



**HAL**  
open science

# Optimal Proportion Computation with Population Protocols

Yves Mocquard, Emmanuelle Anceaume, Bruno Sericola

► **To cite this version:**

Yves Mocquard, Emmanuelle Anceaume, Bruno Sericola. Optimal Proportion Computation with Population Protocols. [Technical Report] IRISA, 263 avenue Général Leclerc, 35000 Rennes. 2016. hal-01354352v1

**HAL Id: hal-01354352**

**<https://hal.science/hal-01354352v1>**

Submitted on 18 Aug 2016 (v1), last revised 19 Aug 2016 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Optimal Proportion Computation with Population Protocols

Yves Mocquard<sup>1\*</sup>      Emmanuelle Anceaume<sup>2</sup>  
   Bruno Sericola<sup>3</sup>  
   <sup>1</sup> yves.mocquard@irisa.fr  
   IRISA / Université de Rennes 1 (France)  
   <sup>2</sup> emmanuelle.anceaume@irisa.fr  
   CNRS / Irisa (France)  
   <sup>3</sup> bruno.sericola@inria.fr  
   INRIA Rennes - Bretagne Atlantique (France)

## Abstract

The computational model of population protocols is a formalism that allows the analysis of properties emerging from simple and pairwise interactions among a very large number of anonymous finite-state agents. Significant work has been done so far to determine which problems are solvable in this model and at which cost in terms of states used by the protocols and time needed to converge. The problem tackled in this paper is the *population proportion* problem: each agent starts independently from each other in one of two states, say  $A$  or  $B$ , and the objective is for each agent to determine the proportion of agents that initially started in state  $A$ , assuming that each agent only uses a finite set of state, and does not know the number  $n$  of agents. We propose a solution which guarantees with any high probability that after  $O(\log n)$  interactions any agent outputs with a precision given in advance, the proportion of agents that start in state  $A$ . The population proportion problem is a generalization of both the majority and counting problems, and thus our solution solves both problems. We show that our solution is optimal in time and space. Simulation results illustrate our theoretical analysis.

**Keywords** Population protocols; Proportion; Majority; Optimal ; Counting; Probability; Performance evaluation.

---

\*This work was partially funded by the French ANR project SocioPlug (ANR-13-INFR-0003), and by the DeScEaNt project granted by the Labex CominLabs excellence laboratory (ANR-10-LABX-07-01)

# 1 Introduction

In 2004, Angluin et al. [2, 3] have proposed a model that allows us to analyze the emergence of global properties based on pairwise interactions. This model, named the population protocol model, provides minimalist assumptions on the computational power of the agents: agents are finite-state automata, identically programmed, they have no identity, they do not know how numerous they are, and they progress in their computation through random pairwise interactions. Their objective is to ultimately converge to a state from which the sought property can be derived from any agent [7]. A considerable amount of work has been done to determine which properties can emerge from pairwise interactions between finite-state agents, together with the derivation of lower bounds on the time and space needed to reach such properties [1, 5, 11, 13, 16]. Among them, is majority. Briefly, each agent starts independently from each other in one of two states, say  $A$  and  $B$ , and the objective for each agent is to eventually output *yes* if a majority of agents started their execution in state  $A$  and *no* otherwise. Section 4 provides an overview of the results recently obtained for the majority task.

In this paper, we focus on a related and more general question. Namely, instead of having each agent answered *yes* if a majority of agents initially started their execution in state  $A$ , one may ask whether it is feasible for each agent to compute *quickly* and with *high precision* the *proportion of agents* that initially started in state  $A$ ? Answering such a question is very important in the context, for example, of animal infectious-disease surveillance, where different kinds of alerts are triggered according to the infected population proportion (*e.g.*, Alert 1 is triggered if less than 0.05% of the population is infected, level 2 if this proportion lies in [0.05%, 3.0%], Alert 3 if it lies in [3.1%, 10%], and so on ...).

We answer by the affirmative to this question, and we propose a population protocol that allows each agent to converge to a state from which, when queried, provides the proportion of agents that are in a given state. Specifically, each agent is a  $(2m + 1)$ -finite state machine,  $m \geq 1$ , where  $m$  is the initial value associated to state  $A$  and  $-m$  is the one associated to state  $B$ . Each agent starts its execution with  $m$  or  $-m$ , and each pair of agents that meet, adopt the average of their values (or as close as they can get when values are restricted to integers, as will be clarified in Section 5). This method preserves the sum of the initial values, and after  $O(\log n)$  pairwise interactions, each agent converges with high probability to a state from which it derives the proportion of agents that started in a given state, and the precision  $\varepsilon$  of the result is in  $O(1/m)$ . Specifically, our protocol guarantees that each agent is capable of computing the proportion of agents that initially started in a specific state by using  $(3/2\varepsilon) + 1$  states, with  $\varepsilon \in (0, 1)$ . This is achieved in no more than  $(-2 \ln \varepsilon + 7.47 \ln n - 13.29 \ln \delta - 3.16)$  interactions with probability  $1 - \delta$ , for any  $\delta \in (0, 1)$ .

Note that our present work improves upon a previous one [15] in which the counting problem was tackled. The counting problem generalizes the majority problem by requiring, for each agent, to converge to a state in which each agent is capable of computing  $n_A$  or  $n_B$ , where  $n_A$  and  $n_B$  represent respectively the number of agents that started in state  $A$  and  $B$ . The originality of that work was a proof of convergence based on tracking the Euclidean distance between the random vector of all agents' values and the limiting distribution. By assuming that  $n$  is known, the algorithm converges to the exact value of  $n_A$  and  $n_B$  in  $O(\log n)$  interactions per agent, but requires  $O(n^{3/2}/\delta^{1/2})$  states [15].

Now, by relying on the proofs presented in the present paper, and by slightly modifying the output function, assuming that  $n$  is known, we show in Section 7, that we solve the counting problem with  $O(\log n)$  interactions and  $O(n)$  states per agent. We also show that any protocol solving the counting problem requires  $\Omega(\log n)$  parallel interactions to converge and  $\Omega(n)$  states. This makes our present algorithm an optimal solution both in space and time to solve both the counting problem and the proportion one.

The remainder of this paper is organized as follows. Section 2 presents the population protocol model. Section 3 specifies the problem addressed in this work. Section 4 provides an overview of the most recent average-based population protocols. The protocol to compute the proportion population is presented in Section 5. Analysis of the protocol is proposed in Section 6. We show in Section 7, that our protocol is

optimal both in space and time. We have simulated our protocol to illustrate our theoretical analysis. Finally, Section 8 concludes.

## 2 Population protocols model

In this section, we present the population protocol model, introduced by Angluin et al. [3]. This model describes the behavior of a collection of agents that interact pairwise. The following definition is from Angluin et al [6]. A population protocol is characterized by a 6-tuple  $(Q, \Sigma, Y, \iota, \omega, f)$ , over a complete interaction graph linking the set of  $n$  agents, where  $Q$  is a finite set of states,  $\Sigma$  is a finite set of input symbols,  $Y$  is a finite set of output symbols,  $\iota : \Sigma \rightarrow Q$  is the input function that determines the initial state of an agent,  $\omega : Q \rightarrow Y$  is the output function that determines the output symbol of an agent, and  $f : Q \times Q \rightarrow Q \times Q$  is the transition function that describes how two agents interact and update their states. Initially all the agents start with a initial symbol from  $\Sigma$ , and upon interactions with agents update their state according to the transition function  $f$ . Interactions between agents are orchestrated by a random scheduler: at each discrete time, any two agents are randomly chosen to interact with a given distribution. Note that it is assumed that the random scheduler is fair, which means that the interactions distribution is such that any possible interaction cannot be avoided forever. The notion of time in population protocols refers to as the successive steps at which interactions occur, while the parallel time refers to as the successive number of steps each agent executes [7]. Agents do not maintain nor use identifiers (agents are anonymous and cannot determine whether any two interactions have occurred with the same agents or not). However, for ease of presentation the agents are numbered  $1, 2, \dots, n$ . We denote by  $C_t^{(i)}$  the state of agent  $i$  at time  $t$ . The stochastic process  $C = \{C_t, t \geq 0\}$ , where  $C_t = (C_t^{(1)}, \dots, C_t^{(n)})$ , represents the evolution of the population protocol. The state space of  $C$  is thus  $Q^n$  and a state of this process is also called a protocol configuration.

## 3 The Proportion Problem

The problem addressed in this work is the following one. We consider a set of  $n$  agents, interconnected by a complete graph, that start their execution in one of two states of  $\Sigma = \{A, B\}$ . Let  $n_A$  be the number of agents whose initial state is  $A$  and  $n_B$  be the number of agents that start in state  $B$ . Let  $\gamma_A = n_A/n$ , be the quantity referred to as the proportion of the agents that initially started in state  $A$ . The output set  $Y$  is a subset of all possible values of  $\gamma_A$ , that is a subset of  $[0, 1]$ . Similarly, we have  $\gamma_B = n_B/n$  and  $\gamma = (n_A - n_B)/n = \gamma_A - \gamma_B$

A population protocol solves the proportion problem within  $\tau$  steps with probability at least  $1 - \delta$ , for any  $\delta \in (0, 1)$  and with precision  $\varepsilon$ , if for any configuration  $C_t$  reachable by the protocol after  $t \geq \tau$  steps, it holds that with probability at least  $1 - \delta$ ,  $|\omega_A(C_t^{(i)}) - \gamma_A| < \varepsilon$ , for any agent  $i$  (without any knowledge of  $n$ ). As will be shown in the following,  $\gamma_A$  does not depend on time  $t$ , however agents are locally able to compute  $\gamma_A$  after a logarithmic number of interactions.

## 4 Related Work

In 2004, Angluin et al. [2, 3] have formalized the population protocol model, and have shown how to express and compute predicates in this model. Then in [4] the authors have completely characterized the computational power of the model by establishing the equivalence between predicates computable in the population model and those that can be defined in the Presburger arithmetic. Since then, there has been a lot of work on population protocols including the majority problem [1, 5, 11, 13, 16], the leader election problem [8, 14], in presence of faults [10], and on variants of the model [9, 12].

The closest problem to the one we address is the computation of the majority. In this problem, all the agents start in one of two distinguished states and they eventually converge to 1 if  $\gamma > 0$  (*i.e.*,  $n_A > n_B$ ),

and to 0 if  $\gamma < 0$  (*i.e.*,  $n_B > n_A$ ). In [11, 13] the authors propose a four-state protocol that solves the majority problem with an expected convergence parallel time logarithmic in  $n$ . However, the expected convergence time is infinite when  $\gamma$  approaches 0. The authors in [5, 16] propose a three-state protocol that converges with some probability  $\delta$ , and whose parallel time is logarithmic in  $n$  if  $\gamma$  is large enough, *i.e.*  $\gamma = O(\sqrt{n} \log n)$ . Alistarh et al. [1] propose a population protocol based on an average-and-conquer method to exactly solve the majority problem. Their algorithm uses two types of interactions, namely, averaging interactions and conquer ones. The first type of interaction is close to the one used in our protocol while the second one is used to diffuse the result of the computation to the zero state agents. This nice additional mechanism, in which the majority value is propagated to all the agents, makes their proof of convergence intricate. Actually, to show their convergence time, they need to assume a rather large number of intermediate states (*i.e.*,  $2d$  states, with  $d = 1,000$ ). This is essentially due to the fact they need to prove that all the agents with maximum positive values and minimal negative values will have sufficiently enough time to halve their values (*i.e.*,  $432n \log m \log n$  rounds with high probability) and then for all the agent whose value has reached  $-1$  (assuming that the initial majority is positive),  $4dn$  more rounds will be necessary to guarantee convergence to the correct value. Note that in practice, their algorithm does not require more than  $n$  state to converge to the majority, however their proof necessitates  $m + 1,000 \log m \log n$  with  $\log n \log m \leq m \leq n$  states, and at least  $432 \log m \log n$  interactions per agent to converge to the majority.

Our protocol bears some resemblance to the average-and-conquer algorithm of Alistarh et al. [1] in the sense that in both protocols interactions consist for the agents to compute the average of their local values to progressively converge to sought states. However, our protocol guarantees that each agent is capable of computing the proportion of agents that initially started in a specific with  $\varepsilon \in (0, 1)$  precision, by using  $(3/2\varepsilon) + 1$  states. This is achieved in no more than  $(-2 \ln \varepsilon + 7.47 \ln n - 13.29 \ln \delta - 3.16)$  interactions with probability  $1 - \delta$ , for any  $\delta \in (0, 1)$ .

## 5 Computing the Proportion

Our protocol uses the average technique to compute the proportion of agents that started their execution in a given state  $A$ . This section describes the rules applied during the interactions, and then prove the correctness and quality of our solution. Parameters  $Q, \Sigma, Y, \iota$  and  $\omega$  are application dependent and will be defined at the end of the section for the computation of  $\gamma_A$ . The transition function  $f$  is given by

$$f(a, b) = \begin{cases} \left( \frac{a+b}{2}, \frac{a+b}{2} \right) & \text{if } a + b \text{ is even} \\ \left( \frac{a+b-1}{2}, \frac{a+b+1}{2} \right) & \text{if } a + b \text{ is odd.} \end{cases} \quad (1)$$

Once the couple  $(i, j)$  is chosen at time  $t$ , the process reaches state  $C_{t+1}$ , at time  $t + 1$ , given by

$$\left( C_{t+1}^{(i)}, C_{t+1}^{(j)} \right) = \begin{cases} \left( \frac{C_t^{(i)} + C_t^{(j)}}{2}, \frac{C_t^{(i)} + C_t^{(j)}}{2} \right) & \text{if } C_t^{(i)} + C_t^{(j)} \text{ is even} \\ \left( \frac{C_t^{(i)} + C_t^{(j)} - 1}{2}, \frac{C_t^{(i)} + C_t^{(j)} + 1}{2} \right) & \text{if } C_t^{(i)} + C_t^{(j)} \text{ is odd} \end{cases} \quad (2)$$

and  $C_{t+1}^{(m)} = C_t^{(m)}$  for  $m \neq i, j$ .

At each discrete instant  $t$ , the two distinct indices  $i$  and  $j$  are chosen among  $1, \dots, n$  with probability  $p_{i,j}(t)$ . We denote by  $X_t$  the random variable representing this choice, that is

$$\mathbb{P}\{X_t = (i, j)\} = p_{i,j}(t).$$

We suppose that the sequence  $\{X_t, t \geq 0\}$  is a sequence of independent and identically distributed random variables. Since  $C_t$  is entirely determined by the values of  $C_0, X_0, X_1, \dots, X_{t-1}$ , this means in

particular that the random variables  $X_t$  and  $C_t$  are independent and that the stochastic process  $C$  is a discrete-time homogeneous Markov chain. As usual in population protocols, we suppose that  $X_t$  is uniformly distributed, i.e. that

$$p_{i,j}(t) = \frac{1}{n(n-1)}.$$

We will use in the sequel the Euclidean norm denoted by  $\|\cdot\|$  and the infinite norm denoted by  $\|\cdot\|_\infty$  defined for all  $x = (x_1, \dots, x_n) \in \mathbb{R}^n$  by

$$\|x\| = \left( \sum_{i=1}^n x_i^2 \right)^{1/2} \quad \text{and} \quad \|x\|_\infty = \max_{i=1, \dots, n} |x_i|$$

It is well-known that these norms satisfy

$$\|x\|_\infty \leq \|x\| \leq \sqrt{n} \|x\|_\infty.$$

**Lemma 1** *For every  $t \geq 0$ , we have*

$$\sum_{i=1}^n C_t^{(i)} = \sum_{i=1}^n C_0^{(i)}.$$

**Proof.** The proof is immediate since the transformation from  $C_t$  to  $C_{t+1}$  described in Relation (2) does not change the sum of the entries of  $C_{t+1}$ . Indeed, from Relation (2), we have  $C_{t+1}^{(i)} + C_{t+1}^{(j)} = C_t^{(i)} + C_t^{(j)}$  and the other entries do not change their values. ■

We denote by  $\ell$  the mean value of the sum of the entries of  $C_t$  and by  $L$  the row vector of  $\mathbb{R}^n$  with all its entries equal to  $\ell$ , that is

$$\ell = \frac{1}{n} \sum_{i=1}^n C_t^{(i)} \quad \text{and} \quad L = (\ell, \dots, \ell).$$

## 6 Analysis of the Proportion Protocol

Our analysis is orchestrated as follows. By relying on Theorem 2, we show in Theorem 5 that the stochastic process  $C_t$  is in the ball of radius  $\sqrt{n/2}$  and center  $L$ , with any high probability, in  $O(\log n)$  parallel time. Then, assuming that the stochastic process  $C_t$  is in the ball of radius  $\sqrt{n/2}$  and that  $\ell - \lfloor \ell \rfloor \neq 1/2$ , we demonstrate that the stochastic process  $C_t$  is in a open ball of radius  $3/2$  and center  $L$  in the  $\|\cdot\|_\infty$  topology, with any high probability in  $O(\log n)$  parallel time (Theorem 6). Then by applying Theorem 5 and Theorem 6 (if  $\ell - \lfloor \ell \rfloor \neq 1/2$ ) or Theorem 4 (otherwise), we derive our main theorem (see Theorem 7) which shows that in both cases the stochastic process  $C_t$  is in a open ball of radius  $3/2$  and center  $L$  in the  $\|\cdot\|_\infty$  topology, with any high probability in  $O(\log n)$  parallel time. Finally, we have all the necessary tools to construct an output function which solves the proportion problem in  $O(\log n - \log \varepsilon - \log \delta)$  parallel time, and with  $O(1/\varepsilon)$  states. This is demonstrated in Theorem 8. Some of the proofs are presented in the Appendix. The interested reader is invited to read them.

**Theorem 2** *For every  $0 \leq s \leq t$  and  $y \geq 0$ , we have*

$$\mathbb{E} (Y_t 1_{\{Y_s \geq y\}}) \leq \left( 1 - \frac{1}{n-1} \right)^{t-s} \mathbb{E} (Y_s 1_{\{Y_s \geq y\}}) + \frac{n}{4} \mathbb{P}\{Y_s \geq y\}, \quad (3)$$

where  $Y_s$  is defined by  $Y_s = \|C_s - L\|^2$ .

**Sketch of the Proof** The proof is very close to Theorem 6 [15] one, but is presented in the appendix to make the paper self-contained. ■

**Lemma 3** For every  $s \geq 0$ , the sequence  $(\|C_t - L\|^2 1_{\{\|C_s - L\|^2 \geq n\}})_{t \geq s}$  is decreasing with  $t$ .

**Proof.** The proof immediate, from Equality (9) in the appendix. Indeed, if  $C_t^{(i)} + C_t^{(j)}$  is odd then  $C_t^{(i)} \neq C_t^{(j)}$  which means, in any case, that

$$\left(C_t^{(i)} - C_t^{(j)}\right)^2 - 1_{\{C_t^{(i)} + C_t^{(j)} \text{ odd}\}} \geq 0,$$

which completes the proof. ■

**Theorem 4** For all  $\delta \in (0, 1)$ , if  $\ell - \lfloor \ell \rfloor = 1/2$  and if there exists a constant  $K$  such that  $\|C_0 - L\|_\infty \leq K$ , then, for every  $t \geq (n-1)(2 \ln K + \ln n - \ln \delta)$ , we have

$$\mathbb{P}\{\|C_t - L\|_\infty \neq 1/2\} \leq \delta.$$

**Sketch of the Proof** If  $\ell - \lfloor \ell \rfloor = 1/2$  then, since all the  $C_t^{(i)}$  are integers, we have  $\|C_t - L\|^2 \geq \frac{n}{4}$ . From Relation (3) in which we set  $s = 0$  and  $y = 0$ , we obtain

$$\mathbb{E}(\|C_t - L\|^2 - n/4) \leq \left(1 - \frac{1}{n-1}\right)^t \mathbb{E}(\|C_0 - L\|^2).$$

Let  $\tau = (n-1)(2 \ln K + \ln n - \ln \delta)$ . and then, for  $t \geq \tau$ , with the same reasoning than in [15], in the countable case

$$\mathbb{P}\{\|C_t - L\|_\infty \neq \frac{1}{2}\} = \mathbb{P}\{\|C_t - L\|^2 - \frac{n}{4} \geq 1\} \leq \delta$$

which completes the sketch of the proof. The reader is invited to read the appendix where the proof in its entirety is presented. ■

**Theorem 5** For all  $\delta \in (0, 4/5)$ , if there exists a constant  $K$  such that  $K \geq \sqrt{n/2}$  and  $\|C_0 - L\| \leq K$  then, for all  $t \geq n\theta$ , we have

$$\mathbb{P}\{\|C_t - L\|^2 \geq n/2\} \leq \delta,$$

where  $\theta = 2 \ln(K) - \ln(n) + 3 \ln(2) - \ln 3 - \left(1 + \frac{\ln 3}{2 \ln 2 - \ln 3}\right) \ln(\delta)$ .

**Sketch of the Proof**

Let  $(T_k)_{k \geq 0}$  be the sequence of instants defined by  $T_0 = 0$  and

$$T_{k+1} = T_k + \left\lceil (n-1) \ln \left( \frac{8\mathbb{E}(Y_{T_k} | Y_{T_k} \geq n/2)}{n} \right) \right\rceil. \quad (4)$$

From theorem 2 and the formula 4 we get

$$\mathbb{E}(Y_{T_{k+1}} | Y_{T_k} \geq n/2) \leq \frac{3n}{8}. \quad (5)$$

Using the conditional Markov inequality, we get

$$\mathbb{P}\{Y_{T_{k+1}} \geq n/2 | Y_{T_k} \geq n/2\} \leq \frac{3}{4}.$$

For every  $k \geq 0$ , we introduce the sequence  $(\alpha_k)$  defined by

$$\alpha_0 = \frac{3n}{8K^2} \text{ and } \alpha_k = \max \left\{ \mathbb{P}\{Y_{T_k} \geq n/2 | Y_{T_{k-1}} \geq n/2\}, \frac{3n}{8K^2} \right\}, \text{ for } k \geq 1.$$

And then we obtain for every  $k \geq 0$ ,

$$\mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2) \leq \frac{3n}{8\alpha_k}.$$

Summing the differences  $T_{i+1} - T_i$  for  $i = 0$  to  $k - 1$ , we obtain, for  $k \geq 1$ ,

$$T_k \leq (n - 1) \left( (k - 1) \ln(3) - \ln \left( \prod_{i=0}^{k-1} \alpha_i \right) \right) + k. \quad (6)$$

and we have

$$\mathbb{P}\{Y_{T_k} \geq n/2\} \leq \prod_{i=1}^k \alpha_i. \quad (7)$$

Now, for all  $\delta \in (0, 4/5)$  there exists  $k \geq 1$  such that

$$\prod_{i=1}^k \alpha_i < \delta \leq \prod_{i=1}^{k-1} \alpha_i \leq \left( \frac{3}{4} \right)^{k-1}.$$

We finally obtain, for  $t \geq n\theta$ , from (7) and using the fact that  $Y_t$  is decreasing

$$\mathbb{P}\{Y_t \geq n/2\} \leq \mathbb{P}\{Y_{n\theta} \geq n/2\} \leq \mathbb{P}\{Y_{T_k} \geq n/2\} \leq \prod_{i=1}^k \alpha_i \leq \delta,$$

which completes the sketch of the proof. The reader is invited to read the appendix where the proof in its entirety is presented. ■

**Theorem 6** For all  $\delta \in (0, 1)$ , if  $\|C_0 - L\| \leq \sqrt{n/2}$  and  $\ell - \lfloor \ell \rfloor \neq 1/2$  then we have, for every  $t \geq 1600(n - 1)(\ln n - \ln \delta - 4 \ln 2 + \ln 3)/189$ ,

$$\mathbb{P}\{\|C_t - L\|_\infty \geq 3/2\} \leq \delta.$$

**Proof.** The proof is presented in the Appendix.

**Theorem 7** For all  $\delta \in (0, 1)$ , if there exists a constant  $K$  such that  $\|C_0 - L\| \leq K$  then, for every  $t \geq n(2 \ln K + 7.47 \ln n - 13.29 \ln \delta - 3.98)$ , we have

$$\mathbb{P}\{\|C_t - L\|_\infty \geq \frac{3}{2}\} \leq \delta.$$

**Proof.** We consider first the case where  $\ell - \lfloor \ell \rfloor = 1/2$ . Since  $\|C_0 - L\|_\infty \leq \|C_0 - L\| \leq K$  and since

$$(n - 1)(2 \ln K + \ln n - \ln \delta) \leq n(2 \ln K + 7.47 \ln n - 13.29 \ln \delta - 3.98),$$

Theorem 4 gives, for  $t \geq n(2 \ln K + 7.47 \ln n - 13.29 \ln \delta - 3.98)$ ,

$$\mathbb{P}\{\|C_t - L\|_\infty \neq \frac{1}{2}\} \leq \delta.$$

Now since the  $C_t^{(i)}$  are integers and since  $\ell - \lfloor \ell \rfloor = 1/2$ , we have

$$\mathbb{P}\{\|C_t - L\|_\infty \geq \frac{3}{2}\} = \mathbb{P}\{\|C_t - L\|_\infty \neq \frac{1}{2}\} \leq \delta.$$



Consider now the case where  $\ell - \lfloor \ell \rfloor \neq 1/2$ . We apply successively Theorem 5 and Theorem 6 replacing  $\delta$  by  $\delta/2$ . We thus introduce the notation

$$\tau_1 = n \left[ 2 \ln(K) - \ln(n) + 3 \ln(2) - \ln 3 - \left( 1 + \frac{\ln 3}{2 \ln 2 - \ln 3} \right) \ln(\delta/2) \right].$$

If  $\|C_0 - L\| < \sqrt{n/2}$  then we have  $\|C_0 - L\|^2 < n/2$  and since  $\|C_t - L\|^2$  is decreasing, we get, for all  $t \geq 0$ ,

$$\mathbb{P}\{\|C_t - L\|^2 < \frac{n}{2}\} \geq \mathbb{P}\{\|C_0 - L\|^2 < \frac{n}{2}\} = 1 \geq 1 - \frac{\delta}{2}.$$

If  $\|C_0 - L\| \geq \sqrt{n/2}$  then, from Theorem 5, we get, for all  $t \geq \tau_1$ ,  $\mathbb{P}\{\|C_t - L\|^2 \geq n/2\} \leq \delta/2$ , or equivalently

$$\mathbb{P}\{\|C_t - L\|^2 < \frac{n}{2}\} \geq 1 - \frac{\delta}{2}.$$

Let us introduce the instant  $\tau_2$  defined by

$$\tau_2 = \tau_1 + \frac{1600(n-1)}{189} (\ln n - \ln(\delta/2) - 4 \ln 2 + \ln 3).$$

We have, for all  $t \geq \tau_2$ ,

$$\begin{aligned} \mathbb{P}\{\|C_t - L\|_\infty < 3/2\} &\geq \mathbb{P}\{\|C_t - L\|_\infty < 3/2, \|C_{\tau_1} - L\|^2 < n/2\} \\ &= \mathbb{P}\{\|C_t - L\|_\infty < 3/2 \mid \|C_{\tau_1} - L\|^2 < n/2\} \mathbb{P}\{\|C_{\tau_1} - L\|^2 < n/2\} \end{aligned}$$

We have seen that  $\mathbb{P}\{\|C_{\tau_1} - L\|^2 < n/2\} \geq 1 - \delta/2$ . Using the fact that the Markov chain  $\{C_t\}$  being homogeneous and applying Theorem 6, we obtain

$$\begin{aligned} \mathbb{P}\{\|C_t - L\|_\infty < 3/2 \mid \|C_{\tau_1} - L\|^2 < n/2\} &= \mathbb{P}\{\|C_{t-\tau_1} - L\|_\infty < 3/2 \mid \|C_0 - L\|^2 < n/2\} \\ &= \mathbb{P}\{\|C_{t-\tau_1} - L\|_\infty < 3/2 \mid \|C_0 - L\| < \sqrt{n/2}\} \\ &\geq 1 - \delta/2. \end{aligned}$$

Putting together these two results gives, for all  $t \geq \tau_2$ ,

$$\mathbb{P}\{\|C_t - L\|_\infty < 3/2\} \geq (1 - \delta/2)^2 \geq 1 - \delta$$

or equivalently

$$\mathbb{P}\{\|C_t - L\|_\infty \geq 3/2\} \leq \delta.$$

The rest of the proof consists to simplify the expression of  $\tau_2$ . We have

$$\begin{aligned} \tau_1 &= n \left[ 2 \ln(K) - \ln(n) + 3 \ln(2) - \ln 3 - \left( 1 + \frac{\ln 3}{2 \ln 2 - \ln 3} \right) \ln(\delta/2) \right] \\ &= n \left[ 2 \ln(K) - \ln(n) + \left( 4 + \frac{\ln 3}{2 \ln 2 - \ln 3} \right) \ln(2) - \ln 3 - \left( 1 + \frac{\ln 3}{2 \ln 2 - \ln 3} \right) \ln(\delta) \right] \end{aligned}$$

and

$$\begin{aligned} \tau_2 &= \tau_1 + \frac{1600(n-1)}{189} (\ln n - \ln(\delta/2) - 4 \ln 2 + \ln 3) \\ &= \tau_1 + \frac{1600(n-1)}{189} (\ln n - \ln \delta - 3 \ln 2 + \ln 3) \\ &\leq n \left[ 2 \ln K + \frac{1411}{189} \ln n - \left( \frac{1789}{189} + \frac{\ln 3}{2 \ln 2 - \ln 3} \right) \ln \delta \right. \\ &\quad \left. - \left( \frac{1348}{63} - \frac{\ln 3}{2 \ln 2 - \ln 3} \right) \ln 2 + \frac{1411}{189} \ln 3 \right] \\ &\leq n (2 \ln K + 7.47 \ln n - 13.29 \ln \delta - 3.98), \end{aligned}$$

which completes the proof. ■

We now apply these results for the computation of the proportion of A  $\gamma_A = \frac{N_A}{N_A + N_B} = \frac{N_A}{n}$ . The set of input is  $\Sigma = \{A, B\}$ , and the input function  $\iota$  is defined by  $\iota(A) = m$  and  $\iota(B) = -m$ , however  $m$  is a positive integer. This means that, for every  $i = 1, \dots, n$ , we have  $C_0^{(i)} \in \{-m, m\}$ . We have

$$\ell = \frac{1}{n} \sum_{i=1}^n C_0^{(i)} = \frac{N_A - N_B}{n} m = (\gamma_A - \gamma_B) m = \gamma m$$

which shows from Lemma 1 that  $\gamma$ ,  $\gamma_A$  and  $\gamma_B$  are time independent. The state set  $Q$  is now the set  $\{-m, -m+1, \dots, m-1, m\}$ . The output function is, for all  $x \in Q$ ,

$$\omega_A(x) = (m+x)/2m$$

Finally, the set of output  $Y$  is the set of all possible values of  $\gamma_A$ , i.e.  $Y = \{0, \frac{1}{2m}, \frac{2}{2m}, \dots, \frac{2m-2}{2m}, \frac{2m-1}{2m}, 1\}$ .

**Theorem 8** For all  $\delta \in (0, 1)$ ,  $\varepsilon \in (0, 1)$ ,  $m = \lceil 3/(4\varepsilon) \rceil$  and for all  $t \geq n(-2 \ln \varepsilon + 7.47 \ln n - 13.29 \ln \delta - 3.16)$ , we have

$$\mathbb{P}\{|\omega_A(C_t^{(i)}) - \gamma_A| < \varepsilon \text{ for all } i = 1, \dots, n\} \geq 1 - \delta.$$

**Proof.** Since  $Q \subset [-m, m]$ , we have  $\|C_0 - L\|_\infty \leq 2m$ . From Theorem 7, since  $K = 2m = 3/(2\varepsilon)$ , we obtain for all  $\delta \in (0, 1)$  and  $t \geq n(-2 \ln \varepsilon + 7.47 \ln n - 13.29 \ln \delta - 3.16)$

$$\mathbb{P}\{\|C_t - L\|_\infty \geq 3/2\} \leq \delta$$

or equivalently

$$\mathbb{P}\{|C_t^{(i)} - (\gamma_A - \gamma_B)m| < 3/2, \text{ for all } i = 1, \dots, n\} \geq 1 - \delta.$$

Since  $\gamma_A + \gamma_B = 1$  we have

$$|C_t^{(i)} - (\gamma_A - \gamma_B)m| = |C_t^i - (2\gamma_A - 1)m| = |m + C_t^i - 2\gamma_A| = |2\omega_A(C_t^{(i)}) - 2\gamma_A|$$

Then

$$\mathbb{P}\{|\omega_A(C_t^{(i)}) - \gamma_A| < 3/(4m), \text{ for all } i = 1, \dots, n\} \geq 1 - \delta$$

So

$$\mathbb{P}\{|\omega_A(C_t^{(i)}) - \gamma_A| < \varepsilon, \text{ for all } i = 1, \dots, n\} \geq 1 - \delta$$

■

Note that the convergence time to get the proportion of agents initially set to A :  $\gamma_A$  with any precision  $\varepsilon$  with any high probability  $1 - \delta$  is  $O(n(\log n - \log \varepsilon - \log \delta))$  and thus the parallel convergence time to get  $\gamma_A$  with any high probability is  $O(\log n - \log \varepsilon - \log \delta)$ .

We can also note that the state set size is  $O(1/\varepsilon)$ .

## 7 Lower Bounds for the "Counting Problem"

In a previous paper [15], we have tackled the counting problem which aims for each agent at computing the exact number of agents that initially started the protocol in say state  $A$ . The interaction rules are the same as the ones used in the present protocol, however the output function is given by  $\omega'_A(x) = \lfloor n(m+x)/(2m) + 1/2 \rfloor$ . By relying on the proof presented in the present paper, we improve upon [15] by showing that the counting problem can be solved in  $O(\log n)$  parallel time with  $O(n)$  states, and we show at the end of this section that it is the lower bound for each case. Specifically,

**Theorem 9** For all  $\delta \in (0, 1)$ , for  $m = \lceil 3n/2 \rceil$  and for all  $t \geq n(9.47 \ln n - 13.29 \ln \delta - 1.77)$ , we have

$$\mathbb{P}\{\omega'_A(C_t^{(i)}) = n_A, \text{ for all } i = 1, \dots, n\} \geq 1 - \delta.$$

**Proof.** We can note that

$$\omega'_A(x) = \lfloor n\omega_A(x) + 1/2 \rfloor$$

From theorem 8 with  $\varepsilon = 1/(2n)$  for  $t \geq n(9.47 \ln n - 13.29 \ln \delta - 1.77)$  we have

$$\mathbb{P}\{|n\omega_A(C_t^{(i)}) - n\gamma_A| < n\varepsilon = 1/2 \text{ for all } i = 1, \dots, n\} \geq 1 - \delta.$$

Because  $n\gamma_A = n_A$  is an integer we have

$$\mathbb{P}\{\omega'_A(C_t^{(i)}) = n_A, \text{ for all } i = 1, \dots, n\} \geq 1 - \delta. \quad \blacksquare$$

Thus each agent can solve the counting problem in  $O(\log n)$  parallel time and with  $O(n)$  state set size.

**Theorem 10** Any algorithm solving "counting problem" takes an expected  $\Omega(\log n)$  parallel time to convergence.

**Proof.** Solving the counting problem bounds to solving the exact majority problem. By an application of theorem C.1 of [1], this algorithm takes expected  $\Omega(\log n)$  parallel time until convergence under a worst-case input.  $\blacksquare$

**Theorem 11** Any algorithm solving the counting problem requires, in expectation,  $\Omega(n)$  states.

**Proof.** To solve the counting problem, the size of the output set  $Y$  must be  $n + 1$ , so the number of states (i.e.,  $|Q|$ ) is at least  $n + 1$ . Thus the lower bound of the number of states is  $\Omega(n)$ .  $\blacksquare$

**Theorem 12** Any algorithm solving the proportion problem with a precision of  $\varepsilon$ , requires, in expectation,  $\Omega(1/\varepsilon)$  states.

**Proof.** The value of  $\gamma_A$  could be any rational value between 0 and 1, the difference between two output values cannot exceed  $2\varepsilon$ , thus the lower bound for the size of the output  $Y$  is  $1/(2\varepsilon) + 1$ , so the number of states (i.e.,  $|Q|$ ) is at least  $1/(2\varepsilon) + 1$ . Thus the lower bound of the number of states is  $\Omega(1/\varepsilon)$ .  $\blacksquare$

Finally, Figure 1 illustrates our theoretical analysis by showing that the parallel time for all the  $n$  agents, with  $n \in [2^5, 2^{19}]$ , to converge to the population proportion with a precision  $\varepsilon = 1/20,000$  is in  $O(\log n)$ .

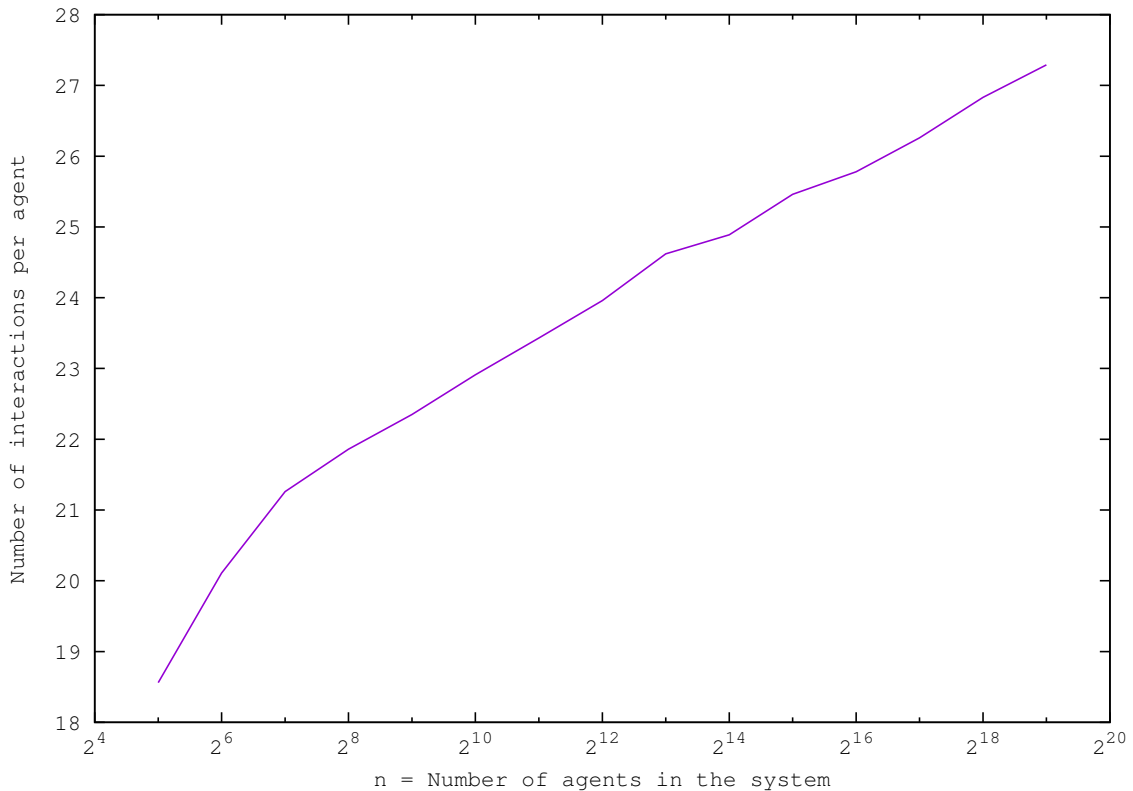


Figure 1: Number of interactions per agent as a function of the size of the system ( $\varepsilon = 0.00005$ ).

## 8 Conclusion

This paper has presented a fast solution to solve the population proportion problem. This problem is a generalization of the majority problem. The protocol we propose is very simple, and guarantees that it is capable of computing the population proportion with a precision of  $\varepsilon \in (0, 1)$ , in no more than  $(-2 \ln \varepsilon + 7.47 \ln n - 13.29 \ln \delta - 3.16)$  interactions per agent with probability  $1 - \delta$ , for any  $\delta \in (0, 1)$ , with  $3/(2\varepsilon) + 1$  states, which makes our protocol optimal both in time and space.

## References

- [1] Dan Alistarh, Rati Gelashvili, and Milan Vojnović. Fast and exact majority in population protocols. In *Proceedings of the 34th annual ACM symposium on Principles of distributed computing (PODC)*, pages 47–56, 2015.
- [2] Dana Angluin, James Aspnes, Zoë Diamadi, Michael J. Fischer, and René Peralta. Computation in networks of passively mobile finite-state sensors. In *Proceedings of the 23rd annual ACM symposium on Principles of distributed computing (PODC)*, 2004.
- [3] Dana Angluin, James Aspnes, Zoë Diamadi, Michael J. Fischer, and René Peralta. Computation in networks of passively mobile finite-state sensors. *Distributed Computing*, 18(4):235–253, 2006.

- [4] Dana Angluin, James Aspnes, and David Eisenstat. Stably computable predicates are semilinear. In *Proceedings of the 25th annual ACM symposium on Principles of distributed computing (PODC)*, pages 292–299, 2006.
- [5] Dana Angluin, James Aspnes, and David Eisenstat. A simple population protocol for fast robust approximate majority. *Distributed Computing*, 20(4):279–304, 2008.
- [6] Dana Angluin, James Aspnes, David Eisenstat, and Eric Ruppert. The computational power of population protocols. *Distributed Computing*, 20(4):279–304, 2007.
- [7] James Aspnes and Eric Ruppert. An introduction to population protocols. *Bulletin of the European Association for Theoretical Computer Science, Distributed Computing Column*, 93:98–117, 2007.
- [8] Joffroy Beauquier, Peva Blanchard, and Janna Burman. Self-stabilizing leader election in population protocols over arbitrary communication graphs. In *Proceedings of the 17th International Conference on Principles of Distributed Systems*, 2013.
- [9] Olivier Bournez, Johanne Cohen, and Mikaël Rabie. Homonym population protocols. In *Proceedings of the 3rd International Conference on Networked Systems (NETYS)*, 2015.
- [10] Carole Delporte-Gallet, Hugues Fauconnier, Rachid Guerraoui, and Eric Ruppert. When birds die: Making population protocols fault-tolerant. In *Proceedings of the 2nd IEEE Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 51–66, 2006.
- [11] Moez Draief and Milan Vojnovic. Convergence speed of binary interval consensus. *SIAM Journal on Control and Optimization*, 50(3):1087–11097, 2012.
- [12] Rachid Guerraoui and Eric Ruppert. Names trump malice: Tiny mobile agents can tolerate byzantine failures. In *Proceedings of the 36th International Colloquium on Automata, Languages and Programming: Part II (ICALP)*, pages 484–495, 2009.
- [13] George B. Mertzios, Sotiris E. Nikolettseas, Christoforos Raptopoulos, and Paul G. Spirakis. Determining majority in networks with local interactions and very small local memory. In *Proceedings of the 41st International Colloquium (ICALP)*, pages 871–882, 2014.
- [14] Ryu Mizoguchi, Hirotaka Ono, Shuji Kijima, and Masafumi Yamashita. On space complexity of self-stabilizing leader election in mediated population protocol. *Distributed Computing*, 25(6):451–460, 2012.
- [15] Yves Mocquard, Emmanuelle Anceaume, James Aspnes, Yann Busnel, and Bruno Sericola. Counting with population protocols. In *Proceedings of the 14th IEEE International Symposium on Network Computing and Applications*, pages 35–42, 2015.
- [16] Etienne Perron, Dinkar Vasudevan, and Milan Vojnovic. Using three states for binary consensus on complete graphs. In *Proceedings of the INFOCOM conference*, pages 2527–2435, 2009.

## A Appendix

**Theorem 2** For every  $0 \leq s \leq t$  and  $y \geq 0$ , we have

$$\mathbb{E} (Y_t 1_{\{Y_s \geq y\}}) \leq \left(1 - \frac{1}{n-1}\right)^{t-s} \mathbb{E} (Y_s 1_{\{Y_s \geq y\}}) + \frac{n}{4} \mathbb{P}\{Y_s \geq y\}, \quad (8)$$

where  $Y_s$  is defined by  $Y_s = \|C_s - L\|^2$ .

**Proof.** From Relations (2) we have, for every  $t \geq 0$ ,

$$Y_{t+1} = Y_t - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \left[ \left( C_t^{(i)} - C_t^{(j)} \right)^2 - 1_{\{C_t^{(i)} + C_t^{(j)} \text{ odd}\}} \right] 1_{\{X_t = (i,j)\}}.$$

Multiplying on both sides by  $1_{\{Y_s \geq y\}}$  gives

$$\begin{aligned} Y_{t+1} 1_{\{Y_s \geq y\}} &= Y_t 1_{\{Y_s \geq y\}} \\ &\quad - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \left[ \left( C_t^{(i)} - C_t^{(j)} \right)^2 - 1_{\{C_t^{(i)} + C_t^{(j)} \text{ odd}\}} \right] 1_{\{Y_s \geq y\}} 1_{\{X_t = (i,j)\}}. \end{aligned} \quad (9)$$

Taking the expectations and using the fact that  $X_t$  and  $C_t$  are independent, we get

$$\begin{aligned} \mathbb{E} (Y_{t+1} 1_{\{Y_s \geq y\}}) &= \mathbb{E} (Y_t 1_{\{Y_s \geq y\}}) \\ &\quad - \frac{1}{2} \mathbb{E} \left( \sum_{i=1}^n \sum_{j=1}^n \left[ \left( C_t^{(i)} - C_t^{(j)} \right)^2 - 1_{\{C_t^{(i)} + C_t^{(j)} \text{ odd}\}} \right] 1_{\{Y_s \geq y\}} \right) p_{i,j}(t). \end{aligned}$$

Since

$$p_{i,j}(t) = \frac{1}{n(n-1)},$$

we obtain

$$\begin{aligned} \mathbb{E} (Y_{t+1} 1_{\{Y_s \geq y\}}) &= \mathbb{E} (Y_t 1_{\{Y_s \geq y\}}) \\ &\quad - \frac{1}{2n(n-1)} \mathbb{E} \left( \sum_{i=1}^n \sum_{j=1}^n \left[ \left( C_t^{(i)} - C_t^{(j)} \right)^2 - 1_{\{C_t^{(i)} + C_t^{(j)} \text{ odd}\}} \right] 1_{\{Y_s \geq y\}} \right). \end{aligned} \quad (10)$$

As shown in [15], we have

$$\sum_{i=1}^n \sum_{j=1}^n \left( C_t^{(i)} - C_t^{(j)} \right)^2 = 2nY_t$$

and if  $q_t$  denotes the number of odd entries of  $C_t$ , we have

$$\sum_{i=1}^n \sum_{j=1}^n 1_{\{C_t^{(i)} + C_t^{(j)} \text{ odd}\}} = 2q_t(n - q_t).$$

The function  $g$  defined, for  $x \in [0, n]$ , by  $g(x) = x(n-x)$  has its maximum at point  $x = n/2$ , so we have  $0 \leq g(x) \leq n^2/4$ . This gives

$$\sum_{i=1}^n \sum_{j=1}^n 1_{\{C_t^{(i)} + C_t^{(j)} \text{ odd}\}} \leq \frac{n^2}{2}.$$

It follows that

$$\mathbb{E}(Y_{t+1}1_{\{Y_s \geq y\}}) \leq \left(1 - \frac{1}{n-1}\right) \mathbb{E}(Y_t 1_{\{Y_s \geq y\}}) + \frac{n}{4(n-1)} \mathbb{P}\{Y_s \geq y\},$$

that is

$$\begin{aligned} \mathbb{E}(Y_t 1_{\{Y_s \geq y\}}) &\leq \left(1 - \frac{1}{n-1}\right)^{t-s} \mathbb{E}(Y_s 1_{\{Y_s \geq y\}}) \\ &\quad + \frac{n}{4(n-1)} \mathbb{P}\{Y_s \geq y\} \sum_{i=0}^{t-1} \left(1 - \frac{1}{n-1}\right)^i. \end{aligned}$$

Since

$$\sum_{i=0}^{t-1} \left(1 - \frac{1}{n-1}\right)^i \leq \sum_{i=0}^{\infty} \left(1 - \frac{1}{n-1}\right)^i = n-1,$$

we get

$$\mathbb{E}(Y_t 1_{\{Y_s \geq y\}}) \leq \left(1 - \frac{1}{n-1}\right)^{t-s} \mathbb{E}(Y_s 1_{\{Y_s \geq y\}}) + \frac{n}{4} \mathbb{P}\{Y_s \geq y\},$$

which completes the proof. ■

**Theorem 4** For all  $\delta \in (0, 1)$ , if  $\ell - \lfloor \ell \rfloor = 1/2$  and if there exists a constant  $K$  such that  $\|C_0 - L\|_{\infty} \leq K$ , then, for every alors,  $t \geq (n-1)(2 \ln K + \ln n - \ln \delta)$ , we have

$$\mathbb{P}\{\|C_t - L\|_{\infty} \neq 1/2\} \leq \delta.$$

**Proof.** If  $\ell - \lfloor \ell \rfloor = 1/2$  then, since all the  $C_t^{(i)}$  are integers, we have  $|C_t^{(i)} - \ell| \geq 1/2$ , for every  $i = 1, \dots, n$ . It follows that

$$\|C_t - L\|^2 \geq \frac{n}{4}.$$

If there exists  $i$  such that  $|C_t^{(i)} - \ell| > 1/2$  then we have  $\|C_t - L\|^2 > n/4$ . Conversely, if  $|C_t^{(i)} - \ell| = 1/2$ , for every  $i$  then we have  $\|C_t - L\|^2 = n/4$ . We thus have shown that

$$\|C_t - L\|^2 = \frac{n}{4} \iff \|C_t - L\|_{\infty} = \frac{1}{2}. \quad (11)$$

Thus, if  $\|C_t - L\|^2 > n/4$  then there exists  $i$  such that  $|C_t^{(i)} - \ell| > 1/2$ . In this case and for this value of  $i$ , since the  $C_t^{(j)}$  are integers and since  $\ell - \lfloor \ell \rfloor = 1/2$ , we necessarily have  $|C_t^{(i)} - \ell| \geq 3/2$ . This means, in this case, that

$$\|C_t - L\|^2 \geq (n-1) \left(\frac{1}{2}\right)^2 + \left(\frac{3}{2}\right)^2 = \frac{n}{4} + 2.$$

We then have

$$\|C_t - L\|^2 > \frac{n}{4} \iff \|C_t - L\|^2 \geq \frac{n}{4} + 2,$$

and

$$\|C_t - L\|^2 < \frac{n}{4} + 1 \implies \|C_t - L\|^2 < \frac{n}{4} + 2 \implies \|C_t - L\|^2 = \frac{n}{4}.$$

Thus

$$\|C_t - L\|^2 < \frac{n}{4} + 1 \iff \|C_t - L\|^2 = \frac{n}{4}. \quad (12)$$

From Relation (8) in which we set  $s = 0$  and  $y = 0$ , we obtain

$$\mathbb{E}(\|C_t - L\|^2 - n/4) \leq \left(1 - \frac{1}{n-1}\right)^t \mathbb{E}(\|C_0 - L\|^2).$$

Let  $\tau = (n-1)(2 \ln K + \ln n - \ln \delta)$ . For  $t \geq \tau$ , we have

$$\left(1 - \frac{1}{n-1}\right)^t \leq e^{-t/(n-1)} \leq e^{-\tau/(n-1)} = \frac{\delta}{nK^2}.$$

Moreover, since  $\|C_0 - L\|^2 \leq n\|C_0 - L\|_\infty^2 \leq nK^2$ , we get  $\mathbb{E}(\|C_0 - L\|^2) \leq nK^2$  and thus  $\mathbb{E}(\|C_t - L\|^2 - n/4) \leq \delta$ . Using the Markov inequality, for  $t \geq \tau$ , we obtain

$$\mathbb{P}\{\|C_t - L\|^2 - \frac{n}{4} \geq 1\} \leq \delta.$$

Putting together equivalences (11) and (12) leads to

$$\|C_t - L\|^2 - \frac{n}{4} < 1 \iff \|C_t - L\|_\infty = \frac{1}{2}$$

and then, for  $t \geq \tau$ ,

$$\mathbb{P}\{\|C_t - L\|_\infty \neq \frac{1}{2}\} = \mathbb{P}\{\|C_t - L\|^2 - \frac{n}{4} \geq 1\} \leq \delta$$

which completes the proof. ■

**Theorem 5** For all  $\delta \in (0, 4/5)$ , if there exists a constant  $K$  such that  $K \geq \sqrt{n/2}$  and  $\|C_0 - L\| \leq K$  then, for all  $t \geq n\theta$ , we have

$$\mathbb{P}\{\|C_t - L\|^2 \geq n/2\} \leq \delta,$$

where  $\theta = 2 \ln(K) - \ln(n) + 3 \ln(2) - \ln 3 - \left(1 + \frac{\ln 3}{2 \ln 2 - \ln 3}\right) \ln(\delta)$ .

**Proof.** Let  $(T_k)_{k \geq 0}$  be the sequence of instants defined by  $T_0 = 0$  and

$$T_{k+1} = T_k + \left\lceil (n-1) \ln \left( \frac{8\mathbb{E}(Y_{T_k} | Y_{T_k} \geq n/2)}{n} \right) \right\rceil, \quad (13)$$

where  $Y_t$  is defined by  $Y_t = \|C_t - L\|^2$ . From Theorem 2, we have, for every  $k \geq 0$ , by taking  $y = n/2$ ,  $t = T_{k+1}$  and  $s = T_k$ ,

$$\mathbb{E}\left(Y_{T_{k+1}} 1_{\{Y_{T_k} \geq n/2\}}\right) \leq \left(1 - \frac{1}{n-1}\right)^{T_{k+1}-T_k} \mathbb{E}\left(Y_{T_k} 1_{\{Y_{T_k} \geq n/2\}}\right) + \frac{n}{4} \mathbb{P}\{Y_{T_k} \geq n/2\},$$

which can also be written as

$$\mathbb{E}\left(Y_{T_{k+1}} | Y_{T_k} \geq n/2\right) \leq \left(1 - \frac{1}{n-1}\right)^{T_{k+1}-T_k} \mathbb{E}\left(Y_{T_k} | Y_{T_k} \geq n/2\right) + \frac{n}{4}.$$

Using the fact that for all  $x \in [0, 1)$ ,  $1 - x \leq e^{-x}$  and by definition of the sequence  $(T_k)$ , we have

$$\left(1 - \frac{1}{n-1}\right)^{T_{k+1}-T_k} \leq e^{-(T_{k+1}-T_k)/(n-1)} \leq \frac{n}{8\mathbb{E}\left(Y_{T_k} | Y_{T_k} \geq n/2\right)}.$$

This leads to

$$\mathbb{E}\left(Y_{T_{k+1}} | Y_{T_k} \geq n/2\right) \leq \frac{3n}{8}. \quad (14)$$

Using the conditional Markov inequality, we get

$$\mathbb{P}\{Y_{T_{k+1}} \geq n/2 | Y_{T_k} \geq n/2\} \leq \frac{2\mathbb{E}\left(Y_{T_{k+1}} | Y_{T_k} \geq n/2\right)}{n} \leq \frac{3}{4}.$$



For every  $k \geq 0$ , we introduce the sequence  $(\alpha_k)$  defined by

$$\alpha_0 = \frac{3n}{8K^2} \text{ and } \alpha_k = \max \left\{ \mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\}, \frac{3n}{8K^2} \right\}, \text{ for } k \geq 1.$$

For  $k \geq 1$ , using the fact that the sequence  $Y_t$  is decreasing (see NCA), we have

$$\begin{aligned} \mathbb{E}(Y_{T_k} \mid Y_{T_{k-1}} \geq n/2) &\geq \mathbb{E}(Y_{T_k} 1_{\{Y_{T_k} \geq n/2\}} \mid Y_{T_{k-1}} \geq n/2) \\ &= \mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2, Y_{T_{k-1}} \geq n/2) \mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\} \\ &= \mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2) \mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\}, \end{aligned}$$

which can be written as

$$\mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2) \leq \frac{\mathbb{E}(Y_{T_k} \mid Y_{T_{k-1}} \geq n/2)}{\mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\}}$$

and, using (14), as

$$\mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2) \leq \frac{3n}{8\mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\}}.$$

On another hand, using again the fact that the sequence  $Y_t$  is decreasing (see NCA) and since  $Y_{T_0} = Y_0 = \|C_0 - L\|^2 \leq K^2$ , we have, for  $k \geq 0$ ,

$$\mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2) \leq \mathbb{E}(Y_{T_0} \mid Y_{T_k} \geq n/2) \leq K^2.$$

Putting together these two inequalities gives, for  $k \geq 1$ ,

$$\begin{aligned} \mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2) &\leq \min \left\{ \frac{3n}{8\mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\}}, K^2 \right\} \\ &\leq \frac{3n}{8} \min \left\{ \frac{1}{\mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\}}, \frac{8K^2}{3n} \right\} \\ &= \frac{3n}{8\alpha_k}. \end{aligned}$$

By definition of  $\alpha_0$ , we have for every  $k \geq 0$ ,

$$\mathbb{E}(Y_{T_k} \mid Y_{T_k} \geq n/2) \leq \frac{3n}{8\alpha_k}.$$

Using this inequality in the definition of the sequence  $(T_k)$  given by (13), we obtain, for  $k \geq 0$ ,

$$T_{k+1} \leq T_k + \lceil (n-1) \ln(3/\alpha_k) \rceil \leq T_k + (n-1) \ln(3/\alpha_k) + 1.$$

Summing the differences  $T_{i+1} - T_i$  for  $i = 0$  to  $k-1$ , we obtain, for  $k \geq 1$ ,

$$T_k \leq (n-1) \left( (k-1) \ln(3) - \ln \left( \prod_{i=0}^{k-1} \alpha_i \right) \right) + k. \quad (15)$$

For  $k \geq 1$ , since  $Y_{T_k}$  is decreasing, we have  $\mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} < n/2\} = 0$ , and so

$$\mathbb{P}\{Y_{T_k} \geq n/2\} = \mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\} \mathbb{P}\{Y_{T_{k-1}} \geq n/2\} \leq \alpha_k \mathbb{P}\{Y_{T_{k-1}} \geq n/2\},$$

which leads to

$$\mathbb{P}\{Y_{T_k} \geq n/2\} \leq \prod_{i=1}^k \alpha_i. \quad (16)$$

Since  $\mathbb{P}\{Y_{T_k} \geq n/2 \mid Y_{T_{k-1}} \geq n/2\} \leq 3/4$  and  $K \geq \sqrt{n/2}$ , we obtain by definition  $\alpha_k \leq 3/4$  for every  $k \geq 0$ . Now, for all  $\delta \in (0, 1)$  there exists  $k \geq 1$  such that

$$\prod_{i=1}^k \alpha_i < \delta \leq \prod_{i=1}^{k-1} \alpha_i.$$

We then have, since  $\alpha_0 = 3n/(8K^2)$ ,

$$\begin{aligned} -\ln \left( \prod_{i=0}^{k-1} \alpha_i \right) &= -\ln \left( \prod_{i=1}^{k-1} \alpha_i \right) - \ln(\alpha_0) \\ &\leq -\ln(\delta) - \ln(n) - \ln(3) + 3\ln(2) + 2\ln(K) \end{aligned}$$

Moreover, since  $\alpha_k \leq 3/4$ , we have  $\delta \leq (3/4)^{k-1}$ , which gives

$$k-1 \leq \frac{-\ln(\delta)}{2\ln(2) - \ln(3)}.$$

Putting these results into (15) and using the definition of  $\theta$ , gives

$$T_k \leq (n-1)\theta + 1 - \frac{\ln(\delta)}{2\ln(2) - \ln(3)} \leq n\theta.$$

Note that this last inequality is valid because we have supposed  $\delta \leq 4/5$ . This is the case in practice, nevertheless to deal with the case where  $\delta \in (4/5, 1)$  it suffices to replace  $\theta$  by  $\theta + 1$ .

We finally obtain, for  $t \geq n\theta$ , from (16) and using the fact that  $Y_t$  is decreasing

$$\mathbb{P}\{Y_t \geq n/2\} \leq \mathbb{P}\{Y_{n\theta} \geq n/2\} \leq \mathbb{P}\{Y_{T_k} \geq n/2\} \leq \prod_{i=1}^k \alpha_i \leq \delta,$$

which completes the proof. ■

**Theorem 6** For all  $\delta \in (0, 1)$ , if  $\|C_0 - L\| \leq \sqrt{n/2}$  and  $\ell - \lfloor \ell \rfloor \neq 1/2$  then we have, for every  $t \geq 1600(n-1)(\ln n - \ln \delta - 4\ln 2 + \ln 3)/189$ ,

$$\mathbb{P}\{\|C_t - L\|_\infty \geq 3/2\} \leq \delta.$$

**Proof.** Let  $\lambda$  be defined by

$$\lambda = \begin{cases} \ell - \lfloor \ell \rfloor & \text{if } \ell - \lfloor \ell \rfloor < \frac{1}{2} \\ \ell - \lceil \ell \rceil & \text{if } \ell - \lfloor \ell \rfloor > \frac{1}{2} \end{cases}$$

Note that  $\lambda$  is positive in the first case and negative in the second one. In both cases we have  $|\lambda| < 1/2$  and  $\ell - \lambda$  is the closest integer to  $\ell$ .

If  $\|C_0 - L\| \leq \sqrt{n/2}$  then, since  $\|C_t - L\|$  is decreasing, we also have  $\|C_t - L\| \leq \sqrt{n/2}$ , for every  $t \geq 0$ . It follows that

$$\|C_t - L\|_\infty \leq \|C_t - L\| \leq \sqrt{n/2}.$$

Since  $|\lambda| \leq 1/2$ , this means that, for every  $i = 1, \dots, n$ , we have

$$-\frac{1}{2} - \frac{\sqrt{n}}{2} \leq \lambda - \frac{\sqrt{n}}{2} \leq C_t^{(i)} - \ell + \lambda \leq \lambda + \frac{\sqrt{n}}{2} \leq \frac{1}{2} + \frac{\sqrt{n}}{2}.$$

Let  $B = \lceil 1/2 + \sqrt{n/2} \rceil$ . For  $k \in \{-B, -B+1, \dots, B\}$ , we denote by  $\alpha_{k,t}$  the number of agents with the value  $\ell - \lambda + k$  at time  $t$ , that is

$$\alpha_{k,t} = \left| \left\{ i \in \{1, \dots, n\} \mid C_t^{(i)} = \ell - \lambda + k \right\} \right|,$$

where the absolute value of a set is its cardinality. It is easily checked that

$$\sum_{k=-B}^B \alpha_{k,t} = n. \quad (17)$$

Moreover we have, by definition of  $\alpha_{k,t}$ ,

$$\sum_{k=-B}^B (\ell - \lambda + k) \alpha_{k,t} = \sum_{i=1}^n C_t^{(i)} = n\ell,$$

which gives using (17)

$$\sum_{k=-B}^B k \alpha_{k,t} = n\lambda. \quad (18)$$

In the same way, again by definition of  $\alpha_{k,t}$ , we have

$$\sum_{k=-B}^B (\ell - \lambda + k)^2 \alpha_{k,t} = \sum_{i=1}^n \left( C_t^{(i)} \right)^2 = \|C_t\|^2.$$

Observing that  $\|C_t - L\|^2 = \|C_t\|^2 - n\ell^2$  and using (17) and (18), we obtain

$$\sum_{k=-B}^B k^2 \alpha_{k,t} = \|C_t - L\|^2 + n\lambda^2. \quad (19)$$

Since  $\|C_t - L\|^2$  is decreasing, using the hypothesis  $\|C_0 - L\|^2 \leq n/2$ , we obtain  $\|C_t - L\|^2 \leq n/2$  and thus

$$\sum_{k=-B}^B k^2 \alpha_{k,t} \leq \frac{n}{2} + n\lambda^2. \quad (20)$$

Let  $x$  be defined by

$$x = \sum_{k=0}^B \alpha_{k,t}.$$

We then have

$$\sum_{k=-B}^{-1} \alpha_{k,t} = n - x$$

and

$$\sum_{k=-B}^{-1} k \alpha_{k,t} \leq \sum_{k=-B}^{-1} -\alpha_{k,t} = -(n - x).$$

Using (18), we get

$$\sum_{k=1}^B k \alpha_{k,t} = n\lambda - \sum_{k=-B}^{-1} k \alpha_{k,t} \geq n\lambda + n - x.$$

We also have using the two previous inequalities

$$\sum_{k=-B}^B k^2 \alpha_{k,t} = \sum_{k=1}^B k^2 \alpha_{k,t} + \sum_{k=-B}^{-1} k^2 \alpha_{k,t} \geq \sum_{k=1}^B k \alpha_{k,t} - \sum_{k=-B}^{-1} k \alpha_{k,t} \geq 2(n-x) + n\lambda.$$

Combining this inequality with (20) we obtain

$$2(n-x) + n\lambda \leq \sum_{k=-B}^B k^2 \alpha_{k,t} \leq \frac{n}{2} + n\lambda^2.$$

These two bounds lead to

$$x \geq \frac{3n}{4} + \frac{n\lambda(1-\lambda)}{2}.$$

Since  $|\lambda| < 1/2$  we have  $\lambda(1-\lambda) > -3/4$ , which gives

$$x = \sum_{k=0}^B \alpha_{k,t} > \frac{3n}{8}.$$

Using the same reasoning to the sum  $\sum_{k=-B}^0 \alpha_{k,t}$  leads to

$$\sum_{k=0}^B \alpha_{k,t} > \frac{3n}{8} \quad \text{and} \quad \sum_{k=-B}^0 \alpha_{k,t} > \frac{3n}{8}. \quad (21)$$

Let us now introduce the sequences  $(N_t)_{t \geq 0}$  and  $(\Phi_t)_{t \geq 0}$  defined by

$$N_t = \sum_{k=2}^B \alpha_{k,t} + \sum_{k=-B}^{-2} \alpha_{k,t} \quad \text{and} \quad \Phi_t = \sum_{k=2}^B k^2 \alpha_{k,t} + \sum_{k=-B}^{-2} k^2 \alpha_{k,t}.$$

Since  $\alpha_{k,t}$  are non negative integers, we have, for every  $t \geq 0$ ,

$$N_t = 0 \iff \Phi_t = 0.$$

We also introduce the sets  $H_t^+$  and  $H_t^-$  defined by

$$H_t^+ = \{i \in \{1, \dots, n\} \mid C_t^{(i)} - \ell + \lambda \geq 2\},$$

$$H_t^- = \{i \in \{1, \dots, n\} \mid C_t^{(i)} - \ell + \lambda \leq -2\}$$

and we define  $H_t = H_t^+ \cup H_t^-$ . It is easily checked that

$$N_t = |H_t| \quad \text{and} \quad \Phi_t = \sum_{i \in H_t} \left( C_t^{(i)} - \ell + \lambda \right)^2$$

Since  $|\lambda| < 1/2$  we have, using (20)

$$4N_t \leq \Phi_t \leq \sum_{k=-B}^B k^2 \alpha_{k,t} \leq \frac{n}{2} + n\lambda^2 \leq \frac{3n}{4}, \quad (22)$$

which gives

$$N_t \leq \frac{3n}{19 \cdot 16}.$$

Let  $I_t^+$  and  $I_t^-$  be the sets defined

$$I_t^+ = \{i \in \{1, \dots, n\} \mid C_t^{(i)} - \ell + \lambda \geq 0\},$$

$$I_t^- = \{i \in \{1, \dots, n\} \mid C_t^{(i)} - \ell + \lambda \leq 0\}.$$

Relations (21) can be rewritten as

$$|I_t^+| \geq \frac{3n}{8} \text{ and } |I_t^-| \geq \frac{3n}{8}. \quad (23)$$

Recall that the random variable  $X_t$ , which is the pair of agents interacting at time  $t$ , is uniformly distributed, i.e., for every  $i, j \in \{1, \dots, n\}$  with  $i \neq j$ , we have

$$\mathbb{P}\{X_t = (i, j)\} = \frac{1}{n(n-1)}.$$

The main way to decrease  $\Phi_t$  is that an agent of  $H_t^+$  interacts with an agent of  $I_t^-$  or that an agent of  $H_t^-$  interacts with an agent of  $I_t^+$ , at time  $t$ , we consider the probability that an agent of  $H_t^+$  interacts with an agent of  $I_t^-$  or that an agent of  $H_t^-$  interacts with an agent of  $I_t^+$ , at time  $t$ . If  $E$  is the set defined by

$$E = A \cup B \cup C \cup D,$$

with  $A = H_t^+ \times I_t^-$ ,  $B = I_t^- \times H_t^+$ ,  $C = H_t^- \times I_t^+$ ,  $D = I_t^+ \times H_t^-$ . It is easy to check that  $(A \cup D) \cap (B \cup C) = \emptyset$ . Moreover we have  $A \cap D = H_t^+ \times H_t^-$  and  $B \cap C = H_t^- \times H_t^+$ . Since the distribution of  $X_t$  is uniform, we have  $\mathbb{P}\{X_t \in A \cup D\} = \mathbb{P}\{X_t \in B \cup C\}$  and so

$$\begin{aligned} \mathbb{P}\{X_t \in E\} &= 2\mathbb{P}\{X_t \in A \cup D\} \\ &= 2(\mathbb{P}\{X_t \in A\} + \mathbb{P}\{X_t \in D\} - \mathbb{P}\{X_t \in A \cap D\}) \\ &= \frac{2(|H_t^+||I_t^-| + |I_t^+||H_t^-| - |H_t^+||H_t^-|)}{n(n-1)}. \end{aligned} \quad (24)$$

Using (23) and the fact that  $|H_t^+||H_t^-| \leq (|H_t^+| + |H_t^-|)^2/2 = (N_t)^2/2$  and  $N_t \leq 3n/16$ , we obtain

$$\begin{aligned} \mathbb{P}\{X_t \in E\} &\geq 2 \left( \frac{3nN_t}{8} - \frac{N_t^2}{4} \right) \frac{1}{n(n-1)} \\ &\geq 2N_t \left( \frac{3n}{8} - \frac{3n}{64} \right) \frac{1}{n(n-1)} = \frac{21N_t}{32(n-1)}. \end{aligned} \quad (25)$$

We consider now the difference  $\Phi_t - \Phi_{t+1}$  in function of the various interactions occuring at time  $t$ . We introduce the notation

$$G_t^+ = I_t^+ \setminus H_t^+ = \{i \in \{1, \dots, n\} \mid C_t^{(i)} - \ell + \lambda \in \{0, 1\}\},$$

$$G_t^- = I_t^- \setminus H_t^- = \{i \in \{1, \dots, n\} \mid C_t^{(i)} - \ell + \lambda \in \{-1, 0\}\}$$

and  $G_t = G_t^+ \cup G_t^-$ .

Suppose that  $X_t = (i, j)$  with  $i \neq j$ . We have the two following different cases.

**Case 1)** If  $(i, j) \in (H_t^+ \times G_t^-) \cup (G_t^- \times H_t^+) \cup (H_t^- \times G_t^+) \cup (G_t^+ \times H_t^-)$ , and if we set, to simplify the writing,

$$a = \left( C_t^{(i)} - \ell + \lambda \right) 1_{\{i \in H_t\}} + \left( C_t^{(j)} - \ell + \lambda \right) 1_{\{j \in H_t\}},$$

$$b = \left( C_t^{(i)} - \ell + \lambda \right) 1_{\{i \in G_t\}} + \left( C_t^{(j)} - \ell + \lambda \right) 1_{\{j \in G_t\}},$$

we have

$$\begin{aligned}\Phi_t - \Phi_{t+1} &= a^2 - \left(\frac{a+b-1_{\{a+b \text{ odd}\}}}{2}\right)^2 1_{\{i \in H_{t+1}\}} \\ &\quad - \left(\frac{a+b+1_{\{a+b \text{ odd}\}}}{2}\right)^2 1_{\{j \in H_{t+1}\}},\end{aligned}\tag{26}$$

which gives

$$\Phi_t - \Phi_{t+1} \geq a^2 - \left(\frac{a+b-1_{\{a+b \text{ odd}\}}}{2}\right)^2 - \left(\frac{a+b+1_{\{a+b \text{ odd}\}}}{2}\right)^2.$$

Distinguishing successively the cases where  $a+b$  is odd and even, we obtain

$$\Phi_t - \Phi_{t+1} \geq \frac{a^2}{2} - b \left(a + \frac{b}{2}\right) - \frac{1_{\{a+b \text{ odd}\}}}{2}.\tag{27}$$

We consider the cases  $b = -1$ ,  $b = 1$  and  $b = 0$  separately.

If  $b = -1$  then we necessarily have  $(i, j) \in (H_t^+ \times G_t^-) \cup (G_t^- \times H_t^+)$ , which means that  $a \geq 2$ .

We thus have  $-b(a+b/2) = a - 1/2 \geq 3/2$  and so

$$\Phi_t - \Phi_{t+1} \geq \frac{a^2}{2} \geq \frac{12a^2}{25}.$$

If  $b = 1$  then we necessarily have  $(i, j) \in (H_t^- \times G_t^+) \cup (G_t^+ \times H_t^-)$ , which means that  $a \leq -2$ .

We thus have  $-b(a+b/2) = -a - 1/2 \geq 3/2$  and so

$$\Phi_t - \Phi_{t+1} \geq \frac{a^2}{2} \geq \frac{12a^2}{25}.$$

If  $b = 0$  then we distinguish the cases :  $a$  is even,  $|a| = 3$  and  $|a| \geq 5$ .

If  $a$  is even then, since  $b = 0$ , we have, from Relation (27),

$$\Phi_t - \Phi_{t+1} \geq \frac{a^2}{2} \geq \frac{12a^2}{25}.$$

If  $a = 3$  then we have, since  $b = 0$ ,  $i \notin H_{t+1}$  ( $i \in G_{t+1}^+$ ) and  $j \in H_{t+1}$ , which gives using Relation (26)

$$\Phi_t - \Phi_{t+1} = 9 - \left(\frac{3+1}{2}\right)^2 = 5 \geq \frac{a^2}{2} \geq \frac{12a^2}{25}.$$

If  $a = -3$  then we have, since  $b = 0$ ,  $i \in H_{t+1}$  and  $j \notin H_{t+1}$  ( $i \in G_{t+1}^-$ ), which gives using Relation (26)

$$\Phi_t - \Phi_{t+1} = 9 - \left(\frac{-3-1}{2}\right)^2 = 5 \geq \frac{a^2}{2} \geq \frac{12a^2}{25}.$$

If  $a$  is odd and  $|a| \geq 5$  then, since  $b = 0$ , we have,

$$a^2 \geq 5 \iff \frac{a^2-1}{2} \geq \frac{12a^2}{25},$$

which gives, from Relation (27),

$$\Phi_t - \Phi_{t+1} \geq \frac{a^2-1}{2} \geq \frac{12a^2}{25}.$$

Thus we have shown that if  $(i, j) \in (H_t^+ \times G_t^-) \cup (G_t^- \times H_t^+) \cup (H_t^- \times G_t^+) \cup (G_t^+ \times H_t^-)$  then

$$\Phi_t - \Phi_{t+1} \geq \frac{12a^2}{25}.$$

**Case 2)** If  $(i, j) \in (H_t^+ \times H_t^-) \cup (H_t^- \times H_t^+)$ , and if we set, to simplify the writing,

$$a = \left(C_t^{(i)} - \ell + \lambda\right) \quad \text{and} \quad b = \left(C_t^{(j)} - \ell + \lambda\right),$$

we have

$$\begin{aligned} \Phi_t - \Phi_{t+1} &= a^2 + b^2 - \left(\frac{a+b-1_{\{a+b \text{ odd}\}}}{2}\right)^2 1_{\{i \in H_{t+1}\}} \\ &\quad - \left(\frac{a+b+1_{\{a+b \text{ odd}\}}}{2}\right)^2 1_{\{j \in H_{t+1}\}}, \end{aligned} \quad (28)$$

which gives

$$\Phi_t - \Phi_{t+1} \geq a^2 + b^2 - \left(\frac{a+b-1_{\{a+b \text{ odd}\}}}{2}\right)^2 - \left(\frac{a+b+1_{\{a+b \text{ odd}\}}}{2}\right)^2.$$

Distinguishing successively the cases where  $a+b$  is odd and even, we obtain

$$\Phi_t - \Phi_{t+1} \geq \frac{a^2}{2} + \frac{b^2}{2} - ab - \frac{1_{\{a+b \text{ odd}\}}}{2}. \quad (29)$$

By definition of  $H_t^+$  and  $H_t^-$  we have  $-ab \geq 4$ , so we obtain

$$\Phi_t - \Phi_{t+1} \geq \frac{a^2}{2} + \frac{b^2}{2} \geq \frac{12a^2}{25} + \frac{12b^2}{25}.$$

Putting together the cases **1)** and **2)**, we get

$$\begin{aligned} E &= (H_t^+ \times G_t^-) \cup (G_t^- \times H_t^+) \cup (H_t^- \times G_t^+) \cup (G_t^+ \times H_t^-) \\ &\quad \cup (H_t^+ \times H_t^-) \cup (H_t^- \times H_t^+). \end{aligned}$$

All these six sets are disjoint so we have, using the results obtained in 1) and 2) and defining  $\beta_{t,i} = \left(C_t^{(i)} - \ell + \lambda\right)^2$ ,

$$\begin{aligned} &\sum_{(i,j) \in E} \mathbb{E}(\Phi_t - \Phi_{t+1} \mid X_t = (i, j)) \\ &\geq \frac{12}{25} \sum_{i \in H_t^+} \sum_{j \in G_t^-} \mathbb{E}(\beta_{t,i}) + \frac{12}{25} \sum_{i \in G_t^-} \sum_{j \in H_t^+} \mathbb{E}(\beta_{t,j}) \\ &\quad + \frac{12}{25} \sum_{i \in H_t^-} \sum_{j \in G_t^+} \mathbb{E}(\beta_{t,i}) + \frac{12}{25} \sum_{i \in G_t^+} \sum_{j \in H_t^-} \mathbb{E}(\beta_{t,j}) \\ &\quad + \frac{12}{25} \sum_{i \in H_t^+} \sum_{j \in H_t^-} [\mathbb{E}(\beta_{t,i}) + \mathbb{E}(\beta_{t,j})] + \frac{12}{25} \sum_{i \in H_t^-} \sum_{j \in H_t^+} [\mathbb{E}(\beta_{t,i}) + \mathbb{E}(\beta_{t,j})] \\ &= \frac{12}{25} \left[ 2|G_t^-| \sum_{i \in H_t^+} \mathbb{E}(\beta_{t,i}) + 2|G_t^+| \sum_{i \in H_t^-} \mathbb{E}(\beta_{t,i}) \right. \\ &\quad \left. + 2|H_t^+| \sum_{i \in H_t^-} \mathbb{E}(\beta_{t,i}) + 2|H_t^-| \sum_{i \in H_t^+} \mathbb{E}(\beta_{t,i}) \right]. \end{aligned}$$

Observing that  $|G_t^-| + |H_t^-| = |I_t^-|$ ,  $|G_t^+| + |H_t^+| = |I_t^+|$  and that  $|I_t^-| \geq 3n/8$  and  $|I_t^+| \geq 3n/8$ , we obtain

$$\begin{aligned} \sum_{(i,j) \in E} \mathbb{E}(\Phi_t - \Phi_{t+1} \mid X_t = (i, j)) &\geq \frac{12}{25} \left[ 2|I_t^-| \sum_{i \in H_t^+} \mathbb{E}(\beta_{t,i}) + 2|I_t^+| \sum_{i \in H_t^-} \mathbb{E}(\beta_{t,i}) \right] \\ &\geq \frac{9n}{25} \mathbb{E}(\Phi_t). \end{aligned} \quad (30)$$

Note that we have used the fact that, for every  $i = 1, \dots, n$ ,  $\beta_{t,i}$  and  $X_t$  are independent. Indeed, for every  $t$ ,  $C_t^{(i)}$  is entirely determined by the values of  $X_0, \dots, X_{t-1}$  and  $(X_s)_{s \geq 0}$  is a sequence of independent random variables.

This leads to

$$\mathbb{E}(\Phi_t - \Phi_{t+1} \mid X_t \in E) = \frac{\sum_{(i,j) \in E} \mathbb{E}(\Phi_t - \Phi_{t+1} \mid X_t = (i, j)) \mathbb{P}\{X_t = (i, j)\}}{\mathbb{P}\{X_t \in E\}}.$$

Since  $\mathbb{P}\{X_t = (i, j)\} = 1/(n(n-1))$  and using (24), we get

$$\mathbb{E}(\Phi_t - \Phi_{t+1} \mid X_t \in E) = \frac{\sum_{(i,j) \in E} \mathbb{E}(\Phi_t - \Phi_{t+1} \mid X_t = (i, j))}{2(|H_t^+||I_t^-| + |I_t^+||H_t^-| - |H_t^+||H_t^-|)}.$$

Since  $|I_t^-| \leq n$  and  $|I_t^+| \leq n$ , we have

$$|H_t^+||I_t^-| + |I_t^+||H_t^-| - |H_t^+||H_t^-| \leq n(H_t^+ + |H_t^-|) = n|H_t| = nN_t.$$

Using this inequality together with (30), we obtain

$$\mathbb{E}(\Phi_t - \Phi_{t+1} \mid X_t \in E) \geq \frac{9\mathbb{E}(\Phi_t)}{50N_t}.$$

Now, we have, using (25)

$$\begin{aligned} \mathbb{E}(\Phi_{t+1}) &= \mathbb{E}(\Phi_t) - \mathbb{E}(\Phi_t - \Phi_{t+1}) \\ &\leq \mathbb{E}(\Phi_t) - \mathbb{E}((\Phi_t - \Phi_{t+1}) \mid X_t \in E) \mathbb{P}\{X_t \in E\} \\ &\leq \mathbb{E}(\Phi_t) - \left( \frac{9\mathbb{E}(\Phi_t)}{50N_t} \right) \left( \frac{21N_t}{32(n-1)} \right) \\ &= \left( 1 - \frac{189}{1600(n-1)} \right) \mathbb{E}(\Phi_t). \end{aligned}$$

We easily get

$$\mathbb{E}(\Phi_t) \leq \left( 1 - \frac{189}{1600(n-1)} \right)^t \mathbb{E}(\Phi_0)$$

Let  $\tau$  be defined by

$$\tau = \frac{1600(n-1)}{189} (\ln n - \ln \delta - 4 \ln 2 + \ln 3).$$

We then have

$$\left( 1 - \frac{189}{1600(n-1)} \right)^t \leq e^{-189t/(1600(n-1))} \leq e^{-189\tau/(1600(n-1))} = \frac{16\delta}{3n}.$$

Using the Markov inequality and Relation (22), which gives  $\mathbb{E}(\Phi_0) \leq 3n/4$ , we obtain

$$\mathbb{P}\{\Phi_t \geq 4\} \leq \frac{\mathbb{E}(\Phi_t)}{4} \leq \frac{\left( \frac{16\delta}{3n} \right) \left( \frac{3n}{16} \right)}{23} = \delta.$$



By definition of  $\Phi_t$ , we have  $\Phi_t \neq 0 \iff \Phi_t \geq 4$ . Using moreover the fact that  $|\lambda| < 1/2$ , we have

$$\begin{aligned}
\Phi_t = 0 &\implies \alpha_{t,k} = 0, \text{ for every } k \in H_t \\
&\implies -1 \leq C_t^{(i)} - \ell + \lambda \leq 1, \text{ for every } i = 1, \dots, n \\
&\implies -1 - \lambda \leq C_t^{(i)} - \ell \leq 1 - \lambda, \text{ for every } i = 1, \dots, n \\
&\implies -3/2 < C_t^{(i)} - \ell < 3/2, \text{ for every } i = 1, \dots, n \\
&\implies \|C_t^{(i)} - \ell\|_\infty < 3/2.
\end{aligned}$$

This leads to

$$\|C_t^{(i)} - L\|_\infty \geq 3/2 \implies \Phi_t \neq 0 \iff \Phi_t \geq 4,$$

that is

$$\mathbb{P}\{\|C_t^{(i)} - \ell\|_\infty \geq 3/2\} \leq \mathbb{P}\{\Phi_t \neq 0\} = \mathbb{P}\{\Phi_t \geq 4\} \leq \delta,$$

which completes the proof. ■