State Complexity of Counting Population Protocols With Leaders

Jérôme Leroux
LaBRI, CNRS, Univ. Bordeaux, France

Abstract

Population protocols are a model of computation in which an arbitrary number of anonymous finite-state agents are interacting in order to decide by stable consensus if an initial configuration extended with some extra agents called leaders satisfies some property. In this paper, we focus on $n$-counting predicates that ask, given an initial configuration, if the number of agents in a given state is at least $n$. In a recent work it was exhibited for infinitely many $n$, a population protocol with at most $O(\log \log(n))$ states that decides the $n$-counting predicate. We prove that this bound is almost optimal, by observing that any population protocol deciding such a predicate requires at least $\Omega((\log \log(n))^{1/3})$ states.

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Population protocols, Petri nets, Distributed computation

Funding Jérôme Leroux: The author is supported by the grant ANR-17-CE40-0028 of the French National Research Agency ANR (project BRAVAS)

1 Introduction

Population protocols were introduced by Angluin et al. in [1, 2] to study the computational power of networks of small 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. This table corresponds intuitively to a conservative Petri net (the number of agents is preserved by each transition) where each line of the interaction table is matched by a transition of a Petri net.

Population protocols decide properties by stable consensus. Intuitively, from any initial configuration extended with some extra agents called leaders, and under some fairness conditions, in any infinite execution either all agents eventually accept or all agents eventually reject. The population protocol is said to be well-specified if the resulting consensus does not depend on the computation, but only on the initial configuration. Deciding if a population protocols is well-specified was proved to be decidable in [8, 9] by observing that the well-specified property 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, 7], it means that deciding the well-specified property of a population protocol is also Ackermannian-complete. In particular, population protocols maybe intrinsically very complicated.

In this paper, population protocols are assumed to be well-specified and the set of initial configurations accepted by a population protocol is called the decided predicate. In [3], Angluin et al. have shown that predicates decidable by population protocols are exactly the predicates definable in Presburger arithmetic. It follows that the state complexity of a Presburger predicate defined as the minimal number of states of a population protocols deciding it is well defined. In [4], by revisiting the construction of population protocols deciding Presburger predicates, some improvement on state complexity upper-bounds was derived.

Computing state complexities is a difficult problem. It follows that focusing on the state complexity of simple Presburger predicates is a natural question. The simplest non trivial
Presburger predicates are clearly the \( n \)-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 \( n \). In [5], it was exhibited an infinite set of natural numbers \( n \) for which the associated counting predicates can be decided by population protocols with \( O(\log \log(n)) \) states. Moreover, very recently in [3] the state complexity of population protocols deciding the \( n \)-counting predicate was proved to be at least \( \Omega(A^{-1}(n)) \) where \( A \) is some Ackermannian function. It follows that there is a gap between the known upper and lower bounds for the state complexity of counting predicates.

In this paper, we close this gap by proving that any population protocol deciding the counting predicate associated to a natural number \( n \) requires at least \( \Omega((\log \log(n))^{\frac{1}{3}\frac{1}{2} n}) \) states. Since our proof techniques allow some generalizations of the model of population protocols, we present our result for population protocols that allow leaders, agent destruction and creation. We call the classical population protocols the conservative ones. Compared to conservative population protocols, the number of reachable configurations from an initial configuration is no longer finite. Due to this observation, the notion of fair executions and well-specified population protocols are (briefly) revisited in this paper. It worth mentioning that our definitions match the classical ones for conservative population protocols.

In Section 2 we recall some basic definitions and results about Petri nets. In Section 3 we introduce the notions of stabilized, stable, and bottom configurations. The two first definitions are central for defining the semantics of (non conservative) population protocols and the last one is used for proving our lower bound. In Section 4 we introduce our generalized model of population protocols that allow leaders, agent destruction and creation. In Section 5 we provide bridges between our definitions and the classical definitions of population protocols. 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 execution kind of bottom configurations. Section 7 recalls the model of Petri net with 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 [11] in order to obtain small solutions for that linear system. Results of the previous sections are combined in Section 8 to obtain the state complexity lower bound \( \Omega((\log \log(n))^{\frac{1}{3}\frac{1}{2} n}) \). Some related open problems and future work are presented in Section 9.

## 2 Petri Nets

We first recall some basic definitions and results about Petri nets.

We assume that an infinite countable set \( C \) of elements called counters is fixed. A configuration \( \rho \) is a mapping \( \rho : C \to \mathbb{N} \) such that the set \( \text{used}(\rho) \overset{\text{def}}{=} \{ c \mid \rho(c) \neq 0 \} \) is finite.

We denote by 0 the zero configuration, i.e. the unique one satisfying \( \text{used}(0) = \emptyset \). Given a counter \( c \), we denote by \( 1_x \) the \( x \)-unit configuration defined by \( 1_x(c) = 1 \) and \( 1_x(c) = 0 \) for every counter \( c \neq x \). We associate with a configuration \( \rho \) the numbers \( \|\rho\|_{\infty} = \max_c \rho(c) \) and \( \|\rho\|_1 = \sum_c \rho(c) \). The sum of two configurations \( \alpha, \beta \) is the configuration \( \alpha + \beta \) defined point-wise by \( (\alpha + \beta)(c) \overset{\text{def}}{=} \alpha(c) + \beta(c) \) for every counter \( c \). The partial-order \( \leq \) over the configurations is also defined point-wise by \( \alpha \leq \beta \) if \( \alpha(c) \leq \beta(c) \) for every counter \( c \).

A transition \( t \) is a pair \((\rho_{\text{pre}}, \rho_{\text{post}})\) of configurations, where \( \rho_{\text{pre}} \) is called the precondition, and \( \rho_{\text{post}} \) the postcondition. We introduce \( \text{used}(t) \overset{\text{def}}{=} \text{used}(\rho_{\text{pre}}) \cup \text{used}(\rho_{\text{post}}) \) and \( \|t\|_{\infty} \overset{\text{def}}{=} \max\{\|\rho_{\text{pre}}\|_{\infty}, \|\rho_{\text{post}}\|_{\infty}\} \). We associate with a transition \( t \) the binary relation \( t \) over the configurations defined by \( \alpha \overset{t}{\rightarrow} \beta \) if there exists a configuration \( \rho_{\text{in}} \) such that \( \alpha = \rho_{\text{in}} + \rho_{\text{pre}} \)
and $\beta = \rho_{\text{pre}} + \rho_{\text{post}}$. Intuitively a transition first removes from $\alpha$ the precondition to get the intermediate configuration $\rho_{\text{pre}}$ and then add the postcondition to get $\beta$. We associate with a word $\sigma = t_1 \ldots t_k$ of transitions $t_1, \ldots, t_k$ the binary relation $\alpha \overset{\sigma}{\rightarrow} \beta$ if there exists a sequence $\rho_0, \ldots, \rho_k$ of configurations such that:

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

A Petri net is a finite set $T$ of transitions. We introduce $\text{used}(T) \overset{\text{def}}{=} \bigcup_{t \in T} \text{used}(t)$, and $T^*$ the set of words of transitions in $T$. We also define $\|T\|_\infty \overset{\text{def}}{=} \max\{|t|_\infty \mid t \in T\}$ if $T$ is a non empty Petri net and zero otherwise. We denote by $\overset{T}{\rightarrow}$ the binary relation over the configurations defined by $\alpha \overset{T}{\rightarrow} \beta$ if there exists a word $\sigma \in T^*$ such that $\alpha \overset{\sigma}{\rightarrow} \beta$. This relation is called the reachability relation of $T$. When $\alpha \overset{T}{\rightarrow} \beta$ we say that $\beta$ is $T$-reachable from $\alpha$.

A transition $t = (\rho_{\text{pre}}, \rho_{\text{post}})$ is said to be conservative if $\|\rho_{\text{pre}}\|_1 = \|\rho_{\text{post}}\|_1$. A Petri net $T$ is said to be conservative if every transition in $T$ is conservative. Notice that every configuration $\beta$ that is $T$-reachable from $\alpha$ satisfies $\|\beta\|_1 = \|\alpha\|_1$ for any conservative Petri net $T$. In particular the set of configurations that are $T$-reachable from any configuration $\rho$ is finite for every conservative Petri net $T$.

We say that a configuration $\rho$ is $T$-coverable from a configuration $\alpha$ if there exists a configuration $\beta \geq \rho$ that is $T$-reachable from $\alpha$. Notice that a configuration $\rho$ is $T$-coverable from a configuration $\alpha$ if, and only if, there exists a word $\sigma \in T^*$ such that $\alpha \overset{\sigma}{\rightarrow} \beta \geq \rho$ for some configuration $\beta$. In that case, the minimal length of such a word $\sigma$ can be bounded using Rackoff’s techniques with respect to $\|\rho\|_\infty$, $\|T\|_\infty$, and $|\text{used}(T)|$. We now recall those techniques.

Given a set $Q$ of counters, we define several restrictions related to $Q$ as follows. Given a configuration $\rho$, we denote by $\rho|_Q$ the configuration defined by $\rho|_Q(c) = \rho(c)$ if $c \in Q$, and zero otherwise. Given a transition $t = (\rho_{\text{pre}}, \rho_{\text{post}})$, we define the transition $t|_Q$ as the pair $t|_Q = (\rho_{\text{pre}}|_Q, \rho_{\text{post}}|_Q)$. Given a Petri net $T$, we introduce the Petri net $T|_Q = (t|_Q \mid t \in T)$. Given a word $\sigma = t_1 \cdots t_k$ of transitions, we introduce the word $\sigma|_Q = t_1|_Q \cdots t_k|_Q$. Notice that $\alpha \overset{\sigma}{\rightarrow} \beta$ implies $\alpha|_Q \overset{\sigma|_Q}{\rightarrow} \beta|_Q$. The converse property is true in some cases as shown by the following lemma.

**Lemma 1.** Assume that $\alpha|_Q \overset{\sigma|_Q}{\rightarrow} \rho$ for some configurations $\alpha, \rho$, some word $\sigma$ of transitions in a Petri net $T$, and some set $Q$ of counters. If $\alpha(c) \geq |\sigma|_\infty$ for every counter $c \in \text{used}(T) \setminus Q$ then there exists a configuration $\beta$ such that $\alpha \overset{\sigma}{\rightarrow} \beta$, $\beta|_Q = \rho$, and $\beta(c) \geq \alpha(c) - |\sigma|_\infty$ for every counter $c \in \text{used}(T) \setminus Q$.

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

We are now ready to recall a classical result used in [12] to prove that the $T$-coverability problem is decidable in exponential space.

**Lemma 2 (12).** If a configuration $\rho$ is $T$-coverable from a configuration $\alpha$, then there exists $\sigma \in T^*$ with a length bounded by $\|\rho\|_\infty + \|T\|_\infty d$ where $d \overset{\text{def}}{=} |\text{used}(T)|$, and a configuration $\beta \geq \rho$ such that $\alpha \overset{\sigma}{\rightarrow} \beta$.

**Proof.** This is a classical result obtained by Rackoff in [12] by induction on $d$. A complete proof with our notations is recalled in appendix.
We introduce the notion of stabilized, stabilizable, and bottom configurations. We assume that $T$ is a Petri net.

A configuration $\rho$ is said to be $(T,Q)$-stabilized for a set $Q$ of counters if used($\delta$) $\subseteq$ $Q$ for every configuration $\delta$ that is $T$-reachable from $\rho$. The following lemma shows that $(T,Q)$-stabilized configurations are characterized by the values of the “small counters”.

**Lemma 3.** Let $\rho$ be a $(T,Q)$-stabilized configuration, let $h$ be a positive integer satisfying 
$h \geq \|T\|_\infty(1+\|T\|_\infty)^d$ where $d \overset{\text{def}}{=} |\text{used}(T)|$, and let $R \overset{\text{def}}{=} \{c \mid \rho(c) < h\}$. Every configuration $\alpha$ such that $\alpha|R \leq \rho|R$ is $(T,Q)$-stabilized.

**Proof.** Let us consider a configuration $\alpha$ such that $\alpha|R \leq \rho|R$. There exists a configuration $\mu$ such that $\rho|R = \alpha|R + \mu$. Assume by contradiction that $\alpha$ is not $(T,Q)$-stabilized. It follows that there exists a configuration $\beta$ that is $T$-reachable from $\alpha$ and such that $\beta(x) > 0$ for some counter $x \notin Q$. Since $x \notin Q$ and $\rho$ is $(T,Q)$-stabilized, we deduce that $\rho(x) = 0$. In particular $x \in R$ since $h > 0$. It follows that the $x$-unit configuration $1_x$ is $T$-coverable from $\alpha$ since $1_x \leq \beta$. Lemma 2 shows there exists a word $\sigma \in T^*$ of length bounded by $(1+\|T\|_\infty)^d$ and a configuration $\gamma$ such that $\alpha \overset{\sigma}{\rightarrow} \gamma \geq 1_x$. It follows that $\alpha|R \overset{\gamma|R}{\rightarrow} \gamma|R$. From this relation and $\rho_R = \alpha|R + \mu$, we deduce that $\rho_R \overset{\sigma|R}{\rightarrow} \gamma|R + \mu$. Lemma 1 shows that there exists a configuration $\delta$ such that $\rho \overset{\sigma}{\rightarrow} \delta$ and $\delta|R = \gamma|R + \mu$. Since $x \in R$, we deduce that $\delta(x) = \gamma(x) + \mu(x) \geq 1_x(x) = 1$. It follows that $x \in \text{used}(\delta)$. As $x \notin Q$, it follows that $\rho$ is not $(T,Q)$-stabilized and we get a contradiction. We have proved the lemma.

**Remark 4.** A similar result was provided in [6] in the context of conservative Petri nets.

A configuration $\alpha$ is said to be $(T,Q)$-stable if every configuration $\beta$ that is $T$-reachable from $\alpha$, there exists a $(T,Q)$-stabilized configuration $\rho$ that is $T$-reachable from $\beta$. Clearly for any configuration $\alpha$ there exists a finite set $Q$ such that $\alpha$ is $(T,Q)$-stabilizable just by considering for $Q$ the set $\text{used}(T) \cup \text{used}(\alpha)$. The following lemma shows that in fact there exists a unique minimal for the inclusion set $Q$ such that $\alpha$ is $(T,Q)$-stabilizable. We denote by stab$_T(\alpha)$ this set.

**Lemma 5.** If a configuration $\alpha$ is $(T,Q_1)$-stabilizable and $(T,Q_2)$-stabilizable then it is $(T,Q_1 \cap Q_2)$-stabilizable.

**Proof.** Let $\beta$ be a configuration $T$-reachable from $\alpha$. Since $\alpha$ is $(T,Q_1)$-stabilizable, there exists a $(T,Q_1)$-stabilized configuration $\mu$ that is $T$-reachable from $\beta$. Since $\alpha$ is $(T,Q_2)$-stabilizable, it follows that there exists a $(T,Q_2)$-stabilized configuration $\rho$ that is $T$-reachable from $\mu$. Let us prove that $\rho$ is $(T,Q)$-stabilized with $Q \overset{\text{def}}{=} Q_1 \cap Q_2$. To do so, let $\delta$ be a configuration $T$-reachable from $\rho$. Since $\rho$ is $(T,Q_2)$-stabilized, we get used($\delta$) $\subseteq$ $Q_2$. Moreover, since $\delta$ is $T$-reachable from $\mu$ we deduce that used($\delta$) $\subseteq$ $Q_1$. It follows that used($\delta$) $\subseteq$ $Q$. We have proved that $\rho$ is $(T,Q)$-stabilized. It follows that $\alpha$ is $(T,Q)$-stabilizable.

The $T$-component of a configuration $\rho$ is the set of configurations $\beta$ such that $\rho \overset{T}{\rightarrow} \beta \overset{T}{\rightarrow} \rho$. A configuration $\rho$ is said to be $T$-bottom if its $T$-component is finite and every configuration $\beta$ such that $\rho \overset{T}{\rightarrow} \beta$ satisfies $\beta \overset{T}{\rightarrow} \rho$.
4 Population Protocols

In this section, we introduce our model of population protocols and some related notions.

A population pre-protocol $P$ is a tuple $(T, \rho_L, I, F)$ where $T$ is a Petri net, $\rho_L$ is a configuration called the configuration of leaders, $I, F$ are two finite sets of counters. When $\rho_L = 0$, the pre-protocol is said to be leaderless. When $T$ is a conservative Petri net, the pre-protocol is said to be conservative. A pre-protocol is said to be correctly-specified if for every configuration $\alpha$ such that $\emptyset \neq \text{used}(\alpha) \subseteq I$ the zero configuration $0$ is not $T$-reachable from $\rho_L + \alpha$ and the set $\text{stab}_T(\rho_L + \alpha)$ is included in $F$ or disjoint from $F$. A correctly-specified population pre-protocol is simply called a population protocol. Given a population protocol $P$, we introduce the set $\text{acc}(P)$ of configurations $\alpha$ such that $\emptyset \neq \text{used}(\alpha) \subseteq I$ and such that $\text{stab}_T(\rho_L + \alpha) \subseteq F$. The set $\text{acc}(P)$ is called the predicate decided by $P$. We also introduce $\text{used}(P) \overset{\text{df}}{=} \text{used}(T) \cup \text{used}(\rho_L) \cup I \cup F$.

A $n$-counting predicate where $n$ is a positive natural number is a set of configurations of the form $\{m1_x \mid m \geq n\}$ for some counter $x$. It is proved in [5] that there exists an infinite set $N$ of positive numbers such that for every $n \in N$, there exists a conservative population protocol $P_n$ deciding a $n$-counting predicate such that $|\text{used}(P_n)| \leq O(\log \log(n))$. In this paper, we show that this result is almost optimal by proving the following theorem.

\begin{theorem}
For every population protocol $P = (T, \rho_L, I, F)$ deciding a $n$-counting predicate, we have the following bound where $d = |\text{used}(P)|$:

$$n \leq (4 + 4\|T\|_\infty + 2\|\rho_L\|_\infty)^{2(d+1)^3}$$

\end{theorem}

For leaderless population protocols, Example 7 shows that there exist conservative leaderless population protocols $P_n$ deciding $n$-counting predicates with $|\text{used}(P_n)| \leq O(\log(n))$ when $n$ is a power of two. In fact, following [5], such a construction can be extended in such a way for every natural number $n$, there exists a conservative leaderless population protocol $P_n$ deciding $n$-counting predicate with $|\text{used}(P_n)| \leq O(\log(n))$. Proving that $|\text{used}(P_n)| \geq \Omega(\log(n))$ for every leaderless conservative population protocol $P_n$ deciding the $n$-counting predicate is still a problem left open in this paper.

\begin{example}[5]
The $2^d$-counting predicates can be decided by conservative leaderless population protocols as follows. We consider $d+2$ distinct counters denoted as $c_0, c_2, \ldots, c_{2^d}$, and we let $Q$ be the set of those counters. We introduce the Petri net $T \overset{\text{df}}{=} T_0 \cup T_1$ where:

$$T_0 \overset{\text{df}}{=} \{(1_{c_{2i}} + 1_{c_{2i+1}} + 1_{c_0}) \mid i \in \{0, \ldots, d-1\}\}$$

$$T_1 \overset{\text{df}}{=} \{(1_{c_{2d}} + 1_{c}, 1_{c_{2d}} + 1_{c_e}) \mid c \in Q\}$$

Just observe that $(T, 0, \{c_{2d}\}, \{c_{2d}\})$ is a conservative leaderless population protocol deciding $\{m1_{c_{2d}} \mid m \geq 2^d\}$.

5 Bridges to Classical Definitions

In this section, we provide bridges between our definitions of population protocols and the classical ones that are only defined for conservative population protocols. This section can be freely skipped since definitions and results provided in this section are not used anywhere else in the paper.
Let $T$ be a Petri net. A $T$-execution from an initial configuration $\rho_0$ is an infinite sequence $(\rho_j)_{j \in \mathbb{N}}$ of configurations such that for every $j \geq 1$ either $\rho_j = \rho_{j-1}$, or there exists a transition $t_j \in T$ such that $\rho_{j-1} \xrightarrow{t_j} \rho_j$. The set of counters limit-used by a $T$-execution is the set of counters $c$ such that $\rho_j(c) > 0$ for infinitely many $j$.

Following \cite{6}, a $T$-execution is said to be $T$-fair if for every configuration $\rho$ we have:

$$|\left\{ j \mid \rho_j \xrightarrow{T} \rho \right\}| = \infty \implies |\left\{ j \mid \rho_j = \rho \right\}| = \infty$$

Let us recall this classical result about $T$-fair $T$-executions.

$\blacktriangleright$ **Lemma 8.** Let $T$ be a conservative Petri net. For every $T$-fair $T$-execution $(\rho_j)_{j \in \mathbb{N}}$, there exists $j \in \mathbb{N}$ such that $\rho_j$ is $T$-bottom.

**Proof.** Since $T$ is conservative, the set of configurations $T$-reachable from $\rho_0$ is finite. It follows that there exists a configuration $\alpha$ such that $\rho_j = \alpha$ for infinitely many $j$. Observe that the $T$-component of $\alpha$ is finite since $T$ is conservative. Now, let $\rho$ be a configuration $T$-reachable from $\alpha$. Observe that for every $j$ such that $\rho_j = \alpha$, we have $\rho_j \xrightarrow{T} \rho$. Since the execution is fair, we derive that there exists $i$ such that $\rho_i = \rho$. Since $\rho_j = \alpha$ for infinitely many $j$, there exists $j \geq i$ such that $\rho_j = \alpha$. From $\rho_i \xrightarrow{T} \rho_j$, we derive $\alpha \xrightarrow{T} \rho$. We have proved that $\alpha$ is $T$-bottom.

Given a configuration $\rho$, we introduce the set $\text{stab}^T_1(\rho)$ as the union of the sets of counters limit-used by $T$-fair $T$-executions from $\rho$.

$\blacktriangleright$ **Lemma 9.** Let $T$ be a conservative Petri net. We have $\text{stab}^T_1(\rho) = \text{stab}^T_0(\rho)$ for every configuration $\rho$.

**Proof.** Let $Q \overset{3\text{rd}}{=} \text{stab}^T_0(\rho)$.

Let us first consider a counter $c \in \text{stab}^T_0(\rho)$. It follows that there exists a $T$-fair $T$-execution $(\rho_j)_{j \in \mathbb{N}}$ such that $\rho_j(c) > 0$ for infinitely many $j$. Lemma 8 shows that there exists $n \in \mathbb{N}$ such that $\rho_n$ is $T$-bottom. It follows that $\rho_j$ is $T$-bottom for any $j \geq n$. In particular, we can assume that $\rho_n(c) > 0$. Since $\rho$ is $(T, Q)$-stabilizable, it follows that $\rho_n$ is $(T, Q)$-stabilizable as well. In particular, there exists a $(T, Q)$-stabilized configuration $\rho$ that is $T$-reachable from $\rho_n$. As $\rho_n$ is $T$-bottom, the configuration $\rho_n$ is $T$-reachable from $\rho$. It follows that $\rho_n$ is $(T, Q)$-stabilized. As $\rho_n(c) > 0$ we deduce that $c \in Q$.

Conversely, let us consider a counter $c \in Q$. Let $Q'$ be the set of counters except $c$. By minimality of $Q$, Lemma 8 shows that $\rho$ is not $(T, Q')$-stabilizable. It follows that there exists a configuration $\alpha$ that is $T$-reachable from $\rho$, such that every configuration $\beta$ that is $T$-reachable from $\alpha$ is not $(T, Q')$-stabilized. As $T$ is conservative, the set of configurations $T$-reachable from $\alpha$ is finite. In particular there exists a $T$-bottom configuration that is $T$-reachable from $\alpha$. By replacing $\alpha$ by this configuration, we can assume without loss of generality that $\alpha$ is $T$-bottom. Moreover, as $\alpha$ is not $(T, Q')$-stabilizable, there exists a configuration $T$-reachable from $\alpha$ that uses $c$. Once again, by replacing $\alpha$ by this configuration, we can assume that $\alpha(c) > 0$. Now, observe that there exists a $T$-fair execution from $\rho$ such that all the configurations of the $T$-component of $\alpha$ are repeated infinitely often. Since $\alpha(c) > 0$, we deduce that the set of counters limit-used by this $T$-execution contains $c$. Hence $c \in \text{stab}^T_0(\rho)$.

Following \cite{8}, a conservative population pre-protocol $(T, \rho_L, I, F)$ is said to be well-specified if for every configuration $\alpha$ such that $\emptyset \neq \text{used}(\alpha) \subseteq I$ the set $\text{stab}^T_0(\rho_L + \rho)$ is
included in $F$ or disjoint from $F$. The set of configurations $\alpha$ such that $\emptyset \neq \text{used}(\alpha) \subseteq I$ and $\text{stab}_F(\rho, \alpha) \subseteq F$, is called the predicate accepted.

The following lemma provides the bridges.

**Theorem 10.** A conservative population pre-protocol is well-specified if and only if it is correctly-specified. Moreover, in that case the predicate decided and the predicate accepted coincide.

**Proof.** This is a direct corollary of Lemma 9.

### 6 Small Bottom Configurations

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 this theorem and are no longer used in the sequel.

**Theorem 11.** Let $T$ be a Petri net, let $d \overset{\text{def}}{=} |\text{used}(T)|$, let $\rho$ be a configuration, and let $b \overset{\text{def}}{=} (4 + 4||T|| + 2||\rho||)^{(d^d(1 + (2 + d^d)^{d+1}))}$. There exist two words $\sigma, w \in T^*$, a set of counters $Q \subseteq \text{used}(T)$, and two configurations $\alpha, \beta$ such that:

- $\rho \xrightarrow{\sigma} \alpha \xrightarrow{w} \beta$.
- $\alpha|_Q = \beta|_Q$.
- $\alpha(c) < \beta(c)$ for every counter $c \in \text{used}(T) \setminus Q$.
- $\alpha|_Q$ is $T|_Q$-bottom.
- The cardinal of the $T|_Q$-component of $\alpha|_Q$ is bounded by $b$.
- $|\sigma|, |w|, d||\alpha||, d||\beta|| \leq b$.

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

**Lemma 12.** Let $T$ be a Petri net, let $\rho$ be a configuration, let $Q$ be a set of counters included in $\text{used}(T)$ such that $\rho|_Q$ is $T|_Q$-bottom, let $s$ be the cardinal of the $T|_Q$-component of $\rho|_Q$, and let $d \overset{\text{def}}{=} |\text{used}(T)\setminus Q|$.

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

- either $\rho'|_Q = \rho|_Q$ and $\rho'(c) > \rho(c)$ for every counter $c \in \text{used}(T) \setminus Q$,
- or there exists a set $Q' \subseteq \text{used}(T)$ 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:

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

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

Let $\rho_0 \overset{\text{def}}{=} \rho$. 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 $c_1, \ldots, c_n$ of distinct counters in $\text{used}(T)\setminus Q$ such that for every $i \in \{1, \ldots, n\}$ we have:

1. $\rho_{i-1} \xrightarrow{\sigma_i} \rho_i$.
2. $|\sigma_i| \leq \lambda_i^{d^d+1}s$. 

State Complexity of Counting Population Protocols With Leaders

(iii) \( \rho_i(c) \geq \lambda_i \) for every \( c \in \{c_1, \ldots, c_n\} \).

So, let us assume that \( \rho_1, \rho_2, \sigma_1, \ldots, \sigma_n, \) and \( c_1, \ldots, c_n \) are built for some \( n \geq 0 \). Since \( c_1, \ldots, c_n \) are distinct elements in \( \text{used}(T) \setminus Q \), it follows that \( n \leq d \).

Let us first assume that \( n = d \). In that case, we have \( \rho_d(c) \geq \lambda_d \) for every \( c \in \text{used}(T) \setminus Q \). As \( \rho|Q \) is a \( T|Q \)-bottom configuration and \( \rho|Q \stackrel{(\sigma_1 \ldots \sigma_d)|Q}{\longrightarrow} \rho_d|Q \) 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 \( \rho_d|Q \stackrel{w|Q}{\longrightarrow} \rho|Q \) and \( |w| < s \). Since \( \lambda_d \geq s \|T\|_\infty \geq |w|\|T\|_\infty \), Lemma 4 shows that \( \rho_d \stackrel{w}{\longrightarrow} \rho' \) for some configuration \( \rho' \) such that \( \rho'|Q = \rho|Q \) and such that for every \( c \in \text{used}(T) \setminus Q \) we have \( \rho'(c) \geq \rho(c) - |w|\|T\|_\infty \geq \lambda_d - s\|T\|_\infty > \rho(c) \) by definition of \( \lambda_d \). Let us introduce \( \sigma \equiv \sigma_1 \ldots \sigma_d w \) and notice that \( |\sigma| \leq (\lambda^d_1 + \ldots + \lambda^d_{d-1} + 1)s \leq (1 + d\lambda^d_1)s \) and we have proved that the lemma holds (first case).

So we can assume that \( n < d \). Let us introduce the set \( R_n = (\text{used}(T) \setminus Q) \setminus \{c_1, \ldots, c_n\} \).

Since \( |R_n| = d - n \), the set \( R_n \) is non empty.

Assume first that for every configuration \( \beta \) such that \( \rho_n \stackrel{T^*}{\longrightarrow} \beta \), we have \( \beta(c) < \lambda_{n+1} \) for every \( c \in R_n \). In that case let \( Q' \equiv Q \cup R_n \). It follows that the cardinal of the set of configurations \( \beta' \) such that \( \rho_n|Q' \stackrel{\alpha}{\longrightarrow} \beta' \) is bounded by \( s\lambda^d_{n+1} \). Hence, there exists a configuration \( \beta' \) that is \( T|Q \)-bottom and a word \( w \in T^* \) such that \( \rho_n|Q' \stackrel{w|Q'}{\longrightarrow} \beta' \) and such that \( |w| < s\lambda^d_{n+1} \). Notice that the cardinal \( \rho_n|Q \) of the \( T|Q \)-component of \( \beta' \) is bounded by \( s\lambda^d_{n+1} \leq s\lambda^d_1 \). As \( \rho_n(e) \geq \lambda_n \) for every \( e \in \{c_1, \ldots, c_n\} \) and \( \lambda_n \geq (s\lambda^d_{n+1} - 1)\|T\|_\infty \geq |w|\|T\|_\infty \), Lemma 3 shows that there exists a configuration \( \rho' \) such that \( \rho_n \stackrel{w}{\longrightarrow} \rho' \) and \( \rho'|Q = \beta' \). Let us consider the word \( \sigma \equiv \sigma_1 \ldots \sigma_d w \). Notice that \( |\sigma| \leq (\lambda^d_1 + \ldots + \lambda^d_{d-n+1} + \lambda^d_{n-1})s \leq d\lambda^d_1 s \) and we have proved that the lemma holds (second case).

Finally, assume that there exists a configuration \( \rho_{n+1} \) such that \( \rho_n \stackrel{\sigma_{n+1}}{\longrightarrow} \rho_{n+1} \) for some word \( \sigma_{n+1} \in T^* \) and such that \( \rho_{n+1}(c_{n+1}) \geq \lambda_{n+1} \) for some counter \( c_{n+1} \in R_n \). We assume that \( |\sigma_{n+1}| \) is minimal. Observe that every intermediate configuration \( \beta \) such that \( \rho_n \stackrel{w}{\longrightarrow} \beta \), with \( \rho_{n+1} \) and \( |w| \geq 1 \) satisfies \( \beta(c) < \lambda_{n+1} \) for every \( c \in R_n \) by minimality of \( |\sigma_{n+1}| \). We deduce that there exists a word \( w \in T^* \) such that \( \rho_n|Q \cup R_n \stackrel{w|Q \cup R_n}{\longrightarrow} \rho_{n+1}|Q \cup R_n \) and such that \( |w| \leq s\lambda^d_{n+1} \). As \( \rho_n(e) \geq \lambda_n \) for every \( e \in \{c_1, \ldots, c_n\} \) and \( \lambda_n \geq (s\lambda^d_{n+1} - 1)\|T\|_\infty \geq |w|\|T\|_\infty \), Lemma 3 shows that there exists a configuration \( \beta \) such that \( \rho_n \stackrel{w}{\longrightarrow} \beta \) and \( \beta|Q \cup R_n = \rho_{n+1}|Q \cup R_n \). In particular \( \beta(c_{n+1}) = \rho_{n+1}(c_{n+1}) \geq \lambda_{n+1} \).

By minimality of \( |\sigma_{n+1}| \), we get \( |\sigma_{n+1}| \leq |w| \leq s\lambda^d_{n+1} \). Now, observe that for every \( e \in \{c_1, \ldots, c_n\} \) we have \( \rho_{n+1}(e) \geq \rho_n(e) - |\sigma_{n+1}|\|T\|_\infty \geq \lambda_n - s\lambda^d_{n+1}\|T\|_\infty \geq \lambda_{n+1} \) by definition of \( \lambda_n \). 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 11. Observe that if \( d = 0 \) the theorem is trivial. So, we can assume that \( d \geq 1 \). Let \( Q_0 \equiv 0, \rho_0 \equiv \rho, \) and \( s_0 \equiv 1 \). 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 \( \text{used}(T) \), a sequence \( \rho_1, \ldots, \rho_n \) of configurations, a sequence \( \sigma_1, \ldots, \sigma_n \) of words in \( T^* \) such that for every \( i \in \{1, \ldots, n\} \):

- \( \rho_{i-1} \stackrel{\sigma_i}{\longrightarrow} \rho_i \).
- \( \rho_i|Q_i \) is \( T|Q_i \)-bottom.
- The cardinal of the \( T|Q_i \)-component of \( \rho_i|Q_i \) is equal to \( s_i \).
- \( Q_{i-1} \subset Q_i \).
- \( |\sigma_i|, s_i \leq (1 + d(1 + s_{i-1})\|T\|_\infty + \|\rho_{i-1}\|_\infty)\lambda^d_{i-1} \).
Assume the sequence built for some $n \geq 0$. Lemma 12 on the configuration $\rho_n$ and the set $Q_n$ shows that there exist a word $\sigma_{n+1}$ such that $|\sigma_{n+1}| \leq 1 + d(1 + s_n ||T||_\infty + \|\rho_n\|_\infty d^i) s_n$, and a configuration $\rho_{n+1}$ such that $\rho_n \triangleright \rho_{n+1}$, such that:

- either $\rho_n |_{Q_n} = \rho_n |_{Q_n}$ and $\rho_{n+1} (c) > \rho_n (c)$ for every $c \in \text{used}(T) \setminus Q_n$,
- or there exists $Q_{n+1}$ such that $Q_n \subset Q_{n+1} \subseteq \text{used}(T)$ 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:

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

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

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

$$|\sigma_i|, s_i \leq (1 + d(1 + s_{i-1} ||T||_\infty + \|\rho_{i-1}\|_\infty d^i)) s_{i-1}$$

$$\leq (1 + d)(2 + 2 ||T||_\infty)^d a^{h-1}(d+1)$$

$$\leq a^{1+h-1(h-1)}$$

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

It follows that $|\sigma| \leq d a^h$, $|w| \leq a^{h+1}$, and $d||\alpha||_\infty, d||\beta||_\infty \leq d(1 + ||T||_\infty) a^{h+1} \leq a^{1 + d^{h+1}}$. Since $d \geq 1$, we deduce that $(1 + d) \leq 2d^i$. In particular $a \leq (4 + 4 ||T||_\infty + 2 ||\rho||_\infty d^i)$. We have proved Theorem 11.

7 Petri Nets with States

A Petri net with states is a triple $(S, T, E)$ where $S$ is a non empty finite set of elements called states, $T$ is a 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 $t = (\rho_{\text{pre}}, \rho_{\text{post}})$ is the function $\Delta (t)$ that maps each counter $c$ on the integer $\Delta (t) (c) \overset{\text{def}}{=} \rho_{\text{post}} (c) - \rho_{\text{pre}} (c)$. The displacedness of an edge $e = (s, t, s')$ is defined as $\Delta (e) \overset{\text{def}}{=} \Delta (t)$. The displacement of a word $\pi = e_1 \ldots e_k$ of edges is $\Delta (\pi) \overset{\text{def}}{=} \sum_{1 \leq j \leq k} \Delta (e_j)$. We denote by $|\pi| \overset{\text{def}}{=} k$ the length of $\pi$. A path $\pi$ from a state $s$ to a state $s'$ is a word $\pi = e_1 \ldots e_k$ of edges in $E$ such that there exists 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 $\theta$ of a Petri net with states is said to be total if $\# \theta (e) > 0$ for every $e \in E$. The cycle is said to be simple if the states $s_1, \ldots, s_k$ are distinct. A multicycle $\Theta$ is a sequence $\theta_1, \ldots, \theta_k$ of cycles. We denote by $|\Theta| \overset{\text{def}}{=} \sum_{j=1}^k \theta_j$, the length of a multicycle $\Theta$. We introduce the Parikh image $\# \Theta \overset{\text{def}}{=} \sum_{j=1}^k \# \theta_j$ and the displacement $\Delta (\Theta) \overset{\text{def}}{=} \sum_{j=1}^k \Delta (\theta_j)$ of such a multicycle $\Theta$. A multicycle $\Theta$ is said to be total if $\# \Theta (e) > 0$ for every $e \in E$.

A Petri net with states $(S, T, E)$ is said to be strongly connected if for every pair $(s, s')$ of 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 states.
10 State Complexity of Counting Population Protocols With Leaders

Lemma 13 (Euler Lemma). For every total multicycle $\Theta$ in a strongly connected Petri net with states there exists a total cycle $\theta$ such that $\# \theta = \# \Theta$.

We deduce the following lemma.

Lemma 14. For any strongly connected Petri net with states $(S, T, E)$, there exists a total cycle $\theta$ with a length bounded by $|E||S|$.

Proof. Every edge $e \in E$ occurs in at least one simple cycle $\theta_e$. It follows that the multicycle $\Theta = (\theta_e)_{e \in E}$ is total. From Lemma 13 we deduce that there exists a total cycle $\theta$ such that $\# \theta = \# \Theta$. Notice that $|\theta| = \sum_{e \in E} |\theta_e| \leq |E||S|$.

A function $a$ from the set of counters to the set of integers such that $\{a(c) \neq 0\}$ is finite, is called an action. Notice that displacements of transitions, edges, paths, and multicycles are actions. We associate with an action $a$ the value $\|a\|_1 \overset{\text{def}}{=} \sum_c |a(c)|$. Given a set $Q$ of counters, we denote by $a|Q$ the action defined by $a|Q(c) \overset{\text{def}}{=} a(c)$ if $c \in Q$, and zero otherwise.

Lemma 15. Let $Q$ be a set of counters, let $\Theta$ be a multicycle of a Petri net with states $(S, T, E)$ such that $\|T\|_\infty > 0$, let $d \overset{\text{def}}{=} \max(\text{used}(T))$ and let $k > \|\Delta(\Theta)|_Q\|_1 (1 + 2|S||T\|_\infty)^{d(d+1)}$.

There exists a multicycle $\Theta'$ such that:

- For every counter $c$ we have:
  - $\Delta(\Theta')(c) \leq 0$ if $\Delta(\Theta)(c) \leq 0$.
  - $\Delta(\Theta')(c) < 0$ if $\Delta(\Theta)(c) \leq -k$.
  - $\Delta(\Theta')(c) \geq 0$ if $\Delta(\Theta)(c) \geq 0$.
  - $\Delta(\Theta')(c) > 0$ if $\Delta(\Theta)(c) \geq k$.

- For every counter $c \in Q$ we have $\Delta(\Theta')(c) = 0$.

- 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 $\Theta$ is a sequence of simple cycles. We introduce the set $A$ of actions $\Delta(\theta)$ where $\theta$ ranges over the simple cycles, and $n \overset{\text{def}}{=} |A|$ its cardinal. Notice that for every $a \in A$ and for every counter $c$, we have $|a(c)| \leq |S||T\|_\infty$ if $c \in \text{used}(T)$, and $a(c) = 0$ otherwise. It follows that $n \leq (1 + 2|S||T\|_\infty)^d$.

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

Notice that $s(c)f(c) = \sum_{a \in A} g(a)a(c)$ for every counter $c$. We introduce the following linear system over the free variables $(\alpha, \beta)$ where $\alpha$ is a configuration and $\beta \in \mathbb{N}^A$:

$$\bigwedge_c s(c)\alpha(c) = \sum_{a \in A} \beta(a)a(c) \tag{1}$$

Notice that $(f, g)$ is a solution of that system. From [11], there exists a finite set $H$ of solutions $(\alpha, \beta)$ 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 $\alpha(c) = 0$ for counter $c \in Q$. Observe that $\sum_{c \in Q} \sum_{(\alpha, \beta) \in H} \alpha(c)$ is equal to $\sum_{c \in Q} |\Delta(\Theta)(c)| = \|\Delta(\Delta)|_Q\|_1$, and it is also equals to $\sum_{c \in Q} \sum_{(\alpha, \beta) \in H \setminus H_0} \alpha(c) \geq |H \setminus H_0|$. In particular we have:

$$|H \setminus H_0| \leq \|\Delta(\Delta)|_Q\|_1$$

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 equals to $\sum_{(\alpha, \beta) \in H \setminus H_0} \beta(e)$ and it is also equals to $\sum_{(\alpha, \beta) \in H \setminus H_0} \beta(e)$.

As $\sum_{(\alpha, \beta) \in H \setminus H_0} \beta(e) \leq |H \setminus H_0|(1 + 2|S||T|| \infty )^{d(d+1)}$ we deduce that $\sum_{(\alpha, \beta) \in H \setminus H_0} \beta(e) > 0$. In particular there exists $(\alpha, \beta) \in H_0$ such that $\beta(e) > 0$.

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

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 counter $c \in R$ a pair $(\alpha_c, \beta_c) \in H_0$ such that $\alpha_c(c) > 0$. Let us introduce $(\alpha', \beta') \equiv \sum_{e \in F} (\alpha_e, \beta_e) + \sum_{c \in R} (\alpha_c, \beta_c)$ and observe that $\alpha'(e) > 0$ for every $e \in F$, $\beta'(e) > 0$ for every $e \in R$, and $\beta'(c) = 0$ for every $c \in Q$. Moreover, since $(\alpha', \beta')$ is a solution of (1), it follows that there exists a multicycle $\Theta'$ 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.

\section{Proof of \textbf{Theorem 6}}

In this section we provide a proof of Theorem 6. The following simple technical lemma will be useful two times in this proof.

\begin{lemma}
Let $T$ be a Petri net, let $\rho$ be a configuration from which the zero configuration $0$ is not $T$-reachable, and $\rho'$ be a configuration $T$-reachable from $\rho$ that is $(T, F')$-stabilized for some set $F'$. Then $\text{stab}_T(\rho)$ has a non empty intersection with $F'$.
\end{lemma}

\begin{proof}
Let $Q \overset{\text{def}}{=} \text{stab}_T(\rho)$. Since $\rho$ is $(T, Q)$-stabilizable, we deduce that $\rho'$ is also $(T, Q)$-stabilizable. Lemma 5 shows that $\rho'$ is $(T, Q \cap F')$-stabilizable. It follows that that exists a configuration $\beta$ that is $T$-reachable from $\rho'$ such that used($\beta$) $\subseteq Q \cap F'$. Since $\beta$ is reachable from $\rho$, we deduce that $\beta \neq 0$. Hence used($\beta$) is not empty. It follows that $Q \cap F'$ is non empty.
\end{proof}

We consider a population protocols $P \overset{\text{def}}{=} (T, \rho_L, \{x\}, F)$ deciding the $n$-counting predicate $\{m \mathbin{\|}_x \mid m \geq n\}$ for some $n \geq 1$. Let $d \overset{\text{def}}{=} \text{used}(P)$. Notice that $x \in \text{used}(T)$ since otherwise $n = 1$ and the proof of Theorem 6 is trivial. We denote by $\overline{x}$ the set of counters distinct from $x$. It follows that $|\text{used}(T)|_{\overline{x}}| \leq d - 1$. Notice that if $d = 1$ then we also have $n = 1$ so we can assume that $d \geq 2$. Let $b \overset{\text{def}}{=} (4 + 4|T|| \infty + 2|\rho_L|| \infty )^{(d-1)d-1(1+2(d-1)d-1)}$.

Theorem 11 applied on the Petri net $T|_{\overline{x}}$ and the configuration $\rho_L|_{\overline{x}}$ shows that there exist two words $\sigma, w \in T^*$, a set $Q \subseteq \text{used}(T|_{\overline{x}})$, and two configurations $\alpha, \beta$ such that:

- $\rho_L|_{\overline{x}} \overset{\alpha|_{\overline{x}}}{\longrightarrow} \alpha \overset{\gamma}{\longrightarrow} \beta$.
- $\alpha|_Q = \beta|_Q$.
- $\alpha(c) < \beta(c)$ for every $c \in \text{used}(T|_{\overline{x}}) \setminus Q$.
- $\alpha|_Q$ is $T|_Q$-bottom.
The cardinal of the $T|Q$-component of $\alpha|Q$ is bounded by $b$.

$|\sigma|, |w|, |d| |\alpha|_\infty, |d| |\beta|_\infty \leq b$.

We introduce $h \triangleq d(1 + ||T||_\infty)b$. Notice that used$(T|_{\{x\}}) = used(T) \setminus \{x\}$, and $|T| \leq (1 + 2||T||_\infty)^2d$. In particular $|T| \leq h^{2d}$.

We introduce the Petri net with 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 $s \overset{\ell}{\rightarrow} Q s'$. 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 14 shows that there exists a total cycle $\theta_E$ 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 state $\alpha|Q$ by considering a rotation of that cycle. We denote by $\sigma_E$ the label in $T^*$ of this total cycle. Observe that $||T||_\infty|\sigma_E| \leq a$ with:

$$a \triangleq h^{2d+3}$$

We introduce the following number $\ell$:

$$\ell \triangleq h^{5d^2}$$

Since $\alpha \overset{w|_\infty|Q}{\rightarrow} \beta$, $\alpha|Q = \beta|Q$, and $\alpha(c) < \beta(c)$ for every $c \in used(T) \setminus (Q \cup \{x\})$, we deduce that there exists a configuration $\gamma$ such that $\gamma(c) \geq a\ell$ for every $c \in used(T) \setminus (Q \cup \{x\})$, such that $\alpha|Q = \gamma|Q$, and such that:

$$\alpha \overset{w|_\infty|Q}{\rightarrow} \gamma$$

Moreover, since $\sigma_{E}$ is the label of a cycle on $\alpha|Q$ we deduce that $\alpha|Q \overset{\sigma_{E}|Q}{\rightarrow} \alpha|Q$. From $\gamma|Q = \alpha|Q$ it follows that $\gamma|Q \overset{\sigma_{E}|Q}{\rightarrow} \alpha|Q$. As $\gamma(c) \geq a\ell \geq ||T||_\infty|\sigma_E|$ for every $c \in used(T) \setminus (Q \cup \{x\})$, Lemma 1 shows that there exists a configuration $\delta$ such that $\delta|Q = \alpha|Q$ and such that:

$$\gamma \overset{\sigma_{\ell}|_\infty}{\rightarrow} \delta$$

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

Assume by contradiction that $n > h^{2d+4} \ell$, and let us introduce the configuration $\rho'$ defined by $\rho' \overset{w|_\infty}{\rightarrow} \rho_x + (n - 1)1_x$. Lemma 3 shows that there exist configurations $\alpha', \gamma', \delta'$ such that $\alpha'|_{1_x} = \alpha$, $\gamma'|_{1_x} = \gamma$, $\delta'|_{1_x} = \delta$ and such that:

$$\rho' \overset{w|_\infty}{\rightarrow} \gamma' \overset{\sigma_{\ell}|_\infty}{\rightarrow} \delta'$$

Since the population protocol is deciding the $n$-counting predicate and $n - 1 < n$, the configuration $\rho'$ is $(T, F')$-stabilizable for some set $F'$ disjoint from $F$. It follows that there exists a $(T, F')$-stabilized configuration $\mu$ and a word $\sigma' \in T^*$ such that $\delta' \overset{\sigma'}{\rightarrow} \mu$. Observe that $w^a \sigma_{\ell}|_\infty \sigma'$ 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 $\Theta$ and the Parikh image of an elementary path $\pi$. Observe $\Delta(\Theta) + \Delta(\pi) = \Delta(w^a \sigma_{\ell}|_\infty \sigma') = \mu - \alpha'$. Notice that $\#\Theta(c) \geq \ell$ for every $c \in E$ since $\sigma_{E}$ is the label of a total cycle on $\alpha|Q$. Since $\pi$ 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 $R \overset{\text{def}}{=} \{ c \mid \mu(c) < h \}$. Since $h \geq \| T \|_\infty (1 + \| T \|_\infty)^d$, Lemma 13 shows that every configuration $\mu'$ such that $\mu|_R = \mu'|_R$ is $(T, F')$-stabilized. Observe that if $x \notin R$ then $\mu + 1_x$ is $(T, F')$-stabilized, and by monotonicity, we deduce that $\rho_L + n 1_x \xrightarrow{T,F} \mu + 1_x$.

Lemma 16 shows that $\text{stab}_T(\rho_L + n 1_x)$ has a non empty intersection with $F'$. In particular the population protocol is not deciding the $n$-counting predicate and we get a contradiction. It follows that $x \in R$.

We introduce $P \overset{\text{def}}{=} R \setminus \{ x \}$. Since $d\| \alpha \|_\infty \leq b$ and $\alpha'|_{\{ x \}} \overset{\text{def}}{=} \alpha|_{\{ x \}}$, we deduce that $d\| \alpha' \|_P \leq b$. From $\Delta(\Theta) = \mu - \alpha' - \Delta(\sigma)$ we deduce:

$$\| \Delta(\Theta) \|_P \leq (d - 1)h + b - db \leq dh$$

Let us introduce $k \overset{\text{def}}{=} dh^{d+1}$. As $1 + 2|S|\| T \|_\infty \leq 1 + h - 2b < h$, we deduce that $k > \| \Delta(\Theta) \|_P \leq (1 + 2|S|\| T \|_\infty)^{d(d+1)}$, Lemma 15 shows that there exists a multicycle $\Theta'$ such that:

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

Let $m \overset{\text{def}}{=} -\Delta(\Theta')(x)$ and let us prove that $m > 0$. We have $\Delta(\Theta)(x) = \mu(x) - \alpha'(x) - \Delta(\sigma)(x)$. Since $x \in R$, we get $\mu(x) < h$. Since $\rho_L + (n - 1)1_x \xrightarrow{T,F} \alpha'$, we deduce that $\alpha'(x) = \rho_L(x) + (n - 1) - \Delta(\sigma)(x) \geq n - h$ since $|\sigma| \leq b$. We deduce that $\Delta(\Theta)(x) < h - n + h + h = 3h - n \leq -k$. Hence $\Delta(\Theta')(x) < 0$. It follows that $m > 0$.

Let $\gamma \overset{\text{def}}{=} m 1_x + \Delta(\Theta')$. Notice that $\gamma(x) = 0$ and $\gamma(c) = 0$ for every counter $c \in P$. In particular $\gamma(c) = 0$ for every $c \notin R$. Let us prove that $\gamma$ is a configuration. For every counter $c \notin R$ we have $\Delta(\Theta)(c) = \mu(c) - \gamma'(c) - \Delta(\pi)(c) \geq db\| T \|_\infty + b - db\| T \|_\infty \geq 0$. It follows that $\Delta(\Theta')(c) \geq 0$. In particular $\gamma(c) \geq 0$. We have proved that $\gamma$ is a configuration.

Finally, observe that $\#\Theta(c) \geq \ell \geq k$ for every $c \in E$. In particular $\#\Theta'(c) > 0$. Lemma 13 shows that $\#\Theta'$ is the Parikh image of a cycle $\theta$ on $x|_Q$. Let $u$ be the label of that cycle. Since $|u| = \| \Theta' \|_1$, we deduce that:

$$|u|\| T \|_\infty \leq \| T \|_\infty (|E| + d)(1 + 2b\| T \|_\infty)^{d(d+1)}$$

$$\leq d(1 + \| T \|_\infty)^{2d+1} \leq \ell$$

Lemma 11 shows that:

$$\gamma' + m 1_x \xrightarrow{T,F} \gamma' + \gamma$$

We have proved:

$$\rho_L + (n - 1 + m)1_x \xrightarrow{\Sigma \omega^u v^\ell} \mu + \gamma$$

Since $(\mu + \gamma)|_R = \mu|_R$ we deduce that $\mu + \gamma$ is $(T, F')$-stabilized. Lemma 16 shows that $\text{stab}_T(\rho_L + (n - 1 + m)1_x)$ has a non empty intersection with $F'$. Hence the population protocol is not deciding the $n$-counting predicate and we get a contradiction. It follows that
\[ n \leq h \cdot 2^{d+4} \cdot \ell = h \cdot 5^{d+2} + 2d + 4. \] Notice that \( d(1 + \|T\|_\infty) \leq 2^d(1 + \|T\|_\infty)^d \leq b. \) Thus \( h \leq b^2. \) We deduce that \( n \leq (4 + 4\|T\|_\infty + 2\|\rho_L\|_\infty)^e \) where:

\[ e \overset{\text{def}}{=} 2(d-1)^{d-1}(1 + (2 + (d-1)^{d-1})^d)(5d^2 + 2d + 4) \]

Since \( d \geq 2 \), we deduce that \( d^d = ((d-1)+1)^d \geq (d-1)^d + d(d-1)^{d-1} + 1 \geq (d-1)^{d-1} + 2d + 1. \) Hence \( 1 + (2 + (d-1)^{d-1})^d \leq 1 + (d-1)^d \leq d^d. \) 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 \( e \) is bounded by \( d^{d^2 + d + 3}. \) As \( d \leq 2^{d-1} \), we deduce that \( e \leq 2^{(d-1)(d^2 + d + 3)}. \) From \( (d-1)(d^2 + d + 3) = d^3 + 2d - 3 \leq (d+1)^3 \), we deduce that \( e \leq 2^{(d+1)^3}. \)

We have proved Theorem \( \ref{thm:main}. \)

9 Conclusion

This paper introduced population protocols that allows agent destruction and creation. Compared to conservative population protocols, the set of reachable configurations from a given initial configuration is no longer finite. Due to this problem, we adapted the definitions of well-specified properties and fair executions by introducing the notion of correctly-specified and stabilizable configurations.

While the predicates decided by conservative population protocols are known to be exactly the ones definable in the Presburger arithmetic, we left as open the expressive power of (generalized) population protocols. We conjecture that the expressive power is unchanged compared to the conservative population protocols but we left it open for future work.

We provided a state complexity lower-bound for population protocols deciding counting predicates that almost matches the upper-bound for conservative population protocols. This result proves 1) that it is impossible to compute a counting predicate with a too small number of counters, and 2) that population protocols do not provide a way to define strictly more succinctly protocols compared to the conservative ones (at least for the counting predicates). In the statement of Theorem \( \ref{thm:main} \) one can easily replace \( \frac{1}{3} \) (obtained thanks to the bound \( d \leq 2^d \)) by \( \frac{1}{2^{d^2 + d + 3}} \) for any \( \varepsilon > 0 \) (by observing that \( d \leq 2^{d^2} \) for any large enough \( d \)). Providing a matching upper-bound, without the \( \frac{1}{2^{d^2 + d + 3}} \) requires an improved version of Theorem \( \ref{thm:main} \) that we left as open.

For leaderless conservative protocols, the state complexity is left open and there is an exponential gap between the known upper and lower bounds.

References

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

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

3. Dana Angluin, James Aspnes, David Eisenstat, and Eric Ruppert. The computational power of population protocols. Distributed Comput., 20(4):279–304, 2007. doi:10.1007/s00446-007-0040-2
4 Michael Blondin, Javier Esparza, Blaise Genest, Martin Helfrich, and Stefan Jaax. Succinct population protocols for presburger arithmetic. In Christophe Paul and Markus Bläser, editors, 37th International Symposium on Theoretical Aspects of Computer Science, STACS 2020, March 10-13, 2020, Montpellier, France, volume 154 of LIPIcs, pages 40:1–40:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.STACS.2020.40.

5 Michael Blondin, Javier Esparza, and Stefan Jaax. Large flocks of small birds: on the minimal size of population protocols. In Rolf Niedermeier and Brigitte Vallée, editors, 35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France, volume 96 of LIPIcs, pages 16:1–16:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.STACS.2018.16.

6 Philipp Czerner and Javier Esparza. Lower bounds on the state complexity of population protocols. In Avery Miller, Keren Censor-Hillel, and Janne H. Korhonen, editors, PODC ’21: ACM Symposium on Principles of Distributed Computing, Virtual Event, Italy, July 26-30, 2021, pages 45–54. ACM, 2021. doi:10.1145/3465084.3467912.

7 Wojciech Czerwinski and Lukasz Orlikowski. Reachability in vector addition systems is ackermann-complete. CoRR, abs/2104.13866, 2021. URL: https://arxiv.org/abs/2104.13866, arXiv:2104.13866.

8 Javier Esparza, Pierre Ganty, Jérôme Leroux, and Rupak Majumdar. Verification of population protocols. In Luca Aceto and David de Frutos-Escrig, editors, 26th International Conference on Concurrency Theory, CONCUR 2015, Madrid, Spain, September 1-4, 2015, volume 42 of LIPIcs, pages 470–482. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015. doi:10.4230/LIPIcs.CONCUR.2015.470.

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

10 Jérôme Leroux. The reachability problem for petri nets is not primitive recursive. CoRR, abs/2104.12695, 2021. URL: https://arxiv.org/abs/2104.12695, arXiv:2104.12695.

11 Loïc Pottier. Minimal solutions of linear diophantine systems: Bounds and algorithms. In Proceedings of the 4th International Conference on Rewriting Techniques and Applications, RTA ’91, pages 162–173, London, UK, UK, 1991. Springer-Verlag. URL: http://dl.acm.org/citation.cfm?id=94/192, doi:10.1016/0304-3975(78)90036-1.

12 Charles Rackoff. The covering and boundedness problems for vector addition systems. Theor. Comput. Sci., 6:223–231, 1978. URL: http://dx.doi.org/10.1016/0304-3975(78)90036-1, doi:10.1016/0304-3975(78)90036-1.
Proof. We recall the proof to help the reader to be familiar with Rackoff proof techniques. In fact, similar but more complex proofs techniques are used in Lemma [12]. We consider a Petri net $T$ and a configuration $\rho$, and we introduce $r \overset{\text{def}}{=} \|\rho\|_\infty$ and $s \overset{\text{def}}{=} \|T\|_\infty$. If $r = 0$ or $s = 0$ the lemma is trivial. So, we can assume that $r, s \geq 1$.

We introduce the sequence $(\lambda_d)_{d \in \mathbb{N}}$ defined by $\lambda_0 = 0$ and by induction by $\lambda_{d+1} = (r + s\lambda_d)^{d+1} + \lambda_d$. Let us prove by induction on $d \geq 1$ that $\lambda_d \leq (r + s)^{d^d}$. The rank $d = 1$ is trivial. Assume the rank $d$ proved for some $d \geq 1$ and let us prove the rank $d + 1$. Notice that $r + s\lambda_d \leq r + s(r + s)^d \leq (r + s)^{1+d^d}$. It follows that $\lambda_{d+1} \leq (r + s)^{d+1} + (r + s)^d \leq 2(r+s)^{d+1} \leq (r+s)^{1+d+1}$ since $r+s \geq 2$. Now, just observe that $(d+1)^{d+1} \geq 1 + d + d^{d+1}$ and we have proved the induction.

Next, let us prove by induction on $d \in \mathbb{N}$ that for every set of counters $Q$ such that $|Q| = d$, and for every configuration $\alpha$ such that $\rho|_Q$ is $T|_Q$-coverable from $\alpha$, there exists a word $\sigma \in T^*$ with a length bounded by $\lambda_d$, and a configuration $\beta$ such that $\alpha \overset{\sigma|_Q}{\rightarrow} \beta \geq \rho|_Q$. When $d = 0$, the proof is immediate. Let us assume the rank $d$ proved, and let us prove the rank $d + 1$. Let $Q$ be a set of counters such that $|Q| = d + 1$, and let $\alpha$ be a configuration such that $\rho|_Q$ is $T|_Q$-coverable from $\alpha$. There exists a minimal $k$ for which there exists a sequence $t_1, \ldots, t_k$ of transitions and a sequence $\rho_0, \ldots, \rho_k$ of configurations such that:

$$\alpha = \rho_0 \xrightarrow{t_1|Q} \rho_1 \cdots \xrightarrow{t_k|Q} \rho_k \geq \rho|_Q$$

Let $b \overset{\text{def}}{=} r + s\lambda_d$. Observe that if for every $j \in \{0, \ldots, k\}$ and for every $c \in Q$ we have $\rho_j(c) < b$, then $\rho_0, \ldots, \rho_k$ are in a set that contains at most $b^{d+1}$ elements. By minimality of $k$, we deduce that $1 + k \leq b^{d+1}$ and we are done since $k \leq \lambda_{d+1}$ in that case. So, we can assume that there exists a minimal $j \in \{0, \ldots, k\}$ such that there exists a counter $x \in Q$ such that $\rho_j(x) \geq b$.

Observe that the configurations $\rho_0, \ldots, \rho_{j-1}$ are in a set with at most $b^{d+1}$ elements. So, by minimality of $j$, we deduce that $j \leq b^{d+1}$.

Let $Q' \overset{\text{def}}{=} Q \setminus \{x\}$. Observe that $\rho|_{Q'}$ is $T|_{Q'}$-coverable from $\rho_j|_{Q'}$. It follows by induction that there exists a word $w \in T^*$ with a length bounded by $\lambda_d$, and a configuration $\beta'$ such that $\rho_j|_{Q'} \xrightarrow{w|_{Q'}} \beta' \geq \rho|_{Q'}$. Since $\rho_j(x) \geq b \geq s\lambda_d \geq s|w|$, Lemma [1] shows that there exists a configuration $\beta$ such that $\beta|_{Q'} = \beta'$ and $\rho_j|_{Q'} \xrightarrow{w|_{Q'}} \beta$. Observe that $\beta(x) \geq \rho_j(x) - s|\sigma| \geq r \geq r(\rho(x))$. Moreover, as $\beta|_{Q'} = \beta' \geq \rho|_{Q'}$, we deduce that $\beta \geq \rho|_Q$.

From $\alpha \xrightarrow{t_1 \cdots t_w} \beta \geq \rho|_Q$, by minimality of $k$, we deduce that $k \leq j + |w| \leq b^{d+1} + \lambda_d = \lambda_{d+1}$. So, we are done also in that case.

Now, let us consider a configuration $\alpha$ from which $\rho$ is $T$-coverable. Let $Q \overset{\text{def}}{=} \text{used}(T)$, and let $d \overset{\text{def}}{=} |Q|$. From the previous induction, we deduce that there exists a word $\sigma \in T^*$ with a length bounded by $\lambda_d$ and a configuration $\beta$ such that $\alpha \xrightarrow{\sigma|_Q} \beta \geq \rho|_Q$. Since $\text{used}(T) \subseteq Q$, it follows that $\sigma|_Q = \sigma$. Moreover, for every counter $c \notin Q$, notice that since $\rho$ is $T$-coverable from $\alpha$, we have $\alpha(c) \geq \rho(c)$. From $\alpha \xrightarrow{\sigma} \beta$ and $c \notin \text{used}(T)$, we also get $\alpha(c) = \beta(c)$. We have proved that $\beta \geq \rho$. The lemma is proved.