Chapter 29

Random Walks II

By Sariel Har-Peled, April 26, 2022[1]

> "Then you must begin a reading program immediately so that you man understand the crises of our age," Ignatius said solemnly. "Begin with the late Romans, including Boethius, of course. Then you should dip rather extensively into early Medieval. You may skip the Renaissance and the Enlightenment. That is mostly dangerous propaganda. Now, that I think about of it, you had better skip the Romantics and the Victorians, too. For the contemporary period, you should study some selected comic books."
> "You're fantastic."
> "I recommend Batman especially, for he tends to transcend the abysmal society in which he's found himself. His morality is rather rigid, also. I rather respect Batman."
>
> John Kennedy Toole, A confederacy of Dunces

29.1. Catalan numbers

For a sequence σ of symbols, let $\#(\sigma, X)$ be the number of times the symbol X appears in σ.

Definition 29.1.1. A sequence/word σ of length $2n$ elements/characters made out of two symbols X and Y, is ***balanced***, if

(I) X appears n times (i.e., $\#(\sigma, X) = n$),
(II) Y appears n times (i.e., $\#(\sigma, Y) = n$),
(III) In any prefix of the string, the number of Xs is at least as large as the number of Ys.

Such a string is known as a ***Dyck word***. If X and Y are the open and close parenthesis characters, respectively, then the word is a balanced/valid parenthesis pattern.

Definition 29.1.2. The ***Catalan number***, denoted by C_n, is the number of balanced strings of length $2n$.

There are many other equivalent definitions of Catalan number.

Definition 29.1.3. A sequence σ made out of two symbols X and Y is ***dominating***, if for any non-empty prefix of σ, the number of Xs is strictly larger than the number of Ys.

Lemma 29.1.4. *Let σ be a cyclic sequence made out symbols X and Y, where $n = \#(\sigma, X)$ and $m = \#(\sigma, y)$, with $n > m$. Then there are exactly $n - m$ locations where cutting the cyclic sequence at these locations, results in a dominating sequence.*

Proof: Consider a location in σ that contains X, and the next location contains Y. Clearly, such a location can not be a start for a dominating sequence. Of course, the next location can also not be a start position for a dominating sequence. As such, these two locations must be interior to a dominating sequence, and deleting both of these symbols from σ, results in a new cyclic sequence, where every dominating start location corresponds to a dominating start location in the original sequence. Observe,

that as long as the number of Xs is larger than the number of Ys, there must be such a location with XY as the prefix. Repeatedly deleting XY substring, results in a string of length $n-m$, where every location is a good start of a dominating sequence. We conclude that there are exactly $n-m$ such locations. ■

Observation 29.1.5. *The number of distinct cyclic sequences of length $m+n$, with m appearances of X, and n appearances of Y is $\frac{(n+m-1)!}{m!n!} = \frac{1}{n+m}\binom{n+m}{n}$, since there are $(n+m-1)!$ different cyclic ways to arrange $n+m$ distinct values.*

Theorem 29.1.6. *For $n \geq 1$, we have that the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$.*

Proof: Consider a dominating sequence σ of length $2n+1$ with $\#(\sigma, X) = n+1$, and $\#(\sigma, Y) = n$. Such a sequence must start with an X, and if we remove the leading X, then what remains is a balanced sequence. Such a sequence σ can be interpreted as a cyclic sequence. By the above lemma, there is a unique shift that is dominating. As such, the number of such cyclic sequence is the Catalan number C_n. By the above observation, the number of such cyclic sequences is

$$\frac{(n+m-1)!}{m!n!} = \frac{(n+n+1-1)!}{(n+1)!n!} = \frac{1}{n+1}\frac{2n!}{n!n!} = \frac{1}{n+1}\binom{2n}{n}.$$

29.2. Walking on the integer line revisited

29.2.1. Estimating the middle binomial coefficient

Lemma 29.2.1. *For $i \geq 11^2$, we have $\frac{1}{4}\cdot\frac{2^{2i}}{\sqrt{i}} \leq \binom{2i}{i} \leq 2\cdot\frac{2^{2i}}{\sqrt{i}}$. and $\binom{2i}{i+\sqrt{i}} \geq \frac{1}{12}\cdot\frac{2^{2i}}{\sqrt{i}}$*

Proof: Observe that $\binom{2i}{i} \geq \binom{2i}{j}$, for any j. We assume that $i \geq 11^2$, and $\sqrt{i}$ is an integer. O bserve that $\binom{2i}{i+\tau} = \frac{2i!}{(i+\tau)!(i-\tau)!} = \frac{2i!}{i!i!}\frac{(i-\tau+1)\cdots(i-1)i}{(i+1)\cdots(i+\tau)} = \binom{2i}{i}\prod_{k=1}^{\tau}\frac{i-\tau+k}{i+k}$. Now, by Lemma **??**, we have

$$\alpha = \prod_{k=1}^{\tau}\frac{i-\tau+k}{i+k} = \prod_{k=1}^{\tau}\left(1-\frac{\tau}{i+k}\right) \geq \left(1-\frac{\tau}{i}\right)^{\tau} \geq \left(1-\frac{\tau^2}{i^2}\tau\right)\exp\left(-\frac{\tau^2}{i}\right) \geq \frac{1}{3},$$

for $\tau \leq \sqrt{i}$, and $i \geq 11^2$. Namely, for any k, such that $-\sqrt{i} \leq k \leq \sqrt{i}$, we have $\binom{2i}{i+k} \geq \binom{2i}{i}/3$. We thus have that

$$1 \geq \frac{1}{2^{2i}}\sum_{k=-\sqrt{i}+1}^{\sqrt{i}}\binom{2i}{i+k} \geq \frac{2\sqrt{i}}{3\cdot 2^{2i}}\binom{2i}{i} \qquad \Longrightarrow \qquad \binom{2i}{i} \leq \frac{2}{3}\cdot\frac{2^{2i}}{\sqrt{i}}.$$

Let $\Delta = \sqrt{i}-1$ and $X \sim \mathrm{bin}(2i, 1/2)$. We have that $\mathbb{E}[X] = i$, and $\mathbb{V}[X] = 2i(1/2)(1/2) = i/2$. Let $\beta = \frac{1}{2^{2i}}\sum_{k=-\Delta}^{\Delta}\binom{2i}{i+k}$. By Chebychev, we have that $1-\beta = \mathbb{P}\left[|X-i| \geq \sqrt{2}\sqrt{i/2}\right] \leq 1/2$. which implies $\beta \geq 1/2$. We have

$$\frac{1}{2} \leq \beta \leq \frac{1}{2^{2i}}\sum_{k=-\Delta}^{\Delta}\binom{2i}{i+k} \leq \frac{2\Delta+1}{2^{2i}}\binom{2i}{i} \qquad \Longrightarrow \qquad \binom{2i}{i} \geq \frac{2^{2i}}{2(2\Delta+1)} \geq \frac{2^{2i}}{4\sqrt{i}}.$$

Lemma 29.2.2. *In a random walk on the line starting at zero, in expectation, after $48n^2$ steps, the walk had visited either $-n$ or $+n$.*

Proof: By Lemma **??**, the probability that after $2i$ steps, for $i = 16n^2$, the walk is in the range $\{-\sqrt{i}+1, \ldots, \sqrt{i}-1\}$ is at most

$$2n\frac{1}{2^{2i}} \cdot \frac{2}{3} \cdot \frac{2^{2i}}{\sqrt{i}} = 2n\frac{2}{3} \cdot \frac{1}{4n} = \frac{1}{3}.$$

Namely, the walk arrived to either $-n$ or $+n$ during the first $32n^2$ steps (note that $n \leq i/2$) with probability $\geq 2/3$. If this did not happen, we continue the walk. As $i \geq 2n$, the same argumentation essentially implies that every $32n^2$ steps, the walk terminates with probability at least $2/3$. As such, in expectation, after $3/2$ such epochs, the walk would terminate. ■

29.3. Solving 2SAT using random walk

Let $\mathsf{G} = G(V, E)$ be a undirected connected graph. For $v \in V$, let $\Gamma(v)$ denote the neighbors of v in G. A random walk on G is the following process: Starting from a vertex v_0, we randomly choose one of the neighbors of v_0, and set it to be v_1. We continue in this fashion, such that $v_i \in \Gamma(v_{i-1})$. It would be interesting to investigate the process of the random walk. For example, questions like: (i) how long does it take to arrive from a vertex v to a vertex u in G? and (ii) how long does it take to visit all the vertices in the graph.

29.3.1. Solving 2SAT

Consider a 2SAT formula F with m clauses defined over n variables. Start from an arbitrary assignment to the variables, and consider a non-satisfied clause in F. Randomly pick one of the clause variables, and change its value. Repeat this till you arrive to a satisfying assignment.

Consider the random variable X_i, which is the number of variables assigned the correct value (according to the satisfying assignment) in the current assignment. Clearly, with probability (at least) half $X_i = X_{i-1} + 1$.

Thus, we can think about this algorithm as performing a random walk on the numbers $0, 1, \ldots, n$, where at each step, we go to the right probability at least half. The question is, how long does it take to arrive to n in such a settings.

Theorem 29.3.1. *The expected number of steps to arrive to a satisfying assignment is $O(n^2)$.*

Proof: For simplicity of exposition assume that n is divisible by 4. Consider the random walk on the integer line, starting from zero, where we go to the left with probability $1/2$, and to the right probability $1/2$. Let Y_i be the location of the walk at the i step. Clearly, $\mathbb{E}[Y_i] \geq \mathbb{E}[X_i]$. By defining the random walk on the integer line more carefully, one can ensure that $Y_i \leq X_i$. Thus, the expected number of steps till Y_i is equal to n is an upper bound on the required quantity.

For an i, Y_{2i} is an even number. Thus, consider the event that $Y_{2i} = 2\Delta \geq n$, let $Y_{2i} = R_{2i} - L_{2i}$, where R_{2i} is the number of steps to the right, and L_{2i} is the number of steps to the left. Observe that

$$\begin{cases} R_{2i} - L_{2i} = 2\Delta \\ R_{2i} + L_{2i} = 2i \end{cases} \implies \begin{cases} R_{2i} & = i + \Delta \\ L_{2i} = i - R_{2i} & = i - \Delta. \end{cases}$$

Thus, for $i \geq n/2$, we have that the probability that in the $2i$th step we have $Y_{2i} \geq n$ is

$$\rho = \sum_{\Delta=n/2}^{i} \frac{1}{2^{2i}} \binom{2i}{i+\Delta}.$$

Lemma **??** below, tells us that for $\rho > 1/3$, is implied if $\Delta \leq \sqrt{i}/6$. That is, $n/2 \leq \sqrt{i}/6$, which holds for $i = 9n^2$.

Next, if X_{2i} fails to arrive to n at the first μ steps, we will reset $Y_\mu = X_\mu$ and continue the random walk, repeating this process as many phases as necessary. The probability that the number of phases exceeds i is $\leq (2/3)^i$. As such, the expected number of steps in the walk is at most

$$\sum_i c' n^2 i (1-\rho)^i = O(n^2),$$

as claimed. ■

Lemma 29.3.2. *We have* $\sum_{k=i+\sqrt{i}/6}^{2i} \frac{1}{2^{2i}} \binom{2i}{k} \geq \frac{1}{3}$.

Proof: It is known[2] that $\binom{2i}{i} \leq 2^{2i}/\sqrt{i}$ (better constants are known). As such, since $\binom{2i}{i} \geq \binom{2i}{m}$, for all m, we have by symmetry that

$$\sum_{k=i+\sqrt{i}/6}^{2i} \frac{1}{2^{2i}} \binom{2i}{k} \geq \sum_{k=i+1}^{2i} \frac{1}{2^{2i}} \binom{2i}{k} - \sqrt{i}/6 \frac{1}{2^{2i}} \binom{2i}{i} \geq \frac{1}{2} - \sqrt{i}/6 \frac{1}{2^{2i}} \cdot \frac{2^{2i}}{\sqrt{i}} = \frac{1}{3}.$$

29.4. Markov chains

Let $\mathtt{S}$ denote a state space, which is either finite or countable. A ***Markov chain*** is at one state at any given time. There is a ***transition probability*** $\mathtt{P}_{ij}$, which is the probability to move to the state j, if the Markov chain is currently at state i. As such, $\sum_j \mathtt{P}_{ij} = 1$ and $\forall i, j$ we have $0 \leq \mathtt{P}_{ij} \leq 1$. The matrix $\mathbf{P} = \{\mathtt{P}_{ij}\}_{ij}$ is the ***transition probabilities matrix***.

$$\mathbf{P} = \begin{pmatrix} & j\text{th column} & \\ i\text{th row} & \mathtt{P}_{ij} & \\ & & \end{pmatrix}$$

The Markov chain start at an initial state X_0, and at each point in time moves according to the transition probabilities. This form a sequence of states $\{X_t\}$. We have a distribution over those sequences. Such a sequence would be referred to as a ***history***.

Similar to Martingales, the behavior of a Markov chain in the future, depends only on its location X_t at time t, and does not depends on the earlier stages that the Markov chain went through. This is the ***memorylessness property*** of the Markov chain, and it follows as $\mathtt{P}_{ij}$ is independent of time. Formally, the memorylessness property is

$$\mathbb{P}\left[X_{t+1} = j \;\middle|\; X_0 = i_0, X_1 = i_1, \ldots, X_{t-1} = i_{t-1}, X_t = i\right] = \mathbb{P}[X_{t+1} = j \mid X_t = i] = \mathtt{P}_{ij}.$$

[2] Probably because you got it as a homework problem, if not wikipedia knows, and if you are bored you can try and prove it yourself.

The initial state of the Markov chain might also be chosen randomly in some cases.

For states $i, j \in \mathtt{S}$, the ***t-step transition probability*** is $\mathtt{P}_{ij}^{(t)} = \mathbb{P}\big[X_t = j \;\big|\; X_0 = i\big]$. The probability that we visit j for the first time, starting from i after t steps, is denoted by

$$\mathtt{r}_{ij}^{(t)} = \mathbb{P}\big[X_t = j \text{ and } X_1 \neq j, X_2 \neq j, \ldots, X_{t-1} \neq j \;\big|\; X_0 = i\big].$$

Let $\mathtt{f}_{ij} = \sum_{t>0} \mathtt{r}_{ij}^{(t)}$ denote the probability that the Markov chain visits state j, at any point in time, starting from state i. The expected number of steps to arrive to state j starting from i is

$$\mathtt{h}_{ij} = \sum_{t>0} t \cdot \mathtt{r}_{ij}^{(t)}.$$

Of course, if $\mathtt{f}_{ij} < 1$, then there is a positive probability that the Markov chain never arrives to j, and as such $\mathtt{h}_{ij} = \infty$ in this case.

Definition 29.4.1. A state $i \in \mathtt{S}$ for which $\mathtt{f}_{ii} < 1$ (i.e., the chain has positive probability of never visiting i again), is a ***transient*** state. If $\mathtt{f}_{ii} = 1$ then the state is ***persistent***.

A state i that is persistent but $\mathtt{h}_{ii} = \infty$ is ***null persistent***. A state i that is persistent and $\mathtt{h}_{ii} \neq \infty$ is ***non null persistent***.

Example 29.4.2. Consider the state 0 in the random walk on the integers. We already know that in expectation the random walk visits the origin infinite number of times, so this hints that this is a persistent state. Let figure out the probability $\mathtt{r}_{00}^{(2n)}$. To this end, consider a walk $X_0, X_1, \ldots, X_{2n}$ that starts at 0 and return to 0 only in the $2n$ step. Let $S_i = X_i - X_{i-1}$, for all i. Clearly, we have $S_i \in \{-1, +1\}$ (i.e., move left or move right). Assume the walk starts by $S_1 = +1$ (the case -1 is handled similarly). Clearly, the walk $S_2, \ldots, S_{2n-1}$ must be prefix balanced; that is, the number of 1s is always bigger (or equal) for any prefix of this sequence.

Strings with this property are known as ***Dyck words***, and the number of such words of length $2m$ is the ***Catalan number*** $C_m = \frac{1}{m+1}\binom{2m}{m}$. As such, the probability of the random walk to visit 0 for the first time (starting from 0) after $2n$ steps, is

$$\mathtt{r}_{00}^{(2n)} = 2\frac{1}{n}\binom{2n-2}{n-1}\frac{1}{2^{2n}} = \Theta\left(\frac{1}{n} \cdot \frac{1}{\sqrt{n}}\right) = \Theta\left(\frac{1}{n^{3/2}}\right).$$

(the 2 here is because the other option is that the sequence starts with -1), using that $\binom{2n}{n} = \Theta\big(2^{2n}/\sqrt{n}\big)$.

Observe that $\mathtt{f}_{00} = \sum_{n=0}^{\infty} \mathtt{r}_{00}^{(2n)} = O(1)$. However, one can be more precise – that is, $\mathtt{f}_{00} = 1$ (this requires a trick)! On the other hand, we have that

$$\mathtt{h}_{00} = \sum_{t>0} t \cdot \mathtt{r}_{00}^{(t)} \geq \sum_{n=1}^{\infty} 2n\mathtt{r}_{00}^{(2n)} = \sum_{n=1}^{\infty} \Theta\big(1/\sqrt{n}\big) = \infty.$$

Namely, 0 (and indeed all integers) are null persistent.

In finite Markov chains there are no null persistent states (this requires a proof, which is left as an exercise). There is a natural directed graph associated with a Markov chain. The states are the vertices, and the transition probability $\mathtt{P}_{ij}$ is the weight assigned to the edge $(i \to j)$. Note that we include only edges with $\mathtt{P}_{ij} > 0$.

Definition 29.4.3. A ***strong component*** (or a *strong connected component*) of a directed graph G is a maximal subgraph C of G such that for any pair of vertices i and j in the vertex set of C, there is a directed path from i to j, as well as a directed path from j to i.

Definition 29.4.4. A strong component C is a ***final strong component*** if there is no edge going from a vertex in C to a vertex that is not in C.

In a finite Markov chain, there is positive probability to arrive from any vertex on C to any other vertex of C in a finite number of steps. If C is a final strong component, then this probability is 1, since the Markov chain can never leave C once it enters it[3]. It follows that a state is persistent if and only if it lies in a final strong component.

Definition 29.4.5. A Markov chain is ***irreducible*** if its underlying graph consists of a single strong component.

Clearly, if a Markov chain is irreducible, then all states are persistent.

Definition 29.4.6. Let $\mathbf{q}^{(t)} = \left(q_1^{(t)}, q_2^{(t)}, \ldots, q_n^{(t)}\right)$ be the ***state probability vector*** (also known as the distribution of the chain at time t), to be the row vector whose ith component is the probability that the chain is in state i at time t.

The key observation is that

$$\mathbf{q}^{(t)} = \mathbf{q}^{(t-1)}\mathbf{P} = \mathbf{q}^{(0)}\mathbf{P}^t.$$

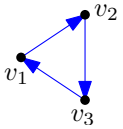
Namely, a Markov chain is fully defined by $\mathbf{q}^{(0)}$ and $\mathbf{P}$.

Definition 29.4.7. A ***stationary distribution*** for a Markov chain with the transition matrix $\mathbf{P}$ is a probability distribution π such that $\pi = \pi\mathbf{P}$.

In general, stationary distribution does not necessarily exist. We will mostly be interested in Markov chains that have stationary distribution. Intuitively it is clear that if a stationary distribution exists, then the Markov chain, given enough time, will converge to the stationary distribution.

Definition 29.4.8. The ***periodicity*** of a state i is the maximum integer T for which there exists an initial distribution $\mathbf{q}^{(0)}$ and positive integer a such that, for all t if at time t we have $q_i^{(t)} > 0$ then t belongs to the arithmetic progression $\left\{a + ti \;\middle|\; i \geq 0\right\}$. A state is said to be ***periodic*** if it has periodicity greater than 1, and is ***aperiodic*** otherwise. A Markov chain in which every state is aperiodic is ***aperiodic***.

Example 29.4.9. The easiest example maybe of a periodic Markov chain is a directed cycle.



For example, the Markov chain on the right, has periodicity of three. In particular, the initial state probability vector $\mathbf{q}^{(0)} = (1, 0, 0)$ leads to the following sequence of state probability vectors

$$\mathbf{q}^{(0)} = (1,0,0) \implies \mathbf{q}^{(1)} = (0,1,0) \implies \mathbf{q}^{(2)} = (0,0,1) \implies \mathbf{q}^{(3)} = (1,0,0) \implies \ldots.$$

Note, that this chain still has a stationary distribution, that is $(1/3, 1/3, 1/3)$, but unless you start from this distribution, you are going to converge to it.

[3] Think about it as hotel California.

A neat trick that forces a Markov chain to be aperiodic, is to shrink all the probabilities by a factor of 2, and make every state to have a transition probability to itself equal to 1/2. Clearly, the resulting Markov chain is aperiodic.

Definition 29.4.10. An ***ergodic*** state is aperiodic and (non-null) persistent.

An ***ergodic*** Markov chain is one in which all states are ergodic.

The following theorem is the fundamental property of Markov chains that we will need. The interested reader, should check the proof in [**n-mc-98**] (the proof is not hard).

Theorem 29.4.11 (Fundamental theorem of Markov chains). *Any irreducible, finite, and aperiodic Markov chain has the following properties.*

(i) *All states are ergodic.*

(ii) *There is a unique stationary distribution π such that, for $1 \leq i \leq n$, we have $\pi_i > 0$.*

(iii) *For $1 \leq i \leq n$, we have $\mathtt{f}_{ii} = 1$ and $\mathtt{h}_{ii} = 1/\pi_i$.*

(iv) *Let $N(i,t)$ be the number of times the Markov chain visits state i in t steps. Then*

$$\lim_{t\to\infty} \frac{N(i,t)}{t} = \pi_i.$$

Namely, independent of the starting distribution, the process converges to the stationary distribution.

29.5. From previous lectures