Voting-based probabilistic consensuses

Author: Camilo Núñez

Thesis director: Sebastian Müeller

Master 1 Mathématiques et Applications
Faculty of Sciences
Aix-Marseille Université
France
June 2023

Abstract:

C'est article est basé sur les resultats obtenues en [4]. Le but de cet TER est d'étudier un cas particulier d'une famille des protocoles de consensus connu sous le nom de "Voter Models" ou "Majority Dynamics". On va d'abord montrer des résultats sur son bon comportement en travaillant uniquement avec des nœuds honnêtes. Après, on discute son comportement en présence de nœuds byzantins, qui est en général très sensible aux conditions initiales.

Abstract:

This article was based on the results obtained on [4]. The goal of this TER was to study a particular case of a family of consensus protocols known as voter models or majority dynamics. We will first show results about its good behavior while working only with honest nodes. Then, we discuss its behavior under the presence of Byzantine nodes, which in general is very susceptible to initial conditions.

Contents

1 Introduction

1.1 Objectives

This article is composed of two main parts, sections 3 and 4. In the section 3 we introduce an instance of the family of the voters models consensus protocols, in which we suppose all the participants are honest. We decided to call it *Toy Model* since it is not usually the case. In this section, we prove 4 statements considering all the mathematical details.

In the section 4, we start considering Byzantine nodes, i.e., nodes that do not follow the protocol honestly. The goal of this section is to study how we can achieve a consensus in the presence of Byzantine nodes. Here we will only introduce the intuition of how these systems behave since the formal proofs of the statements that will be presented require the use of probabilistic tools whose mathematical proofs are out of the scope of this paper.

1.2 Why probabilistic voter models?

The interest in consensus protocols lies in the fact that it is fundamental in every Distributed Ledger Technology (DLT), which is usually used in cryptocurrency systems. Consensus protocols are used to guarantee security in decentralized currency systems, along with cryptographic tools.

There are different kinds of consensus protocols and their behavior depends on the kind of network they are working on. In cryptocurrency systems, for example, the usual scenario are large, permissionless[1], and decentralized networks. Although Proof of Work (PoF) was a solution for reaching consensus on permissionless, decentralized networks, it has the disadvantages of high energy consumption and requiring high communication complexity[2].

Regarding the main question of this subsection, probabilistic voters models have the advantage of having reduced communication complexity. These models also have some inconveniences that we will discuss in the section 4. Still, in general, the authors of [4] considered the low communication complexity a sufficiently good motivation to study these consensus protocol models.

1.3 Description

Voters models are probabilistic models where in each round, a node contacts only a small number of other nodes in order to learn their opinions, and possibly change its own. They were introduced in the 1970s by Holley and Liggett [2] and Clifford and Sudbury [1]. These models have no single rigorous definition, so we will roughly define them, as it was done in [4], as models accomplishing the following conditions:

- The model consists of a connected [3] graph, typically non-oriented, comprising a set of nodes that can be finite or infinite.
- At discrete or continuous moments in time, each node possesses an opinion, also known as a spin in statistical physics literature, which can be either 0 or 1.

[1] There is no authorization required to participate in the system.

[2] In consensus protocols, it is, roughly speaking, the number of sent messages required to reach a consensus. It can be defined as the average number of messages needed to reach a consensus.

[3] There exists a path between each pair of nodes.

- At random or deterministic time intervals, a specific node reaches out to a random subset of its neighboring nodes and inquires about their current opinions. Subsequently, the node updates its own opinion based on a specific rule, which considers the received opinions, as well as potentially its own current opinion. These updates can occur synchronously or asynchronously.
- The rule must be consistent. This means that if a node queries only say opinion-0 nodes, its final opinion must be 0.
- The rule has to be monotonic. This means that if a node decides on an opinion $i \in \{0, 1\}$ based on the rule, it would maintain the same decision if some of the received opinions are flipped from $1 - i$ to i. Essentially, when an opinion garners more support, a node cannot cease to prefer it.

2 Preliminaries

The purpose of this section is to introduce concepts for readers who are not familiar with stochastic processes or just to agree on the definitions that will be used. We will also present, without proof, some statements that will be used eventually.

Definition 2.1. *A stochastic process or just a process is a sequence $(X_n)_{n\in\mathbb{N}}$ of random variables over a probability space $(\Omega, \mathcal{F}, \mathbb{P})$.*

Definition 2.2. *Given a σ-algebra $\mathcal{F}$, an increasing sequence $(\mathcal{F}_i)_{i\in\mathbb{N}} \subseteq \mathcal{F}$ of σ-algebras is called a filtration of $\mathcal{F}$. We say that the process $(X_i)_{i\in\mathbb{N}}$ is adapted to $(\mathcal{F}_i)_{i\in\mathbb{N}}$ if X_i is $\mathcal{F}_i$-measurable for all $i \in \mathbb{N}$.*

Definition 2.3. *Given a random variable X over $(\Omega, \mathcal{F}, \mathbb{P})$, and $\mathcal{F}_0 \subseteq \mathcal{F}$, we define the conditional expectation of X with respect to $\mathcal{F}_0$, denoted $\mathbb{E}[X \mid \mathcal{F}_0]$, as the unique random variable over $(\Omega, \mathcal{F}_0, \mathbb{P})$ such that for all $A \in \mathcal{F}_0$, $\int_A Y d\omega = \int_A X d\omega$.*

Definition 2.4. *Given an adapted process $(X_i)_{i\in\mathbb{N}}$, we say that the process is a martingale if for all $i \in \mathbb{N}$*

- $\mathbb{E}[|X_i|] < \infty$
- $(X_i)_{i\in\mathbb{N}}$ *is adapted to* $(\mathcal{F}_i)_{i\in\mathbb{N}}$
- $\mathbb{E}[|X_{i+1}| \mid \mathcal{F}_i] = X_i$.

Definition 2.5. *Given a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ and a filtration $(\mathcal{F}_i)_{i\in\mathbb{N}}$, we say that a random variable $T : (\Omega, \mathcal{F}, \mathbb{P}) \to (\mathbb{N}, \mathcal{P}(\mathbb{N}))$ is a stopping time if for all $i \in \mathbb{N}$ we have that $[T = i] \in \mathcal{F}_i$.*

Definition 2.6. *We say a process $(X_i)_{i\in\mathbb{N}}$ in $L^1[(\Omega, \mathcal{F}, \mathbb{P})]$ is uniformly integrable if*

$$\lim_{a\to+\infty} \left(\sup_{i\in I} \mathbb{E}\left[|X_i| \, \mathbf{1}_{\{|X_i|>a\}} \right] \right) = 0.$$

The proof of the following two theorems can be found in the corollaries of theorem 12.5.3 in [3].

Theorem 2.7. *The two following statements are equivalent for a martingale* $(X_n)_{n\in\mathbb{N}}$:

(i) X_n *converges to* X_∞ *a.s and in the space* L^1.

(ii) The sequence $(X_n)_{n\in\mathbb{N}}$ *is uniformly integrable.*

Theorem 2.8. *If* $(X_n)_{n\in\mathbb{N}}$ *is an adapted process converging a.s to* X_∞*, we define* X_T *for every stopping time* T*, finite or not, as*

$$X_T = \sum_{n=0}^{\infty} \mathbf{1}_{\{T=n\}} X_n + \mathbf{1}_{\{T=\infty\}} X_\infty.$$

Under this conditions we have that X_T *is* $\mathcal{F}_T$*-measurable.*

The proof of the following theorem is part of the proof of theorem 12.5.4 of [3].

Theorem 2.9. *Let* $(X_n)_{n\in\mathbb{N}}$ *be a uniformly integrable martingale. Then, for any two stopping times such that* $S \leq T$*, we have that*

$$X_S = E\left[X_T \mid \mathcal{F}_S\right].$$

3 Toy Model

3.1 A simple majority dynamics model and its properties

To start dealing with consensus protocols it is a good idea to understand what the "objective of the game" is. The reader should keep in mind that the questions and results are focused on solving the following situation: An ancient city A (no social media allowed) will be invaded by another ancient city B. Suppose that the people from city A know they have, say, 72 hours to agree between two strategies, 0 or 1. It does not really matter what the chosen strategy is, the goal is to fight in a coherent way and have more chances of winning. Suppose as well that the city does not have a king. If the population is very high not only there is not a central authority that will decide the strategy but no single person can communicate with every other person in the city. The solution for this is to find a protocol that every person should follow in order to reach a consensus state as soon as possible. Being said this, we introduce the toy model.

Our toy model works like this: There are n nodes in the system and at each time step, one of them is chosen randomly. The selected node then picks three nodes at random and counts their opinions equally. In particular, it may choose itself and may also choose a node more than once. The selected node then adopts the majority opinion of the three chosen nodes until it is selected again.

We are not considering any Byzantine nodes in this subsection, so we assume that all nodes are following the protocol honestly.

We will assume that n is a positive integer greater than or equal to 20, and that it is also divisible by 4. This assumption simplifies calculations and avoids dealing with fractional values in certain instances. Please note that this assumption is just made for the sake of convenience in this toy model.

Remark:

> We remind the reader that the Binomial(k, p) distribution (k and p are called the parameters) is the probability distribution that arises when we take k objects from a box, assuming that after every time we take an object it is replaced with another of the same nature. The parameter p stands for the probability of obtaining an object of the desired nature in each one of the k rounds.
>
> If we consider the random variable X that denotes the number of objects of the desired nature that we get after the k rounds. The explicit formula for its probability distribution (which is the Binomial(k, p)) is
>
> $$\mathbb{P}(X = i) = \binom{k}{i} p^i (1-p)^{k-i}$$
>
> for every $i \in \{0, \ldots, k\}$.

Let's define X_k as the number of nodes with opinion 1 at time k. Assuming $X_k = m$, we can represent by the random variable η_k the number of opinion-1 nodes among three independently chosen nodes (with the possibility of selecting the same node multiple times). In this case, η_k follows a Binomial$(3, \frac{m}{n})$ distribution.

If one of the m opinion-1 nodes was selected (which happens with probability $\frac{m}{n}$), it will switch its opinion to 0 with probability

$$\begin{aligned}
\mathbb{P}_{X_k=m}(\eta < 2) &= \mathbb{P}_{X_k=m}(\eta = 0 \cup \eta = 1) \\
&= \mathbb{P}_{X_k=m}(\eta = 0) + \mathbb{P}_{X_k=m}(\eta = 1) \\
&= \left(1 - \frac{m}{n}\right)^3 + 3\left(1 - \frac{m}{n}\right)\left(\frac{m}{n}\right)^2.
\end{aligned}$$

Where the $\mathbb{P}_{X_k=m}$ denotes for the probability conditioned to the event $[X_k = m]$. Likewise, if a node with current opinion 0 was selected (which happens with probability $1 - \frac{m}{n}$), it will switch its opinion to 1 with probability $\left(\frac{m}{n}\right)^3 + 3\left(1 - \frac{m}{n}\right)\left(\frac{m}{n}\right)^2$. In particular, and as expected, 0 and n are absorbing states: if $X_{k_0} \in \{0, n\}$ for some k_0 then $X_k = X_{k_0}$ for all $k > k_0$. In other words, the process $(X_i)_{i \in \mathbb{N}}$ is a (one-dimensional) random walk on $\{0, \ldots, n\}$ with the following transition probabilities: On $X_k = m \in \{1, \ldots, n-1\}$ we have

$$X_{k+1} = \begin{cases} m-1, & \text{with probability } p_m \\ m+1, & \text{with probability } q_m \\ m, & \text{with probability } v_m = 1 - p_m - q_m \end{cases} \tag{1}$$

where

$$
\begin{aligned}
p_m &= \frac{m}{n}\left(\left(1-\frac{m}{n}\right)^3 + 3\left(1-\frac{m}{n}\right)^2\frac{m}{n}\right) \\
&= \frac{m}{n}\left(1-\frac{m}{n}\right)\left(\left(1-\frac{m}{n}\right)^2 + 3\frac{m}{n}\left(1-\frac{m}{n}\right)\right) \\
q_m &= \left(1-\frac{m}{n}\right)\left(\left(\frac{m}{n}\right)^3 + 3\left(1-\frac{m}{n}\right)\left(\frac{m}{n}\right)^2\right) \\
&= \frac{m}{n}\left(1-\frac{m}{n}\right)\left(\left(\frac{m}{n}\right)^2 + 3\frac{m}{n}\left(1-\frac{m}{n}\right)\right) \\
v_m &= 1 - \frac{m}{n}\left(1-\frac{m}{n}\right)\left(1+4\frac{m}{n}\left(1-\frac{m}{n}\right)\right). \qquad (2)
\end{aligned}
$$

To see this in more detail, we will develop p_m. The other two transitions can be proved analogously. We know that

$$p_m = P_{X_k=m}(A \cap [\eta < 2])$$

where A is the event where the chosen node is opinion-1. Since we are assuming the elections this node will make are independent from its election, we have that

$$p_m = P_{X_k=m}(A \cap [\eta < 2]) = P_{X_k=m}(A)P_{X_k=m}([\eta < 2]).$$

Finally, since we are also assuming the election of the initial node is uniformly distributed, we have that $P_{X_k=m}(A) = \frac{m}{n}$, and therefore

$$p_m = \frac{m}{n}\left(\left(1-\frac{m}{n}\right)^3 + 3\left(1-\frac{m}{n}\right)^2\frac{m}{n}\right).$$

Let's revisit the random walk described in equation (1). It's worth noting that the transition probabilities mentioned above are symmetric. Specifically, $p_{n-m} = q_m$ and $q_{n-m} = p_m$, which implies that

$$\frac{p_{n-m}}{q_{n-m}} = \frac{q_m}{p_m} \qquad (3)$$

Let us define the function $V : \{0, \ldots, n-1\} \mapsto \mathbb{R}$ (frequently called the potential) by $V(0) = 0$ and

$$V(k) = \sum_{j=1}^{k} \log \frac{p_j}{q_j}. \qquad (4)$$

Then, (3) implies that $V(n-1) = 0$ and, in general, $V(m) = V(n-1-m)$ (that is, it is symmetric around $\frac{n-1}{2}$); in particular, $V\left(\frac{n}{2}-1\right) = V\left(\frac{n}{2}\right)$. To check this, assume without loss of generality that $m < \frac{n}{2}$. Using that

$$\log(\frac{a}{b}) = -\log(\frac{b}{a}) \text{ , } \log\left(\frac{p_{\frac{n}{2}}}{q_{\frac{n}{2}}}\right) = \log(1) = 0 \text{ and } (3)$$

we have that

$$V(m) = \sum_{j=1}^{j=m} \frac{p_j}{q_j} = \sum_{j=1}^{j=m} \frac{p_j}{q_j} + \sum_{j=m+1}^{\frac{n}{2}-1} \frac{p_j}{q_j} + \sum_{j=\frac{n}{2}+1}^{n-1-m} \frac{p_j}{q_j} = V(n-m-1).$$

Furthermore, when $m \leq \frac{n}{2}$, we observe that p_m is greater than q_m. As a result, $V(m)$ is greater than 0 for values of m between 0 and n. The function $V(m)$ is strictly increasing on the interval $[0, \frac{n}{2} - 1]$ and strictly decreasing on the interval $[\frac{n}{2}, n-1]$. This function serves as the "landscape profile" or "potential landscape" that the walker traverses. Through further analysis, it can be determined that this profile closely resembles the one depicted in Figure 1.

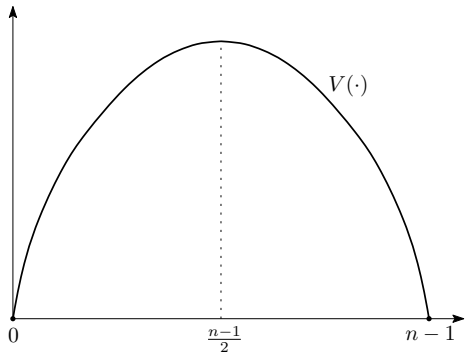

Figure 1: The potential landscape. Image taken from [4]

We also have that

$$\frac{p_m}{q_m} = f\left(\frac{m}{n}\right), \quad \text{where } f(u) = \frac{(1-u)^2 + 3u(1-u)}{u^2 + 3u(1-u)}.$$

As we can see in Figure 2, f is a strictly decreasing function on the interval $(0,1)$ with $f\left(\frac{1}{2}\right) = 1$ (and also $f(1-u) = 1/f(u)$). Note also that $\log \frac{p_m}{q_m}$ approaches to 0 when m is close to $\frac{n}{2}$.

One of the interesting features of the potential landscape defined in (4) is that it can be used to compute the escape probabilities from an interval. Our first theorem is a useful tool for this purpose.

The hitting time of a set A is denoted as τ_A and defined as the minimum number of steps required for the process to reach a state in A. In other words $\tau_A := \min\{n \geq 1 : X_n \in A\}$. Similarly, we use τ_a to represent the hitting time of a singleton set $\{a\}$. We will also use the notations $\mathbb{P}_x$ and $\mathbb{E}_x$ to refer to the probability and expectations, respectively, with respect to the process starting at the state x, that is, $\mathbb{P}_x$ and $\mathbb{E}_x$ represent the probability and expectation conditioned on the event $[X_0 = x]$. We are finally ready to prove our first theorem.

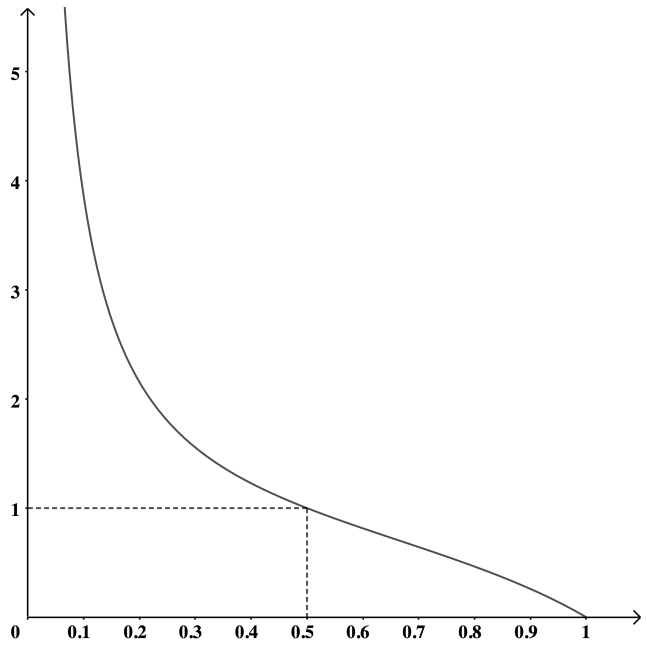

Figure 2: The behaviour of $\frac{p_m}{q_m} = f(\frac{m}{n})$.

Theorem 3.1. *For $0 \leq a < x < b \leq n$ it holds that*

$$\mathbb{P}_x[\tau_b < \tau_a] = \frac{\sum_{y=a}^{x-1} e^{V(y)}}{\sum_{y=a}^{b-1} e^{V(y)}}$$

Proof. Define

$$g(m) := 1 + \frac{p_1}{q_1} + \cdots + \frac{p_1 \cdots p_{m-1}}{q_1 \cdots q_{m-1}} = \sum_{j=0}^{m-1} e^{V(j)}.$$

Note that

$$\begin{aligned} g(m) &= g(X_j = m) = \mathbb{E}[g(X) \mid X_j = m] \\ &= p_m g(m-1) + q_m g(m+1) + v_m g(m) \end{aligned} \tag{5}$$

for m in $\{1, \ldots, n-1\}$.

Let's see now how this can be used to prove that $(g(X_j))_{j \in \mathbb{N}}$ is a martingale with respect to the filtration $(\mathcal{F}_j = \sigma(X_0, \ldots, X_j))_{j \in \mathbb{N}}$ of the σ-algebra $\mathcal{F} = \sigma(\bigcup_{j=0}^{\infty} X_j)$. It is important to remark that $X_{j \wedge \tau_{\{0,n\}}} = X_j$ since 0 and n are absorbing states. In other words, the process is stopped automatically when it reaches consensus. Also, since $g : \{0, \ldots, n\} \to \mathbb{R}$ is strictly increasing and therefore injective; and measurable since we use the discrete σ-algebra in $\{0, \ldots, n\}$, we have that $\sigma(g(X_0), \ldots, g(X_j)) = \sigma(X_0, \ldots, X_j)$. Let's check that $(g(X_j))_{j \in \mathbb{N}}$ accomplishes the 3 conditions to be a martingale.

- Let $j \in \mathbb{N}$, $g(X_j)$ is integrable since $|g(X_j)| \leq |g(n)|$.
- $(g(X_j))_{j\in\mathbb{N}}$ is clearly adapted to $(\sigma(g(X_0), \ldots, g(X_j)))_{j\in\mathbb{N}}$ and therefore to $(\mathcal{F}_j)_{j\in\mathbb{N}}$ due to what we proved above.
- Finally, to see that $\mathbb{E}[g(X_{j+1}) \mid \mathcal{F}_j] = g(X_j)$ for every $j \in \mathbb{N}$, we will prove that $\int_A g(X_{j+1})d\omega = \int_A g(X_j)d\omega$ for every $A \in \mathcal{F}_j$.

  Since

  $$\sigma(\{[X_k = m] : k \in \{0, 1, \ldots, j\} \text{ and } m \in \{0, \ldots, n\}\}) = \mathcal{F}_j$$

  We only have to prove it for all $A \in \{[X_k = m] : k \in \{0, \ldots, j\} \text{ and } m \in \{0, \ldots, n\}\}$. Let $j \in \mathbb{N}$, $k \in \{0, \ldots, j\}$ and $m \in \{0, \ldots, n\}$.

  If $k = j - 1$ we have that

  $$\begin{aligned}\int_{X_j=m} g(X_{j+1})d\omega &= \mathbb{E}[g(X_{j+1}) \mid X_j = m]\mathbb{P}(X_j = m) \\ &= (p_j g(m-1) + v_j g(m) + q_j g(m+1))\mathbb{P}(X_j = m) \\ &= g(m)\mathbb{P}(X_j = m) \\ &= \mathbb{E}[g(X_j) \mid X_j = m]\mathbb{P}(X_j = m) \\ &= \int_{X_j=m} g(X_j)d\omega\end{aligned}$$

  If $k < j - 1$, we proceed as follows.

$$
\begin{aligned}
&\int_{X_k=m} g(X_{j+1}) \\
&= \mathbb{E}[g(X_{j+1}) \mid X_k = m]\mathbb{P}(X_k = m) \\
&:= \mathbb{E}_{X_k=m}[g(X_{j+1})]\mathbb{P}(X_k = m) \\
&= \mathbb{P}(X_k = m)\sum_{i=0}^{n} \mathbb{E}_{X_k=m}[g(X_{j+1}) \mid X_j = i]\mathbb{P}_{X_k=m}(X_j = i) \\
&\text{(Total probability theorem)} \\
&= \mathbb{P}(X_k = m)\sum_{i=0}^{n} \mathbb{E}[g(X_{j+1}) \mid X_j = i]\mathbb{P}_{X_k=m}(X_j = i) \\
&((X_i)_{i\in\mathbb{N}} \text{ is a Markov chain}) \\
&= \mathbb{P}(X_k = m)\sum_{i=0}^{n} \mathbb{E}[g(X_j) \mid X_j = i]\mathbb{P}_{X_k=m}(X_j = i) \\
&\text{(We proved before that } \mathbb{E}[g(X_{j+1}) \mid X_j] = X_j) \\
&= \mathbb{P}(X_k = m)\sum_{i=0}^{n} \mathbb{E}_{X_k=m}[g(X_j) \mid X_j = i]\mathbb{P}_{X_k=m}(X_j = i) \\
&= \mathbb{P}(X_k = m)\mathbb{E}_{X_k=m}[g(X_j)] \\
&= \int_{X_k=m} g(X_j)d\omega.
\end{aligned}
$$

Now, let's see that $\mathbb{P}_x[\tau_b < \tau_a]g(b) + \mathbb{P}_x[\tau_a < \tau_b]g(a) = g(x)$. For this, we have to prove first that

$$\mathbb{E}_x[X_{\tau_{\{a,b\}}}] = \mathbb{E}_x[\mathbb{E}[g(X_{\tau_{\{0,n\}}}) \mid \mathcal{F}_{\tau_{\{a,b\}}}]] \tag{6}$$

Since $(g(X_i))_{i\in\mathbb{N}}$ is a martingale, theorems (2.7), (2.8) tell us that $g(X_{\tau_{\{a,b\}}})$ is $\mathcal{F}_{\tau_{\{a,b\}}}$ measurable.
Since $[X_0 = x] \in \mathcal{F}_{\tau_{\{a,b\}}}$, we have that

$$\mathbb{E}[g(X_{\tau_{\{a,b\}}})\mathbb{1}_{[X_0=x]}] = \mathbb{E}[\mathbb{E}[g(X_{\tau_{\{a,b\}}}) \mid \mathcal{F}_{\tau_{\{a,b\}}}]\mathbb{1}_{[X_0=x]}]$$

and therefore,

$$\mathbb{E}_x[g(X_{\tau_{\{a,b\}}})] = \mathbb{E}_x[\mathbb{E}[g(X_{\tau_{\{a,b\}}}) \mid \mathcal{F}_{\tau_{\{a,b\}}}]]$$

Since $|g(X_j)| \leq |g(n)|$, $(g(X_j))_{j\in\mathbb{N}}$ is clearly uniformly integrable. Also, $\tau_{\{a,b\}} \leq \tau_{\{0,n\}}$ for all $\omega \in [X_0 = x]$. If we define $S = \tau_{\{a,b\}}\mathbb{1}_{[X_0=x]}$, $T = \tau_{\{0,n\}}\mathbb{1}_{[X_0=x]}$ it is straight forward to see that S and T are stopping times such that $S \leq T$, and therefore, we accomplish all the requirements

to use theorem (2.9). Thus, we have that

$$\begin{aligned} g(X_S) = \mathbb{E}[g(X_T) \mid \mathcal{F}_S] &\Rightarrow \mathbb{E}_x[g(X_S)] = \mathbb{E}_x[\mathbb{E}[g(X_T) \mid \mathcal{F}_S]] \\ &\Rightarrow \mathbb{E}_x[g(X_{\tau_{\{a,b\}}})] = \mathbb{E}_x[\mathbb{E}[g(X_{\tau_{\{0,n\}}}) \mid \mathcal{F}_{\tau_{\{a,b\}}}]] \end{aligned}$$

As desired.

Finally,

$$\begin{aligned} \mathbb{P}_x[\tau_b < \tau_a]g(b) + \mathbb{P}_x[\tau_a < \tau_b]g(a) &= \mathbb{E}_x[g(X_{\tau_{\{a,b\}}}))] \\ &= \mathbb{E}_x[\mathbb{E}[g(X_{\tau_{\{0,n\}}}) \mid \mathcal{F}_{\tau_{\{a,b\}}}]] \\ &= \mathbb{E}_x[\mathbb{E}[g(X_{\tau_{\{0,n\}}})]] \\ &(g(X_j) \text{ is a martingale}) \\ &= \mathbb{E}_x[\mathbb{E}[g(X_0)]] = g(x) \end{aligned}$$

Therefore, we have that

$$g(x) = \mathbb{P}_x\left[\tau_b < \tau_a\right] g(b) + \left(1 - \mathbb{P}_x\left[\tau_b < \tau_a\right]\right) g(a).$$

solving the above for $\mathbb{P}_x\left[\tau_b < \tau_a\right]$ we obtain the desired result.

□

The next result tells us that the initial "significantly leading" opinion, that is, an opinion shared by a proportion $\alpha > 1/2$, does not ultimately prevail with a probability exponentially small in n.

Corollary 3.2. *Assume that* $0 \leq x \leq \frac{n}{2}$. *then*

$$\mathbb{P}_x[\tau_0 < \tau_n] = \mathbb{P}_{n-x}[\tau_n < \tau_0] \geq 1 - xe^{-(V(\frac{n}{2}) - V(x))}. \tag{7}$$

In particular, if $\frac{x}{n} \leq \alpha < \frac{1}{2}$, *it holds that*

$$\mathbb{P}_x[\tau_0 < \tau_n] \geq 1 - \frac{n}{2}e^{-c_\alpha n}, \tag{8}$$

where $c_\alpha > 0$ *depends on* α *but not on* n.

Proof. Suppose $X_0 = x$. Since it is necessary to pass thru $\frac{n}{2}$ in order to hit n, we have that $\forall \omega \in \Omega$, $\tau_0(\omega) < \tau_{\frac{n}{2}(\omega)} \Rightarrow \tau_0(\omega) < \tau_n(\omega)$ and therefore $\{\tau_0 < \tau_{\frac{n}{2}}\} \subseteq \{\tau_0 < \tau_n\}$, which implies $\mathbb{P}_x[\tau_0 < \tau_n] \geq \mathbb{P}_x[\tau_0 < \tau_{\frac{n}{2}}]$. We will bound the latter probability. Since, as we can see in figure 1, V is monotonous on $\{0, \ldots, \frac{n}{2} - 1\}$,

$$\sum_{y=0}^{x-1} e^{V(y)} \leq xe^{V(x-1)} \leq xe^{V(x)}$$

and

$$e^{V(\frac{n}{2})} = e^{V(\frac{n}{2}-1)} \leq \sum_{y=0}^{\frac{n}{2}-1} e^{V(y)}$$

Therefore, we have that $\mathbb{P}_x[\tau_{\frac{n}{2}} < \tau_0] = \frac{\sum_{y=0}^{x-1} e^{V(y)}}{\sum_{y=a}^{\frac{n}{2}-1} e^{V(y)}} \leq \frac{xe^{V(x)}}{e^{V(\frac{n}{2})}}$. Which implies that $\mathbb{P}_x[\tau_0 < \tau_n] \geq \mathbb{P}_x[\tau_0 < \tau_{\frac{n}{2}}] = \mathbb{P}_x[(\tau_{\frac{n}{2}} < \tau_0)^c] \geq 1 - \frac{xe^{v(x)}}{e^{v(n/2)}}$, which proves (7).

To obtain (8), we define $z = \lfloor \frac{(\alpha+\frac{1}{2})}{2} n \rfloor = \lfloor (\frac{1}{4} + \frac{\alpha}{2})n \rfloor$. Let's find a lower bound for $V(\frac{n}{2}) - V(x)$ with the form $c_\alpha n$.

$$V(\frac{n}{2}) - V(x) = \sum_{j=x+1}^{\frac{n}{2}} \log \frac{p_j}{q_j} \geq \sum_{j=x+1}^{z} \log \frac{p_z}{q_z}$$

Since $(\frac{1}{4} - \frac{\alpha}{2})n - \alpha n = (\frac{1}{4} - \frac{\alpha}{2})n$, $z - \alpha n \geq (\frac{1}{4} - \frac{\alpha}{2})n - 1$. Therefore, we have that

$$\begin{aligned} V(\frac{n}{2}) - V(x) &\geq \left(\left(\frac{1}{4} - \frac{\alpha}{2} \right) n - 1 \right) \log \frac{p_z}{q_z} \\ &\geq \left(\left(\frac{1}{4} - \frac{\alpha}{2} \right) n - 1 \right) \log(f(\frac{z}{n})) \\ &\geq \left(\left(\frac{1}{4} - \frac{\alpha}{2} \right) n - 1 \right) \log(f(\frac{\alpha}{2} + \frac{1}{4})) \\ &= nc_\alpha - \log(f(\frac{\alpha}{2} + \frac{1}{4})) \end{aligned}$$

with $\log(f(\frac{\alpha}{2} + \frac{1}{4})) > 0$ since $f(\frac{\alpha}{2} + \frac{1}{4}) > 1$. This is not quite the way we wanted to express the bound but it will give us the desired result.

By (7) we have that

$$\begin{aligned} \mathbb{P}_x[\tau_0 < \tau_n] &\geq 1 - xe^{-(V(\frac{n}{2}) - V(x))} \\ &\geq 1 - xe^{-nc_\alpha - \log(f(\frac{\alpha}{2} + \frac{1}{4}))} \\ &\geq 1 - \frac{n}{2} e^{-nc_\alpha - \log(f(\frac{\alpha}{2} + \frac{1}{4}))} \\ &\geq 1 - \frac{n}{2} e^{-nc_\alpha} e^{-\log(f(\frac{\alpha}{2} + \frac{1}{4}))} \\ &= 1 - \frac{n}{2} e^{-nc_\alpha} (f(\frac{\alpha}{2} + \frac{1}{4})))^{-1} \\ &\geq 1 - \frac{n}{2} e^{-nc_\alpha} \end{aligned}$$

□

Remark: We used the fact that for every $\beta > 0$ and every $n \in \mathbb{N}$ $\frac{\lfloor \beta \rfloor}{n} \leq \frac{\beta}{n}$.

Now we will compute a bound for the expected time required to reach consensus regardless of the state where we start.

Theorem 3.3. *For any $x \in \{1, \ldots, n-1\}$ it holds that $\mathbb{E}_x \tau_{\{0,n\}} \leq \frac{256}{15} n(1 + \log n)$*

Proof. First, denote

$$Y_t = \begin{cases} X_t, & \text{if } X_t \leq \frac{n}{2} \\ n - X_t, & \text{if } X_t > \frac{n}{2} \end{cases}$$

By the fact that $(X_t)_{t\in\mathbb{N}}$ is a Markov chain, $(Y_t)_{t\in\mathbb{N}}$ is a Markov chain with state space $\left\{0,\ldots,\frac{n}{2}\right\}$. Due to the symmetry of $(X_t)_{t\in\mathbb{N}}$, the process $(Y_t)_{t\in\mathbb{N}}$ has the same transition probabilities as X on $\left\{0,\ldots,\frac{n}{2}-1\right\}$.

For the process $(Y_t)_{t\in\mathbb{N}}$, denote by T_m the expected hitting time of 0 starting from m. Let's check that for $0 < m < \frac{n}{2}$ we have that

$$T_m = 1 + p_m T_{m-1} + v_m T_m + q_m T_{m+1}, \tag{9}$$

Given an event $B \in \sigma(\bigcup_{i=0}^{\infty} X_i)$, we already know $P(B \mid X_0 = m)$ defines another probability measure, so we can think of $\mathbb{E}_m[Z]$ as the regular expectation of the random variable Z with this new measure. Then, we have that

$$\begin{aligned} \mathbb{E}_m[\tau_0] &= \mathbb{E}[\tau_0 \mid X_1 = m-1]\mathbb{P}_m(X_1 = m-1) \\ &\quad + \mathbb{E}_m[\tau_0 \mid X_1 = m]P_m(X_1 = m) \\ &\quad + \mathbb{E}_m[\tau_0 \mid X_1 = m+1]P_m(X_1 = m+1) \\ &= (T_{m-1}+1)p_m + (T_m+1)v_m + (T_{m+1}+1)q_m \\ &= 1 + p_m T_{m-1} + v_m T_m + q_m T_{m+1} \end{aligned}$$

In particular, we have

$$T_{\frac{n}{2}} = \frac{1}{2}T_{\frac{n}{2}} + \frac{1}{2}T_{\frac{n}{2}-1} + 1 \tag{10}$$

To prove Lemma 3.3 , we use the Lyapunov's functions method. This method will permit us to estimate $T_{\frac{n}{2}}$ without too heavy calculations.

To explain the idea of this method, consider the function $f : \left\{0,\ldots,\frac{n}{2}\right\} \mapsto \mathbb{R}_+$ defined by $f(0) = 0$ and $f(m) = T_m$ for $m \in \left\{1,\ldots,\frac{n}{2}\right\}$. Then, observe that (9) and (10) imply that for every $m \in \{1,\ldots,\frac{n}{2}\}$

$$\mathbb{E}_m\left[f\left(Y_1\right) - f(m)\right] = \mathbb{E}_m[f(Y_1) - f(X_0)] = -1 \tag{11}$$

Now, instead of trying to calculate f, the idea is to find a Lyapunov function $g : \left\{0,\ldots,\frac{n}{2}\right\} \mapsto \mathbb{R}_+$which behaves similarly to f in the sense that when $m \neq 0$, for some $\varepsilon > 0$

$$\mathbb{E}_m\left(g\left(Y_1\right) - g(m)\right) \leq -\varepsilon \tag{12}$$

After proving this we will proceed the following way.

1. First, we check that

$$\mathbb{E}_m[g(Y_{k+1}) - g(Y_k) \mid \mathcal{F}_k] \leq -\varepsilon \mathbb{1}_{\tau > k} \tag{13}$$

for every $k \in \mathbb{N}$. It is straight forward to see that

$$\mathbb{E}_m[g(Y_{k+1}) - g(Y_k) \mid Y_k = i] = \mathbb{E}_{Y_k=i}[g(Y_{k+1}) - g(Y_k)]\mathbb{P}_m(Y_k = i)$$

Then, if $\omega \in [\tau_0 > k]$, there exists some $i \in \{1, \ldots, n/2\}$ such that $Y_k(\omega) \in \{1, \ldots, n/2\}$ and we have that

$$\begin{aligned}\mathbb{E}_m[g(Y_{k+1}(\omega)) - g(Y_k(\omega)) \mid \mathcal{F}_k] &= \mathbb{E}_m[g(Y_{k+1}(\omega)) - g(Y_k(\omega)) \mid Y_k = i] \\ &\quad ((Y_i)_{i\in\mathbb{N}} \text{ is a Markov chain}) \\ &= \mathbb{E}_{Y_k=i}[g(Y_{k+1}) - g(Y_k)] \\ &= \mathbb{E}_i[g(Y_1) - g(Y_0)] \leq -\varepsilon\end{aligned}$$

2. Second, by taking the expectation at both sides of (13) we get that

$$\mathbb{E}_m[g(Y_{k+1})] - \mathbb{E}_m[g(Y_k)] \leq -\varepsilon \mathbb{P}_m(\tau_0 > k)$$

for every $k \in \mathbb{N}$.

Then, using the telescopic property we obtain

$$0 \leq \mathbb{E}_m[g(Y_{r+1})] \leq \mathbb{E}_m[g(Y_0)] - \varepsilon \sum_{i=0}^{r} \mathbb{P}_m(\tau_0 > i)$$

we get for any $r \in \mathbb{N}$.

3. Finally

$$\begin{aligned}\mathbb{E}_m[\tau_0] &= \lim_{r\to\infty} \sum_{i=0}^{r} \mathbb{P}_m(\tau_0 > i) \leq \varepsilon \mathbb{E}_m[g(Y_0)] = \varepsilon g(m) \\ &\leq g\left(\frac{n}{2}\right) = \Delta_1 + \cdots + \Delta_{\frac{n}{2}} \\ &\leq n + \sum_{m=1}^{\frac{n}{4}-1} \frac{n}{m} + \sum_{m=\frac{n}{4}}^{\frac{n}{2}-\lceil\sqrt{n}\rceil-1} \frac{n}{\frac{n}{2}-m} + \sum_{m=\frac{n}{2}-\lceil\sqrt{n}\rceil}^{\frac{n}{2}} \left(\frac{n}{2} - m\right) \\ &\leq n + n(\log(\frac{n}{4} - 1) + 1) + n(\log(\frac{n}{4}) - \log(\sqrt{n}) + \frac{n}{2} \\ &- (\frac{n}{2} - \lceil\sqrt{n}\rceil)^2 - \frac{(\frac{n}{2} - \sqrt{n})(\frac{n}{2} + 1)}{2} \\ &\leq n + n\log(\frac{n}{4}) + n + n\log(\frac{n}{4}) - \log(\sqrt{n}n + \frac{n}{2}\sqrt{n} \\ &- \frac{3}{2}(\frac{n}{2} - \sqrt{n})^2 - \frac{n}{4} + \frac{\sqrt{n}}{2} \\ &\leq 2n(1 + \log(n)) - \log(\sqrt{n})n + \frac{n}{2}\sqrt{n} - \frac{3}{8}n^2 \\ &+ \frac{3}{2}n\sqrt{n} - \frac{3}{2}n - \frac{n}{4} + \frac{\sqrt{n}}{2} \\ &2n(1 + \log(n)) - \log(\sqrt{n})n + 2n\sqrt{n} - \frac{3}{8}n^2 - \frac{7}{4}n + \frac{\sqrt{n}}{2} \\ &\leq 2n(1 + \log n)\end{aligned}$$

Remark: $1+\sum_{i=2}^{n}\frac{1}{i}\leq\int_{0}^{n}\frac{dx}{x}=\log(n)$.
Now, let's find the epsilon.
For $m=\frac{n}{2}$,

$$\mathbb{E}_{\frac{n}{2}}\left(g\left(Y_1\right)-g\left(\frac{n}{2}\right)\right)=-\frac{1}{2}\Delta_{\frac{n}{2}}\leq-\frac{1}{2}.$$

For $m<\frac{n}{2}$

$$\begin{aligned}\mathbb{E}_m\left(g\left(Y_1\right)-g(m)\right)&=p_m g(m-1)+v_m g(m)+q_m g(m+1)-g(m)\\&=p_m(g(m-1)-g(m))+q_m(g(m+1)-g(m))\\&=-p_m\Delta_m+q_m\Delta_{m+1}\end{aligned}$$

Note also that, since $p_m\geq q_m$, for the sake of upper bounds we can always drop the "+2" (as well as "+2- δ_n") part from the calculations. For $m<\frac{n}{4}$ (equivalently, $\frac{m}{n}<\frac{1}{4}$), we have

$$\begin{aligned}-p_m\Delta_m+q_m\Delta_{m+1}&\leq-\frac{m}{n}\left(1-\frac{m}{n}\right)\left(\frac{n}{m}\left(\left(1-\frac{m}{n}\right)^2+3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)\right.\\&\quad\left.-\frac{n}{m+1}\left(\left(\frac{m}{n}\right)^2+3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)\right)\\&\leq-\left(1-\frac{m}{n}\right)\left(\left(1-\frac{m}{n}\right)^2-\left(\frac{m}{n}\right)^2\right)\\&=-\left(1-\frac{m}{n}\right)\left(1-2\frac{m}{n}\right)\\&\leq-\frac{3}{8}\end{aligned}$$

Then, for $\frac{n}{4}\leq m<\frac{n}{2}-\lceil\sqrt{n}\rceil$ we can write

$$\begin{aligned}&-p_m\Delta_m+q_m\Delta_{m+1}\\&\leq-\frac{m}{n}\left(1-\frac{m}{n}\right)\left(\frac{n}{\frac{n}{2}-m}\left(\left(1-\frac{m}{n}\right)^2+3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)\right.\\&\left.-\frac{n}{\frac{n}{2}-m-1}\left(\left(\frac{m}{n}\right)^2+3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)\right)\\&=-\frac{m}{n}\left(1-\frac{m}{n}\right)\left(\frac{n}{\frac{n}{2}-m}\left(1-\frac{m}{n}\right)^2-\frac{n}{\frac{n}{2}-m}\left(\frac{m}{n}\right)^2+\frac{n}{\frac{n}{2}-m}\left(\frac{m}{n}\right)^2\right.\\&\left.-\frac{n}{\frac{n}{2}-m-1}\left(\frac{m}{n}\right)^2-3\frac{m}{n}\left(1-\frac{m}{n}\right)\frac{n}{\left(\frac{n}{2}-m\right)\left(\frac{n}{2}-m-1\right)}\right)\\&=-\frac{m}{n}\left(1-\frac{m}{n}\right)\left(2-\left(\left(\frac{m}{n}\right)^2+3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)\frac{n}{\left(\frac{n}{2}-m\right)\left(\frac{n}{2}-m-1\right)}\right)\end{aligned}$$

(note that $h(1-h)\in\left[\frac{3}{16},\frac{1}{4}\right]$ for $h\in\left[\frac{1}{4},\frac{1}{2}\right]$ and that the last fraction is ≤ 1)

$$\leq-\frac{3}{16}$$

Finally, for $\frac{n}{2} - \lceil\sqrt{n}\rceil \leq m < \frac{n}{2}$ we have

$$\begin{aligned}
&- p_m\Delta_m + q_m\Delta_{m+1} \\
&\leq -\frac{m}{n}\left(1-\frac{m}{n}\right)\left(\left(\frac{n}{2}-m\right)\left(\left(1-\frac{m}{n}\right)^2 + 3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)\right. \\
&\left. - \left(\frac{n}{2}-m-1\right)\left(\left(\frac{m}{n}\right)^2 + 3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)\right) \\
&= -\frac{m}{n}\left(1-\frac{m}{n}\right)\left(\left(\frac{n}{2}-m\right)\left(1-2\frac{m}{n}\right) + \left(\frac{m}{n}\right)^2 + 3\frac{m}{n}\left(1-\frac{m}{n}\right)\right)
\end{aligned}$$

(again use that $h(1-h) \in \left[\frac{3}{16}, \frac{1}{4}\right]$ for $h \in \left[\frac{1}{4}, \frac{1}{2}\right]$ and that the first term in the parentheses is nonnegative)

$$\leq -\frac{15}{128}$$

Gathering the pieces, we find that (12) holds with $\varepsilon = \frac{15}{128}$. □

It was also proved in [4] that $n(1 + log(n))$ is actually the correct order of $\mathbb{E}_x[\tau_{\{0,n\}}]$.

The last result of this section will gives us a good bound to the probability of requiring a longer time than expected to reach consensus.

Corollary 3.4. *For any x and any positive integer k it holds that*

$$\mathbb{P}_x\left[\tau_{\{0,n\}} > k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right] \leq 2^{-k}.$$

Proof. Using Markov inequality we have that

$$\begin{aligned}
\mathbb{P}_x\left[\tau_{\{0,n\}} > \left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right] &\leq \mathbb{P}_x\left[\tau_{\{0,n\}} > 2\left\lceil\mathbb{E}_x[\tau_{0,n}]n(1+\log n)\right\rceil\right] \\
&\leq \mathbb{P}_x\left[\frac{\tau_{\{0,n\}}}{\mathbb{E}_x[\tau_{\{0,n\}}}] \geq 2\right] \\
&\leq \frac{1}{2}
\end{aligned}$$

Let's check the desired result inductively. The basis is the previous inequality so we go directly to the induction.

Let $n \in \mathbb{N}$. We suppose that $\mathbb{P}_x\left[\tau_{\{0,n\}} > k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right] \leq 2^{-k}$ holds.

Using the theorem of total probability we have that

$$\begin{aligned}
&\mathbb{P}_x\left[\tau_{\{0,n\}} > (k+1)\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right] \\
=&\mathbb{P}_x\left[\tau_{\{0,n\}} > (k+1)\left\lceil\frac{512}{15}n(1+\log n)\right\rceil \middle| \tau_{\{0,n\}} > k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right] \\
*&\mathbb{P}_x\left[\tau_{\{0,n\}} > k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right]
\end{aligned}$$

Since $(X_n)_{n\in\mathbb{N}}$ is a Markov chain, and

$$\left[\tau_{\{0,n\}} > k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right] = \bigcap_{i=0}^{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil}[X_i \notin \{0,n\}]$$
$$= [X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} \notin \{0,n\}]$$

We obtain

$$\begin{aligned}
&\mathbb{P}_x\left[\tau_{\{0,n\}} > (k+1)\left\lceil\frac{512}{15}n(1+\log n)\right\rceil \Big| \tau\{0,n\} > k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right]\\
=&\mathbb{P}_x\left[\tau_{\{0,n\}} > (k+1)\left\lceil\frac{512}{15}n(1+\log n)\right\rceil \Big| [X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} \notin \{0,n\}]\right]\\
=&\sum_{m=1}^{n-1}\mathbb{P}_x\left[\tau_{\{0,n\}} > (k+1)\left\lceil\frac{512}{15}n(1+\log n)\right\rceil \Big| X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} = m\right]\\
&*\mathbb{P}_x\left[X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} = m \Big| [X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} \notin \{0,n\}]\right]\\
=&\sum_{m=1}^{n-1}\mathbb{P}_m\left[\tau_{\{0,n\}} > \left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right]\\
&*\mathbb{P}_x\left[X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} = m \Big| [X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} \notin \{0,n\}]\right]\\
\leq&\frac{1}{2}\sum_{m=1}^{n-1}\mathbb{P}_x\left[X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} = m \Big| [X_{k\left\lceil\frac{512}{15}n(1+\log n)\right\rceil} \notin \{0,n\}]\right]\\
=&\frac{1}{2}
\end{aligned}$$

Thus,

$$\mathbb{P}_x\left[\tau_{\{0,n\}} > (k+1)\left\lceil\frac{512}{15}n(1+\log n)\right\rceil\right] \leq 2^{-k-1}.$$

□

To conclude this section, we summarize the obtained results until now.

- Theorem (3.3) and Corollary (3.4) give us a good idea of the time we can expect the system will take to find consensus. Only computing a bound for the expectation would not be enough since the random variable may differ a lot from its mean.
- Another remark from Theorem (3.3), is that, since a particular node is selected roughly every n rounds, and we know that $\frac{\mathbb{E}_x\tau_{\{0,n\}}}{n} = O(\frac{256}{15}(1+\log n))$, a node will, on average, change its state a logarithmic number of times.
- Based on Corollary (3.2), we know that when the overall opinions are already skewed towards one side, the system will likely achieve consensus on that dominant opinion.

4 Enter Byzantine nodes

We saw in the last section that getting a roughly accurate prediction of the time that it takes to reach a consensus was actually possible when all the nodes are honest regardless of the initial state of the system. However, this is no longer possible when not all the nodes are honest, that is when they do not follow the protocol properly. We will call these nodes *Byzantine nodes*. We will also assume here that all the Byzantine nodes are controlled by a central authority which we will also suppose to be omniscient, that is, it would always be able to know the level of consensus among the honest nodes. This assumption is clearly exaggerated but in any case, it is always better to work with the worst case.

4.1 Behaviour in a potential landscape

As it was mentioned in the objectives of this article, from this section on there will be no more formal proofs except for a few exceptions. In general we will give either an explanation of the intuition behind the statements we make or give an outline of the proof. The next statement are four claims that will be useful during the the following sections. For a better understanding of it we refer the reader to [5, 4]

Claim 4.1. *The random walk on top of a potential roughly behaves in the following way:*

(i) it "prefers" to go downhill;

(ii) the probability that it goes in an "improbable direction" is roughly[4] *the exponential of minus the difference of "heights to overcome" (for example, on Figure 3,* $\mathbb{P}_x\left[\tau_{a'} < \tau_{b'}\right] \approx e^{-\left(h-h'\right)}\Big)$*;*

(iii) its stationary distribution at x *is roughly proportional to* $e^{-\hat{V}(x)}$*; so, in the long run, the process will stay for the overwhelming amount of time at the bottom(s) (global minima) of the potential;*

(iv) The time to go out of a potential well of depth h' *(such as the one where the walker currently is in Figure 3) is roughly an Exponential random variable with the expected value* $\approx e^{h'}$*.*

Claim (i) is evident since being in a slope at some state, say m, means that the left and right neighbor's proportion between $\tilde{q}_i$ and $\tilde{p}_i$ are both ≥ 1 or both ≤ 1, and this, in turn, implies that also m has the same proportion, which translates into having a greater probability of going downhill.

To justify claim (ii) we recall lemma (3.1) and remark the fact that we did not use the values of the transition probabilities but rather relayed on the fact that it was a nearest neighbor random walk, so this lemma can be applied to any random walk with the same characteristics. What is done next is the

[4] By roughly we mean up to factors of smaller order.

usual heuristics "the sum of the exponentials is usually roughly the order of its maximal term".

Image 3 explains what (iv) means. Claims (iii) and (iv) are very complicated to explain in detail, so we will just ask the reader to take a vote of confidence. They are exposed here in order to explain two natural intuitions of potential wells. Claim (iii) tells us that the system will prefer in the long term the metastable[5] states, and clam (iv) tells us getting out of a potential well can take a really long time, so if they are not consensus states they are something we should worry about.

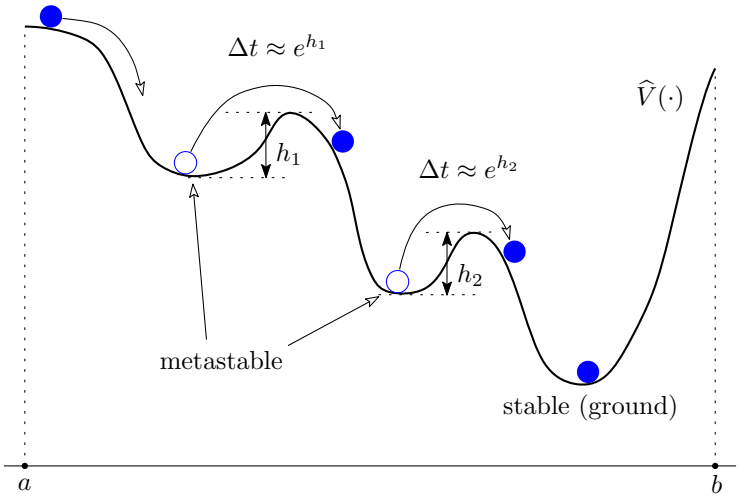

Figure 3: The time required for a walker to get out of a potential well is roughly e^h, where h is the height of the well. Image taken from [4]

4.2 New potential landscapes

Let's focus now on how the voters model described in the previous section behaves under the presence of Byzantine nodes. Here we are assuming that n is large so the potential landscape gets very similar to its continuous version, something like in Figure 3. Also, since n is large, we refer to the elements of $\{0, \dots, n\}$ by an for some $a \in [0, 1]$. Let $q \in (0, \frac{1}{2})$, we will suppose that we have qn Byzantine nodes and therefore $(1-q)n$ honest nodes.

Although the are many strategies the adversary can use, we will suppose for now that he uses *help the weakest*. The goal of this strategy is to prevent consensus itself, it does so by voting for the weakest opinion every time a Byzantine node is selected to give his opinion.

Let's use the notation $\widetilde{X}_k$ to represent the count of nodes with honest opinions at time k. Byzantine nodes, which lack genuine opinions, do not affect the

[5]Roughly speaking, a state where the system spends a long time but leaves eventually

system's state if they are selected. Assuming that $X_k = m$, we can examine two scenarios.

Case 1: $m \leq \frac{(1-q)n}{2}$. In this case, any Byzantine node, if queried, will vote for 1 . So, the number of 1-opinions among three independently chosen nodes will have the Binomial $\left(3, \frac{m}{n} + q\right)$ distribution. Then, if one of the m honest opinion-1 nodes was selected (which happens with probability $\frac{m}{n}$), it will switch its opinion to 0 with probability $\left(1 - \frac{m}{n} - q\right)^3 + 3\left(1 - \frac{m}{n} - q\right)^2 \left(\frac{m}{n} + q\right)$; likewise, if an honest node with current opinion 0 was selected (which happens with probability $1 - q - \frac{m}{n}\big)$, it will switch its opinion to 1 with probability $\left(\frac{m}{n} + q\right)^3 + 3\left(1 - \frac{m}{n} - q\right)\left(\frac{m}{n} + q\right)^2$

Case 2: $m > \frac{(1-q)n}{2}$. In this case, a Byzantine node, if queried, will vote for 0 , and therefore the number of 1-opinions among three independently chosen nodes has the Binomial $\left(3, \frac{m}{n}\right)$ distribution. Then, as before, if one of the m honest opinion-1 nodes was selected, it will switch its opinion to 0 with probability $\left(1 - \frac{m}{n}\right)^3 + 3\left(1 - \frac{m}{n}\right)^2 \left(\frac{m}{n}\right)$; if an honest node with current opinion 0 was selected, it will switch its opinion to 1 with probability $\left(\frac{m}{n}\right)^3 + 3\left(1 - \frac{m}{n}\right)\left(\frac{m}{n}\right)^2$.

Note, in particular, that 0 and $(1-q)n$ are not absorbing states anymore - because even if all the honest nodes agree, there is a chance that the selected honest node will choose at least two Byzantine ones for opinions and those will convince it to switch.

It is important to note that the states 0 and $(1-q)n$ are no longer absorbing states. This is because even if all the honest nodes reach a consensus, there is still a possibility that a selected honest node might choose at least two Byzantine nodes, making it switch its opinion.

That is, we find that the process $(\tilde{X}_k)_{k\in\mathbb{N}}$ is a (one-dimensional) random walk on $\{0, \ldots, (1-q)n\}$, and on $\widetilde{X}_k = m$ we have

$$\tilde{X}_{k+1} = \begin{cases} m-1, & \text{with probability } \tilde{p}_m, \\ m+1, & \text{with probability } \tilde{q}_m, \\ m, & \text{with probability } \tilde{v}_m = 1 - \tilde{p}_m - \tilde{q}_m, \end{cases}$$

where

$$\tilde{p}_m = \begin{cases} \frac{m}{n}\left(\left(1 - \frac{m}{n} - q\right)^3 + 3\left(\frac{m}{n} + q\right)\left(1 - \frac{m}{n} - q\right)^2\right), & \text{if } m \leq \frac{(1-q)n}{2}, \\ \frac{m}{n}\left(\left(1 - \frac{m}{n}\right)^3 + 3\frac{m}{n}\left(1 - \frac{m}{n}\right)^2\right), & \text{if } m > \frac{(1-q)n}{2}, \end{cases}$$

$$\tilde{q}_m = \begin{cases} \left(1 - \frac{m}{n} - q\right)\left(\left(\frac{m}{n} + q\right)^3 + 3\left(\frac{m}{n} + q\right)^2\left(1 - \frac{m}{n} - q\right)\right), & \text{if } m \leq \frac{(1-q)n}{2}, \\ \left(1 - \frac{m}{n} - q\right)\left(\left(\frac{m}{n}\right)^3 + 3\left(\frac{m}{n}\right)^2\left(1 - \frac{m}{n}\right)\right), & \text{if } m > \frac{(1-q)n}{2}. \end{cases}$$

We define the potential $\widehat{V}$ as in equation (4), replacing p's and q's with $\tilde{p}$'s and $\tilde{q}$'s. By analyzing the transition probabilities mentioned above, we can observe that $\widehat{V}$ has a similar pattern as depicted in Figure 5. In order to see this, we want to identify the values of $m \leq \frac{(1-q)n}{2}$ for which the drift $\tilde{q}_m - \tilde{p}_m$ becomes zero. This corresponds to the flat points of $\widetilde{V}$, typically its maximums

and minimums. To simplify the analysis, let's use the abbreviation $\alpha = \frac{m}{n}$ and solve the equation (in α)

$$\begin{aligned}&\alpha\left((1-\alpha-q)^3+3(\alpha+q)(1-\alpha-q)^2\right)\\&=(1-\alpha-q)\left((\alpha+q)^3+3(\alpha+q)^2(1-\alpha-q)\right).\end{aligned}$$

Note that one can divide both sides by $(1-\alpha-q)$ and then cancel the α^3 terms. The two real roots that we are interested in are

$$\begin{aligned}\alpha_0(q)&=\frac{1}{4}\left(1-\sqrt{1-\frac{8q}{1-q}}\right)-q,\\\alpha_1(q)&=\frac{1}{4}\left(1+\sqrt{1-\frac{8q}{1-q}}\right)-q,\end{aligned}$$

which only exist for $q\in\left(0,\frac{1}{9}\right]$. By looking at figure 4 we can see that

$$\alpha_0(q)\asymp{}^6q^2 \text{ as } q\to 0. \tag{14}$$

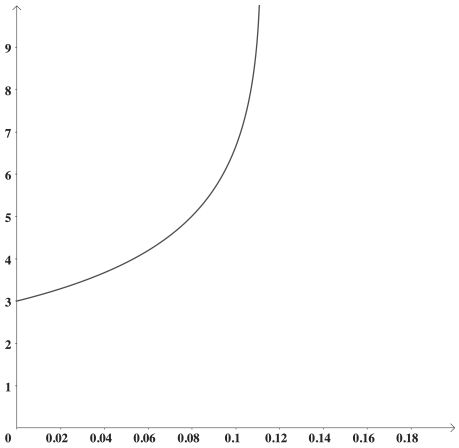

Figure 4: $\lim_{q\to 0}\frac{\alpha_0(q)}{q^2}=3$.

Define also the "symmetric" points $\alpha_0^*(q)=1-q-\alpha_0(q)$ and $\alpha_1^*(q)=1-q-\alpha_1(q)$. To be able to distinguish between the situations in the top left and top right pictures in Figure 5, it is then important to be able to compare the values of $\widehat{V}\left(\alpha_0 n(q)\right)$ and $\widehat{V}\left(\frac{(1-q)n}{2}\right)$; we will compute then the sign of the sum $\widehat{V}\left(\frac{(1-q)n}{2}\right)-\widehat{V}\left(\alpha_0 n(q)\right)=\sum_{m=n\alpha_0(q)}^{(1-q)n/2}\log\frac{\hat{p}_m}{\hat{q}_m}$. Since

$$\sum_{\alpha_0(q)n}^{\frac{(1-q)n}{2}}\log\frac{\hat{p}_m}{\hat{q}_m}\approx\int_{\alpha_0(q)n}^{\frac{(1-q)n}{2}}\log\frac{\frac{x}{n}\left(\left(1-\frac{x}{n}-q\right)^3+3\left(\frac{x}{n}+q\right)\left(1-\frac{x}{n}-q\right)^2\right)}{\left(1-\frac{x}{n}-q\right)\left(\left(\frac{x}{n}+q\right)^3+3\left(\frac{x}{n}+q\right)^2\left(1-\frac{x}{n}-q\right)\right)}dx$$

[6] This means that $\lim_{q\to 0}\frac{\alpha_0}{q^2}\in(0,\infty)$.

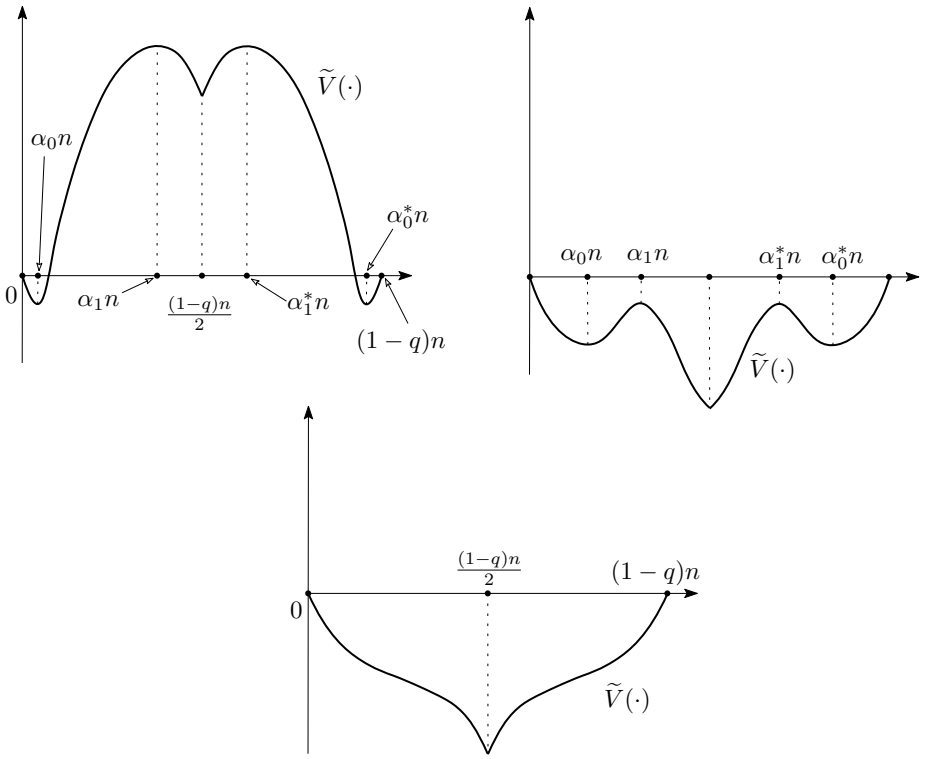

Figure 5: The potential profile for the majority dynamics with Byzantine nodes: with $q < 0.09029$ (top left), $0.09029 < q < \frac{1}{9}$ (top right), $q > \frac{1}{9}$ (bottom). Image taken from [4]

By doing a change of variables, we can approximate the sum with the following integral and note that the equation (in q)

$$\int_{\alpha_0(q)}^{\frac{1-q}{2}} \log \frac{s\left((1-s-q)^2+3(s+q)(1-s-q)\right)}{(s+q)^3+3(s+q)^2(1-s-q)} ds = 0$$

has the solution $q^* \approx 0.09029$ (obtained numerically). As a result, we can expect the phase transition between the top left and top right images in Figure 5 to occur approximately at q^*.

The key difference with the non-Byzantine case is that now in this $\widetilde{V}$-picture there are possibly three potential wells. This could be a problem since getting out of a potential well may take a lot of time. Let's analyze Figure (5).

- When $q < q^*$, the system exhibits three locally attractive states: two pre-consensus states and one "balanced" state, where opinions are evenly divided. However, the pre-consensus states have a stronger influence. Over time, the system tends to favor and remain in these pre-consensus states due to the property stated in Claim 4.1 (*iii*).

- When $q^* < q < \frac{1}{9}$, the three states mentioned earlier still exist. However, the balanced state becomes the ground[7] state.
- When $q \geq \frac{1}{9}$, there are no pre-consensus states in the system. In this scenario, the system transitions directly to the "balanced" ground state from any initial state, without the presence of intermediate pre-consensus states.

Let's now analyze the case where $q < q^*$, which is comparatively easier due to the reduced number of Byzantine nodes. According to Theorem (3.1) applied to the current scenario, if the process starts sufficiently far from the interval $[\alpha_1(q)n, \alpha_1^*(q)n]$ (representing the central potential well), the system will converge to the corresponding pre-consensus state with an exponentially high probability. An important practical observation is that, when in a pre-consensus state, the honest nodes have the ability to determine the preferred state of the system. For example, they can average the last N received responses, resulting in a significant majority choosing the same preferred state with a very high probability. This outcome can be viewed as a positive result, demonstrating that practical consensus can be achieved even in the presence of Byzantine nodes, provided the initial opinion configuration is sufficiently far from the "balanced" state. However, it is worth noting that the presence of the central potential well introduces some significant practical challenges, as we will explore further.

Now, let's consider the question: What happens if we increase the communication complexity by requesting opinions from more than three nodes. In other words, what happens if $k > 3$? What advantages does this increase offer? For simplicity, let's assume that k is an odd number to avoid the possibility of draws. The following lemma provides insight into this matter, stating that although the central potential well decreases in size, it never completely disappears.

We will now show that the size of the central potential well does not tend to zero.

Lemma 4.2. *The size of the central potential well is always at least of size qn.*

Proof. Notice that if the state of the system is close to $\frac{(1-2q)}{2}n$, this is, the state where there is exactly the same amount of opinion-0 and Byzantine nodes + 1-opinion honest nodes, then (since the Byzantine nodes would vote for 1) a chosen peer would vote for 0 or 1 roughly with equal probabilities; however, since the probability of selecting an honest node with opinion 1 is significantly less than the probability of selecting an honest node with opinion 0 , the process will have a drift to the right (meaning that it is inside the central potential well). For completeness, observe also that for a fixed $a < \frac{(1-2q)}{2}$ one can find a large enough k such that an is out of the central well. Indeed, the probability that a randomly chosen node would vote for 1 would then be *honest opinion*-1 *nodes + Bizantine nodes* $= a + q < \frac{(1-2q)}{2} + q = \frac{1}{2}$, and then it is clear that the

[7]That is, stronger in the sense that the system will prefer to stay there in the long term. This is justified by Claim 4.1 (*iii*).

probability that a Binomial$(k, a+q)$ random variable does not exceed $\frac{k-1}{2}$ can be made as small as we want by the choice of k. This shows that, as we grow k, the central potential well "shrinks towards" $\left[\frac{(1-2q)}{2}n, \frac{n}{2}\right]$, but that interval (of length qn) is always a part of it. □

To finalize this subsection on a not-so-optimistic note, observe that we have analyzed only one adversarial strategy: the "help-the-weakest". This point also explains why analyzing the system via simulations is not a straightforward task - these need to be performed for any adversarial strategy, and there are infinitely many of them. It is also necessary to mention that, in principle, with more complicated adversarial strategies or node's finalizations rules the process may not even be a Markov chain which would make its analysis much more difficult.

Concluding this subsection on a less optimistic tone, it is important to note that we have only examined one adversarial strategy: The "help-the-weakest" strategy. This observation highlights the reason why analyzing the system solely through simulations is not a straightforward task. Simulations would need to be conducted for each adversarial strategy, and the number of possible strategies is infinite. Additionally, it should be mentioned that with more complex adversarial strategies or node finalization rules, the process may not even be a Markov chain. This would considerably complicate its analysis.

5 Conclusions

Voters models are probably the most natural candidates for consensus protocols due to their low communication complexity. In section 3 we saw that they behave well when all the nodes are honest. However, in section 4 we saw that when there are Byzantine nodes, there are many limitations in their study, e.g., the simulations will never give us a clear idea of the performance of the protocol since one specific adversary strategy must be established. Regarding the case that we studied, which was the adversarial strategy "help the weakest", the main limitation was the potential well that is created and has a lower bound on its size independently of the communication complexity used by the model.

References

[1] Peter Clifford and Aidan Sudbury. A model for spatial conflict. *Biometrika*, 60(3):581–588, 1973.

[2] Richard A Holley and Thomas M Liggett. Ergodic theorems for weakly interacting infinite systems and the voter model. *The annals of probability*, pages 643–663, 1975.

[3] Jean-François Le Gall. Intégration, probabilités et processus aléatoires. *Ecole Normale Supérieure de Paris*, 2006.

[4] Serguei Popov and Sebastian Müller. Voting-based probabilistic consensuses and their applications in distributed ledgers. *Annals of Telecommunications*, pages 1–23, 2022.

[5] Yakov Grigor'evich Sinai. The limit behavior of a one-dimensional random walk in a random environment. *Teor. Veroyatnost. i Primenen*, 27(2):247–258, 1982.