State Complexity of Protocols With Leaders

Jérôme Leroux
jerome.leroux@labri.fr
LaBRI, CNRS, Univ. Bordeaux
Talence, France

ABSTRACT

Population protocols are a model of computation in which an arbitrary number of anonymous finite-memory agents are interacting in order to decide by stable consensus a predicate. In this paper, we focus on the counting predicates that asks, given an initial configuration, whether the number of agents in some initial state i is at least n. In 2018, Blondin, Esparza, and Jaax shown that with a fix number of leaders, there exists infinitely many n for which the counting predicate is stably computable by a protocol with at most $O(\log\log(n))$ states. We provide in this paper a matching lower-bound (up to a square root) that improves the inverse-Ackermannian lower-bound presented at PODC in 2021.

CCS CONCEPTS

• **Theory of computation → Distributed computing models**.

KEYWORDS

Population protocols, State complexity, Petri nets, Counting predicates

ACM Reference Format:
Jérôme Leroux. 2022. State Complexity of Protocols With Leaders. In *Proceedings of the 2022 ACM Symposium on Principles of Distributed Computing (PODC '22), July 25–29, 2022, Salerno, Italy.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3519270.3538421

1 INTRODUCTION

Population protocols were introduced by Angluin, Aspnes, Diamadi, Fischer, and Peralta in [2, 3] to study the computational power of networks of resource-limited mobile agents. In this model, each agent has a state in a finite set of states. When agents interact, their states are updated accordingly to a finite interaction table that depends on the total number of agents. When this table is independent of the number, the protocol is said to be *universal*. Such a table corresponds intuitively to a Petri net where each line of the interaction table is matched by a *rendez-vous transition* of the Petri net. In this model, an agent may accept or reject depending only on it own state. A population protocol is said to be stably computing a predicate, if for any initial configuration, eventually and forever, under some natural fairness conditions, either all agents accept or all agents reject. Moreover, this outcome should only depend on the initial configuration and not on the way interactions are performed.

Deciding if a universal protocol stably computes some unknown predicate is a problem called the *well-specification problem*. This problem was proved to be decidable in [12, 13] by observing that well-specification problem is equivalent to the reachability problem for Petri nets up to elementary reductions. Since this last problem was recently proved to be Ackermannian-complete [10, 14], it means that deciding the well-specification problem is Ackermannian-complete. Intuitively, population protocols maybe intrinsically very complicated.

Despite this Ackermannian complexity result, in [5], Angluin, Aspnes, Eisenstat, and Ruppert have shown that predicates stably computable by universal population protocols cannot be more complicated than the one definable in the Presburger arithmetic. Combined with [2, 3], it follows that predicates stably computable by universal population protocols are exactly the predicates definable in the Presburger arithmetic.

Since deciding if a universal population protocol is stably computing some Presburger predicate is Ackermannian-complete, a natural question is the conciseness of population protocols. Intuitively, is it possible to define a population protocol computing predicates that are very complex compared to the number of states of the protocol ? This problem is related to the so-called *state complexity* of a Presburger predicate intuitively defined as the minimal number of states of a population protocols deciding it.

State complexity upper-bounds are obtained thanks to algorithms computing from predicates protocols stably computing it with a number of states as small as possible. In [6], by revisiting the construction of population protocols deciding Presburger predicates, some improvement on state complexity upper-bounds was derived. On the other side, state complexity lower-bounds is also a difficult task since such a bound requires to prove that there is no way to stably compute a predicate with a given amount of states. In this context, focusing on the state complexity of simple Presburger predicates is a natural question. The simplest non trivial Presburger predicates are clearly the counting predicates that corresponds to the set of configurations such that the number of agents in a given state is larger than or equal to some positive number n. In 2018, Blondin, Esparza, and Jaax shown in [7] that with a fix number of leaders (agents starting the computation in a special state compared to the other one), there exist infinitely many n for which the counting predicate is stably computable by a protocol with at most $O(\log\log(n))$ states.

This state complexity upper-bound was recently completed by a state complexity lower-bound in [9]. In that paper, Czerner and Esparza shown that the number of states of a universal population protocol deciding a counting predicate with a fix number of

PODC '22, July 25–29, 2022, Salerno, Italy

ACM ISBN 978-1-4503-9262-4/22/07…$15.00
https://doi.org/10.1145/3519270.3538421

leaders is at least $\Omega(A^{-1}(n))$ where A is some Ackermannian function, leaving a gap between the $O(\log\log(n))$ upper-bound and the $\Omega(A^{-1}(n))$ lower-bound.

Main result. In this paper, we follow the classical model of population protocols. We close the previously mentioned state complexity gap by proving that for any $h < \frac{1}{2}$ and for any $L \in \mathbb{N}$, any universal population protocol stably computing a n-counting predicate with L leaders requires at least $\Omega((\log\log(n))^h)$ states.

Outline. In Section 2 we recall some basic definitions and results about protocols. In Section 3 we introduce the state complexity problem for counting predicates with leaders and we formally state the main results of this paper. Section 4 recalls classical results about Petri nets. Those results are completed in Section 5 with additional Petri net results oriented to population protocol. In fact, in that section we introduce the notions of stabilized configurations and show that those configurations are characterized by their small values. Those results are obtained thanks to Rackoff's techniques originally introduced in the context of the coverability problem for Petri nets. Section 6 contains the central technical lemma. It is a lemma about Petri nets that intuitively shows that from any initial configuration we can reach with short executions kind of bottom configurations. Section 7 recalls the model of Petri net with control-states and provides a result on small cycles satisfying some properties. This last result is obtained by introducing a linear system and by applying Pottier's techniques [15] in order to obtain small solutions for that linear system. Results of the previous sections are combined in Section 8 to obtain our state complexity lower-bound. Some related open problems and future work are presented in Section 9.

2 POPULATION PROTOCOLS

In this section, we introduce the classical model of population protocols based on the presentation used in [5].

Let P be a finite set of elements called *states*. Intuitively P is the set of possible states of each agent. Since agents are anonymous, a population of agents can be seen as a multiset of states, counting for each state $p \in P$ the number of agents in the population having p as current state. More formally, a *P-configuration* (or just a *configuration* if P is clear from the context) is a mapping in $\mathbb{N}^P$. The P-configuration that maps any state on zero is said to be *empty* and it is denoted by $0|_P$ or just 0 when P is clear from the context. Given a configuration ρ, the number $|\rho| \stackrel{\text{def}}{=} \sum_{p\in P} \rho(p)$ is called the *number of agents* in ρ, and the set $\text{support}(\rho) = \{p \in P \mid \rho(p) > 0\}$ is called the *support* of ρ. Let Q be another finite set of states. We associate with a P-configuration ρ the Q-configuration $\rho|_Q$ defined for every $q \in Q$ by $\rho|_Q(q) = \rho(q)$ if $q \in P$ and zero otherwise. Notice that Q is not necessarily a subset of P. Given $p \in P$ we simply denote by $p|_P$ (or just p when P is clear from the context) the mapping in $\mathbb{N}^P$ that maps p on 1 and the other states on zero. The sum $\alpha + \beta$ of two configurations α, β and the product $n.\rho$ where $n \in \mathbb{N}$ and ρ is a configuration are defined component-wise as expected.

A *population protocol* is a family $(P_s, T_s, \gamma_s)_{s\geq 1}$ where P_s is a finite set of *states*, $T_s \subseteq P_s^4$ is the set of possible interactions, and $\gamma_s : P_s \to \{0, 1\}$ is the *output function*. We introduce the function γ that maps any non empty P-configuration ρ on $\{0, 1, \star\}$ as follows:

$$\gamma(\rho) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } \text{support}(\rho) \subseteq \{p \mid \gamma_s(p) = 0\} \\ 1 & \text{if } \text{support}(\rho) \subseteq \{p \mid \gamma_s(p) = 1\} \\ \star & \text{otherwise.} \end{cases}$$

where $s = |\rho|$.

We also introduce the binary relation $\to$ over the non-empty P-configurations defined by $\alpha \to \beta$ if there exists $s \geq 1$ such that $|\alpha| = s = |\beta|$ and there exists $(p, q, p', q') \in T_s$ such that $\alpha \geq p + q$ and $\beta = \alpha - p - q + p' + q'$. Intuitively $\alpha \to \beta$ if α contains two distinct agents in states p and q that interact with a rendez-vous and move to the states p' and q' respectively. The reflexive and transitive closure of $\to$ is denoted as $\stackrel{*}{\to}$.

For each $j \in \{0, 1\}$, we introduce the following set S_j called the *j-output stable configurations*:

$$S_j \stackrel{\text{def}}{=} \{\alpha \in \mathbb{N}^P \backslash \{0\} \mid \forall \beta\ \alpha \stackrel{*}{\to} \beta \Rightarrow \gamma(\beta) = j\}$$

A *predicate* is a mapping $\phi : \mathbb{N}^I \backslash \{0\} \to \{0, 1, \star\}$. A *predicate* is said to be *total* if $\phi(\rho) \neq \star$ for every $\rho \in \mathbb{N}^I \backslash \{0\}$. We say that a protocol stably computes ϕ if for every non empty P-configuration ρ such that $\text{support}(\rho) \subseteq I$, if $\phi(\rho|_I) = j$ for some $j \in \{0, 1\}$ then for every α such that $\rho \stackrel{*}{\to} \alpha$, there exists $\beta \in S_j$ such that $\alpha \stackrel{*}{\to} \beta$. A predicate ϕ is *stably computable* if there exists a protocol that stably computes it.

3 STATE-COMPLEXITY OF PROTOCOLS

A protocol is said to be *universal* if the tuple (P_s, T_s, γ_s) does not depend on $s \geq 1$. In that case it is simply denoted as (P, T, γ). In [4], total predicates that are stably computable by universal population protocols are proved to be exactly the predicates definable in the Presburger arithmetic. The state-complexity of a Presburger predicate ϕ is the minimal number of states of a universal protocol that stably computes it. We denote by $\text{comp}(\phi)$ this number of states. Notice that the state complexity is defined in a universal setting since the minimal number $|P_k|$ such that there exists a population protocol $(P_s, T_s, \gamma_s)_{s\geq 1}$ stably computing any (not necessarily Presburger) predicate ϕ is exactly $\text{comp}(\phi_k)$ where $\phi_k : \mathbb{N}^I \backslash \{0\} \to \{0, 1, \star\}$ is the Presburger predicate defined by:

$$\phi_k(\rho) = \begin{cases} \phi(\rho) & \text{if } |\rho| = k \\ \star & \text{otherwise} \end{cases}$$

In the sequel, we only consider universal population protocols.

Since our paper focuses on the so-called counting predicates, let us first introduce those predicates. A n-counting predicate with L leaders is a predicate of the form $\phi_{j=L\Rightarrow i\geq n} : \mathbb{N}^I \backslash \{0\} \to \{0, 1, \star\}$ where $I \stackrel{\text{def}}{=} \{i, j\}$ with i, j two distinct states satisfying for every $\rho \in \mathbb{N}^I \backslash \{0\}$:

$$\phi_{j=L\Rightarrow i\geq n}(\rho) = \begin{cases} 1 & \text{if } \rho(j) = L \wedge \rho(i) \geq n \\ 0 & \text{if } \rho(j) = L \wedge \rho(i) < n \\ \star & \text{if } \rho(j) \neq L \end{cases}$$

Remark 1. *The notion of leaders introduced in [7] is not exactly the same as the one introduced in this paper, but concerning the state complexity, the two notions coincide.*

In [7], it is exhibited an infinite set of natural numbers n for which there exists a universal population protocol stably computing a n-counting predicate with a fix number of leaders and a number of states bounded by $O(\log\log(n))$. This paper left open the optimality of that bound. In this paper we show that such a bound is almost optimal by proving the following main theorem.

Theorem 3.1. *For every universal population protocol (P, T, γ) that stably computes a n-counting predicate with L leaders, we have:*

$$n \leq (12 + 2L)^{|P|^{(|P|+2)^2}}$$

We deduce the following state complexity lower-bound as a corollary.

Corollary 3.2. *For every $L \in \mathbb{N}$ and $h < \frac{1}{2}$ we have:*

$$\mathrm{comp}(\phi_{j=L \Rightarrow i \geq n}) = \Omega((\log\log(n))^h)$$

Proof. Let us consider $\varepsilon > 0$ such that $\frac{1}{2+\varepsilon} \geq h$. Notice that for $d \in \mathbb{N}$ large enough, we have $d \leq 2^{(d+2)^\varepsilon}$. It follows that $d^{(d+2)^2} \leq 2^{(d+2)^{2+\varepsilon}}$ for d large enough. Theorem 3.1 shows that we have :

$$n \leq (12 + 2L)^{|P|^{(|P|+2)^2}}$$

It follows that if n is large enough, then $|P|$ is large enough to satisfy $|P|^{(|P|+2)^2} \leq 2^{(|P|+2)^{2+\varepsilon}}$. It follows that $\log\log(n) \leq \log\log(12 + 2L) + \log(2)(|P| + 2)^{2+\varepsilon}$. In particular:

$$|P| \geq \left(\frac{\log\log(n) - \log\log(12 + 2L)}{\log(2)}\right)^h - 2$$

We have proved the corollary. □

4 PETRI NETS

The proof of our lower-bound is based on Petri nets. In this section, we introduce definitions related to Petri nets and show how population protocols are related to Petri nets.

A *P-transition* (or simply a *transition* when the finite set of states P is clear from the context) is a *pair* of P-configurations. We associate with a transition t the binary relation $\xrightarrow{t}$ over the configurations defined by $\alpha \xrightarrow{t} \beta$ if there exists a configuration ρ such that $(\alpha, \beta) = t + (\rho, \rho)$. Oberve that if t is the transition (α_t, β_t) then for every α, β we have $\alpha \xrightarrow{t} \beta$ if, and only if, $\alpha \geq \alpha_t$ and $\beta = \alpha - \alpha_t + \beta_t$. A transition t is called a *rendez-vous* if $t = (p + q, p' + q')$ for some states $p, q, p', q' \in P$. Notice that in that case $\alpha \xrightarrow{t} \beta$ if, and only if, $\alpha \geq p + p'$ and $\beta = \alpha - p - p' + q + q'$. Given a word $\sigma = t_1 \dots t_k$ of transitions, we introduce the binary relation $\xrightarrow{\sigma}$ over the configurations defined by $\alpha \xrightarrow{\sigma} \beta$ if there exists a sequence $\rho_0, \dots, \rho_k$ of configurations such that:

$$\alpha = \rho_0 \xrightarrow{t_1} \rho_1 \cdots \xrightarrow{t_k} \rho_k = \beta$$

A P-Petri net T (or simply a Petri net when P is clear from the context) is a finite set of P-transitions. The reachability relation of a Petri net T is the binary relation $\xrightarrow{T^*}$ over the configurations defined by $\alpha \xrightarrow{T^*} \beta$ if there exists $\sigma \in T^*$ such that $\alpha \xrightarrow{\sigma} \beta$.

Let us consider a universal population protocol (P, T, γ). We associate to each tuple $t = (p, q, p', q') \in T$ the rendez-vous P-transition $\bar{t} \stackrel{\text{def}}{=} (p+q, p'+q')$. We also denote by $\bar{T} \stackrel{\text{def}}{=} \{\bar{t} \mid t \in T\}$ the P-Petri net obtained from T. Notice that for every P-configurations α, β, we have $\alpha \xrightarrow{*} \beta$ if, and only if, $\alpha \xrightarrow{\bar{T}^*} \beta$. It follows that without any ambiguity, we can identify the tuple $(p, q, p', q') \in P^4$ with the rendez-vous P-transition $(p + q, p' + q')$. In the sequel, universal population protocol are triples (P, T, γ) where T is a P-Petri net containing only rendez-vous transitions.

5 SMALL STABLE CONFIGURATIONS

A P-configuration ρ is said to be (T, F)-*stabilized* where T is a P-Petri net, and F is a subset of P if for every configuration β such that $\rho \xrightarrow{T^*} \beta$, we have $\mathrm{support}(\beta) \subseteq F$. In this section, we show that (T, F)-stabilized configurations are characterized by "small values". This result is obtained by applying classical Rackoff's techniques originally introduced for the Petri net coverability problem. The definition of stabilized configurations is related to the output stable configurations of protocols as shown by the following lemma.

Lemma 5.1. *Let (P, T, γ) be a universal population protocol, and let $F_j \stackrel{\text{def}}{=} \gamma^{-1}(\{j\})$ for $j \in \{0, 1\}$. A configuration is (T, F_j)-stabilized if, and only if, it is empty or j-output stable.*

Proof. By definition. □

Let us introduce some notations. Given a P-configuration ρ, we introduce $\|\rho\|_\infty \stackrel{\text{def}}{=} \max_{p \in P} \rho(p)$. Given a transition $t = (\alpha_t, \beta_t)$, we also introduce $\|t\|_\infty \stackrel{\text{def}}{=} \max\{\|\alpha_t\|_\infty, \|\beta_t\|_\infty\}$. Given a Petri net T, we define $\|T\|_\infty \stackrel{\text{def}}{=} \max_{t \in T} \|t\|_\infty$.

Given a finite set Q of states, we define several restrictions related to Q as follows. Let us recall that given a P-configuration ρ, we previously defined $\rho|_Q$ as the Q-configuration defined by $\rho|_Q(q) \stackrel{\text{def}}{=} \rho(q)$ if $q \in Q$, and zero otherwise. Given a P-transition $t = (\alpha_t, \beta_t)$, we define the Q-transition $t|_Q$ as the pair $t|_Q \stackrel{\text{def}}{=} (\alpha_t|_Q, \beta_t|_Q)$. Notice that if $\alpha \xrightarrow{t} \beta$ then $\alpha|_Q \xrightarrow{t|_Q} \beta|_Q$. In fact, in that case there exists a configuration ρ such that $(\alpha, \beta) = t + (\rho, \rho)$. We deduce that $(\alpha|_Q, \beta|_Q) = t|_Q + (\rho|_Q, \rho|_Q)$ and in particular $\alpha|_Q \xrightarrow{t|_Q} \beta|_Q$. Given a P-Petri net T, we introduce the Q-Petri net $T|_Q \stackrel{\text{def}}{=} \{t|_Q \mid t \in T\}$. Given a word $\sigma = t_1 \dots t_k$ of P-transitions, we introduce the word $\sigma|_Q = t_1|_Q \dots t_k|_Q$ of Q-transitions. By induction on the length of σ, we deduce that $\alpha \xrightarrow{\sigma} \beta$ for some P-configurations α, β implies $\alpha|_Q \xrightarrow{\sigma|_Q} \beta|_Q$. The converse property is true in some cases as shown by the following lemma.

Lemma 5.2. *Assume that $\alpha|_Q \xrightarrow{\sigma|_Q} \rho$ for some P-configuration α and some Q-configuration ρ, some word σ of transitions in a P-Petri net T, and some finite set Q. If $\alpha(p) \geq |\sigma|\|T\|_\infty$ for every $p \in P \backslash Q$ then there exists a configuration β such that $\alpha \xrightarrow{\sigma} \beta$, $\beta|_Q = \rho$, and $\beta(p) \geq \alpha(p) - |\sigma|\|T\|_\infty$ for every $p \in P \backslash Q$.*

Proof. Simple induction on $|\sigma|$. □

A configuration ρ is said to be *T-coverable* from a configuration α where T is a Petri net if there exists a word $\sigma \in T^*$ such that $\alpha \xrightarrow{\sigma} \beta \geq \rho$ for some configuration β. The minimal length of such a word σ can be bounded using Rackoff's techniques with respect to $\|\rho\|_\infty$, $\|T\|_\infty$, and $|Q|$ as shown by the following result introduced in [16] to prove that the T-coverability problem is decidable in exponential space.

Lemma 5.3 ([16]). *If a configuration ρ is T-coverable from a configuration α where T is a P-Petri net, then there exists $\sigma \in T^*$ with a length bounded by $(\|\rho\|_\infty + \|T\|_\infty)^{|P|^{|P|}}$, and a configuration β such that $\alpha \xrightarrow{\sigma} \beta \geq \rho$.*

Proof. This is a classical result obtained by Rackoff in [16] by induction on $|P|$. □

We deduce the following lemma that shows that (T, F)-stabilized configurations are characterized by "small values" (the values $\rho(p)$ for $p \in R$). In the statement of that lemma the relation $\leq$ over the P-configurations is defined by $\alpha \leq \beta$ if there exists a P-configuration ρ such that $\beta = \alpha + \rho$.

Lemma 5.4. *Let ρ be a (T, F)-stabilized P-configuration with $F \subseteq P$, let h be a positive integer satisfying $h \geq \|T\|_\infty (1 + \|T\|_\infty)^{|P|^{|P|}}$, and let $R \stackrel{\text{def}}{=} \{p \in P \mid \rho(p) < h\}$. Every P-configuration α such that $\alpha|_R \leq \rho|_R$ is (T, F)-stabilized.*

Proof. Let us consider a P-configuration α such that $\alpha|_R \leq \rho|_R$. There exists a R-configuration μ such that $\rho|_R = \alpha|_R + \mu$. Assume by contradiction that α is not (T, F)-stabilized. It follows that there exists a configuration β such that $\alpha \xrightarrow{T^*} \beta$ and $\beta(p) > 0$ for some place $p \in P \backslash F$. Since $p \notin F$ and ρ is (T, F)-stabilized, we deduce that $\rho(p) = 0$. In particular $p \in R$ since $h > 0$. Since $p|_P$ is T-coverable from α, Lemma 5.3 shows there exists a word $\sigma \in T^*$ of length bounded by $(1 + \|T\|_\infty)^{|P|^{|P|}}$ and a configuration η such that $\alpha \xrightarrow{\sigma} \eta \geq p|_P$. It follows that $\alpha|_R \xrightarrow{\sigma|_R} \eta|_R$. From this relation and $\rho_R = \alpha|_R + \mu$, we deduce that $\rho_R \xrightarrow{\sigma|_R} \eta|_R + \mu$. Lemma 5.2 shows that there exists a configuration δ such that $\rho \xrightarrow{\sigma} \delta$ and $\delta|_R = \eta|_R + \mu$. Since $p \in R$, we deduce that $\delta(p) = \eta(p) + \mu(p) \geq p|_P(p) = 1$. As $p \notin F$, it follows that ρ is not (T, F)-stabilized and we get a contradiction. We have proved the lemma. □

Remark 2. *A similar result was provided in [9] in the context of Petri nets given as finite set of rendez-vous tranistions.*

6 BOTTOM CONFIGURATIONS

Let T be a P-Petri net. The *T-component* of a P-configuration ρ is the set of configurations β such that $\rho \xrightarrow{T^*} \beta \xrightarrow{T^*} \rho$. A configuration ρ is said to be *T-bottom* if its T-component is finite and every configuration β such that $\rho \xrightarrow{T^*} \beta$ satisfies $\beta \xrightarrow{T^*} \rho$.

In this section we prove the following theorem that intuitively provides a way to reach with short words kind of bottom configurations with small size (small and short meaning doubly-exponential in that context). Other results proved in this section are only used for proving the following theorem and are no longer used in the sequel.

Theorem 6.1. *Let T be a P-Petri net, let ρ be a P-configuration, and let $b \stackrel{\text{def}}{=} (4 + 4\|T\|_\infty + 2\|\rho\|_\infty)^{d^d(1+(2+d^d)^{d+1})}$ with $d \stackrel{\text{def}}{=} |P|$. There exist two words $\sigma, w \in T^*$, a set of places $Q \subseteq P$, and two P-configurations α, β such that:*

- $\rho \xrightarrow{\sigma} \alpha \xrightarrow{w} \beta$.
- $\alpha|_Q = \beta|_Q$.
- $\alpha(p) < \beta(p)$ *for every state* $p \in P \backslash Q$.
- $\alpha|_Q$ *is* $T|_Q$*-bottom.*
- *The cardinal of the* $T|_Q$*-component of* $\alpha|_Q$ *is bounded by* b.
- $|\sigma|, |w|, d\|\alpha\|_\infty, d\|\beta\|_\infty \leq b$.

The proof of the previous theorem is obtained by iterating the following lemma in order to obtain an increasing sequence of sets Q.

Lemma 6.2. *Let T be a P-Petri net, let ρ be a P-configuration, let Q be a set of states included in P such that $\rho|_Q$ is $T|_Q$-bottom, let s be the cardinal of the $T|_Q$-component of $\rho|_Q$, and let $d \stackrel{\text{def}}{=} |P \backslash Q|$.*

There exist a word $\sigma \in T^*$ such that $|\sigma| \leq (1 + d(1 + s\|T\|_\infty + \|\rho\|_\infty)^{d^d})s$, and a P-configuration ρ' such that $\rho \xrightarrow{\sigma} \rho'$ and such that:

- *either $\rho'|_Q = \rho|_Q$ and $\rho'(p) > \rho(p)$ for every $p \in P \backslash Q$,*
- *or there exists a set $Q' \subseteq P$ that strictly contains Q such that $\rho'|_{Q'}$ is $T|_{Q'}$-bottom and the cardinal s' of the $T|_{Q'}$-component of $\rho'|_{Q'}$ satisfies:*

$$s' \leq (1 + d(1 + s\|T\|_\infty + \|\rho\|_\infty)^{d^d})s$$

Proof. Let us introduce the sequence $\lambda_1, \ldots, \lambda_d$ of natural numbers satisfying $\lambda_d \stackrel{\text{def}}{=} 1 + s\|T\|_\infty + \|\rho\|_\infty$ and satisfying $\lambda_n \stackrel{\text{def}}{=} s\lambda_{n+1}^{d-n}\|T\|_\infty + \lambda_{n+1}$ for every $n \in \{1, \ldots, d-1\}$. Observe that $\lambda_1 \geq \cdots \geq \lambda_d$. Moreover, $\lambda_n \leq \lambda_d \lambda_{n+1}^{d-n}$ for every $1 \leq n < d$. We deduce by induction that $\lambda_1^d \leq \lambda_d^{d^d}$.

Let $\rho_0 \stackrel{\text{def}}{=} \rho$. We are going to build by induction on n a sequence $\rho_1, \ldots, \rho_n$ of configurations, a sequence $\sigma_1, \ldots, \sigma_n$ of words in T^*, and a sequence $p_1, \ldots, p_n$ of states in $P \backslash Q$ such that for every $i \in \{1, \ldots, n\}$ we have:

(i) $\rho_{i-1} \xrightarrow{\sigma_i} \rho_i$.
(ii) $|\sigma_i| \leq \lambda_i^{d-i+1} s$.
(iii) $\rho_i(p) \geq \lambda_i$ for every $p \in \{p_1, \ldots, p_i\}$.

So, let us assume that $\rho_1, \ldots, \rho_n, \sigma_1, \ldots, \sigma_n$, and $p_1, \ldots, p_n$ are built for some $n \geq 0$. Since $p_1, \ldots, p_n$ are distinct elements in $P \backslash Q$, it follows that $n \leq d$.

Let us first assume that $n = d$. In that case, we have $\rho_d(p) \geq \lambda_d$ for every $p \in P \backslash Q$. As $\rho|_Q$ is a $T|_Q$-bottom configuration and $\rho|_Q \xrightarrow{(\sigma_1 \ldots \sigma_d)|_Q} \rho_d|_Q$ and since the cardinal of the $T|_Q$-component of $\rho|_Q$ is bounded by s, we deduce that there exists a word $w \in T^*$ such that $\rho_d|_Q \xrightarrow{w|_Q} \rho|_Q$ and $|w| < s$. Since $\lambda_d \geq s\|T\|_\infty \geq |w|\|T\|_\infty$, Lemma 5.2 shows that $\rho_d \xrightarrow{w} \rho'$ for some configuration ρ' such that $\rho'|_Q = \rho|_Q$ and such that for every $p \in P \backslash Q$ we have $\rho'(p) \geq \rho(p) - |w|\|T\|_\infty \geq \lambda_d - s\|T\|_\infty > \rho(p)$ by definition of λ_d. Let us introduce $\sigma \stackrel{\text{def}}{=} \sigma_1 \ldots \sigma_d w$ and notice that $|\sigma| \leq (\lambda_1^d + \cdots + \lambda_d^{d-d+1} + 1)s \leq (1 + d\lambda_1^d)s$ and we have proved that the lemma holds (first case).

So we can assume that $n < d$. Let us introduce the set $R_n = (P\backslash Q)\backslash\{p_1, \ldots, p_n\}$. Since $|R_n| = d - n$, the set R_n is non empty.

Assume first that for every configuration β such that $\rho_n \xrightarrow{T^*} \beta$ we have $\beta(p) < \lambda_{n+1}$ for every $p \in R_n$. In that case let $Q' \stackrel{\text{def}}{=} Q \cup R_n$. It follows that the cardinal of the set of configurations β' such that $\rho_n|_{Q'} \xrightarrow{T|^*_{Q'}} \beta'$ is bounded by $s\lambda_{n+1}^{d-n}$. Hence, there exists a configuration β' that is $T|_{Q'}$-bottom and a word $w \in T^*$ such that $\rho_n|_{Q'} \xrightarrow{w|_{Q'}} \beta'$ and such that $|w| < s\lambda_{n+1}^{d-n}$. Notice that the cardinal s' of the $T|_{Q'}$-component of β' is bounded by $s\lambda_{n+1}^{d-n} \leq s\lambda_1^d$. As $\rho_n(p) \geq \lambda_n$ for every $p \in \{p_1, \ldots, p_n\}$ and $\lambda_n \geq (s\lambda_{n+1}^{d-n} - 1)\|T\|_\infty \geq |w|\|T\|_\infty$, Lemma 5.2 shows that there exists a configuration ρ' such that $\rho_n \xrightarrow{w} \rho'$, and $\rho'|_{Q'} = \beta'$. Let us consider the word $\sigma \stackrel{\text{def}}{=} \sigma_1 \ldots \sigma_n w$. Notice that $|\sigma| \leq (\lambda_1^d + \cdots + \lambda_n^{d-n+1} + \lambda_{n+1}^{d-n})s \leq d\lambda_1^d s$ and we have proved that the lemma holds (second case).

Finally, assume that there exists a configuration ρ_{n+1} such that $\rho_n \xrightarrow{\sigma_{n+1}} \rho_{n+1}$ for some word $\sigma_{n+1} \in T^*$ and such that $\rho_{n+1}(p_{n+1}) \geq \lambda_{n+1}$ for some state $p_{n+1} \in R_n$. We assume that $|\sigma_{n+1}|$ is minimal. Observe that every intermediate configuration β such that $\rho_n \xrightarrow{u} \beta \xrightarrow{v} \rho_{n+1}$ with $uv = \sigma_{n+1}$ and $|v| \geq 1$ satisfies $\beta(p) < \lambda_{n+1}$ for every $p \in R_n$ by minimality of $|\sigma_{n+1}|$. We deduce that there exists a word $w \in T^*$ such that $\rho_n|_{Q\cup R_n} \xrightarrow{w|_{Q\cup R_n}} \rho_{n+1}|_{Q\cup R_n}$ and such that $|w| \leq s\lambda_{n+1}^{d-n}$. As $\rho_n(p) \geq \lambda_n$ for every $p \in \{p_1, \ldots, p_n\}$ and $\lambda_n \geq s\lambda_{n+1}^{d-n}\|T\|_\infty \geq |w|\|T\|_\infty$, Lemma 5.2 shows that there exists a configuration β such that $\rho_n \xrightarrow{w} \beta$ and $\beta|_{Q\cup R_n} = \rho_{n+1}|_{Q\cup R_n}$. In particular $\beta(p_{n+1}) = \rho_{n+1}(p_{n+1}) \geq \lambda_{n+1}$. By minimality of $|\sigma_{n+1}|$, we get $|\sigma_{n+1}| \leq |w| \leq s\lambda_{n+1}^{d-n}$. Now, observe that for every $p \in \{p_1, \ldots, p_n\}$ we have $\rho_{n+1}(p) \geq \rho_n(p) - |\sigma_{n+1}|\|T\|_\infty \geq \lambda_n - s\lambda_{n+1}^{d-n}\|T\|_\infty \geq \lambda_{n+1}$ by definition of λ_n. We have extended our sequence in such a way (i), (ii), and (iii) are fulfilled.

We have proved the lemma. □

Now, let us prove Theorem 6.1. Observe that if $d = 0$ the theorem is trivial. So, we can assume that $d \geq 1$. Let $Q_0 \stackrel{\text{def}}{=} \emptyset$, $\rho_0 \stackrel{\text{def}}{=} \rho$, and $s_0 \stackrel{\text{def}}{=} 1$. Notice that $\rho_0|_{Q_0}$ is $T|_{Q_0}$-bottom and the cardinal of the $T|_{Q_0}$-component of $\rho_0|_{Q_0}$ contains s_0 elements. We build by induction on n a sequence $Q_1, \ldots, Q_n$ of subsets of P, a sequence $\rho_1, \ldots, \rho_n$ of configurations, a sequence $\sigma_1, \ldots, \sigma_n$ of words in T^* such that for every $i \in \{1, \ldots, n\}$:

- $\rho_{i-1} \xrightarrow{\sigma_i} \rho_i$.
- $\rho_i|_{Q_i}$ is $T|_{Q_i}$-bottom.
- The cardinal of the $T|_{Q_i}$-component of $\rho_i|_{Q_i}$ is equal to s_i.
- $Q_{i-1} \subset Q_i$.
- $|\sigma_i|, s_i \leq (1 + d(1 + s_{i-1}\|T\|_\infty + \|\rho_{i-1}\|_\infty)^{d^d})s_{i-1}$.

Assume the sequence built for some $n \geq 0$. Lemma 6.2 on the configuration ρ_n and the set Q_n shows that there exist a word σ_{n+1} such that $|\sigma_{n+1}| \leq (1 + d(1 + s_n\|T\|_\infty + \|\rho_n\|_\infty)^{d^d})s_n$, and a configuration ρ_{n+1} such that $\rho_n \xrightarrow{\sigma_n} \rho_{n+1}$, such that:

- either $\rho_{n+1}|_{Q_n} = \rho_n|_{Q_n}$ and $\rho_{n+1}(p) > \rho_n(p)$ for every $p \in P\backslash Q_n$,
- or there exists Q_{n+1} such that $Q_n \subset Q_{n+1} \subseteq P$ such that $\rho_{n+1}|_{Q_{n+1}}$ is $T|_{Q_{n+1}}$-bottom and the cardinal s_{n+1} of its $T|_{Q_{n+1}}$-component satisfies:

$$s_{n+1} \leq (1 + d(1 + s_n\|T\|_\infty + \|\rho_n\|_\infty)^{d^d})s_n$$

Observe that in the second case we have extended the sequences. In the first case, let $\alpha \stackrel{\text{def}}{=} \rho_n$, $\beta \stackrel{\text{def}}{=} \rho_{n+1}$, $\sigma \stackrel{\text{def}}{=} \sigma_1 \ldots \sigma_n$, $w \stackrel{\text{def}}{=} \sigma_{n+1}$, and $Q \stackrel{\text{def}}{=} Q_n$. Since $Q_0 \subset Q_1 \cdots \subset Q_n$ are subsets of P, we deduce that $n \leq d$. Let us introduce $a = (1 + d)(2 + 2\|T\|_\infty + \|\rho\|_\infty)^{d^d}$ and $h = 2 + d^d$ and let us prove by induction on i that we have $|\sigma_i|, |s_i| \leq a^{h^i}$ and $\|\rho_i\|_\infty \leq (1 + \|T\|_\infty)a^{h^i}$ with the convention $\sigma_0 = \varepsilon$.

The rank $i = 0$ is immediate. Assume the rank $i - 1$ proved. We have:

$$\begin{aligned}
|\sigma_i|, s_i &\leq (1 + d(1 + s_{i-1}\|T\|_\infty + \|\rho_{i-1}\|_\infty)^{d^d})s_{i-1} \\
&\leq (1 + d)(2 + 2\|T\|_\infty)^{d^d} a^{h^{i-1}(d^d+1)} \\
&\leq a^{1+h^{i-1}(h-1)} \\
&\leq a^{h^i}
\end{aligned}$$

Since $\rho_{i-1} \xrightarrow{\sigma_i} \rho_i$, we deduce that $\|\rho_i\|_\infty \leq \|\rho_{i-1}\|_\infty + |\sigma_i|\|T\|_\infty \leq (1 + \|T\|_\infty)a^{h^i}$. The induction is proved.

It follows that $|\sigma| \leq da^{h^d}$, $|w| \leq a^{h^{d+1}}$, and $d\|\alpha\|_\infty, d\|\beta\|_\infty \leq d(1 + \|T\|_\infty)a^{h^{d+1}} \leq a^{1+h^{d+1}}$. Since $d \geq 1$, we deduce that $(1 + d) \leq 2^{d^d}$. In particular $a \leq (4 + 4\|T\|_\infty + 2\|\rho\|_\infty)^{d^d}$. We have proved Theorem 6.1.

7 PETRI NETS WITH CONTROL-STATES

A *P-Petri net with control-states* (or simply a Petri net with control-states when the finite set of states P is clear from the context) is a triple (S, T, E) where S is a non empty finite set of elements called *control-states*, T is a P-Petri net, and $E \subseteq S\times T\times S$ is a set of elements called *edges*. The *Parikh image* of a word $\pi = e_1 \ldots e_k$ of edges is the mapping $\#\pi \in \mathbb{N}^E$ defined by $\#\pi(e) = |\{j \in \{1, \ldots, k\} \mid e_j = e\}|$. The *displacement* of a transition $t = (\alpha_t, \beta_t)$ is the function $\Delta(t) \in \mathbb{Z}^P$ defined by $\Delta(t)(p) = \beta_t(p) - \alpha_t(p)$ for every $p \in P$. The *displacement* of an edge $e = (s, t, s')$ is defined as $\Delta(e) \stackrel{\text{def}}{=} \Delta(t)$. The displacement of a word $\pi = e_1 \ldots e_k$ of edges is $\Delta(\pi) \stackrel{\text{def}}{=} \sum_{1\leq j\leq k} \Delta(e_j)$. We denote by $|\pi| \stackrel{\text{def}}{=} k$ the *length* of π. A *path* π from a control-state s to a control-state s' is a word $\pi = e_1 \ldots e_k$ of edges in E such that there exist control-states $s_0, \ldots, s_k$ in S and transitions $t_1, \ldots, t_k$ in T such that $s_0 = s$, $s_k = s'$, and such that $e_j = (s_{j-1}, t_j, s_j)$ for every $1 \leq j \leq k$. Such a path is called a *cycle* if $s = s'$. A cycle θ of a Petri net with control-states is said to be *total* if $\#\theta(e) > 0$ for every $e \in E$. The cycle is said to be *simple* if the control-states $s_1, \ldots, s_k$ are distinct. A *multicycle* Θ is a sequence $\theta_1, \ldots, \theta_k$ of cycles. We denote by $|\Theta| \stackrel{\text{def}}{=} \sum_{j=1}^k |\theta_j|$, the *length* of a multicycle Θ. We introduce the *Parikh image* $\#\Theta \stackrel{\text{def}}{=} \sum_{j=1}^k \#\theta_j$ and the *displacement* $\Delta(\Theta) \stackrel{\text{def}}{=} \sum_{j=1}^k \Delta(\theta_j)$ of such a multicycle Θ. A multicycle Θ is said to be *total* if $\#\Theta(e) > 0$ for every $e \in E$.

A *Petri net with control-states* (S, T, E) is said to be *strongly connected* if for every pair (s, s') of control-states in S, there exists

a path from s to s'. Let us recall the classical Euler lemma in the context of Petri nets with control-states.

Lemma 7.1 (Euler Lemma). *For every total multicycle Θ in a strongly connected Petri net with control-states there exists a total cycle θ such that $\#\theta = \#\Theta$.*

We deduce the following lemma.

Lemma 7.2. *For any strongly connected Petri net with control-states (S, T, E), there exists a total cycle θ with a length bounded by $|E||S|$.*

Proof. Every edge $e \in E$ occurs in at least one simple cycle θ_e. It follows that the multicycle $\Theta = (\theta_e)_{e\in E}$ is total. From Lemma 7.1 we deduce that there exists a total cycle θ such that $\#\theta = \#\Theta$. Notice that $|\theta| = \sum_{e\in E} |\theta_e| \leq |E||S|$. □

A mapping $a \in \mathbb{Z}^P$ is called a *P-action* (or simply an action if P is clear from the context). Notice that displacements of transitions, edges, paths, and multicyles are actions. We associate with an action a the value $\|a\|_1 \stackrel{\text{def}}{=} \sum_{p\in P} |a(p)|$. Given a finite set Q, we denote by $a|_Q$ the action defined for every $q \in Q$ by $a|_Q(q) \stackrel{\text{def}}{=} a(q)$ if $q \in P$, and zero otherwise.

Lemma 7.3. *Let Θ be a multicycle of a P-Petri net with control-states (S, T, E) with $\|T\|_\infty > 0$, let $Q \subseteq P$, let $d \stackrel{\text{def}}{=} |P|$, and let $k > \|\Delta(\Theta)|_Q\|_1 (1 + 2|S|\|T\|_\infty)^{d(d+1)}$.*

There exists a multicycle Θ' such that:

- *For every $p \in P$ we have:*
  - *$\Delta(\Theta')(p) \leq 0$ if $\Delta(\Theta)(p) \leq 0$.*
  - *$\Delta(\Theta')(p) < 0$ if $\Delta(\Theta)(p) \leq -k$.*
  - *$\Delta(\Theta')(p) \geq 0$ if $\Delta(\Theta)(p) \geq 0$.*
  - *$\Delta(\Theta')(p) > 0$ if $\Delta(\Theta)(p) \geq k$.*
- *For every $q \in Q$ we have $\Delta(\Theta')(q) = 0$.*
- *For every edge $e \in E$ we have $\#\Theta'(e) > 0$ if $\#\Theta(e) \geq k$.*
- *$|\Theta'| \leq (|E| + d)(1 + 2|S|\|T\|_\infty)^{d(d+1)}$.*

Proof. Since every cycle can be decomposed into a sequence of simple cycles without changing the Parikh image, we can assume without loss of generality that Θ is a sequence of simple cycles. We introduce the set A of actions $\Delta(\theta)$ where θ ranges over the simple cycles, and $n \stackrel{\text{def}}{=} |A|$ its cardinal. Notice that for every $a \in A$ and for every $p \in P$, we have $|a(p)| \leq |S|\|T\|_\infty$. It follows that $n \leq (1 + 2|S|\|T\|_\infty)^d$.

We denote by s the sign function of a formally defined by $s(c) \stackrel{\text{def}}{=} 1$ if $\Delta(\Theta)(c) \geq 0$, $s(c) \stackrel{\text{def}}{=} -1$ otherwise. We also introduce the P-configuration f defined by $f(p) \stackrel{\text{def}}{=} |\Delta(\Theta)(p)|$ for every $p \in P$, and the function $g : A \to \mathbb{N}$ such that $g(a)$ is the number of simple cycle θ that occurs in Θ such that $\Delta(\theta) = a$.

Notice that $s(p)f(p) = \sum_{a\in A} g(a)a(p)$ for every $p \in P$. We introduce the following linear system over the free variables $(\alpha, \beta) \in \mathbb{N}^P \times \mathbb{N}^A$:

$$\bigwedge_{p\in P} s(p)\alpha(p) = \sum_{a\in A} \beta(a)a(p) \tag{1}$$

Notice that (f, g) is a solution of that system. From [15], there exists a finite set H of solutions (α, β) of that system such that $(f, g) = \sum_{(\alpha,\beta)\in H} (\alpha, \beta)$ and such that for every $(\alpha, \beta) \in H$, we have $\|\alpha\|_1 + \|\beta\|_1 \leq (2 + \sum_{a\in A} \|a\|_\infty)^d$. As $\sum_{a\in A} \|a\|_\infty \leq (1 + 2|S|\|T\|_\infty)^d |S|\|T\|_\infty$ we deduce (by using $|S|\|T\|_\infty \geq 1$):

$$\|\alpha\|_1 + \|\beta\|_1 \leq (1 + 2|S|\|T\|_\infty)^{d(d+1)} \tag{2}$$

We introduce the set H_0 of pairs $(\alpha, \beta) \in H$ such that $\alpha(q) = 0$ for every $q \in Q$. Observe that we have:

$$\begin{aligned}\|\Delta(\Delta)|_Q\|_1 &= \sum_{q\in Q} |\Delta(\Theta)(q) \\ &= \sum_{q\in Q} \sum_{(\alpha,\beta)\in H} \alpha(q) \\ &= \sum_{q\in Q} \sum_{(\alpha,\beta)\in H\setminus H_0} \alpha(q) \\ &\geq |H\setminus H_0|\end{aligned}$$

We introduce the set F of edges $e \in E$ such that $\Theta(e) \geq k$. Let $e \in F$. The sum $\sum_{(\alpha,\beta)\in H} \beta(e)$ is equal to $\#\Theta(e)$ and it is also equal to $\sum_{(\alpha,\beta)\in H\setminus H_0} \beta(e) + \sum_{(\alpha,\beta)\in H_0} \beta(e)$. As $\sum_{(\alpha,\beta)\in H\setminus H_0} \beta(e)$ is less than or equal to $|H\setminus H_0|(1+2|S|\|T\|_\infty)^{d(d+1)}$, we deduce that $\sum_{(\alpha,\beta)\in H_0} \beta(e) > 0$. In particular there exists $(\alpha, \beta) \in H_0$ such that $\beta(e) > 0$.

We also introduce the set R of $p \in P$ such that $|\Delta(\Theta)(p)| \geq k$. Let $p \in R$. The sum $\sum_{(\alpha,\beta)\in H} \alpha(p)$ is equals to $|\Delta(\Theta)(p)|$ and it is also equals to $\sum_{(\alpha,\beta)\in H\setminus H_0} \alpha(p)+\sum_{(\alpha,\beta)\in H_0} \alpha(p)$. As $\sum_{(\alpha,\beta)\in H\setminus H_0} \alpha(p) \leq |H\setminus H_0|(1 + 2|S|\|T\|_\infty)^{d(d+1)}$ we deduce that $\sum_{(\alpha,\beta)\in H_0} \alpha(p) > 0$. In particular there exists $(\alpha, \beta) \in H_0$ such that $\alpha(p) > 0$.

Now, let us introduce for each $e \in F$ a pair $(\alpha_e, \beta_e) \in H_0$ such that $\beta_e(e) > 0$, and let us introduce for each $p \in R$ a pair $(\alpha_p, \beta_p) \in H_0$ such that $\alpha_p(p) > 0$. Let us introduce $(\alpha', \beta') \stackrel{\text{def}}{=} \sum_{e\in F} (\alpha_e, \beta_e) + \sum_{p\in R} (\alpha_p, \beta_p)$ and observe that $\alpha'(e) > 0$ for every $e \in F$, $\beta'(p) > 0$ for every $p \in R$, and $\beta'(q) = 0$ for every $q \in Q$. Moreover, since (α', β') is a solution of (1), it follows that there exists a multicycle Θ' such that $\#\Theta' = \beta'$. In particular $\Delta(\Theta') = \Delta(\beta')$. Notice that $\Delta(\Theta') = \alpha'$, and $|\Theta'| = \|\beta'\|_1 \leq (|F| + |R|)(1 + 2|S|\|T\|_\infty)^{d(d+1)} \leq (|E| + d)(1 + 2|S|\|T\|_\infty)^{d(d+1)}$ and we have proved the lemma. □

8 PROOF OF THEOREM 3.1

In this section we provide a proof of Theorem 3.1.

We consider a universal population protocol (P, T, γ) that stably computes a n-counting predicate with L leaders, i.e. a predicate $\phi_{j=L\Rightarrow i\geq n}$ where i, j are two distinct states. Since T is a Petri net given as a finite set of rendez-vous transitions, we get $\|T\|_\infty \leq 2$. Let $I \stackrel{\text{def}}{=} \{i, j\}$. Let $d \stackrel{\text{def}}{=} |P|$ and $F = \gamma^{-1}(\{0\})$. Notice that if $d \geq 2$ since $I \subseteq P$. We introduce the following numbers:

$$b \stackrel{\text{def}}{=} (12 + 2L)^{(d-1)^{d-1}(1+(2+(d-1)^{d-1})^d)}$$

$$h \stackrel{\text{def}}{=} 3db$$

$$k \stackrel{\text{def}}{=} dh^{d^2+d+1}$$

$$a \stackrel{\text{def}}{=} h^{2d+3}$$

$$\ell \stackrel{\text{def}}{=} h^{5d^2}$$

$$r \stackrel{\text{def}}{=} 2(d-1)^{d-1}(1 + (2 + (d-1)^{d-1})^d)(5d^2 + 2d + 4)$$

We introduce $P' \stackrel{\text{def}}{=} P\backslash\{i\}$. It follows that $|P'| = d-1$. Theorem 6.1 applied on the Petri net $T|_{P'}$ and the configuration $L.j|_{P'}$ shows that there exist two words $\sigma, w \in T^*$, a set $Q \subseteq P'$, and two configurations α, β such that:

- $L.j|_{P'} \xrightarrow{\sigma|_{P'}} \alpha \xrightarrow{w|_{P'}} \beta$.
- $\alpha|_Q = \beta|_Q$.
- $\alpha(p) < \beta(p)$ for every $p \in P'\backslash Q$
- $\alpha|_Q$ is $T|_Q$-bottom.
- The cardinal of the $T|_Q$-component of $\alpha|_Q$ is bounded by b.
- $|\sigma|, |w|, d\|\alpha\|_\infty, d\|\beta\|_\infty \leq b$.

Notice that $|T| \leq (1+2\|T\|_\infty)^{2d} \leq h^{2d}$.

We introduce the Petri net with control-states (S, T, E) where S is the $T|_Q$-component of $\alpha|_Q$, and E is the set of edges $(s,t,s') \in S \times T \times S$ such that $s \xrightarrow{t|_Q} s'$. Observe that $|E| \leq |S||T|$ since for every (s,t,s') in E the value of s' is determined by the pair (s,t). It follows that we have:

$$|E| \leq h^{2d+1}$$

Lemma 7.2 shows that there exists a total cycle θ_E of (S,T,E) with a length bounded by $|S||E|$. Without loss of generality we can assume that this total cycle is on the control-state $\alpha|_Q$ by considering a rotation of that cycle. We denote by σ_E the label in T^* of this total cycle. Observe that $\|T\|_\infty|\sigma_E| \leq a$.

Since $\alpha \xrightarrow{w|_{P'}} \beta$, $\alpha|_Q = \beta|_Q$, and $\alpha(p) < \beta(p)$ for every $p \in P'\backslash Q$, we deduce that there exists a configuration η such that $\eta(p) \geq a\ell$ for every $p \in P'\backslash Q$, such that $\alpha|_Q = \eta|_Q$, and such that:

$$\alpha \xrightarrow{w^{a\ell}|_{P'}} \eta$$

Moreover, since σ_E is the label of a cycle on $\alpha|_Q$ we deduce that $\alpha|_Q \xrightarrow{\sigma_E|_Q} \alpha|_Q$. From $\eta|_Q = \alpha|_Q$ it follows that $\eta|_Q \xrightarrow{\sigma_E^\ell|_Q} \alpha|_Q$. As $\eta(p) \geq a\ell \geq \|T\|_\infty|\sigma_E^\ell|$ for every $p \in P'\backslash Q$, Lemma 5.2 shows that there exists a P'-configuration δ such that $\delta|_Q = \alpha|_Q$ and such that:

$$\eta \xrightarrow{\sigma_E^\ell|_{P'}} \delta$$

Observe that $|\sigma w^{a\ell}\sigma_E^\ell|\|T\|_\infty \leq (b+ba\ell)\|T\|_\infty + a\ell \leq 2ba\ell(\|T\|_\infty + 1) \leq a\ell h \leq h^{2d+4}\ell$.

Assume by contradiction that $n > h^{2d+4}\ell$, and let us introduce the configuration ρ' defined by $\rho' \stackrel{\text{def}}{=} L.j + (n-1).i$ where i is the state such that $I = \{i\}$. Lemma 5.2 shows that there exist P-configurations α', η', δ' such that $\alpha'|_{P'} = \alpha$, $\eta'|_{P'} = \eta$, $\delta'|_{P'} = \delta$ and such that:

$$\rho' \xrightarrow{\sigma} \alpha' \xrightarrow{w^{\alpha\ell}} \eta' \xrightarrow{\sigma_E^\ell} \delta'$$

Since the population protocol is stably computing the $(i \geq n)$ predicate and $n-1 < n$, there exists a 0-output stable configuration μ and a word $\sigma' \in T^*$ such that $\delta' \xrightarrow{\sigma'} \mu$. Lemma 5.1 shows that μ is (T,F)-stabilized. Observe that $w^{\alpha\ell}\sigma_E^\ell\sigma'$ is the label of a path of (S,T,E) from $\alpha|_Q$ to $\mu|_Q$. It follows that the Parikh image of that path can be decomposed as the Parikh image of a multicycle Θ and the Parikh image of an elementary path π. Observe $\Delta(\Theta) + \Delta(\pi) = \Delta(w^{\alpha\ell}\sigma_E^\ell\sigma') = \mu - \alpha'$. Notice that $\#\Theta(e) \geq \ell$ for every $e \in E$ since σ_E is the label of a total cycle on $\alpha|_Q$. Since π is an elementary path, we deduce that $\|\Delta(\pi)\|_1 \leq d|S|\|T\|_\infty \leq db\|T\|_\infty \leq h - db$.

We introduce the set $R \stackrel{\text{def}}{=} \{p \in P \mid \mu(p) < h\}$. Since $h \geq \|T\|_\infty(1+\|T\|_\infty)^{d^d}$, Lemma 5.4 shows that every configuration μ' such that $\mu|_R = \mu'|_R$ is (T,F)-stabilized. Observe that if $i \notin R$ then $\mu + i$ is (T,F)-stabilized, and by additivity, we deduce that $L.j + n.i \xrightarrow{T^*} \mu + i$. Since $\mu + i$ is (T,F)-stabilized, this configuration cannot reach a 1-output stable configuration. In particular the protocol is not stably computing the predicate $\phi_{j=L \Rightarrow i \geq n}$ and we get a contradiction. It follows that $i \in R$.

We introduce $R' \stackrel{\text{def}}{=} R\backslash\{i\}$. Since $d\|\alpha\|_\infty \leq b$ and $\alpha'|_{P'} = \alpha|_{P'}$, we deduce that $d\|\alpha'|_{R'}\|_\infty \leq b$. From $\Delta(\Theta) = \mu - \alpha' - \Delta(\pi)$ we deduce:

$$\|\Delta(\Theta)|_{R'}\|_1 \leq (d-1)h + b + h - db \leq dh$$

As $1+2|S|\|T\|_\infty \leq 1+h-2b < h$, we deduce that $k > \|\Delta(\Theta)|_{R'}\|_1(1+2|S|\|T\|_\infty)^{d(d+1)}$, Lemma 7.3 shows that there exists a multicycle Θ' such that:

- For every $p \in P$ we have:
  - $\Delta(\Theta')(p) \leq 0$ if $\Delta(\Theta)(p) \leq 0$.
  - $\Delta(\Theta')(p) < 0$ if $\Delta(\Theta)(p) \leq -k$.
  - $\Delta(\Theta')(p) \geq 0$ if $\Delta(\Theta)(p) \geq 0$.
  - $\Delta(\Theta')(p) > 0$ if $\Delta(\Theta)(p) \geq k$.
- For every $p \in R'$ we have $\Delta(\Theta')(p) = 0$.
- For every $e \in E$ we have $\#\Theta'(e) > 0$ if $\#\Theta(e) \geq k$.
- $\|\Theta'\|_1 \leq (|E|+d)(1+2|S|\|T\|_\infty)^{d(d+1)}$

Let $m \stackrel{\text{def}}{=} -\Delta(\Theta')(i)$ and let us prove that $m > 0$. We have $\Delta(\Theta)(i) = \mu(i) - \alpha'(i) - \Delta(\pi)(i)$. Since $i \in R$, we get $\mu(i) < h$. Since $L.j + (n-1).i \xrightarrow{\sigma} \alpha'$, we deduce that $\alpha'(i) = (n-1) - \Delta(\sigma)(i) \geq n-h$ since $|\sigma| \leq b$. We deduce that $\Delta(\Theta)(i) < h - n + h + h \leq 3h - n \leq -k$. Hence $\Delta(\Theta')(i) < 0$. It follows that $m > 0$.

Let $\eta \stackrel{\text{def}}{=} m.i + \Delta(\Theta')$. Notice that $\eta(i) = 0$ and $\eta(p) = 0$ for every $p \in R'$. In particular $\eta(p) = 0$ for every $p \in R$. Let us prove that η is a configuration. For every $p \in P\backslash R$ we have $\Delta(\Theta)(p) = \mu(p) - \eta'(p) - \Delta(\pi)(p) \geq db\|T\|_\infty + b - b - db\|T\|_\infty \geq 0$. It follows that $\Delta(\Theta')(p) \geq 0$. In particular $\eta(p) \geq 0$. We have proved that η is a configuration.

Finally, observe that $\#\Theta(e) \geq \ell \geq k$ for every $e \in E$. In particular $\#\Theta'(e) > 0$. Lemma 7.1 shows that $\#\Theta'$ is the Parikh image of a cycle θ on $x|_Q$. Let u be the label of that cycle. Since $|u| = \|\Theta'\|_1$, we deduce that:

$$\begin{aligned} |u|\|T\|_\infty &\leq \|T\|_\infty(|E|+d)(1+2b\|T\|_\infty)^{d(d+1)} \\ &\leq d(1+\|T\|_\infty)^{2d}(1+2b\|T\|_\infty)^{d^2+d+1} \\ &\leq \ell \end{aligned}$$

Lemma 5.2 shows that:

$$\eta' + m.i \xrightarrow{u} \eta' + \eta$$

We have proved:

$$L.j + (n-1+m).i \xrightarrow{\sigma w^{a\ell} u \sigma_E^\ell \sigma'} \mu + \eta$$

Since $(\mu+\eta)|_R = \mu|_R$ we deduce that $\mu + \eta$ is (T,F)-stabilized. It follows that this configuration cannot reach a 1-output stable configuration. In particular the protocol is not stably computing the predicate $\phi_{j=L \Rightarrow i \geq n}$ and we get a contradiction. It follows that $n \leq h^{2d+4}\ell = h^{5d^2+2d+4}$.

Notice that $d(1+\|T\|_\infty) \leq 2^d(1+\|T\|_\infty)^d \leq b$. Thus $h \leq b^2$. We deduce that $n \leq 14^r$. Since $d \geq 2$, we deduce that $d^d = ((d-1)+1)^d \geq (d-1)^d + d(d-1)^{d-1} + 1 \geq (d-1)^{d-1} + 2 + 1$. Hence $1+(2+(d-1)^{d-1})^d \leq 1+(d^d-1)^d \leq d^{d^2}$. Moreover, $2(d-1)^{d-1} \leq d^d$. Notice that $2d \leq d^2$ and $4 \leq d^2$. Hence $5d^2+2d+4 \leq 7d^2 \leq d^5$ since $7 \leq d^3$. We deduce that r is bounded by d^{d^2+d+3}. As $d^2+d+3 \leq (d+2)^2$, we get $r \leq d^{(d+2)^2}$.

We have proved Theorem 3.1.

9 CONCLUSION

We provided in this paper state complexity lower-bounds of the form $\Omega(\log\log(n)^h)$ for any $h < \frac{1}{2}$ for protocols stably computing the n counting predicates with a fix number of leaders. This lower-bound almost matches the upper-bound $O(\log\log(n))$ introduced in [7] by Blondin, Esparza, and Jaax. We left as open the exact asymptotic state complexity.

Notice that the state complexity of the leaderless n-counting predicate is still open since there is an exponential gap between the upper-bound $O(\log(n))$ given in [7] and the lower-bound introduced in this paper. Nevertheless, a recent paper, not yet reviewed but available on arXiv [8] shows that our lower-bound is also optimal without leader. In fact, this last paper exhibits for infinitly many n, a universal population protocol computing the leaderless n-counting predicate with $O(\log\log(n))$ states.

As future work, a natural extension of this paper is the computation of the state complexity of protocols computing the n-counting predicates (with or without leaders) in the non universal setting. As already mentionned, this is equivalent to the computation of the state complexity of the predicate ϕ defined as follows for every configuration $\rho \in \mathbb{N}^I$ with $I \stackrel{\text{def}}{=} \{i,j,k\}$:

$$\phi(\rho) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } \rho(j) = L \wedge |\rho| = s \wedge \rho(i) \geq n \\ 0 & \text{if } \rho(j) = L \wedge |\rho| = s \wedge \rho(i) < n \\ \star & \text{if } \rho(j) \neq L \vee |\rho| \neq s \end{cases}$$

When $s < n$, the state complexity of ϕ is one since a protocol with agents that can just output zero is computing the predicate in that case. So, the natural question is how we can take benefit from the fact that the population is bounded by some given s when s is large compared to n.

Another related problem, not considered in this paper, is the state complexity of protocols under some expected time of convergence constraints. Such a notion can be easily defined by equipping the population protocols with a probabilistic semantics. In this context, a natural question is the state complexity of counting predicates under rapid convergence constraint. Time-space trade-off has been considered in [1] in the context of population protocol that stably compute leader elections (a population protocol that converges to a configuration with just one agent in a given leader state), or the majority predicate that consists in stably computing the predicate $\rho(i) < \rho(j)$. Designing protocols that meet some rapid convergence constraints can be chalenging, even for very simple tasks like broadcasting a bit of information from a leader agent or detecting if a leader is present in the population [11].

ACKNOWLEDGMENTS

This work is supported by the grant ANR-17-CE40-0028 of the French National Research Agency ANR (project BRAVAS). The author would like to thank Javier Esparza and Philipp Czerner for fruitfull discussions, and reviewers for interesting feedbacks.

REFERENCES

[1] Dan Alistarh, James Aspnes, David Eisenstat, Rati Gelashvili, and Ronald L. Rivest. 2017. Time-Space Trade-offs in Population Protocols. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, Philip N. Klein (Ed.). SIAM, 2560–2579. https://doi.org/10.1137/1.9781611974782.169

[2] Dana Angluin, James Aspnes, Zoë Diamadi, Michael J. Fischer, and René Peralta. 2004. Computation in networks of passively mobile finite-state sensors. In *Proceedings of the Twenty-Third Annual ACM Symposium on Principles of Distributed Computing, PODC 2004, St. John's, Newfoundland, Canada, July 25-28, 2004*, Soma Chaudhuri and Shay Kutten (Eds.). ACM, 290–299. https://doi.org/10.1145/1011767.1011810

[3] Dana Angluin, James Aspnes, Zoë Diamadi, Michael J. Fischer, and René Peralta. 2006. Computation in networks of passively mobile finite-state sensors. *Distributed Comput.* 18, 4 (2006), 235–253. https://doi.org/10.1007/s00446-005-0138-3

[4] Dana Angluin, James Aspnes, and David Eisenstat. 2006. Stably computable predicates are semilinear. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing, PODC 2006, Denver, CO, USA, July 23-26, 2006*, Eric Ruppert and Dahlia Malkhi (Eds.). ACM, 292–299. https://doi.org/10.1145/1146381.1146425

[5] Dana Angluin, James Aspnes, David Eisenstat, and Eric Ruppert. 2007. The computational power of population protocols. *Distributed Comput.* 20, 4 (2007), 279–304. https://doi.org/10.1007/s00446-007-0040-2

[6] Michael Blondin, Javier Esparza, Blaise Genest, Martin Helfrich, and Stefan Jaax. 2020. Succinct Population Protocols for Presburger Arithmetic. In *37th International Symposium on Theoretical Aspects of Computer Science, STACS 2020, March 10-13, 2020, Montpellier, France (LIPIcs, Vol. 154)*, Christophe Paul and Markus Bläser (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 40:1–40:15. https://doi.org/10.4230/LIPIcs.STACS.2020.40

[7] Michael Blondin, Javier Esparza, and Stefan Jaax. 2018. Large Flocks of Small Birds: on the Minimal Size of Population Protocols. In *35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France (LIPIcs, Vol. 96)*, Rolf Niedermeier and Brigitte Vallée (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 16:1–16:14. https://doi.org/10.4230/LIPIcs.STACS.2018.16

[8] Philipp Czerner. 2022. Leaderless Population Protocols Decide Double-exponential Thresholds. https://doi.org/10.48550/ARXIV.2204.02115

[9] Philipp Czerner and Javier Esparza. 2021. Lower Bounds on the State Complexity of Population Protocols. In *PODC '21: ACM Symposium on Principles of Distributed Computing, Virtual Event, Italy, July 26-30, 2021*, Avery Miller, Keren Censor-Hillel, and Janne H. Korhonen (Eds.). ACM, 45–54. https://doi.org/10.1145/3465084.3467912

[10] Wojciech Czerwinski and Lukasz Orlikowski. 2021. Reachability in Vector Addition Systems is Ackermann-complete. *CoRR* abs/2104.13866 (2021). arXiv:2104.13866 https://arxiv.org/abs/2104.13866

[11] Bartlomiej Dudek and Adrian Kosowski. 2018. Universal protocols for information dissemination using emergent signals. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, Ilias Diakonikolas, David Kempe, and Monika Henzinger (Eds.). ACM, 87–99. https://doi.org/10.1145/3188745.3188818

[12] Javier Esparza, Pierre Ganty, Jérôme Leroux, and Rupak Majumdar. 2015. Verification of Population Protocols. In *26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1.4, 2015 (LIPIcs, Vol. 42)*, Luca Aceto and David de Frutos-Escrig (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 470–482. https://doi.org/10.4230/LIPIcs.CONCUR.2015.470

[13] Javier Esparza, Pierre Ganty, Jérôme Leroux, and Rupak Majumdar. 2017. Verification of population protocols. *Acta Informatica* 54, 2 (2017), 191–215. https://doi.org/10.1007/s00236-016-0272-3

[14] Jérôme Leroux. 2021. The Reachability Problem for Petri Nets is Not Primitive Recursive. *CoRR* abs/2104.12695 (2021). arXiv:2104.12695 https://arxiv.org/abs/2104.12695

[15] Loic Pottier. 1991. Minimal Solutions of Linear Diophantine Systems: Bounds and Algorithms. In *Proceedings of the 4th International Conference on Rewriting Techniques and Applications (RTA '91)*. Springer-Verlag, London, UK, UK, 162–173. http://dl.acm.org/citation.cfm?id=647192.720494

[16] Charles Rackoff. 1978. The Covering and Boundedness Problems for Vector Addition Systems. *Theor. Comput. Sci.* 6 (1978), 223–231. https://doi.org/10.1016/0304-3975(78)90036-1