Population protocols

Abstract. If you have any questions, feel free to ask your questions by mail (`peva.blanchard@epfl.ch`), or come by the office INR 211.

Consider population comprising two species of agents σ_g (green) and σ_b (blue). We study the following predicate:

$$P: \quad \#\sigma_g - 2 \cdot \#\sigma_b \leq 4 \tag{1}$$

where $\#\sigma_c$ denotes the number of agents with color c. Recall the protocol $\mathcal{A}$ defined in the lecture.

- state space: leader bit $l \in \{L, \perp\}$; counter $u \in \{-s, \dots, s\}$ where $s \geq 5$ is a fixed constant; output bit $b \in \{0, 1\}$.
- initialization: leader bit $l_{init} = 1$ (all leaders); counter $u_{init} = 1$ if green agent, $u_{init} = -2$ otherwise (blue agent); output bit $b_{init} = 0$
- rules: when two agents x, y meet, $(l_x, u_x, b_x),\ (l_y, u_y, b_y) \to (l'_x, u'_x, b'_x),\ (l'_y, u'_y, b'_y)$
  - if both non-leaders ($l_x = l_y = \perp$), then nothing changes.
  - if, e.g., agent x is a leader ($l_x = L$), then

$$\begin{aligned} l'_x &= L, \quad l'_y = \perp \\ u'_x &= q(u_x, u_y) \underset{def}{=} \max\{-s, \min\{s, u_x + u_y\}\} \\ u'_y &= r(u_x, u_y) \underset{def}{=} u_x + u_y - q(u_x, u_y) \\ b'_x &= b'_y = b_x \end{aligned}$$

We assume the following fairness condition.

Definition 1 (Global fairness). *An execution E is fair if and only if for every configuration C occurring infinitely often in E, for every configuration C' reachable from C, C' also occurs infinitely often in E.*

Intuitively, it means that if something is reachable infinitely often, then it is actually reached infinitely often.

The goal of this exercice is to prove that $\mathcal{A}$ computes the predicate P. First, some warm-up.

Question 1. What does it mean for a population protocol to compute the predicate P?

Proof. A population protocol $\mathcal{B}$ computes the predicate P if for any population size n, for any initial assignment (proportion of each species) I, in any fair execution, eventually all the agents permanently output $P(I)$. □

Question 2. Show that in any fair execution of $\mathcal{A}$, there is eventually a single leader.

Proof. Let $E = C_1, C_2, \dots$ be a fair execution, where C_i is the i-th configuration. Let $l(C)$ be the number of leaders in the configuration C. Initially, $l(C_1) = n$ where n is the population size. By the rules of the protocol, one leader disappears only if two leaders meet. Therefore, $l(C_i) \geq 1$ for all i. Moreover, the number of leaders is non-increasing, i.e., $l(C_{i+1} \leq l(C_i)$ for all i. Thus, it must be constant at some point, i.e., for all sufficiently large i, $l(C_i) = k$. Let C be any configuration that appears infinitely often in the execution (so $l(C) = k$). If $k \geq 2$, then there exists a transition $C \to C'$ obtained by making two leaders in C meet. In particular, $l(C') = k - 1$. The fairness condition ensures that C' occurs infinitely often in the execution, whence $l(C') = k$; this is a contradiction. Thus, $k = 1$, i.e., there is a unique leader eventually. □

Question 3. Show that, for any configuration C in an execution,

$$\sum_{\text{agent } x} u_x(C) = \#\sigma_g - 2 \cdot \#\sigma_b$$

where $u_x(C)$ is the value of the counter of agent x in configuration C.

Proof. From the initialization procedure, the equality holds for the initial configuration of the execution. Assume the equality holds for a configuration C and let $C \to C'$ be any transition from C. Let (x, y) be the two agents involved in this transition. If none of them are leaders, then nothing changes, i.e., $C = C'$, and the equality obviously holds for C'. Assume x is a leader (and the initiator if y is also a leader). By the rules of the protocol, we have, for all agents $z \notin \{x, y\}$

$$\begin{aligned}
u_x(C') &= q(u_x(C), u_y(C)) \\
u_y(C') &= u_x(C) + u_y(C) - q(u_x(C), u_y(C) \\
u_z(C') &= u_z(C)
\end{aligned}$$

Thus the equality also holds for C'. □

Thanks to the previous claims, we can focus on the suffix E' (of the execution E) in which there is a single leader λ. We have to prove that, eventually, the counter u_λ of λ satisfies:

$$u_\lambda = \max\{-s, \min\{s, \#\sigma_g - 2 \cdot \#\sigma_b\}\} \tag{2}$$

The proof relies on the (classical) *potential method*. For any configuration C in the suffix E', consider the quantity

$$p(C) = \sum_{x \neq \lambda} |u_x(C)| \tag{3}$$

Intuitively, this function measures the (non-negative) mass of the *non-leaders*. We will show that p cannot increase, and thus, is eventually constant.

Consider a transition $C \to C'$ in the execution suffix E' due to the meeting of the leader λ and (non-leader) agent x. We use the following notations:

$$\begin{aligned}
u_\lambda = u_\lambda(C) \; u'_\lambda = u_\lambda(C') \\
u_x = u_x(C) \; u'_x = u_x(C')
\end{aligned}$$

Question 4. Assume that $u_x \geq 0$. Show that

$$\begin{aligned}
u'_\lambda &= u_\lambda + \min\{u_x, s - u_\lambda\} \\
u'_x &= u_x - \min\{u_x, s - u_\lambda\}
\end{aligned}$$

Conclude that, in this case, p does not increase during the transition.

Proof. We have

$$\begin{aligned}
u'_\lambda &= \max\{-s, \min\{s, u_\lambda + u_x\}\} \\
&= \max\{-s, \underbrace{u_\lambda}_{\geq -s} + \underbrace{\min\{s - u_\lambda, u_x\}}_{\geq 0}\} \\
&= u_\lambda + \min\{s - u_\lambda, u_x\} \\
u'_x &= u_x + u_\lambda - u'_\lambda \\
&= u_x - \min\{s - u_\lambda, u_x\}
\end{aligned}$$

In particular, $|u'_x| \leq |u_x|$. We have

$$\begin{aligned}
p' &= \sum_{z \neq \lambda} |u'_z| \\
&= \sum_{z \notin \{x, \lambda\}} |u'_z| + |u'_x| \\
&= \sum_{z \notin \{x, \lambda\}} |u_z| + |u'_x| \text{ since the other agents states have not changed} \\
&\leq p
\end{aligned}$$

□

Question 5. Show that p does not increase either if $u_x \leq 0$.

Proof. We have

$$\begin{aligned} u'_\lambda &= \max\{-s, \min\{s, \underbrace{u_\lambda + u_x}_{\leq u_\lambda \leq s}\}\} \\ &= \max\{-s, u_\lambda + u_x\} \\ &= u_\lambda - \min\{-u_x, s + u_\lambda\} \\ u'_x &= u_x + u_\lambda - u'_\lambda \\ &= u_x + \min\{-u_x, s + u_\lambda\} \end{aligned}$$

In particular, $|u'_x| \leq |u_x|$, and $p' \leq p$. □

We conclude that p is eventually constant (non-increasing sequence of integer values). Let E'' be the suffix (of E') during which p is constant.

Question 6. For any configuration C in E'' show that, if it is impossible decrease p from C, then one of the following cases holds:

- $p(C) = 0$
- $u_\lambda(C) = s$ and for any $x \neq \lambda$, $u_x(C) \geq 0$
- $u_\lambda(C) = -s$ and for any $x \neq \lambda$, $u_x(C) \leq 0$

Conclude that

$$u_\lambda(C) = \max\{-s, \min\{s, \#\sigma_g - 2 \cdot \#\sigma_b\}\}$$

Proof. We assume that no transitions from C make p decrease. Assume that $p = p(C) \neq 0$ (otherwise, we are done). Then, there exists an agent x such that $u_x \neq 0$. Consider the transition $C \to C'$ obtained by making λ and x meet. We first show that necessarily, $|u_\lambda| = s$. Indeed, if $-s < u_\lambda < s$, the answers to questions 4 and 5 show that $|u'_x| < |u_x|$ and thus $p' < p$; this is a contradiction.

Assume that $u_\lambda = s$. If there were some agent z with $u_z < 0$, then the transition obtained from C by making z and λ meet yield $|u'_z| < |u_z|$ (again from the expressions given in answers to question 5), and thus $p' < p$; this is a contradiction. Thus, for all $z \neq \lambda$, $u_z \geq 0$. The case $u_\lambda = -s$ is proved similarly. □

Question 7. Show that $\mathcal{A}$ computes the predicate P. *(don't forget the fairness assumption)*

Proof. It suffices to check that eventually the counter u_λ of the (eventually) unique leader λ satisfies

$$u_\lambda = \max\{-s, \min\{s, \#\sigma_g - 2 \cdot \#\sigma_b\}\}$$

Consider the suffix of the execution during which the quantity p is constant. By question 6, there are three cases:

- $p = 0$. Then for all $x \neq \lambda$, $u_x = 0$. Thus

$$u_\lambda = \sum_x u_x = \#\sigma_g - 2 \cdot \#\sigma_b$$

- $u_\lambda = s$ and $u_x \geq 0$ for all $x \neq \lambda$. Then

$$s + \underbrace{\sum_{x \neq \lambda} u_x}_{\geq 0} = \#\sigma_g - 2 \cdot \#\sigma_b$$

- $u_\lambda = -s$ and $u_x \geq 0$ for all $x \neq \lambda$. Then

$$-s + \underbrace{\sum_{x \neq \lambda} u_x}_{\leq 0} = \#\sigma_g - 2 \cdot \#\sigma_b$$

The claim holds in all these cases. □