2)$  we immediately conclude that

$$\frac{d}{dt}\bigg|_{t=0} \rho(F_{T,V}(t)) = \pi^t(T \circ V) \mathbf{1} \quad (69)$$

To evaluate the second derivative, we take  $E = E_1 + \epsilon E_2$  for some  $E_1$  and  $E_2$  and collect powers of  $\epsilon$ :

$$\pi^t(E_1 + \epsilon E_2) \mathbf{1} \epsilon + \pi^t(E_1 + \epsilon E_2) Q (E_1 + \epsilon E_2) \mathbf{1} \epsilon^2 + \dots \quad (70)$$

$$= \pi^t E_1 \mathbf{1} \epsilon + \pi^t(E_2 + E_1 Q E_1) \mathbf{1} \epsilon^2 + \dots \quad (71)$$

Therefore the second derivative is given by the  $\epsilon^2$  term,

$$\frac{d^2 \rho(T + \epsilon E)}{d\epsilon^2}\bigg|_{\epsilon=0} = 2\pi^t(E_2 + E_1 Q E_1) \mathbf{1}$$

In our case, we have  $F_{T,V}(t) = T + \epsilon T \circ V + \epsilon^2 T \circ V^{\circ 2} / 2 + O(\epsilon^3)$ , so we see we should take  $E_1 = T \circ V$  and  $E_2 = T \circ V^{\circ 2} / 2$ , obtaining the formula

$$\frac{d^2}{dt^2}\bigg|_{t=0} \rho(F_{T,V}(t)) = \pi^t (T \circ V^{\circ 2} + 2(T \circ V) Q (T \circ V)) \mathbf{1} \quad (72)$$

In the following discussion, we will also have reason to consider the third derivative, so we derive a similar formula. The same Theorem 4.1 in [HR92] also provides the  $\epsilon^3$  term:

---

<sup>3</sup>note that this is *not* the same as the more well-known pseudoinverse, although they happen to coincide in some cases

$$\rho_3(E) = \pi^t EQ(\pi^t E \mathbf{1} I - E) Q E \mathbf{1} \text{ (sic.)}$$

**Regrettably there is a sign error in this formula and actually the RHS should be multiplied by -1!!**

Now we take  $E = E_1 + \epsilon E_2 + \epsilon^2 E_3$  and expand to third order in  $\epsilon$  similar to above. There will be three contributions:

$$\begin{aligned} \rho(T + \epsilon E)[\epsilon^3] &= \rho_1(E_1 + \epsilon E_2 + \epsilon^2 E_3)[\epsilon^2] + \rho_2(E_1 + \epsilon E_2 + \epsilon^2 E_3)[\epsilon] + \rho_3(E_1 + \epsilon E_2 + \epsilon^2 E_3)[\epsilon^0] \\ \rho_1(E_1 + \epsilon E_2 + \epsilon^2 E_3)[\epsilon^2] &= \pi^t E_3 \mathbf{1} \\ \rho_2(E_1 + \epsilon E_2 + \epsilon^2 E_3)[\epsilon] &= \pi^t (E_1 Q E_2 + E_2 Q E_1) \mathbf{1} \\ \rho_3(E_1 + \epsilon E_2 + \epsilon^2 E_3)[\epsilon^0] &= \pi^t E_1 Q (E_1 - \pi^t E_1 \mathbf{1} I) Q E_1 \mathbf{1} \end{aligned}$$

where note that we have corrected the sign in the formula for  $\rho_3$ . As before, we now take  $E_1 = T \circ V$ ,  $E_2 = T \circ V^{\circ 2}/2$  and  $E_3 = T \circ V^{\circ 3}/6$ . Assuming zero mean  $\pi^t(T \circ V) \mathbf{1} = 0$  for simplicity, we get

$$\begin{aligned} \frac{1}{6} \frac{d^3}{dt^3} \Big|_{t=0} \rho(F_{T,V}(t)) &= \pi^t \left( \frac{T \circ V^{\circ 3}}{6} + \frac{(T \circ V) Q (T \circ V^{\circ 2}) + (T \circ V^{\circ 2}) Q (T \circ V)}{2} \right. \\ &\quad \left. + (T \circ V) Q (T \circ V) Q (T \circ V) \right) \mathbf{1} \end{aligned} \tag{73}$$

In principle derivatives of arbitrary order can be derived using this method although the formulas get a bit involved.

## 8 Local limit theorem

Let  $V$  be a value function and assume that the limiting mean  $\pi^t(T \circ V) \mathbf{1}$  is equal to zero. The objective of this section is to prove a limit theorem like

$$P(Y_n^{T,V} > 0) = \frac{1}{2} + C_{T,V}/\sqrt{n} + O(1/n) \tag{74}$$

and work out an explicit expression for  $C_{T,V}$ .

### 8.1 Edgeworth-like expansion of the characteristic function

The standard proof of the central limit theorem hinges on the following simple fact:

$$(1 + A/n + O(n^{-3/2}))^n \rightarrow e^A$$

For the local limit theorem, it turns out we will need a more refined version of this limit, in which the error term inside the  $n$ th power is taken to the next higher order. This comes down to just simple power series manipulation:

**Proposition 8.0.1.** *For fixed  $A$  and  $B$  we have*

$$(1 + A/n + B/n^{-3/2} + O(1/n^2))^n = e^A(1 + B/\sqrt{n} + O(1/n)) \quad (75)$$

*Proof.* For notational simplicity, we define  $a = 1/\sqrt{n}$ . Now:

$$\log(1 + Aa^2 + Ba^3 + O(a^4)) = Aa^2 + Ba^3 + O(a^4) \quad (76)$$

$$\log(1 + Aa^2 + Ba^3 + O(a^4))/a^2 = A + Ba + O(a^2) \quad (77)$$

$$e^{\log(1 + Aa^2 + Ba^3 + O(a^4))/a^2} = e^{A + Ba + O(a^2)} \quad (78)$$

$$= e^A e^{Ba + O(a^2)} \quad (79)$$

$$= e^A(1 + Ba + O(a^2)) \quad (80)$$

$$(81)$$

and changing back to  $a = 1/\sqrt{n}$  we get the indicated result.  $\square$

Note that we could also iterate this argument to obtain coefficients for higher powers. For example,

$$(1 + A/n + B/n^{-3/2} + C/n^2 + O(n^{-5/2}))^n = e^A(1 + B/\sqrt{n} + (C + B^2)/n + O(n^{-3/2}))$$

In principle this could be extended to obtain error terms of arbitrary order on the right hand side.

Now let's consider the situation of the characteristic function  $c_n(t)$  of  $Y_n$ . For fixed  $t$ , the contribution to  $c_n(t/\sqrt{n})$  will be dominated by  $\rho(F(it/\sqrt{n}))^n$ . Using a Taylor expansion of  $\rho$  we get

$$\begin{aligned} c_n(t/\sqrt{n}) &= \rho(F(it/\sqrt{n}))^n(1 + O(1/n)) \\ &= (1 - \sigma^2 t^2/2n - i\kappa t^3/n^{3/2} + O(1/n))^n(1 + O(1/n)) \\ &= e^{-\sigma^2 t^2/2}(1 - i\kappa t^3/\sqrt{n} + O(1/n))(1 + O(1/n)) \\ &= e^{-\sigma^2 t^2/2}(1 - i\kappa t^3/\sqrt{n} + O(1/n)) \end{aligned}$$

where  $\sigma^2 := \frac{d^2}{dt^2}|_{t=0}\rho(F_{T,V}(t))$  as given by equation 72 and  $\kappa := \frac{1}{6}\frac{d^3}{dt^3}|_{t=0}\rho(F_{T,V}(t))$  as given by equation 73.

## 8.2 proof of local limit theorem

We are now in a position to establish the claimed asymptotic in Equation 74. As before, we let  $c_n(t)$  (resp.  $\phi_n(z)$ ) denote the characteristic function (resp. probability generating function) of  $Y_n$ .

Arguing exactly as in the derivation of Equation 16 we have the formula

$$P(Y_n > 0) = \int_C \frac{\phi_n(z)}{1 - z} dz \quad (82)$$

where  $C$  lies within the unit disc. Our strategy will be to approximate the integral using an asymptotic expansion of the characteristic function. However,



the above formula doesn't quite work for this, since the  $z$  in the integral have norm strictly less than 1, whereas the characteristic function is the restriction of  $\phi_n$  to the unit circle. So basically we want to let  $C$  approach the unit circle, but the issue is that the denominator has a singularity at  $z = 1$ .

On the other hand, we know  $\int_C \frac{1}{1-z} dz = 0$  for any such  $C$ , therefore we can rewrite the integral as

$$P(Y_n > 0) = \int_C \frac{\phi_n(z) - 1}{1 - z} dz \quad (83)$$

Now crucially  $\phi_n(1) = 1$  (by the normalization of a characteristic function), and the numerator is a Laurent series in  $z$ , therefore it is divisible by  $1 - z$ . In particular, the integrand has a removable singularity at  $z = 1$ , so we may safely take the limit in which  $C$  approaches the unit circle, obtaining

$$\begin{aligned} P(Y_n > 0) &= \int_{|z|=1} \frac{\phi_n(z) - 1}{1 - z} dz \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{c_n(t) - 1}{1 - e^{it}} e^{it} dt \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{c_n(t) - 1}{e^{-it/2} - e^{it/2}} e^{it/2} dt \\ &= \frac{1}{2\pi i} \int_{-\pi}^{\pi} \frac{c_n(t) - 1}{t} G(it) dt \\ (G(t) &:= \frac{te^{t/2}}{2\sinh(-t/2)}) \\ &= \frac{1}{2\pi i} \int_{-\sqrt{n}\pi}^{\sqrt{n}\pi} \frac{c_n(t/\sqrt{n}) - 1}{t} G(it/\sqrt{n}) dt \\ &= \frac{1}{2\pi} \int_{-\sqrt{n}\pi}^{\sqrt{n}\pi} \text{Imag}\left(\frac{c_n(t/\sqrt{n}) - 1}{t} G(it/\sqrt{n})\right) dt \end{aligned}$$

Note that  $(c_n(t) - 1)/t$  and  $G(it)$  are both well-behaved at the origin. We have the following approximations:

$$c_n(t/\sqrt{n}) = e^{-\sigma^2 t^2/2} (1 - it^3 \kappa/\sqrt{n} + O(1/n)) \quad (84)$$

$$G(it/\sqrt{n}) = 1 + O(1/n) - it/2\sqrt{n} \quad (85)$$

where  $\sigma^2$  and  $\kappa$  are as before (the first follows from the discussion in the previous section, and the second is simple calculus). So

$$\text{Imag}((c_n(t/\sqrt{n}) - 1)G(it/\sqrt{n})/t) = \frac{1}{2\sqrt{n}} - \frac{e^{-\sigma^2 t^2/2}}{2\sqrt{n}} - \frac{e^{-\sigma^2 t^2/2} t^2 \kappa}{\sqrt{n}} + O(e^{-\sigma^2 t^2/2}/n) \quad (86)$$

$$P(Y_n > 0) = \frac{1}{2\pi} \int_{-\sqrt{n}\pi}^{\sqrt{n}\pi} \frac{1}{2\sqrt{n}} - \frac{e^{-\sigma^2 t^2/2}}{2\sqrt{n}} - \frac{e^{-\sigma^2 t^2/2} t^2 \kappa}{\sqrt{n}} + O(e^{-\sigma^2 t^2/2}/n) dt \quad (87)$$

The first term clearly evaluates to  $1/2$ . As for the others, we can extend the limits of integration to  $\pm\infty$  while incurring only an exponential error. This approximation therefore does not affect the leading  $O(1/\sqrt{n})$  term, so after making this change and using standard Gaussian integral formulas we obtain

$$P(Y_n > 0) = \frac{1}{2} - \frac{\sigma^{-1}}{2\pi} \frac{\sqrt{2\pi}}{2\sqrt{n}} + \frac{1}{2\pi} \frac{-\sqrt{2\pi}\kappa\sigma^{-3}}{\sqrt{n}} + O(1/n) \quad (88)$$

$$= \frac{1}{2} + \frac{-\sigma^{-3}\kappa - \sigma^{-1}/2}{\sqrt{2\pi n}} + O(1/n) \quad (89)$$

In summary, we have the following Local Limit Theorem, which holds provided that  $\pi^t(T \circ V)\mathbf{1} = 0$ .

$$\begin{aligned} C_{T,V} &:= \lim_{n \rightarrow \infty} (P(Y_n > 0) - \frac{1}{2})\sqrt{2\pi n} = -\frac{\kappa}{\sigma^3} - \frac{1}{2\sigma} \\ \sigma^2 &:= \frac{d^2}{dt^2}|_{t=0}\rho(F_{T,V}(t)) \\ \kappa &:= \frac{1}{6} \frac{d^3}{dt^3}|_{t=0}\rho(F_{T,V}(t)) \end{aligned} \quad (90)$$

Intuitively, the  $\kappa/\sigma^3$  term is a skewness (third-order) correction, while the  $1/(2\sigma)$  term is a discreteness correction, corresponding to the point mass at  $P(Y_n = 0)$ .

Using the formulas 72 and 73 we conclude that we can actually express  $C_{T,V}$  **entirely in terms of explicit linear-algebraic expressions** involving  $T$  and  $V$ . For general  $T$  and  $V$ , it seems unlikely that the expression for  $C_{T,V}$  can be further simplified in any meaningful way.

## 9 specialization to string counting problems

We can now use the above theory to analyze the generalization of the original Alice and Bob problem to the case where the substrings to be counted both have length  $L+1$  for some  $L \geq 1$ . We introduce the notation  $head_k(s)$  to mean the string obtained by deleting the last  $k$  elements of the string  $s$ . In case,  $k \geq \text{len}(s)$ , then  $head_k(s)$  is taken to be the empty string. Similarly, define  $tail_k(s)$  by deleting the first  $k$  elements of  $s$ . We also denote  $head := head_1$  and  $tail := tail_1$ .

Now we can define the Markovian structure corresponding to the generalized problem. Let  $s_A, s_B$  be the substrings for Alice and Bob respectively, which each have length  $L+1$ . We will consider only binary strings, as the generalization to strings in some finite alphabet involves no new ideas beyond the binary case. We take state space to be the set of all binary strings of length  $L$ , where a transition  $s \rightarrow s'$  exists if and only if  $tail(s) = head(s')$ . Let  $T_L$  be the corresponding transition matrix.

The Value function is the following sparse matrix:

$$V = e_{head(s_A)} e_{tail(s_A)}^T - e_{head(s_B)} e_{tail(s_B)}^T \quad (91)$$

where  $e$  is a unit vector. So in particular  $Y_n$  is equal to Alice's score minus Bob's score, after  $n + L$  flips (obviously both players must have score of zero after the first  $L$  flips).

A very convenient property of the particular transition structure  $T_L$  is that it exactly converges to the stationary distribution after a finite number of steps.

**Proposition 9.0.1.** *The transition matrix  $T_L$  satisfies  $(T_L)^L = \mathbf{1}\mathbf{1}^T/2^L$*

This is because after each step we erase the least-recent bit from the current state and add a new (random) bit. After doing this  $L$  times, we have erased all of the original state and replaced it with  $L$  uniformly random bits.

This proposition also immediately implies:

**Proposition 9.0.2.** *The transition matrix  $T_L$  is irreducible and has a stationary distribution  $\pi = \mathbf{1}/2^L$ .*

Now the Local Limit Theorem (Equation 90) is directly applicable and we can just read off an analytic formula for  $C_{T,V} = \lim_n (P(Y_n > 0) - \frac{1}{2})\sqrt{2\pi n}$ .

The resulting formula involves the group inverse matrix  $Q = (I - T_L)^g$ . In principle, we could just compute this matrix numerically, but for large  $L$  this may not be feasible since the matrix has size exponential in  $L$ . On the other hand, by examining the formulas for  $\sigma$  and  $\kappa$  we see that, due to the sparse structure of  $V$ , we actually only need to know 4 special values  $Q_{tail(s_A), head(s_A)}$ ,  $Q_{tail(s_A), head(s_B)}$ ,  $Q_{tail(s_B), head(s_A)}$ ,  $Q_{tail(s_B), head(s_B)}$  in order to compute  $C_{T,V}$ .

It turns out that, due to the special structure of  $T_L$ , there is a way to easily read off specific entries of  $Q$  without computing the full matrix. We now turn our attention towards finding a formula for  $Q_{s,s'}$ .

**Proposition 9.0.3.** *The group inverse  $(I - T_L)^g$  is given by*

$$(I - T_L)^g = -\frac{L}{2^L} \mathbf{1}\mathbf{1}^T + \sum_{j=0}^{L-1} (T_L)^j \quad (92)$$

*Proof.* Let  $Q_L$  be the matrix on the right hand side of the equation. Observe that

$$Q_L(I - T_L) = (I - T_L)Q_L = I - \mathbf{1}\mathbf{1}^T/2^L \quad (93)$$

Indeed,

$$Q_L(I - T_L) = \left(-\frac{L}{2^L} \mathbf{1}\mathbf{1}^T + \sum_{j=0}^{L-1} (T_L)^j\right) (I - T_L) \quad (94)$$

$$= I - (T_L)^L \quad (95)$$

where we used the fact that  $\mathbf{1}^t T_L = \mathbf{1}^t$ . And since  $(T_L)^L = \mathbf{1}\mathbf{1}^t/2^L$  (Proposition 9.0.1) the claim follows. We can verify the second equation  $(I - T_L)Q_L = I - \mathbf{1}\mathbf{1}^t/2^L$  with a symmetric argument.

Now we can directly verify the group inverse properties. Firstly, it is clear that  $(I - T_L)Q_L = Q_L(I - T_L)$ . Secondly,

$$(I - T_L)Q_L(I - T_L) = (I - T_L)(I - \mathbf{1}\mathbf{1}^t/2^L) \quad (96)$$

$$= I - \mathbf{1}\mathbf{1}^t/2^L - T_L + T_L \mathbf{1}\mathbf{1}^t/2^L \quad (97)$$

$$= I - \mathbf{1}\mathbf{1}^t/2^L - T_L + \mathbf{1}\mathbf{1}^t/2^L \quad (98)$$

$$= I - T_L \quad (99)$$

as required. And finally,

$$Q_L(I - T_L)Q_L = Q_L(I - \mathbf{1}\mathbf{1}^t/2^L) \quad (100)$$

$$= Q_L - Q_L \mathbf{1}\mathbf{1}^t/2^L \quad (101)$$

But  $Q_L \mathbf{1} = -L + \sum_{j=0}^{L-1} (T_L)^j \mathbf{1} = -L\mathbf{1} + \sum_{j=0}^{L-1} \mathbf{1} = -L\mathbf{1} + L\mathbf{1} = 0$ . So  $Q_L(I - T_L)Q_L = Q_L$  as required.  $\square$

Thus  $Q$  can be expressed as a polynomial in  $T_L$ . So we now consider how to read off entries of  $(T_L)^k$ . For strings  $s, s'$  of length  $L$ , and an integer  $k \geq 0$ , we introduce the **match function**:

$$m_k(s, s') = \mathbf{1}_{\text{tail}_k(s) = \text{head}_k(s')} \quad (102)$$

Note that  $m_k$  is identically equal to 1 if  $k \geq L$  (since in this case, both substrings being compared are empty) and  $m_0$  is the delta function  $\mathbf{1}_{s=s'}$ .

The transition matrix can thus be expressed as

$$(T_L)_{s,s'} = m_1(s, s')/2 \quad (103)$$

Since the powers of  $T_L$  correspond to  $k$ -step transition probabilities, it is straightforward to see that

$$((T_L)^k)_{s,s'} = m_k(s, s')/2^{\min(L,k)} \quad (104)$$

for any  $k \geq 0$ .

Putting together this observation with the above proposition, we see

**Proposition 9.0.4.** *Let  $s, s'$  be strings of length  $L$ . The corresponding entry of the group inverse  $(I - T_L)^g$  is*

$$((I - T_L)^g)_{s,s'} = -\frac{L}{2^L} + \sum_{j=0}^{L-1} \frac{m_j(s, s')}{2^j} \quad (105)$$

where the match function is given by Equation 102.

## 10 Experimental Validation

The above analysis was rather involved. The purpose of this section is to lend credibility to the statement of the Local Limit Theorem by comparing the prediction with numerical simulations.

In what follows, we fix  $T$  to be the string-counting transition function  $T_L$  defined in the previous section, for  $L = 4$  (thus  $T_L$  has size  $16 \times 16$ ). We take  $V$  to be a value function that satisfies  $\mathbf{1}^t(T \circ V)\mathbf{1} = 0$ , but otherwise arbitrary. **Note that this is actually a far more general setting than the generalized Alice and Bob problem.** In the present setting, *every* string of length 5 is associated with some score for either Alice or Bob, in such a way that the average score for the two players is equal. In the generalized Alice and Bob problem, it is assumed that there are exactly two substrings that have non-zero associated scores.

The local limit theorem (Equation 90) states that the limit  $\lim_n \sqrt{2\pi n}(P(Y_n^{T,V} > 0) - \frac{1}{2})$  is well-defined and is equal to  $C_{T,V} := -\frac{\kappa}{\sigma^3} - \frac{1}{2\sigma}$ , where  $\kappa$  and  $\sigma$  have certain explicit formulas in terms of  $T$  and  $V$ .

On the other hand, for any fixed  $n$ , we can exactly compute  $P(Y_n^{T,V} > 0)$  using, e.g. dynamic programming.

So to validate the LLT, we can simply compare  $\widehat{C_{T,V,n}}$  to the analytic expression  $C_{T,V}$ , where

$$\widehat{C_{T,V,n}} := \sqrt{2\pi n}(P(Y_n^{T,V} > 0) - \frac{1}{2}) \quad (106)$$

In the simulation, we first generate 200 different value functions  $V$  and then compare the corresponding quantities  $\widehat{C_{T,V,n}}$  and  $C_{T,V}$  for several values of  $n$ . The results are shown in Figure 10. We see that indeed the analytic formula  $C_{T,V}$  closely predicts the empirical values, with the correspondence getting tighter for increasing  $n$ , and essentially exact for the maximal considered value of  $n = 500$ .

## References

- [HR92] M Haviv and Y Ritov. “Taylor expansions of eigenvalues of perturbed matrices with applications to spectral radii of nonnegative matrices”. In: *Linear Algebra and its Applications* (1992).
- [Wil93] H Wilf. *generatingfunctionology*. Academic Press, 1993.
- [Sta23] R Stanley. *Enumerative Combinatorics*. Vol. 2. Cambridge UP, 2023.
- [EZ24] Shalosh B. Ekhad and Doron Zeilberger. “How to Answer Questions of the Type: If you toss a coin  $n$  times, how likely is HH to show up more than HT?” In: *arxiv:2405.13561* (2024).
- [Lit24] Daniel Litt. In: *X-post* (March 16 2024). URL: <https://x.com/littmath/status/1769044719034647001>.

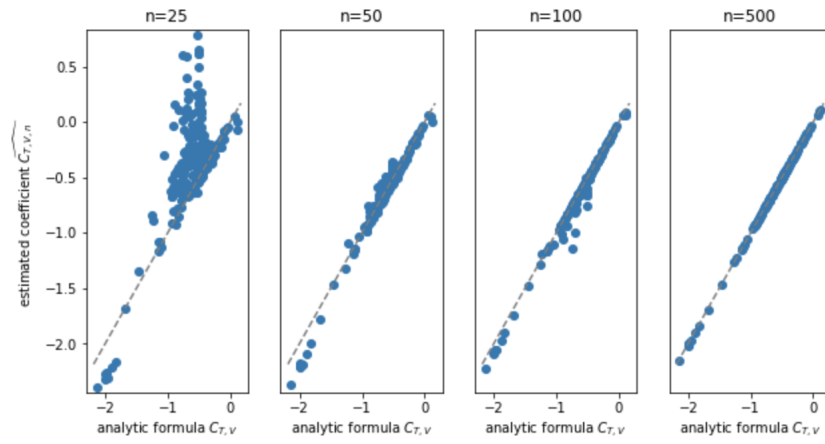


Figure 1: Illustration of Local Limit Theorem. Each dot corresponds to a different value function. The dotted gray segment is the line  $y = x$ .