

# Almost logarithmic-time space optimal leader election in population protocols

Leszek Gąsieniec<sup>1</sup>, Grzegorz Stachowiak<sup>2</sup>, and Przemysław Uznański<sup>3</sup>

<sup>1</sup>University of Liverpool, UK

<sup>2</sup>University of Wrocław, Poland

<sup>3</sup>ETH Zürich, Switzerland

## Abstract

The model of population protocols refers to a large collection of simple indistinguishable entities, frequently called *agents*. The agents communicate and perform computation through pairwise interactions. We study fast and space efficient leader election in population of cardinality  $n$  governed by a random scheduler, where during each time step the scheduler uniformly at random selects for interaction exactly one pair of agents.

We propose the first  $o(\log^2 n)$ -time leader election protocol. Our solution operates in expected parallel time  $\mathcal{O}(\log n \log \log n)$  which is equivalent to  $\mathcal{O}(n \log n \log \log n)$  pairwise interactions. This is the fastest currently known leader election algorithm in which each agent utilises asymptotically optimal number of  $\mathcal{O}(\log \log n)$  states. The new protocol incorporates and amalgamates successfully the power of assorted *synthetic coins* with variable rate *phase clocks*.

# 1 Introduction

The computational model of *population protocols* was introduced in the seminal paper by Angluin *et al.* [AAD<sup>+</sup>04]. Their model provides a universal platform for the formal analysis of pairwise interactions within a large collection of indistinguishable entities, frequently referred to as *agents*. In this model the agents rely on very limited communication and computation power. The actions of agents are prompted by their pairwise interactions with the outcome determined by a finite state machine  $\mathcal{F}$ . When two agents engage in an interaction they mutually examine the content of their local states, and on the conclusion of this encounter their states change according to the transition function forming an integral part of  $\mathcal{F}$ . A population protocol terminates with success when eventually all agents stabilise w.r.t. the output (which depends only on their states).

The number of states utilised by the finite state machine  $\mathcal{F}$  constitutes the *space complexity* of the protocol. In the *probabilistic variant* of population protocols, introduced in [AAD<sup>+</sup>04] and used in this paper, in each step the interacting pair of agents is chosen uniformly at random by the *random scheduler*. In this variant one is also interested in the *time complexity*, i.e., the time needed to stabilise (converge) the protocol. More recently the studies on population protocols focus on performance in terms of *parallel time* defined as the total number of pairwise interactions (leading to stabilisation) divided by the size of the population. The parallel time can be also interpreted as the local time observed by agents proportional to the number of interactions it participates in.

Populations protocols attracted studies on several central problems in distributed computing. This includes work on *majority* problem, a special instance of *consensus* [Fis83], in which the final configuration of states reflects the unique colour of the larger fraction of the population. The majority problem was first posed in the context of population protocols in [AAD<sup>+</sup>04] and later a 3-state one-way protocol for approximate majority was given in [AAE08]. In more recent work [AGV15] Alistarh *et al.* consider time-precision trade-offs in exact majority population protocols. Further studies on time-space trade-offs can be found in [AAE<sup>+</sup>17, BCER17] and [AAG18], where in the latter an asymptotically space-optimal protocol is given. The convergence (stabilisation) of majority protocols was also studied in more specific network topologies [DV12, MNRS14, GHMS15], as well as in the deterministic setting [MNRS14, GHM<sup>+</sup>16]. A nice survey on a range of combinatorial problems suitable for population protocols can be found in [MCS11].

In this paper the focus is on leader election where in the final configuration a unique agent must converge to a *leader state* and every other agent has to stabilise in a *follower state*. While the problem is quite well understood and covered in the literature it received greater attention in the context of population protocols only recently, partly due to several developments in a related model of chemical reactions [CCDS14, Dot14]. In particular, the work of Doty and Soloveichik [DS15] led to the result that leader election cannot be solved in sublinear time when agents are equipped with a fixed (constant) number of states. On the other hand Alistarh and Gelashvili [AG15] proposed a new leader election algorithm operating in time  $\mathcal{O}(\log^3 n)$  and utilising  $\mathcal{O}(\log^3 n)$  states. In more recent work [AAE<sup>+</sup>17] Alistarh *et al.* consider a general trade-off between the number of states utilised by agents and the time complexity of the solution. They provide a separation argument distinguishing between slowly stabilising population protocols which utilise  $o(\log \log n)$  states and rapidly stabilising protocols requiring  $\Omega(\log \log n)$  states. This result coincides nicely with another fundamental observation due to Chatzigiannakis *et al.* [CMN<sup>+</sup>11] which indicates that population protocols utilising  $o(\log \log n)$  states can only cope with semi-linear predicates while the availability of  $\mathcal{O}(\log n)$  states enables computation of symmetric predicates. Another recent development includes a protocol which elects the leader in time  $\mathcal{O}(\log^2 n)$  whp and in expectation utilising  $\mathcal{O}(\log^2 n)$  states per agent [BCER17]. The number of states was later reduced to  $\mathcal{O}(\log n)$  by Berenbrink *et al.* in [BKKO18] through the application of two types of synthetic coins.

The recent progress in leader election is also aligned with improved understanding of *phase clocks* capable of counting parallel time approximately. The relevant work includes *leader-less* phase clocks adopted by Alistarh *et al.* in [AAG18] and *junta-driven* phase clocks

Paper	States	Time	Runtime guarantee
[AG15]	$\mathcal{O}(\log^3 n)$	$\mathcal{O}(\log^3 n)$ $\mathcal{O}(\log^4 n)$	expected w.h.p.
[AAE+17]	$\mathcal{O}(\log^2 n)$	$\mathcal{O}(\log^{5.3} n \cdot \log \log n)$ $\mathcal{O}(\log^{6.3} n)$	expected w.h.p.
[BCER17]	$\mathcal{O}(\log^2 n)$	$\mathcal{O}(\log^2 n)$	w.h.p.
[AAG18]	$\mathcal{O}(\log n)$	$\mathcal{O}(\log^2 n)$	expected
[BKKO18]	$\mathcal{O}(\log n)$	$\mathcal{O}(\log^2 n)$	w.h.p.
[GS18]	$\mathcal{O}(\log \log n)$	$\mathcal{O}(\log^2 n)$	w.h.p.
This work	$\mathcal{O}(\log \log n)$	$\mathcal{O}(\log n \cdot \log \log n)$	expected

Table 1: Recent progress in leader election via population protocols.

utilised in the fastest currently known space-optimal leader election algorithm operating in time  $\mathcal{O}(\log^2 n)$ -time due to Gąsieniec and Stachowiak [GS18]. The concept of phase clocks is also closely related to *oscillators* which are used to model behaviour of periodic dynamic systems. An interesting study of 3-state oscillators can be found in Czyzowicz *et al.* [CGK<sup>+</sup>15] and the follow up work by Dudek and Kosowski [DK18].

**Our results** In this paper we propose the first leader election protocol which operates in time  $o(\log^2 n)$  and in addition utilises the minimum number of states by each agent. In particular, we propose a new protocol which operates in time  $\mathcal{O}(\log n \log \log n)$  with each agent’s operating space limited to  $\mathcal{O}(\log \log n)$  states. The solution is always correct, however the improved time performance refers to the expected time, i.e., we can guarantee the high probability only in time  $\mathcal{O}(\log^2 n)$  as in [GS18].

The new algorithm utilises partition of the original population into three sub-populations including *coins* (C) responsible for generation of asymmetric coins with  $\log \log n$  different bias levels, *leaders* (L) among which the unique leader is eventually drawn, and *inhibitors* (I) delegated to maintain variable-rate phase clocks.

Note that due to space limitation all proofs are located in Appendix A.

**Related work** Leader election is one of the fundamental problems in Distributed Computing besides broadcasting, mutual-exclusion, consensus, see, e.g., an excellent text book by Attiya and Welch [AW04]. The problem was originally studied in networks with nodes having distinct labels [Lan77], where an early work focuses on the ring topology in synchronous [FL87, HS80] as well as in asynchronous models [Bur80, Pet82]. Also, in networks populated by mobile agents the leader election was studied first in networks with labelled nodes [HKM<sup>+</sup>08]. However, very often leader election is used as a powerful symmetry breaking mechanism enabling feasibility and coordination of more complex protocols in systems based on uniform (indistinguishable) entities. There is a large volume of work [Ang80, ASW88, AS91, BSV<sup>+</sup>96, BV99, YK89, YK96] on leader election in anonymous networks. In [YK89, YK96] we find a good characterisation of message-passing networks in which leader election is feasible when the nodes are anonymous. In [YK89], the authors study the problem of leader election in general networks under the assumption that node labels are not unique. In [FKK<sup>+</sup>04], the authors study feasibility and message complexity of leader election in rings with possibly non-unique labels, while in [DP04] the authors provide solutions to a generalised leader election problem in rings with arbitrary labels. The work in [FP11] focuses on the time complexity of leader election in anonymous networks where this complexity is expressed in terms of multiple network parameters. In [DP14], the authors study feasibility of leader election for anonymous agents that navigate in a network asynchronously. Another important study on trade-offs between the time complexity and knowledge available in anonymous trees can be found in recent work of Glacet *et al.* [GMP16].

Finally, a good example of recent extensive studies on the exact space complexity in related models refers to plurality consensus. In particular, in [BFGK16] Berenbrink *et al.* proposed a plurality consensus protocol for  $C$  original opinions converging in  $\mathcal{O}(\log C \log \log n)$  synchronous rounds using only  $\log C + \mathcal{O}(\log \log C)$  bits of local memory. They also show a slightly slower solution converging in  $\mathcal{O}(\log n \log \log n)$  rounds utilising only  $\log C + 4$  bits of the local memory. This disproved the conjecture by Becchetti *et al.* [BCN<sup>+</sup>15] and indicated that any protocol with local memory  $\log C + \mathcal{O}(1)$  has the worst-case running time  $\Omega(k)$ . In [GP16] Ghaffari and Parter propose an alternative algorithm converging in time  $\mathcal{O}(\log C \log n)$  in which all messages and the local memory are bounded to  $\log C + \mathcal{O}(1)$  bits. In addition, some work on the application of the random walk in plurality consensus protocols can be found in [BCN<sup>+</sup>15, GHMS15].

## 2 Preliminaries

In this paper we study population protocols defined on populations of agents of size  $n$  in which the *random scheduler* connects sequentially (or in parallel) pairs of agents uniformly at random. The agents are identical and the protocol assumes all agents start in the same initial state. Our protocol utilises the classical model of population protocols [AAD<sup>+</sup>04, AAE08] in which each interaction refers to an ordered pair of agents (responder, initiator). The interaction triggers an update of states in both agents according to some predefined deterministic *transition function*. We focus on two complexity measures including *space complexity* defined as the *number of states* utilised by each agent, and *time complexity* reflecting the number of interactions required to stabilise the population protocol. We also consider *parallel time* defined as the total number of interactions divided by the size of the population. This time measure can be also seen as the local time observed by an agent, i.e., the number of pairwise interactions in which the agent is involved in. We aim at protocols formed of  $\mathcal{O}(n \cdot \text{poly } \log n)$  interactions equivalent to the parallel running time  $\mathcal{O}(\text{poly } \log n)$ .

In order to maintain clarity of presentation we assume that each state has a name drawn from either a fixed size set of suitable names or a small range of integer values. However, when it is clear from the context we tend to omit the name of this field. Moreover, since each node belongs to exactly one of 3 sub-populations, for simplicity we shorten the notation omitting the part *role =* and writing for example  $C\langle \dots \rangle$  instead of  $\langle \text{role} = C, \dots \rangle$ . This notation allows us to refer only to the relevant fields, i.e., those affected during one particular type of interaction. One should keep in mind also that interactions may trigger several non-conflicting rules. For example, rules of transition of clocks happen in parallel to the rules of transition of coins.

Consider an event  $X$ , and let  $\eta > 0$  be some predefined constant. We say that an event occurs with *negligible* probability, if there is an integer  $n_0$ , s.t., the probability of this event for  $n > n_0$  is at most  $n^{-\eta}$ . An event occurs *with high probability* (whp) if its probability is at least  $1 - n^{-\eta}$  for  $n > n_0$ . If the event refers to a behaviour of an algorithm, we say it occurs with high probability if the constants used in the algorithm can be fine-tuned so that the probability of this event is at least  $1 - n^{-\eta}$ . Analogously an event  $X$  occurs *with very high probability* (wvhp) if for any  $a > 0$  there exists an integer  $n_a$  such that event  $X$  occurs with probability is at least  $1 - n^{-a}$  for  $n > n_a$ . In particular if an event occurs with probability  $1 - \exp(-\log^{1+\epsilon} n)$  for some  $\epsilon > 0$ , it occurs with very high probability.

## 3 Phase clock

The actions of our leader election protocol are coordinated by a phase clock utilising junta of clock leaders. A similar approach can be found in [GS18]. The junta leaders are drawn from sub-population *coins* denoted by  $C$ . With the help of the phase clock every agent in  $C$  keeps track of *phase*  $\in \{0, 1, \dots, \Gamma - 1\}$ , for a suitable large constant  $\Gamma$ , and maintains its

$\text{timemode} \in \{\text{injunta}, \text{follower}\}$ . Let  $+_{\Gamma}$  denote addition modulo  $\Gamma$  and

$$\max_{\Gamma}(x, y) = \begin{cases} \max(x, y) & \text{if } |x - y| \leq \Gamma/2, \\ \min(x, y) & \text{if } |x - y| > \Gamma/2. \end{cases}$$

The transition rules of interaction with respect to the phase clock include:

$$\langle \text{follower}, \text{phase} = t_1 \rangle + \langle \text{follower}, \text{phase} = t_2 \rangle \rightarrow \langle \text{follower}, \text{phase} = t_1 \rangle + \langle \text{follower}, \text{phase} = T_1 \rangle$$

$$\langle \text{injunta}, \text{phase} = t_1 \rangle + \langle \text{follower}, \text{phase} = t_2 \rangle \rightarrow \langle \text{injunta}, \text{phase} = t_1 \rangle + \langle \text{follower}, \text{phase} = T_2 \rangle,$$

where  $T_1 = \max_{\Gamma}(t_1, t_2)$  and  $T_2 = \max_{\Gamma}(t_1, t_2 + \Gamma/2)$ . Every agent is initialised to  $\langle \text{follower}, \text{phase} = 0 \rangle$ . During execution of coin preprocessing protocol, see Section 5, some agents in  $C$  become *junta members*. We say that the phase clock *passes through 0* whenever its current phase  $x$  of the clock is reduced in absolute terms. We denote this transition by  $\xrightarrow{0}$ .

**Definition 3.1** (c.f., [GS18]). *The passes through 0 of agents  $a$  and  $b$  are equivalent if they both occur in a period when the respective agent's clock phases  $x_a$  and  $x_b$  satisfy  $3\Gamma/4 <_{\Gamma} x_a, x_b <_{\Gamma} \Gamma/4$ .*

**Theorem 3.2** (c.f., Theorem 3.1 and Fact 3.1 in [GS18]). *For any constant  $\varepsilon, \eta, d > 0$ , there exists a constant  $\Gamma$ , s.t., if the number of junta members is at most  $n^{1-\varepsilon}$  at any time whp  $1 - n^{-\eta}$ , the following conditions are satisfied whp until each agent completes  $n^{\eta}$  passes through 0:*

- *All passes through 0 form equivalence classes for all agents and the number of interactions between the closest passes through 0 in different equivalence classes is at least  $d \cdot n \log n$ .*
- *The number of interactions between two subsequent passes through 0 in any agent is  $\mathcal{O}(n \log n)$ .*

By Theorem 3.2, the rounds for different agents form equivalence classes whp that are referred to as *rounds of the protocol*. The *updated* agent is the one which acts as responder during the relevant interaction. Interactions with both start- and end-phase in  $\{0, 1, \dots, \Gamma/2 - 1\}$  are denoted by  $\xrightarrow{\text{early}}$  and those with start- and end-phase in  $\{\Gamma/2, \dots, \Gamma - 1\}$  are denoted by  $\xrightarrow{\text{late}}$ . Finally, applying Theorem 3.2 and with  $\Gamma$  being twice as big as required by Theorem 3.2, we can guarantee that passes through 0 and through  $\Gamma/2$  form strictly separate equivalence classes.

## 4 High level description

An execution of our algorithm consists of three consecutive epochs whp. These include the *initialisation* epoch, the *fast elimination* epoch and the *final elimination* epoch. For the case when any epoch fails, which happens with negligible probability, we use as backup the slow leader election protocol working in time  $\mathcal{O}(n \log n)$  [AAE08]. During the initialisation epoch the whole population is divided into sub-populations, where the descriptor role  $\in \{C, I, L\}$  differentiates agents between the three sub-populations of *coins*, *inhibitors* and *leaders* respectively. At the start of the protocol all agents are subject to symmetry breaking rules. Each agent gets assigned to one of the three roles (or gets deactivated), and this role is never changed. The two symmetry breaking rules adopted during the initial partition process are as follows:

$$0 + 0 \rightarrow X + L, \quad X + X \rightarrow C + I, \quad (1)$$

where 0 describes an agent before initialisations, and  $X$  refers to an intermediate stage before entering sub-population  $C$  or  $I$ .

During the initialisation epoch a *junta* of size at most  $n^{0.77}$  is elected from  $C$  whp, which allows to start the phase clock using this junta as clock leaders. This phase clock synchronises

all actions of our algorithm until it concludes. In our approach it is important to terminate the initialisation epoch and in turn to stabilise the roles of agents in time  $\mathcal{O}(\log n)$ . With this in mind we adopt two extra rules, s.t., whenever a node in state 0 or X reaches the end of the first round, it deactivates itself:

$$0 + \star \xrightarrow{0} D + \star, \quad X + \star \xrightarrow{0} D + \star, \quad (2)$$

where D denotes *deactivated* agents that, except for passing clock state, do not play any meaningful role in the leader election protocol.

**Lemma 4.1.** *With high probability, only  $\mathcal{O}(n/\log n)$  agents are not initialised in the course of the protocol, i.e.,  $n - \mathcal{O}(n/\log n)$  agents join C, I or L during the first  $\mathcal{O}(n \log n)$  interactions.*

*Proof.* By Theorem 3.2, the first round of the phase clock is completed with high probability during the first  $d \cdot n \log n$  interactions, for some constant  $d$ . We first show that after  $4 \cdot n \log n$  interactions at most  $n/\log n$  not yet initialised in state 0 agents remain. Let  $\mathcal{X}$  be the random variable denoting the number of agents in state 0.

Assume  $\mathcal{X} = \alpha n$ , for some  $\alpha > 0$ . We prove that the number of interactions it takes to reduce  $\mathcal{X}$  by a factor of 2 is at most  $4n/\alpha$ , with very high probability. Let  $\sigma$  be a 0-1 sequence of length  $4n/\alpha$  referring to the relevant  $4n/\alpha$  interactions. In this sequence an entry is set to 1 if during the corresponding interaction the number of not yet initialised agents is reduced, and 0 otherwise. For as long as  $\mathcal{X} > \alpha n/2$ , the probability of having 1 at each position in  $\sigma$  is at least  $\alpha^2/4$  and in turn the expected number of 1s in  $\sigma$  is at least  $\alpha n$ . Thus by Chernoff bound the number of 1s in  $\sigma$  is at least  $\alpha n/2$  with very high probability. This implies that at least  $\alpha n/2$  agents in state 0 get initialised. And iterating this process  $\log \log n$  times we get reduction of agents in state 0 to  $n/\log n$  in at most  $\mathcal{O}(n \log n)$  consecutive interactions. A similar reasoning can be used for agents in the intermediate state X in the next (subsequent to reduction of agents in state 0)  $\mathcal{O}(n \log n)$  interactions. Thus one can conclude that after  $\mathcal{O}(n \log n)$  initial interactions the number of not yet initialised agents is at most  $2n/\log n$ .  $\square$

Using Lemma 4.1 one can immediately conclude that during the first round all  $\mathcal{O}(n/\log n)$  not initialised agents, i.e., those not given roles C, L or I, become deactivated with high probability by rule (2). Below we explain functionality of the three adopted sub-populations.

**Coin** Agents in this group differentiate themselves into non-empty levels  $0, 1, 2, \dots, \Phi$ , where  $\Phi = \log \log n - 3$ . The number of agents on level  $\Phi$  is at most  $n^{0.77}$  and these agents form the junta running the phase clock. The levels are also used to simulate  $\Phi + 1$  types of asymmetric coins, s.t., if the probability of drawing heads by  $\ell$ -th coin is  $q$  the probability of drawing heads by  $(\ell + 1)$ -st coin is roughly  $q^2$ . In terms of implementation, tossing  $\ell$ -th asymmetric coin is realised by an agent interacting with another agent in C. And the outcome is *heads* if this coin agent is on level  $\ell$  or higher.

**Leader** Agents in this group are leader candidates, i.e., each agent in this group has a chance to become the unique leader. In due course the number of candidates is reduced to one. The main challenge is in fast but also safe candidate elimination, i.e., we need to guarantee that our protocol does not eliminate all candidates.

**Inhibitor** Agents in this group split into  $\Psi = \Theta(\log \log n)$  distinct *levels* with level  $i$  targeting size  $\mathcal{O}(n/2^i)$ , i.e., the sizes of levels span from  $\mathcal{O}(n)$  to  $\mathcal{O}(n/\log^c n)$ , for a constant  $c > 0$ . We use level  $i$  to request returning signals with the expected response time  $2^{\mathcal{O}(i)}$  rounds. These signals are used to guide through the late elimination process when we safely reduce the number of leaders from  $\mathcal{O}(\text{poly } \log n)$  to a single one.

The first (initialisation) epoch generates at least one leader candidate and with high probability the number of candidates is almost  $n/2$ . The protocol will eventually elect a single leader among leader candidates in L during the second and the third epoch. The second epoch related to fast elimination reduces the number of elev (not rejected yet) leader

candidates to  $\mathcal{O}(\log n)$  agents in time  $\mathcal{O}(\log n \log \log n)$  both with high probability and in average sense. Fast elimination uses the sub-population  $\mathsf{C}$  to simulate assorted biased coins. The third epoch eliminates all but one competitor which becomes the unique leader. This process requires utilisation of inhibitors from  $\mathsf{I}$  to guarantee survival of at least one leader candidate. The third epoch works in  $\mathcal{O}(\log n \log \log n)$  expected time and in  $\mathcal{O}(\log^2 n)$  time with high probability.

The leader candidates elimination process during the second and the third epoch works as follows. The protocol operates in consecutive rounds, each taking time  $\mathcal{O}(\log n)$ . For each agent a round is defined as the time between two subsequent passes of the phase clock through value zero. In the first half of each round still active leader candidates flip a coin to decide whether they intend to survive (*heads*) this round or not (*tails*). If any *heads* are drawn during this round, the relevant information is distributed (via one-way epidemic [AAE08]) to all agents during the second half of the round. This results in elimination of all active candidates which drew *tails*. However, if no *heads* are drawn the round is considered *void*.

In the fast elimination process we utilise asymmetric coins implemented through interactions with agents in diverse population of  $\mathsf{C}$ . The first asymmetric coin  $\Phi$  is used 4 times to reduce the population of elev leader candidates to size at most  $n/n^{0.77}$ . Further we use each of asymmetric coins  $\Phi - 1, \Phi - 2, \dots, 1$  exactly twice. Using a biased coin with *heads* coming with probability  $q$  guarantees whp reduction of elev leader candidates by a factor close to  $q$ . On the conclusion of this process (all coins are used) the number of elev leader candidates is down to  $\mathcal{O}(\log n)$  whp.

In contrast, in the third epoch symmetric almost fair coins are used in the elimination process indefinitely. This results in elimination of all but a single leader candidate in  $\mathcal{O}(\log \log n)$  rounds. In order to guarantee that the protocol is *always* correct, i.e., we never eliminate the last alive leader candidate we use the support of agents in sub-population  $\mathsf{I}$ .

## 5 Coins

Let  $\Phi = \lfloor \log \log n \rfloor - 3$ . The states of coins, i.e., agents belonging to sub-population  $\mathsf{C}$  store the following information: *level*  $\in \{0, 1, 2, \dots, \Phi\}$ , reflecting the level of asymmetry, and *mode*  $\in \{\text{adv}, \text{stop}\}$  indicating whether a coin is still willing to increment its level. We also need an extra constant space to store the current state of the phase clock. When formed after application of split rule (1) each coin is initialized to  $\mathsf{C}\langle \text{level} = 0, \text{adv} \rangle$ .

**Coin preprocessing** In what follows we introduce the rules governing level incrementation. Note that these closely resemble the rules from *forming junta* protocol proposed in [GS18].

$$\begin{aligned} \mathsf{C}\langle \text{level} = x, \text{adv} \rangle + Y &\rightarrow \mathsf{C}\langle \text{level} = x, \text{stop} \rangle + Y, && \text{for } Y \neq \mathsf{C}, \\ \mathsf{C}\langle \text{level} = x, \text{adv} \rangle + \mathsf{C}\langle \text{level} = y \rangle &\rightarrow \mathsf{C}\langle \text{level} = x, \text{stop} \rangle + \mathsf{C}\langle \text{level} = y \rangle, && \text{for } x > y, \\ \mathsf{C}\langle \text{level} = x, \text{adv} \rangle + \mathsf{C}\langle \text{level} = y \rangle &\rightarrow \mathsf{C}\langle \text{level} = x + 1, \text{adv} \rangle + \mathsf{C}\langle \text{level} = y \rangle, && \text{for } x \leq y, x < \Phi. \end{aligned}$$

Once the level of a coin in  $\mathsf{C}$  reaches  $\Phi$  it stops growing. Moreover, we give name *injunta* to all coins which managed to reach *level* =  $\Phi$ . In order to characterise properties of coins we formulate a series of lemmas. Let  $n_{\mathsf{C}}$  be the total number of coins. By Lemma 4.1 and rules (1) and (2),  $n_{\mathsf{C}} = \frac{n}{4} - \mathcal{O}(n/\log n)$  with very high probability. Let  $C_{\ell}$  be the number of coins which reach level  $\ell$  or higher. The value of  $C_{\ell}$  depends on the execution thread of the protocol. We first observe that  $n_{\mathsf{C}} = C_0$ , and further estimates on  $C_{\ell}$ , for  $\ell > 0$  are determined by Lemmas 5.1 (upper bound) and 5.2 (lower bound).

**Lemma 5.1** (Lemma 4.2. in [GS18]). *Assume  $n^{-1/3} \leq q < 1$  and  $C_{\ell} = q \cdot n$ , then  $C_{\ell+1} \leq \frac{11}{10}q^2 \cdot n$  with very high probability.*

The lower bound argument (similar to the proof of Lemma 5.1) is given below.

**Lemma 5.2.** *Assume  $n^{-1/3} \leq q < 1$  and  $C_{\ell} = q \cdot n$ , then  $C_{\ell+1} \geq \frac{9}{20}q^2 \cdot n$  whp.*

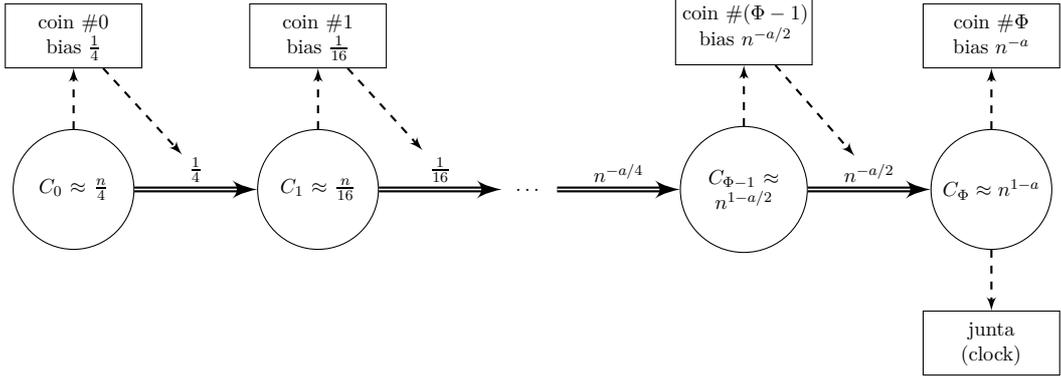


Figure 1: An idealized scheme of coin sub-populations and their relation to biased coins. In the picture  $0.23 \leq a \leq 0.55$ . Solid lines denote evolution of the population and dashed lines refer to the relevant functionality.

*Proof.* Each coin contributing to value  $C_\ell$  arrives at level  $\ell$  during some interaction  $t$ . These coins arrive sequentially. Consider  $(i+1)$ -st coin  $v$  that got to level  $\ell$ . At the time the coin arrives there are already  $i$  coins on levels  $\ell' \geq \ell$ . Consider the first interaction  $\tau$  succeeding  $t$  in which coin  $v$  acts as the responder. During this interaction the initiator is a coin on level  $\ell' \geq \ell$  with probability  $p_\tau \geq i/n$ . Thus  $v$  moves to level  $\ell+1$  with probability at least  $i/n$  as otherwise the responder would end up in state  $(\ell, 0)$  and would not contribute to  $C_{\ell+1}$ . Consider now the sequence of  $C_\ell$  such interactions  $\tau$ , in which each of  $C_\ell$  coins act as responder after getting to level  $\ell$ . We can attribute to this sequence a binary 0-1 sequence  $\sigma$  of length  $C_\ell$ , s.t., if during interaction  $\tau$  a coin ends up in state  $(\ell, 0)$ , the respective entry in  $\sigma$  becomes 0, and otherwise this entry becomes 1 (this happens with probability at least  $p_\tau$ ). The expected number of these 1s is at least  $\sum_i i/n = (C_\ell - 1)C_\ell/2n = (q^2 \cdot n - q)/2$ . And by Chernoff bound  $C_{\ell+1} < \frac{9}{20}q^2 \cdot n$  with very high probability.  $\square$

**Lemma 5.3.** For  $n$  large enough and  $\Phi = \lfloor \log \log n \rfloor - 3$  we have  $n^{0.45} \leq C_\Phi \leq n^{0.77}$  whp.

*Proof.* We start with  $9n/40 \leq n_C = C_0 \leq n/4$  with very high probability. By Lemma 5.1 and Lemma 5.2 iterated  $\ell$  times we conclude that with very high probability

$$(9/20)^{2^{\ell+1}-1} \cdot \frac{n}{2^{2^{\ell+1}}} \leq C_\ell \leq (11/10)^{2^\ell-1} \cdot \frac{n}{2^{2^{\ell+2}}}.$$

Note that if we adopt  $\Phi = \lfloor \log \log n \rfloor - 3$ , we get

$$C_\Phi \geq (9/20)^{2^{\Phi+1}} \cdot \frac{n}{2^{2^{\Phi+1}}} \geq n \cdot (9/40)^{2^{\log \log n - 2}} \geq \frac{n}{2^{2.2 \cdot 2^{\log \log n / 4}}} \geq n/n^{0.55} = n^{0.45}.$$

On the other hand

$$C_\Phi \leq (11/10)^{2^\Phi} \cdot \frac{n}{2^{2^{\Phi+2}}} \leq n \cdot (11/160)^{2^{\log \log n - 4}} \leq \frac{n}{2^{3.8 \cdot 2^{\log \log n / 16}}} \leq n/n^{0.23} = n^{0.77}. \quad \square$$

**Lemma 5.4** (Analogue of Lemma 4.5. in [GS18]). The bounds from Lemma 5.1, Lemma 5.2 and Lemma 5.3 hold after  $\mathcal{O}(n \log n)$  interactions.

*Proof. (Sketch)* In coin preprocessing protocol we need to stabilise first sub-population of coins in time  $\mathcal{O}(\log n)$ . The time complexity analysis of the remaining part of the protocol is analogous to the one used in forming junta protocol in [GS18].  $\square$

## 6 Fast elimination

The goal in fast elimination epoch is to reduce the number of active leader candidates to  $\mathcal{O}(\log n)$  whp. We also guarantee that at least one agent remains in the group of active leaders **A** whp. All other leader candidates join group **P** of passive agents.

The state of each leader candidate in this epoch consists of:  $\text{cnt} \in \{0, 1, \dots, 2\Phi + 3\}$ ,  $\text{leadermode} \in \{\mathbf{A}, \mathbf{P}, \mathbf{W}\}$  (in fast elimination **W** standing for withdrawn from leader election process is not used),  $\text{flip} \in \{\text{none}, \text{heads}, \text{tails}\}$ ,  $\text{void} \in \{\text{true}, \text{false}\}$  (telling whether the round is void), and a constant number of phase clock values. Each leader candidate is initialised at the beginning of the first round of the second epoch to  $L\langle \text{cnt} = 2\Phi + 3, \mathbf{A}, \text{none}, \text{void} = \text{true} \rangle$ .

After the first round of the phase clock, when the roles of all agents are fixed and levels of all coins are computed whp, agents enter the fast elimination epoch. This is ensured by starting the counter at one larger than the intended number of coin uses. At the beginning of the fast elimination all leader candidates are active (**A**). In fast elimination we use the sub-population **C** of coins as the source of  $\Phi$  different types of asymmetric coins. The coin result is generated, when a leader candidate interacts with another agent acting as the responder. The outcome of using  $\ell$ -th biased coin is *heads* when the interaction refers to a coin on level at least  $\ell$ , and *tails* otherwise. When  $C_\ell = q \cdot n$ , the probability of drawing *heads* at this level is  $q$ . Thus when there are substantially more than  $1/q$  active leader candidates almost certainly at least one of them has to draw *heads*. In turn the number of active leader candidates will be reduced by factor of  $1/q$  in expectation. On the other hand, if the number of active leader candidates does not exceed  $1/q$ , no agent may draw *heads*. In order to have good understanding of the situation the agents with *heads* drawn inform others (using one-way epidemic) about this fact. Thus if an agent draws *tails* and receives a message about other agent(s) having *heads*, it can safely become passive (**P**). This elimination cycle can be carried in one round in time  $\mathcal{O}(\log n)$ .

During fast elimination active leader candidates utilise coins, s.t., each coin  $1, 2, \dots, \Phi - 2, \Phi - 1$  is used exactly twice and coin  $\Phi$  is applied four times. In other words, the elimination process can be represented by a sequence  $(\gamma)_1^{2\Phi+2} = [1, 1, 2, 2, \dots, \Phi - 1, \Phi - 1, \Phi, \Phi, \Phi, \Phi]$  which tells us which coin level is used with what  $\text{cnt}$  value. In total, the elimination process operates in  $\mathcal{O}(\log \log n)$  rounds translating to time  $\mathcal{O}(\log n \log \log n)$ . We are also able to guarantee reduction of the number of remaining active leader candidates to  $\mathcal{O}(\log n)$  whp.

The following transitions are used in the second epoch. When the phase clock passes through zero we have

$$L\langle \text{cnt} = x \rangle + \star \xrightarrow{0} L\langle \text{cnt} = x - 1, \text{none}, \text{void} = \text{true} \rangle + \star, \quad \text{for } x \geq 1. \quad (3)$$

When  $x = 1$ , at the end of the round we move to the third epoch. Otherwise, in the first half of the round application of the coin from the current level  $\gamma(x)$  is guaranteed whp, for all active leader candidates. For  $x \neq 2\Phi + 3$ :

$$L\langle \mathbf{A}, \text{cnt} = x, \text{none} \rangle + C\langle \text{level} = y \rangle \xrightarrow{\text{early}} L\langle \mathbf{A}, \text{cnt} = x, \text{heads}, \text{void} = \text{false} \rangle + C\langle \text{level} = y \rangle, \quad (4)$$

$$L\langle \mathbf{A}, \text{cnt} = x, \text{none} \rangle + C\langle \text{level} = y \rangle \xrightarrow{\text{early}} L\langle \mathbf{A}, \text{cnt} = x, \text{tails} \rangle + C\langle \text{level} = y \rangle, \quad (5)$$

when  $\gamma(x) \leq y$  and  $\gamma(x) > y$  respectively.

In the second half of the round the broadcast (via one-way epidemic) informing about drawn *heads* is performed as follows

$$L\langle \mathbf{A}, \text{tails}, \text{void} = \text{true} \rangle + L\langle \text{void} = \text{false} \rangle \xrightarrow{\text{late}} L\langle \mathbf{P}, \text{tails}, \text{void} = \text{false} \rangle + L\langle \text{void} = \text{false} \rangle, \quad (6)$$

$$L\langle \text{void} = \text{true} \rangle + L\langle \text{void} = \text{false} \rangle \xrightarrow{\text{late}} L\langle \text{void} = \text{false} \rangle + L\langle \text{void} = \text{false} \rangle. \quad (7)$$

The following lemmas guarantee the correctness of the second epoch whp.

**Lemma 6.1.** *There exists a constant  $c > 0$ , s.t., for any  $q < 1$  when  $N \geq c \log n / q$  agents toss an asymmetric coin resulting in heads with probability  $q$ , the following holds:*

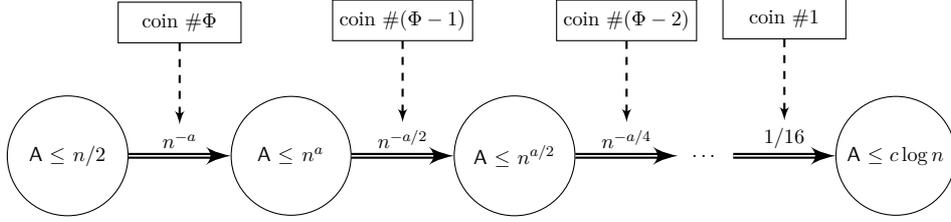


Figure 2: An idealised scheme of the fast elimination process.

1. none of the agents draws heads with a negligible probability, and
2. more than  $2q \cdot N$  agents draw heads with a negligible probability.

*Proof.* The probability that all agents draw *tails* is at most  $(1 - q)^{c \log n / q} \leq e^{-c \log n} = n^{-c}$ . The expected number of agents which draw *heads* is  $q \cdot N \geq c \log n$ . By Chernoff bound the probability that more than  $2q \cdot N$  agents draw *heads* is smaller than  $e^{-Nq} \leq n^{-c}$ .  $\square$

**Lemma 6.2.** *Applying coin (from level)  $\Phi$  four times and then coins  $\Phi - 1, \Phi - 2, \dots, \ell + 1, \ell$  twice reduces the number of active leader candidates to at most  $c \log n / q$ , where  $q$  is the probability of tossing heads by coin  $\ell \geq 1$ .*

*Proof.* Induction is on  $\ell$ . In the base case when  $\ell = \Phi$  we apply coin  $\Phi$  four times. By Lemma 5.3 we have  $q \geq n^{-0.23}$ . So applying this coin four times gives reduction of the number of active leader candidates to at most  $\max\{16n \cdot n^{-4 \cdot 0.23}, c \log n / q\} = c \log n / q$  whp.

Now assume the thesis holds for level  $\ell + 1$  and we prove it for  $\ell$ . By inductive hypothesis and Lemma 5.2, after application of coin  $\ell + 1$  twice there are at most  $c \log n / q' \leq 20c \log n / 9q^2$  active leader candidates ( $q'$  is the counterpart of  $q$  at level  $\ell + 1$ ). Applying this coin twice gives further reduction of active leader candidates to at most  $\max\{80c \log n / 9, c \log n / q\} = c \log n / q$  whp.  $\square$

## 7 Final elimination

The protocol executes  $\Theta(\log \log n)$  rounds of fast elimination (applying coins from level  $\Phi$  down to 1) with  $\mathcal{O}(\log n)$  active leaders left whp. All other leader candidates become passive. In order to finalize leader election we utilise coin (from level) 0. However we target construction of Las Vegas type algorithm which always elects exactly one leader. In order to guarantee this we continue using leader modes A (active), P (passive) and W (withdrawn). In contrast to withdrawn candidates, active and passive candidates may still become the unique leader. We use a joint term *alive* candidates for these two groups.

All alive candidates keep track of a the counter **drag** which is increasing during the final elimination epoch. However, only active candidates can increment this counter. If a passive candidate detects an increase of the counter value it transitions to withdrawn state. This is safe because there must have been an active candidate with a higher **drag** value. In other words, we guarantee that not all alive candidates transition into withdrawn state. As the required number of rounds can be relatively large (i.e., as big as  $\log n$ ), due to space limitation we cannot use **drag** counter explicitly as the counter of rounds. Instead, we will use a counter with  $\Theta(\log \log n)$  states. This counter will have the  $i$ -th incrementation roughly during round  $c \cdot 4^i$  (for some constant  $c$ ) of final elimination. This process will rely on inhibitor agents (I) preprocessed at the same time as coins (C).

**Preprocessing:** Preprocessing begins with the first pass through 0 of the phase clock. Inhibitor agents keep track of  $\text{drag} \in \{0, 1, \dots, \Psi\}$ ,  $\text{mode} \in \{\text{adv}, \text{stop}\}$  (flag whether agent is *advancing* or *stopped*) and elevation  $\text{elev} \in \{\text{low}, \text{high}\}$ . The agents are initialized to  $l(\text{drag} =$

$0, \text{adv}, \text{low}\rangle$ , and drag counts how many subsequent successful coin flips they managed to obtain.

$$\begin{aligned} \mathbb{I}\langle \text{drag} = x, \text{adv} \rangle + Y &\xrightarrow{\text{late}} \mathbb{I}\langle \text{drag} = x + 1, \text{adv} \rangle + Y, & \text{for } Y \neq \mathbb{C}, \\ \mathbb{I}\langle \text{drag} = x, \text{adv} \rangle + \mathbb{C} &\xrightarrow{\text{late}} \mathbb{I}\langle \text{drag} = x, \text{stop} \rangle + \mathbb{C}. \end{aligned}$$

We denote by  $n_I$  the total number of inhibitor agents in  $\mathbb{I}$ . By Lemma 4.1,  $n_I = n/4 - \mathcal{O}(n/\log n)$ . Let  $D_\ell$  be the number of agents that reach **drag**  $\ell$ .

**Lemma 7.1.** *After the first round of the clock  $D_\ell = n4^{-\ell}(1 \pm o(1))$  whp.*

*Proof.* Let  $D'_\ell = D_\ell + \dots + D_\Psi$  be the number of inhibitor agents reaching slowness  $\ell$  or higher and  $p = \frac{n_c}{n}$  be the ratio of coins in the population. By Lemma 4.1 after  $\mathcal{O}(n \log n)$  interactions of the first round  $p = \frac{1}{4} - \mathcal{O}(1/\log n)$  and remains stable with high probability. An inhibitor agent reaches level  $\ell$  by a series of  $\ell$  successful synthetic coin flips, which happens with probability  $p^\ell = 4^{-\ell}(1 - \ell \cdot \mathcal{O}(1/\log n))$ . By Chernoff bound we have  $D'_\ell = n_I \cdot p^\ell \pm \mathcal{O}(\sqrt{p^\ell \cdot n_I \log n_I})$ , with high probability. We have  $\ell = \mathcal{O}(\log \log n)$ ,  $n_I = \Theta(n)$  and  $D_\ell = D'_\ell - D'_{\ell+1}$ , for  $\ell < \Psi$  and  $D_\Psi = D'_\Psi$ . Thus there exists  $D'_\ell = 4^{-\ell} \cdot n \cdot (1 \pm o(1))$  and the claimed bound holds.

In addition, we observe that with high probability during the initial  $\Theta(n \log n)$  interactions each inhibitor agent experiences  $\Omega(\log n)$  interactions with coin agents, determining its **drag** during the second round of the clock.  $\square$

**Slowed-down inhibitor communication:** Inhibitor agents get activated through interaction with leader agents which reached the appropriate **drag** value, and this communication is done via one-way epidemic (between inhibitors of the same **drag**), i.e.

$$\begin{aligned} \mathbb{I}\langle \text{drag} = x, \text{stop}, \text{low} \rangle + \mathbb{L}\langle \mathbb{A}, \text{drag} = x \rangle &\rightarrow \mathbb{I}\langle \text{drag} = x, \text{stop}, \text{high} \rangle + \mathbb{L}\langle \mathbb{A}, \text{drag} = x \rangle, & (8) \\ \mathbb{I}\langle \text{drag} = x, \star \rangle + \mathbb{I}\langle \text{drag} = x, \text{high} \rangle &\rightarrow \mathbb{I}\langle \text{drag} = x, \text{high} \rangle + \mathbb{I}\langle \text{drag} = x, \text{high} \rangle. \end{aligned}$$

**Safe withdrawal:** All active leader candidates with **drag**  $> 0$  are subject to coin-flipping rules (4) and (5). More precisely, in the first half of the round each of them draws the coin from level 0 whp. As rules (6) and (7) apply to agents with coin-flips resulting in success inform (via one-way epidemic) other agents accordingly.

We give below an updated reset rule (analogue of (3)) observing that this rule does not change the **drag** value, and updated rules for leaders:

$$\begin{aligned} \mathbb{L}\langle \star, \text{void} = \star \rangle + \star &\xrightarrow{0} \mathbb{L}\langle \text{none}, \text{void} = \text{false} \rangle + \star, \\ \mathbb{L}\langle \star, \text{drag} = x \rangle + \mathbb{L}\langle \text{drag} = y \rangle &\rightarrow \mathbb{L}\langle \mathbb{W}, \text{drag} = y \rangle + \mathbb{L}\langle \text{drag} = y \rangle, & \text{for } x < y, & (9) \end{aligned}$$

$$\mathbb{L}\langle \mathbb{A}, \text{heads}, \text{drag} = x \rangle + \mathbb{I}\langle \text{drag} = x, \text{high} \rangle \rightarrow \mathbb{L}\langle \mathbb{A}, \text{heads}, \text{drag} = x + 1 \rangle + \mathbb{I}\langle \text{drag} = x, \text{high} \rangle. \quad (10)$$

Let  $A \leq c \log n$  be the number of active leaders with **drag**  $= \ell$ . Let  $T_\ell$  be a random variable denoting the number of interactions between the first occurrence of an active leader candidate with **drag**  $= \ell$  and the first occurrence of an active leader candidate with **drag**  $= \ell + 1$ .

**Lemma 7.2.** *There exist constants  $c_1, c_2 > 0$  such that for  $\ell \leq \Psi$  we have  $\Pr[T_\ell \leq c_1 4^\ell n \log n] \leq n^{-0.5}$  and whp  $T_\ell \leq c_2 4^\ell n \log n$ .*

*Proof.* Consider the first interaction  $t$  in which a leader candidate assumes **drag**  $= \ell$ . We are to prove inequalities on the number of interactions  $T_\ell$  till the first interaction  $t'$  in which a leader candidate assumes **drag**  $= \ell + 1$ .

We start with the first inequality, which is in fact a lower bound on  $T_\ell$ . When the first leader with **drag**  $= \ell$  occurs it starts propagation (via one-way epidemic) of state **high**

amongst inhibitors with  $\mathbf{drag} = \ell$ . In the context of the lower bound argument, we can consider a situation in which  $A \leq c \log n$  informed agents spread rumour to  $D_\ell$  uninformed agents in the population. By Lemma 7.1  $D_\ell = \Theta(n/4^\ell)$ . We observe the following. If the informed part of population is of size  $x$ , then a single interaction increments this size with probability approximately  $\frac{D_\ell}{n} \cdot \frac{x}{n} = 4^{-\ell} \cdot \frac{x}{n} (1 \pm o(1))$ . Thus, when  $A < x < 1/2 \cdot D_\ell$  it takes  $\Theta(n \cdot 4^\ell)$  interactions to go from  $x$  informed agents to  $2x$ , with high probability (which follows from Chernoff bound). So it takes  $\Theta(4^\ell n \log n)$  interactions, i.e., more than  $c_1 4^\ell n \log n$  for some  $c_1 > 0$ , to reach the sub-population of inhibitors that are high with  $\mathbf{drag} = \ell$  of cardinality  $n^{0.4}$ . During this time the probability of having an interaction incrementing value  $\mathbf{drag}$  to  $\ell + 1$  is  $\Theta(4^\ell n^{-0.6} \log^2 n)$ . For  $n$  large enough this probability is smaller than  $n^{-0.5}$ .

With respect to the upper bound, consider the same communication process. Observe that if a single inhibitor with  $\mathbf{drag} = \ell$  gets high, all inhibitors with  $\mathbf{drag} = \ell$  get high in  $\mathcal{O}(4^\ell n \log n)$  subsequent interactions, with high probability. In further  $\mathcal{O}(4^\ell n \log n)$  interactions some active leader with  $\mathbf{drag} = \ell$  interacts with one of these inhibitors whp. Thus there is a constant  $c_2 > 0$  such that  $T_\ell \leq c_2 4^\ell n \log n$  whp.  $\square$

We now establish the bound on time the protocol requires to elect a single leader whp. Recall that at the beginning of the third epoch, there are at most  $c \log n$  active leaders.

**Lemma 7.3.** *Assume that the preprocessing, the phase clock and coin propagations work properly. After  $\mathcal{O}(\log \log n)$  rounds in expectation and  $\mathcal{O}(\log n)$  rounds with high probability the number of active leaders is reduced from  $c \log n$  to 1.*

*Proof.* Consider a sequence  $F_0, F_1, \dots, F_i$  referring to the number of active leaders after  $i$  rounds of elimination. Let  $B$  be the number of rounds needed to obtain a single active leaders, that is  $B = \min\{i : F_i = 1\}$ . Let  $F'_i$  be as follows: for  $i \leq B$ ,  $F'_i = F_i$  and otherwise  $F'_i = (5/6)^{i-B}$ . Let  $p = (1 - \mathcal{O}(1/\log n))/4$  be the probability of drawing heads and  $q = 1 - p$ .

Let  $A_i$  be the event that all leader candidates drew tails which happens with probability  $q^{F_i}$ . When  $A_i$  occurs  $F_{i+1} = F_i$ . Otherwise, with probability  $1 - q^{F_i}$ , the value of  $F_{i+1}$  corresponds to the number of successes during consecutive  $F_i$  coin-flips. Thus,  $\mathbb{E}[F_{i+1} | F_i] = F_i(p + q^{F_i})$ . Assume that  $F_i \geq 2$ . Then  $\mathbb{E}[F_{i+1} | F_i] \leq F_i \cdot (13/16 + o(1)) \leq F_i \cdot 5/6$  for large enough  $n$ . Thus, by the definition of  $F'_i$ , we have  $\mathbb{E}[F'_{i+1} | F'_i] \leq F'_i \cdot 5/6$ . In turn  $\Pr[B > i] = \Pr[F_i > 1] = \Pr[F'_i > 1] < \mathbb{E}[F'_i] = F_0 \cdot (5/6)^i$ . Since  $F_0 \leq c \log n$ , we get

$$\Pr[B > \log_{6/5}(c \log n \cdot n^\eta)] < n^{-\eta},$$

and

$$\mathbb{E}[B] = \sum_{i=0}^{\infty} \Pr[B > i] \leq \sum_{i=0}^{\infty} \min(1, F_0 \cdot (5/6)^i) = \mathcal{O}(\log F_0) + \mathcal{O}(1). \quad \square$$

We now compute the time needed to elect a single leader, i.e., to preserve a single agent in state A and to change states of all agents in state P to W.

**Lemma 7.4.** *Assume that the preprocessing, the phase clock and coin propagations work properly and that exactly one active leader enters  $\mathbf{drag} = \Psi$ . After  $\mathcal{O}(\log n \log \log n)$  rounds in expectation and  $\mathcal{O}(\log^2 n)$  rounds with high probability there is exactly one leader remaining in state A and all other candidates are moved to W.*

*Proof.* Let  $T$  be the number of rounds it takes to go from  $c \log n$  to 1 of agents in state A. By Lemma 7.3  $T$  is  $\mathcal{O}(n \log n \log \log n)$  in expectation and  $\mathcal{O}(n \log^2 n)$  with high probability. It is enough to consider the round number  $T' > T$ , s.t., between  $T$  and  $T'$  all leader agents increase their  $\mathbf{drag}$ , since any such interaction moves all P to W. Let  $x$  be the highest  $\mathbf{drag}$  value achieved by a P candidate. This candidate moves to state W as soon as it encounters a higher value of  $\mathbf{drag}$  in another candidate. In the proof we use value  $T_x$  defined just before Lemma 7.2.

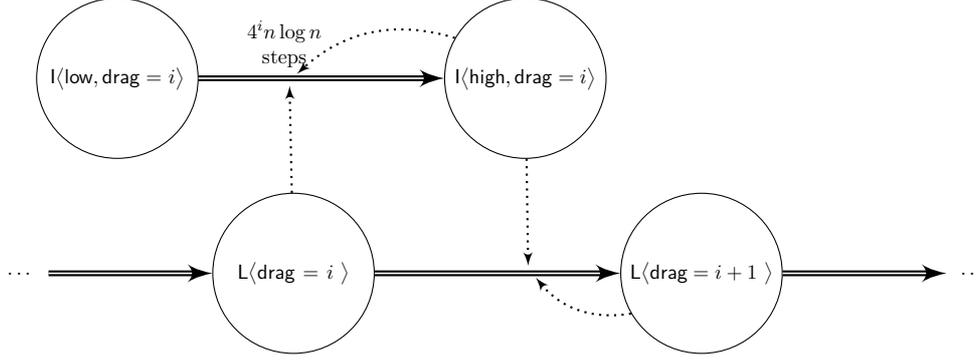


Figure 3: The implementation of slowing down drag counter, where dotted arrows indicate enabled transitions.

Note that by Lemma 7.3 drag value  $x$  is smaller than  $\Psi$ . By Lemma 7.2 we also have  $\sum_{y=1}^{\Psi} T_y = \mathcal{O}(n \log^2 n)$  whp. Finally, the value of  $\Psi$  is propagated amongst leaders in  $\mathcal{O}(n \log n)$  interactions whp, which completes the proof of the time bound obtained whp.

Let  $T_A = \Theta(n \log n \log \log n)$  be the number of interactions of first two epochs. In order to obtain the improved time bound in expectation we observe that by Lemma 7.2 there exists an integer constant  $k$  such that for any  $y$ :  $T_y + T_{y+1} + \dots + T_{y+k} \geq c_1 4^y n \log n$  whp, where  $c_1$  is the constant defined in Lemma 7.2. Because of this  $T \geq T_A + T_1 + \dots + T_x = \Omega(n \log n (\log \log n + 4^x))$  whp. Note that  $T_{x+1} \leq c_2 4^x n \log n$  whp, and the time of propagation of value  $x+1$  amongst leaders is  $\mathcal{O}(n \log n)$ . Thus  $T' = \mathcal{O}(n \log n (\log \log n + 4^x))$ . Finally, whp the extra time cost of getting all passive agents withdrawn increases the total number of interactions at most a constant number of times. With remaining negligible probability the expected value of  $T'$  is at most the average number of interactions to get all leader candidates to drag =  $\Psi$  which is  $\mathcal{O}(n \log^2 n)$ .  $\square$

## 8 Slow protocol backup

We have shown earlier that our protocol elects a single leader in expected time  $\mathcal{O}(\log n \log \log n)$  and with high probability in time  $\mathcal{O}(\log^2 n)$ . However, we still need to provide guarantee that our protocol always elects the unique leader. In other words, the probability of eliminating all possible candidates must be null.

We first show that the population of leaders is always reduced to at most one eventually. This is achieved by running in the background the elimination protocol discussed before. Formally speaking, we say that  $L\langle A \rangle$  and  $L\langle P \rangle$  agents are mapped to the leader in the output, and  $L\langle W \rangle$ ,  $C$ ,  $I$ ,  $X$ ,  $D$  and  $0$  state are mapped to non-leader in the output.

We also adopt an extra interaction rule in which when two agents  $A, B \in \{L\langle A \rangle, L\langle P \rangle\}$  interact  $B$  changes its state to  $L\langle W \rangle$

$$A + B \rightarrow A + L\langle W \rangle \quad (11)$$

when  $A$  has no smaller priority than  $B$ . The priority relationship is defined as follows. An agent of higher drag has greater priority and in case of a tie  $L\langle A \rangle$  wins with  $L\langle P \rangle$ , and further the agent with a smaller level wins, and finally heads wins with none and tails.

We first observe that with high probability rule (11) may only speed up the elimination process analysed in Sections 6 and 7, since it reduces the number of  $L\langle A \rangle$  agents, and whp this rule never eliminates during one round all agents with heads.

**Lemma 8.1.** *Throughout execution of the leader election protocol there is always at least one agent in state  $L\langle A \rangle$  or  $L\langle P \rangle$ .*

*Proof.* Leader candidates equipped in state  $L\langle A \rangle$  are formed by application of rule (1). Only rules (9) and (11) can change states of agents from  $L\langle A \rangle$  and  $L\langle P \rangle$  to  $L\langle W \rangle$ . However, neither

of these rules can eliminate the last agent of this type which possesses the highest value of drag.  $\square$

We conclude this section with the main result of this paper.

**Theorem 8.2 (Main result).** *Presented protocol always elects a leader. Election happens in expected time  $\mathcal{O}(\log n \log \log n)$ , and  $\mathcal{O}(\log^2 n)$  time with high probability.*

*Proof.* By Lemma 5.4 in  $\mathcal{O}(\log n)$  rounds whp we elect a junta of the appropriate size as indicated by Lemma 5.3. This junta starts the phase clock. By Lemma 6.2, fast elimination epoch leaves  $\mathcal{O}(\log n)$  active leaders in  $\mathcal{O}(\log n \cdot \log \log n)$  rounds, with high probability. By Lemma 7.4, slow elimination epoch leaves a single leader in expected time  $\mathcal{O}(\log n \cdot \log \log n)$  and in time  $\mathcal{O}(\log^2 n)$  with high probability. In addition, by Lemma 8.1 we never eliminate all leader candidates, and rule (11) guarantees that whp in  $\mathcal{O}(n)$  rounds in expectation and in  $\mathcal{O}(n \log n)$  whp a single leader is chosen, which does not affect the overall running time.  $\square$

## 9 Conclusion

In this paper we presented the first  $o(\log^2 n)$ -time leader election protocol. Our algorithm operates in parallel time  $\mathcal{O}(\log n \log \log n)$  which is equivalent to  $\mathcal{O}(n \log n \log \log n)$  pairwise interactions. The solution is always correct, however the obtained speed up refers to the expected time, and our protocol works whp only in time  $\mathcal{O}(\log^2 n)$  time, as in [GS18]. The first two epochs operate in time  $\mathcal{O}(\log n \log \log n)$  whp. Thus the main bottleneck is the last epoch when we reduce the number of leader candidates from  $\mathcal{O}(\log n)$  to a single one. We would like to claim that likely the hardest problem in leader election is reduction from two leader candidates to a single one. And if one is able to solve this problem rapidly whp, they should be able to solve leader election with the same time complexity too.

## References

- [AAD<sup>+</sup>04] D. Angluin, J. Aspnes, Z. Diamadi, M.J. Fischer, and R. Peralta. Computation in networks of passively mobile finite-state sensors. In *PODC*, pages 290–299, 2004.
- [AAE08] D. Angluin, J. Aspnes, and D. Eisenstat. A simple population protocol for fast robust approximate majority. *Distributed Computing*, 21(2):87–102, 2008.
- [AAE<sup>+</sup>17] D. Alistarh, J. Aspnes, D. Eisenstat, R. Gelashvili, and R.L. Rivest. Time-space trade-offs in population protocols. In *SODA*, pages 2560–2579, 2017.
- [AAG18] D. Alistarh, J. Aspnes, and R. Gelashvili. Space-optimal majority in population protocols. In *SODA*, pages 2221–2239, 2018.
- [AG15] D. Alistarh and R. Gelashvili. Polylogarithmic-time leader election in population protocols. In *ICALP*, pages 479–491, 2015.
- [AGV15] D. Alistarh, R. Gelashvili, and M. Vojnović. Fast and exact majority in population protocols. In *PODC*, pages 47–56, 2015.
- [Ang80] D. Angluin. Local and global properties in networks of processors (extended abstract). In *STOC*, pages 82–93, 1980.
- [AS91] H. Attiya and M. Snir. Better computing on the anonymous ring. *J. Algorithms*, 12(2):204–238, 1991.
- [ASW88] H. Attiya, M. Snir, and M.K. Warmuth. Computing on an anonymous ring. *J. ACM*, 35(4):845–875, 1988.
- [AW04] H. Attiya and J. Welch. *Distributed Computing: Fundamentals, Simulations and Advanced Topics*. John Wiley & Sons, 2004.

- [BCER17] A. Bilke, C. Cooper, R. Elsässer, and T. Radzik. Brief announcement: Population protocols for leader election and exact majority with  $O(\log^2 n)$  states and  $O(\log^2 n)$  convergence time. In *PODC*, pages 451–453, 2017.
- [BCN<sup>+</sup>15] L. Becchetti, A.E.F. Clementi, E. Natale, F. Pasquale, and R. Silvestri. Plurality consensus in the gossip model. In *SODA*, pages 371–390, 2015.
- [BFGK16] P. Berenbrink, T. Friedetzky, G. Giakkoupis, and P. Kling. Efficient plurality consensus, or: the benefits of cleaning up from time to time. In *ICALP*, pages 136:1–136:14, 2016.
- [BKKO18] P. Berenbrink, D. Kaaser, P. Kling, and L. Otterbach. Simple and efficient leader election. In *SOSA*, pages 9:1–9:11, 2018.
- [BSV<sup>+</sup>96] P. Boldi, Sh. Shammah, S. Vigna, B. Codenotti, P. Gemmel, and J. Simon. Symmetry breaking in anonymous networks: Characterizations. In *ISTCS*, pages 16–26, 1996.
- [Bur80] J.E. Burns. A formal model for message passing systems. Technical Report TR-91, Computer Science Department, Indiana University, September 1980.
- [BV99] P. Boldi and S. Vigna. Computing anonymously with arbitrary knowledge. In *PODC*, pages 181–188, 1999.
- [CCDS14] H.-L. Chen, R. Cummings, D. Doty, and D. Soloveichik. Speed faults in computation by chemical reaction networks. In *DISC*, pages 16–30, 2014.
- [CGK<sup>+</sup>15] J. Czyzowicz, L. Gąsieniec, A. Kosowski, E. Kranakis, P.G. Spirakis, and P. Uznański. On convergence and threshold properties of discrete lotka-volterra population protocols. In *ICALP*, pages 393–405, 2015.
- [CMN<sup>+</sup>11] I. Chatzigiannakis, O. Michail, S. Nikolaou, A. Pavlogiannis, and P.G. Spirakis. Passively mobile communicating machines that use restricted space. *Theor. Comput. Sci.*, 412(46):6469–6483, 2011.
- [DK18] B. Dudek and A. Kosowski. Universal protocols for information dissemination using emergent signals. In *STOC*, to appear, 2018.
- [Dot14] D. Doty. Timing in chemical reaction networks. In *SODA*, pages 772–784, 2014.
- [DP04] S. Dobrev and A. Pelc. Leader election in rings with nonunique labels. *Fundam. Inform.*, 59(4):333–347, 2004.
- [DP14] D. Dereniowski and A. Pelc. Leader election for anonymous asynchronous agents in arbitrary networks. *Distributed Computing*, 27(1):21–38, 2014.
- [DS15] D. Doty and D. Soloveichik. Stable leader election in population protocols requires linear time. In *DISC*, pages 602–616, 2015.
- [DV12] M. Draief and M. Vojnović. Convergence speed of binary interval consensus. *SIAM J. Control and Optimization*, 50(3):1087–1109, 2012.
- [Fis83] M.J. Fischer. The consensus problem in unreliable distributed systems (a brief survey). In *FCT*, pages 127–140, 1983.
- [FKK<sup>+</sup>04] P. Flocchini, E. Kranakis, D. Krizanc, F.L. Luccio, and N. Santoro. Sorting and election in anonymous asynchronous rings. *J. Parallel Distrib. Comput.*, 64(2):254–265, 2004.
- [FL87] G.N. Frederickson and N.A. Lynch. Electing a leader in a synchronous ring. *J. ACM*, 34(1):98–115, 1987.
- [FP11] E.G. Fusco and A. Pelc. How much memory is needed for leader election. *Distributed Computing*, 24(2):65–78, 2011.
- [GHM<sup>+</sup>16] L. Gąsieniec, D.D. Hamilton, R. Martin, P.G. Spirakis, and G. Stachowiak. Deterministic population protocols for exact majority and plurality. In *OPODIS*, pages 14:1–14:14, 2016.

- [GHMS15] L. Gąsieniec, D.D. Hamilton, R. Martin, and P.G. Spirakis. The match-maker: Constant-space distributed majority via random walks. In *SSS*, pages 67–80, 2015.
- [GMP16] Ch. Glacet, A. Miller, and A. Pelc. Time vs. information tradeoffs for leader election in anonymous trees. In *SODA*, pages 600–609, 2016.
- [GP16] M. Ghaffari and M. Parter. A polylogarithmic gossip algorithm for plurality consensus. In *PODC*, pages 117–126, 2016.
- [GS18] L. Gąsieniec and G. Stachowiak. Fast space optimal leader election in population protocols. In *SODA*, pages 2653–2667, 2018.
- [HKM<sup>+</sup>08] M. Amine Haddar, A. Hadj Kacem, Y. Métivier, M. Mosbah, and M. Jmaiel. Electing a leader in the local computation model using mobile agents. In *AICCSA*, pages 473–480, 2008.
- [HS80] D.S. Hirschberg and J.B. Sinclair. Decentralized extrema-finding in circular configurations of processors. *Commun. ACM*, 23(11):627–628, 1980.
- [Lan77] G. Le Lann. Distributed systems - towards a formal approach. In *IFIP Congress*, pages 155–160, 1977.
- [MCS11] O. Michail, I. Chatzigiannakis, and P.G. Spirakis. *New Models for Population Protocols*. Synthesis Lectures on Distributed Computing Theory. Morgan & Claypool Publishers, 2011.
- [MNRS14] G.B. Mertzios, S.E. Nikolettseas, Ch. Raptopoulos, and P.G. Spirakis. Determining majority in networks with local interactions and very small local memory. In *ICALP*, pages 871–882, 2014.
- [Pet82] G.L. Peterson. An  $o(n \log n)$  unidirectional algorithm for the circular extrema problem. *ACM Trans. Program. Lang. Syst.*, 4(4):758–762, October 1982.
- [YK89] M. Yamashita and T. Kameda. Electing a leader when processor identity numbers are not distinct (extended abstract). In *Distributed Algorithms, 3rd International Workshop, Nice, France, September 26-28, 1989, Proceedings*, pages 303–314, 1989.
- [YK96] M. Yamashita and T. Kameda. Computing on anonymous networks: Part 1 - characterizing the solvable cases. *IEEE Trans. Parallel Distrib. Syst.*, 7(1):69–89, 1996.