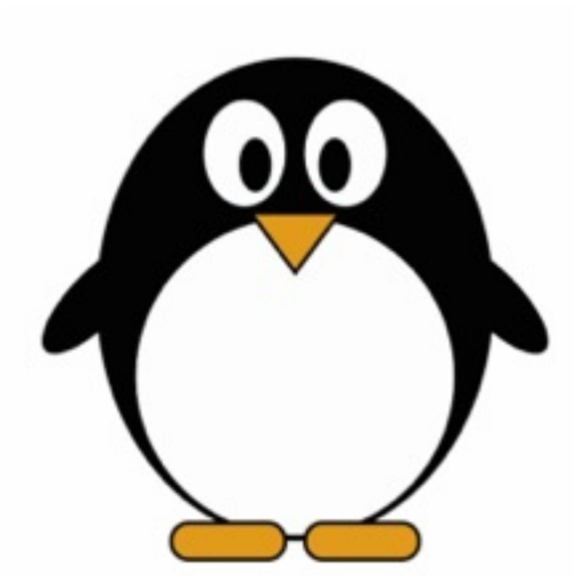
Computability in Population Protocols

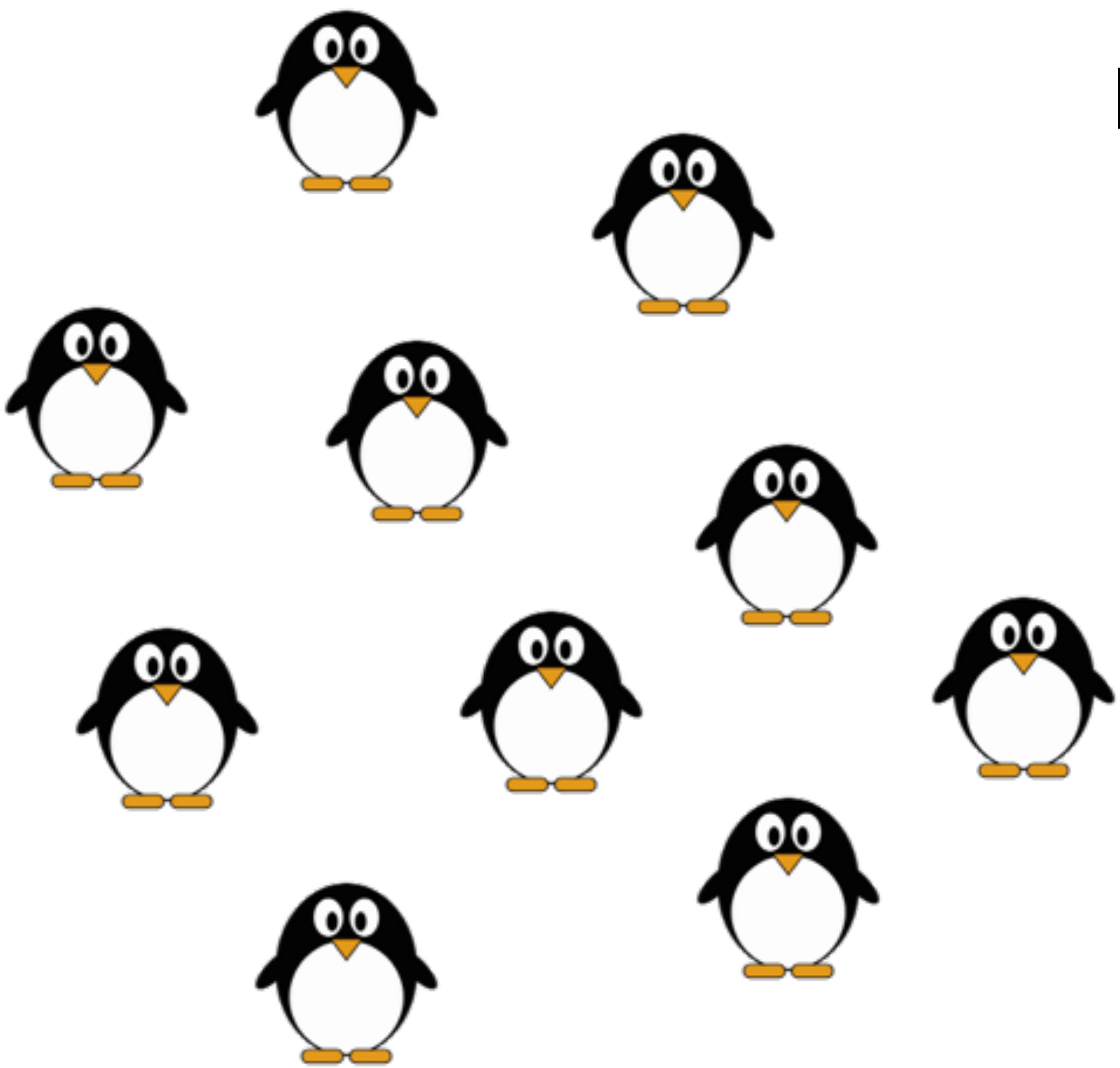
Peva Blanchard
EPFL 2014/2015

Population Protocol



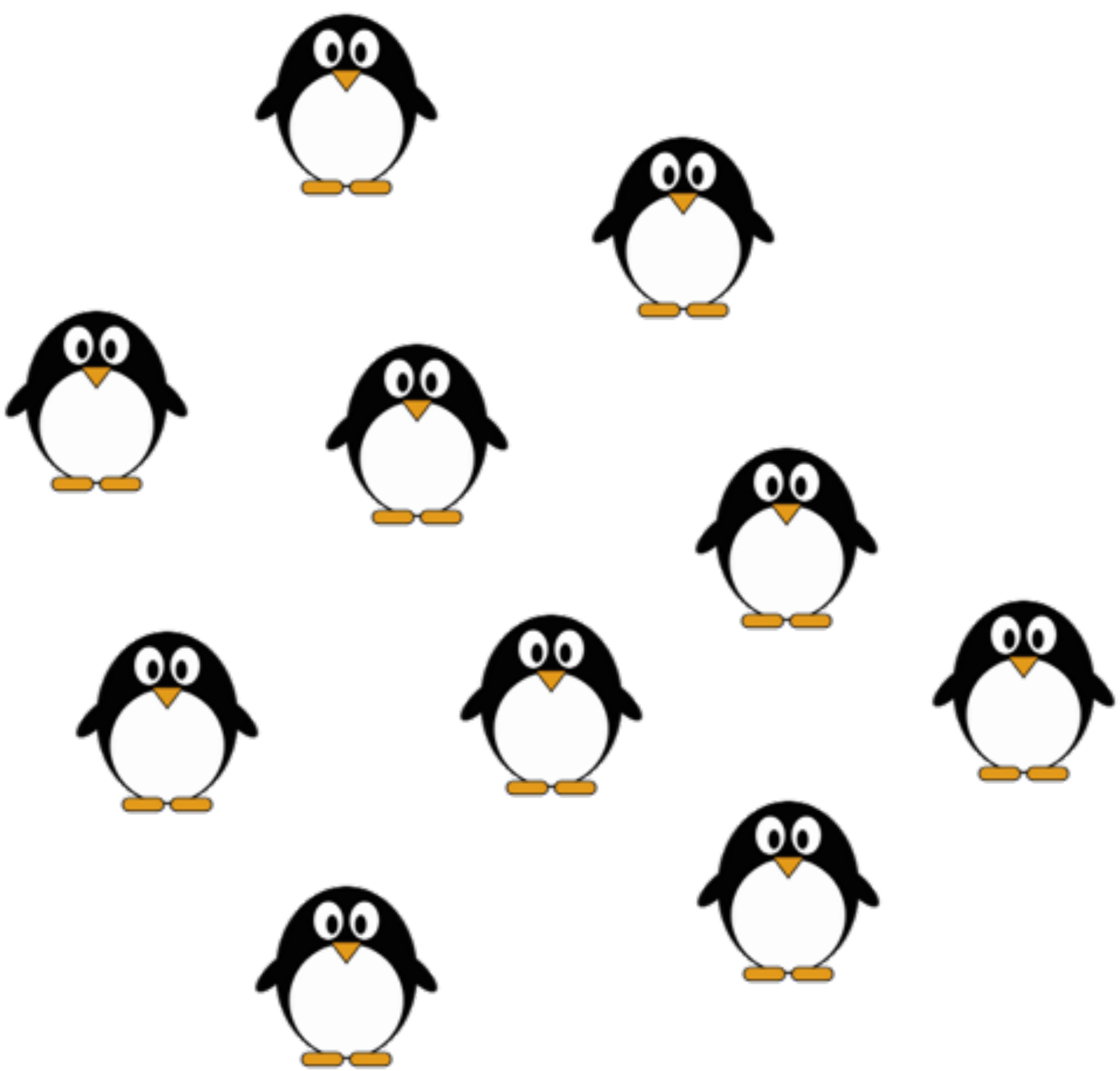
Agent : no id, small memory

Population Protocol



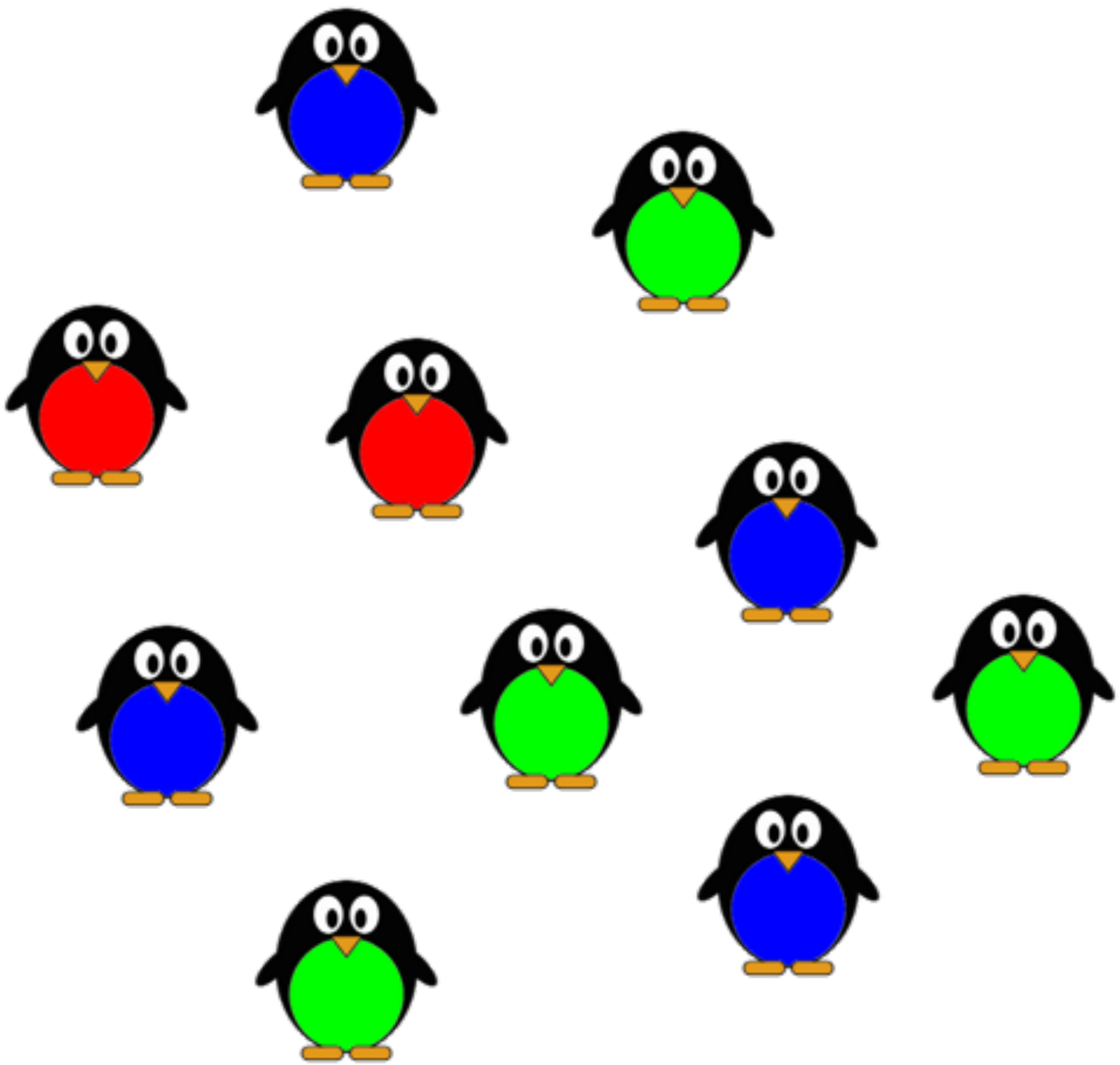
Population arbitrary size n

Population Protocol



Initially: sensors give data

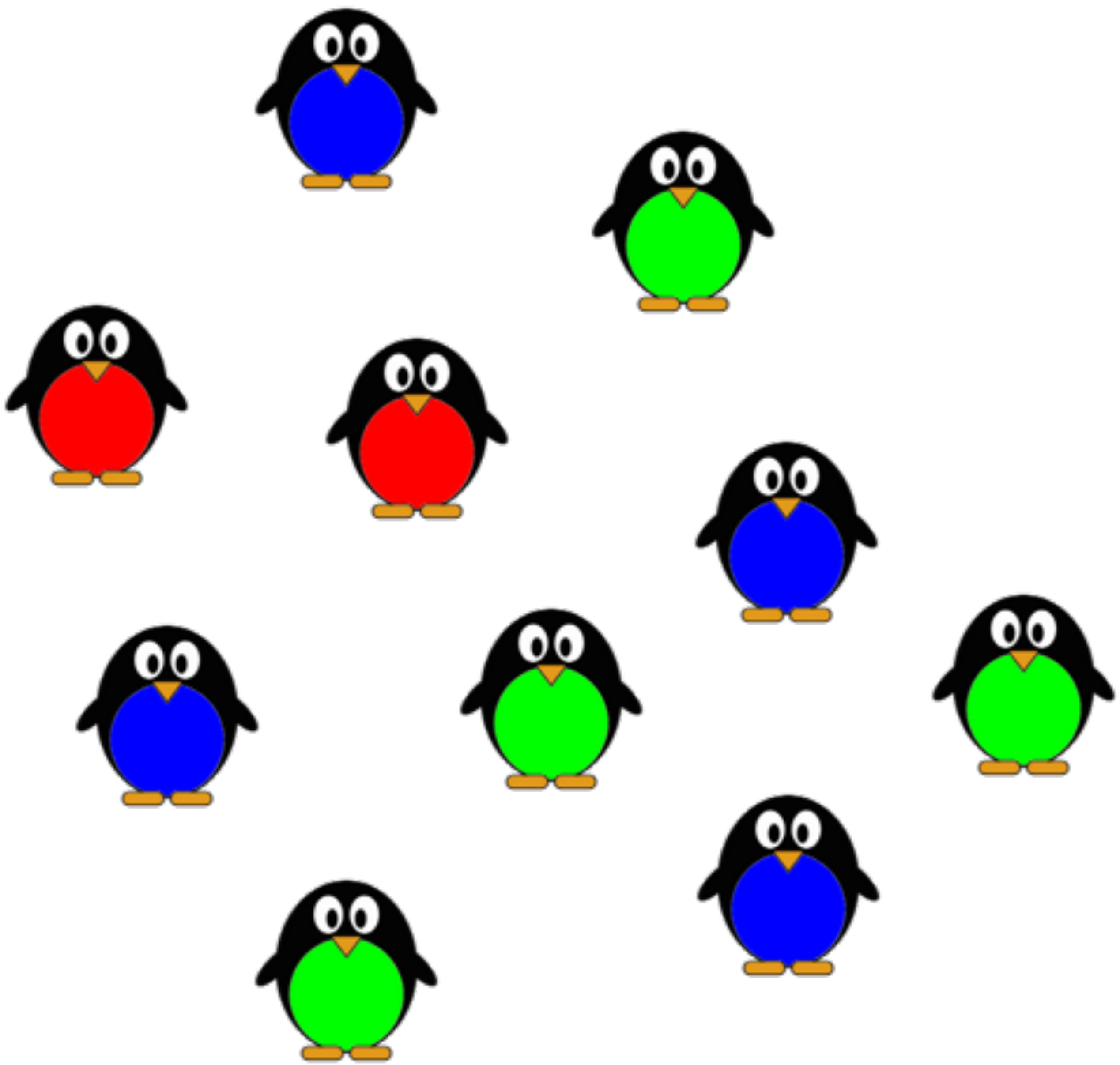
Population Protocol



Initially: sensors give data

red green blue

Population Protocol



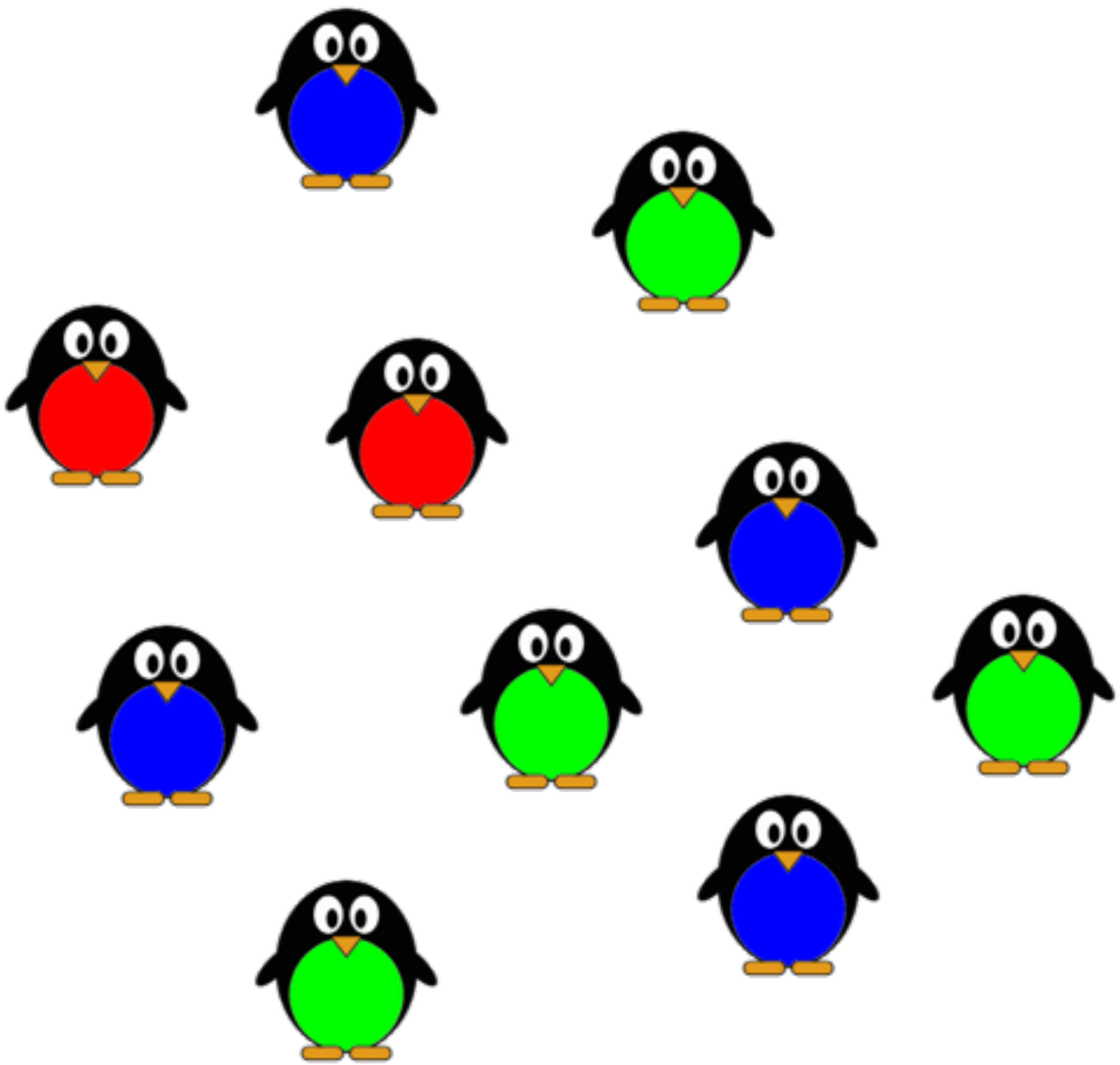
Initially: sensors give data

red green blue

↓

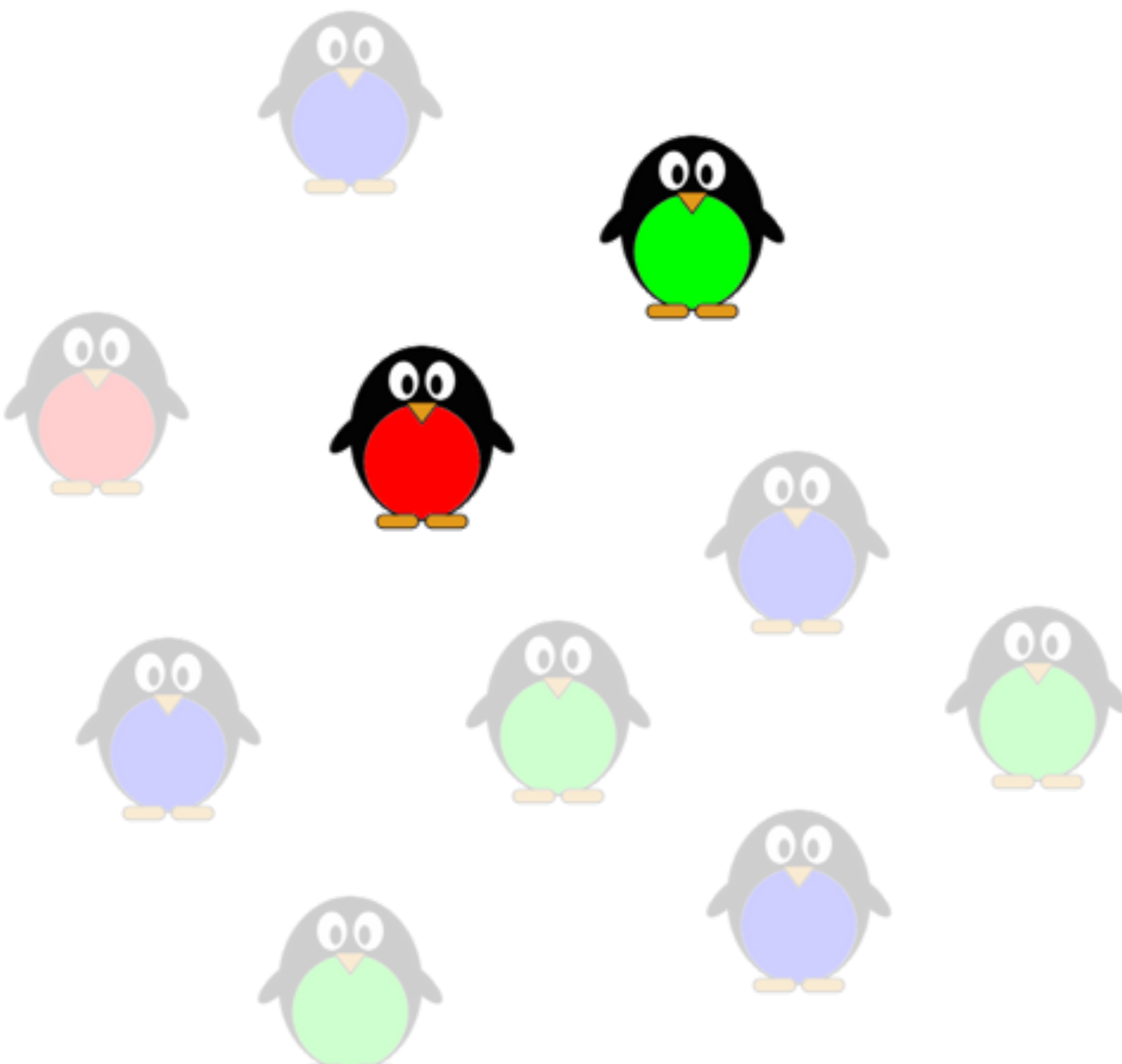
initial states

Population Protocol



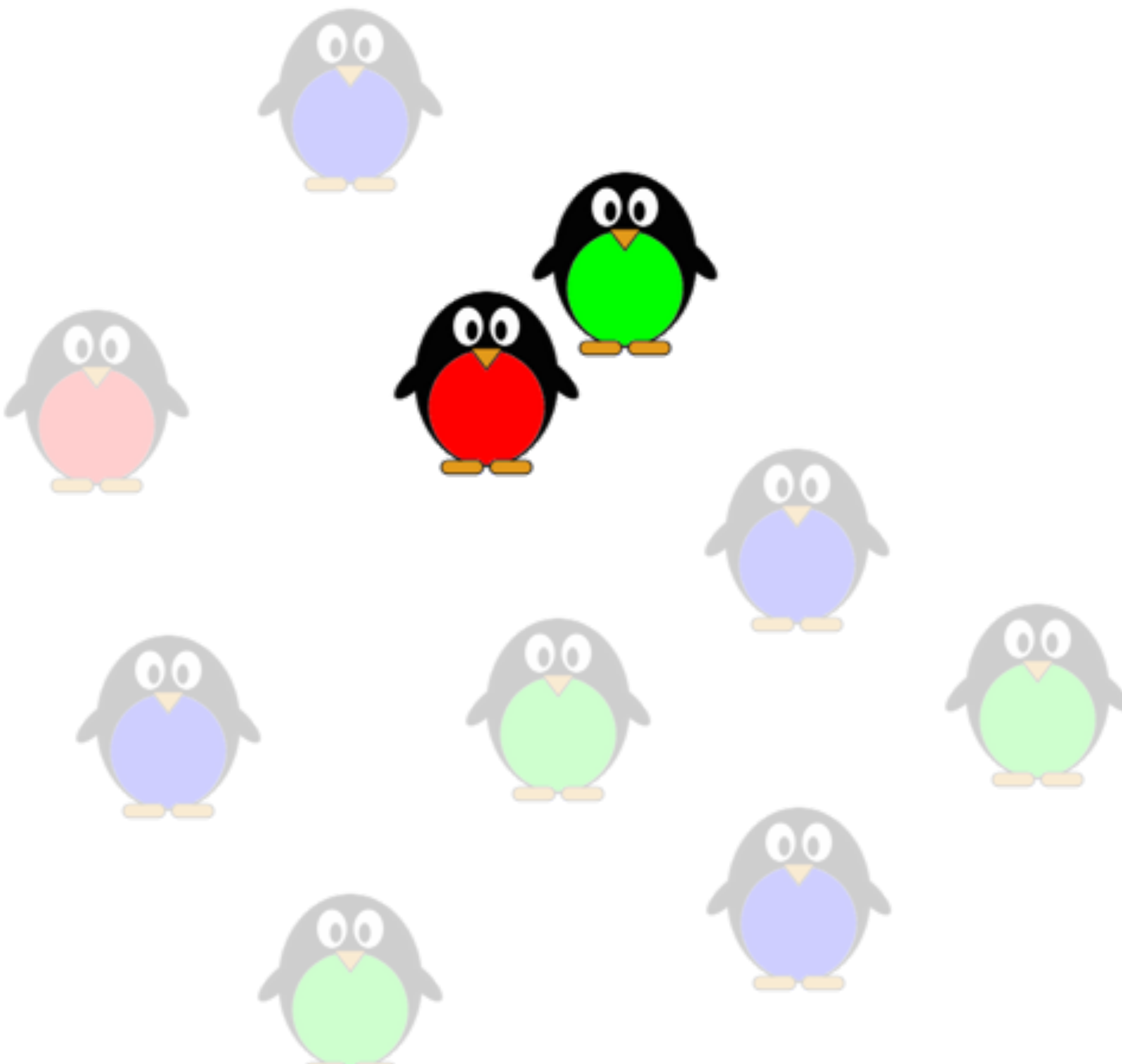
Agents move

Population Protocol



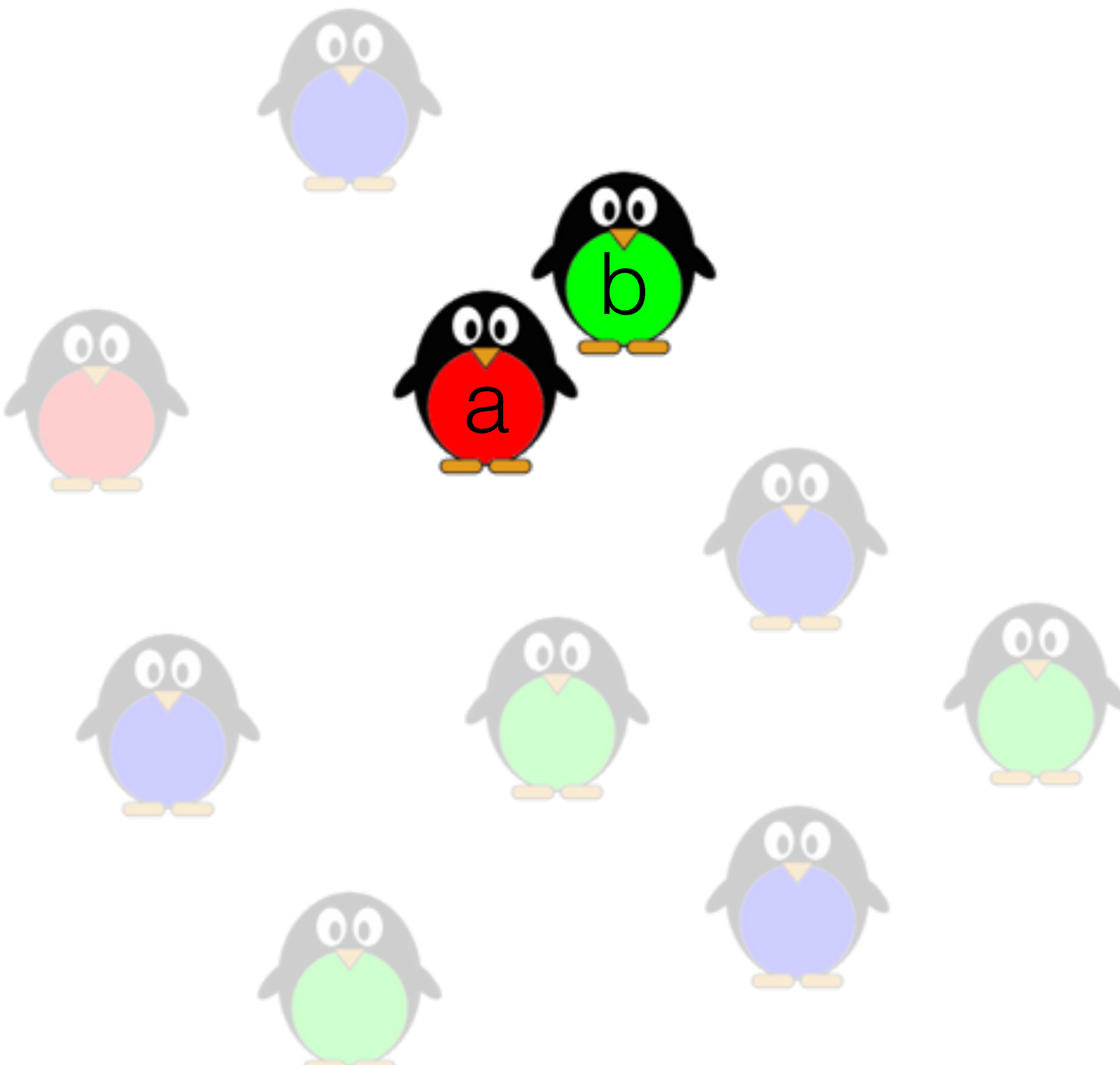
Agents move

Population Protocol



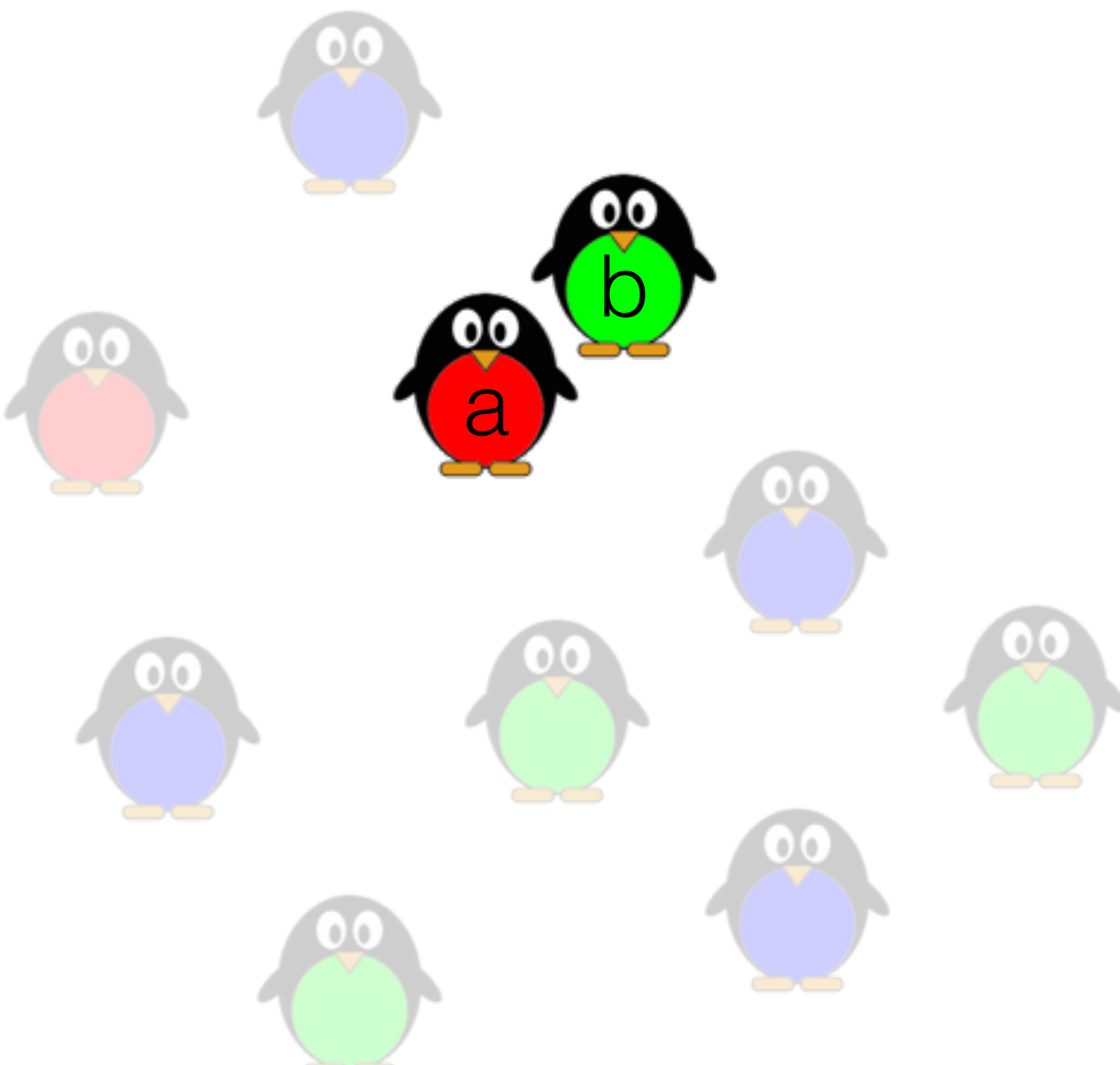
Agents move

Population Protocol



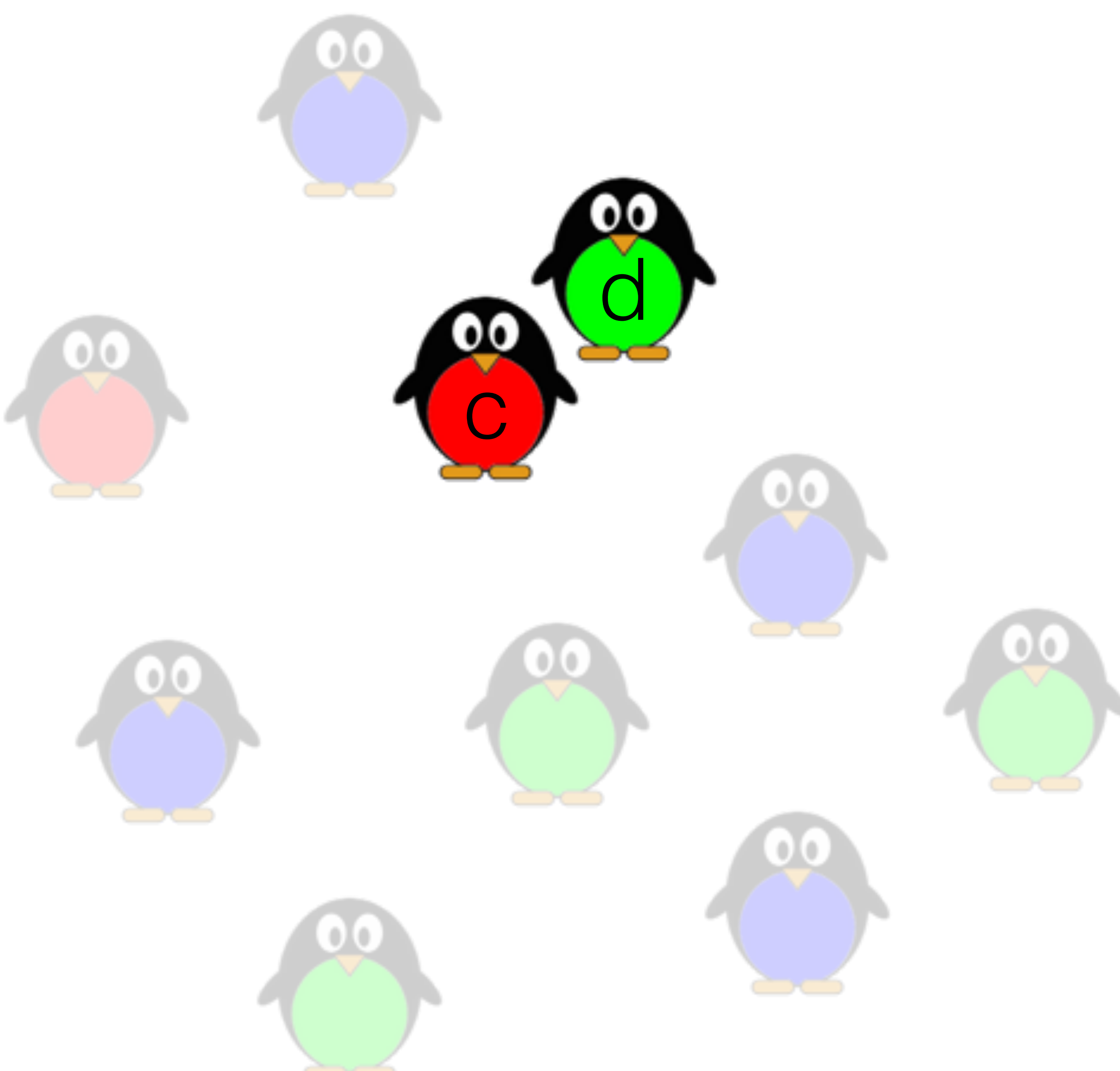
Agents move

Population Protocol



Protocol rule

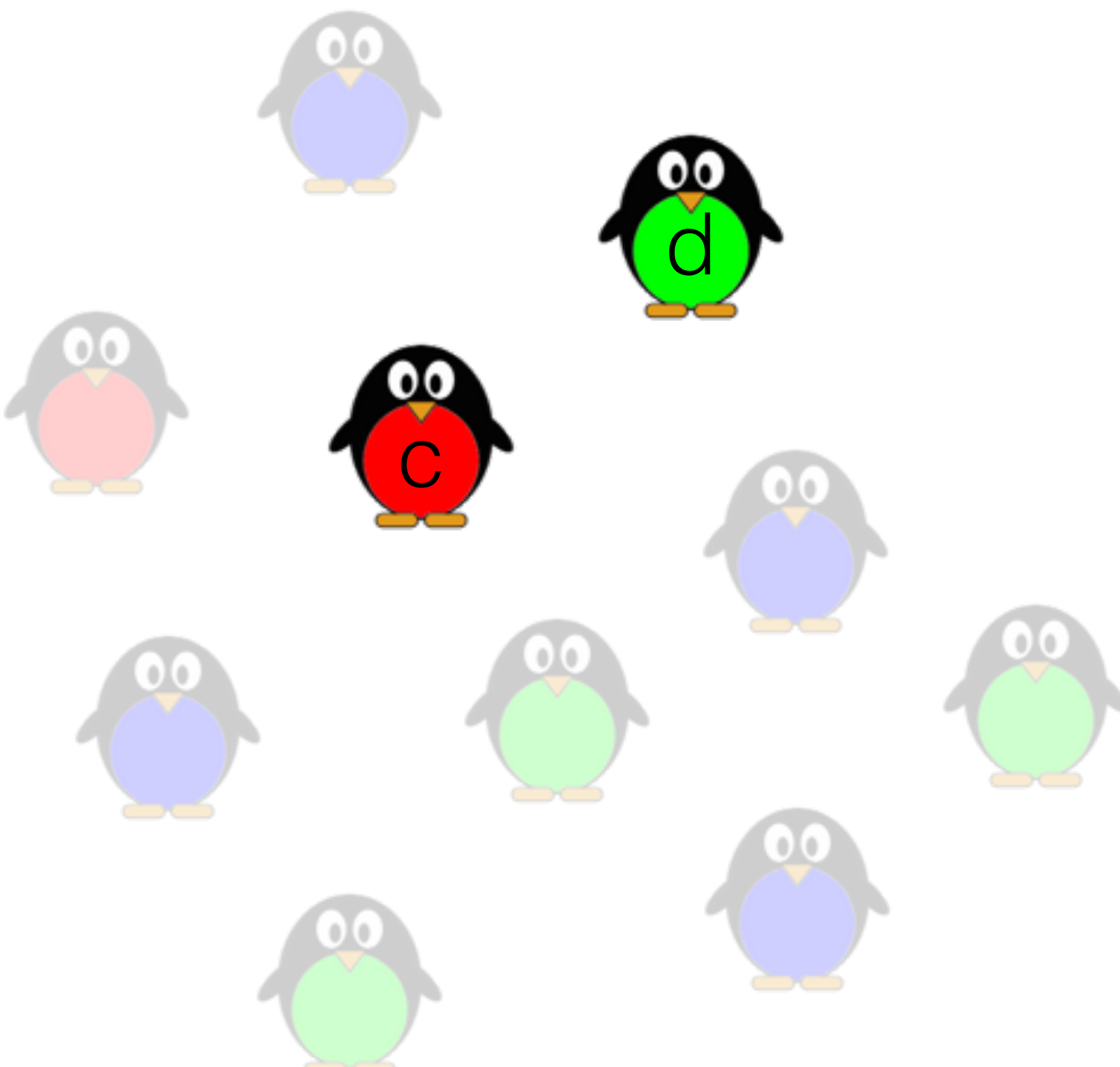
Population Protocol



Protocol rule

a,b ⟶ c,d

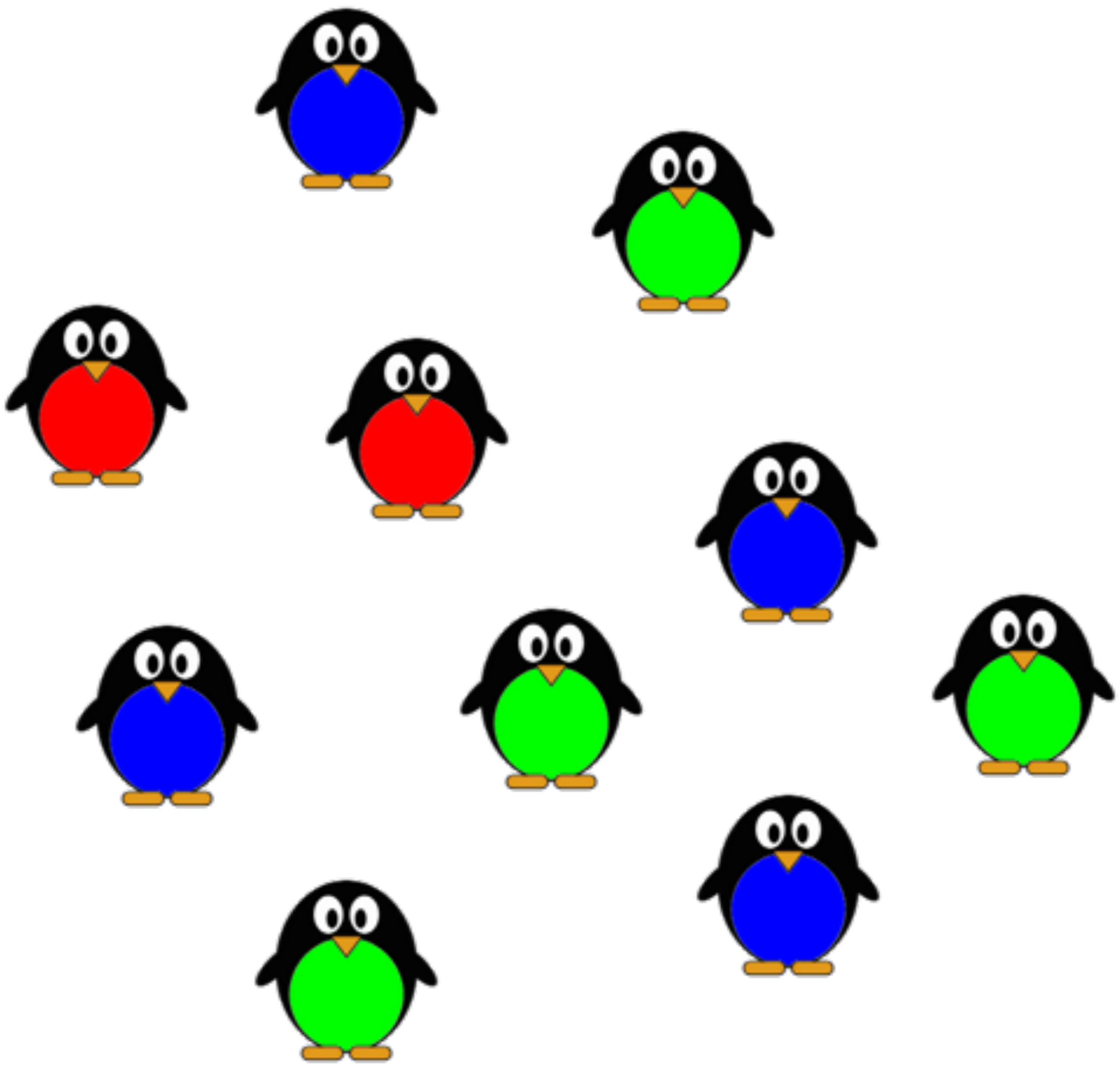
Population Protocol



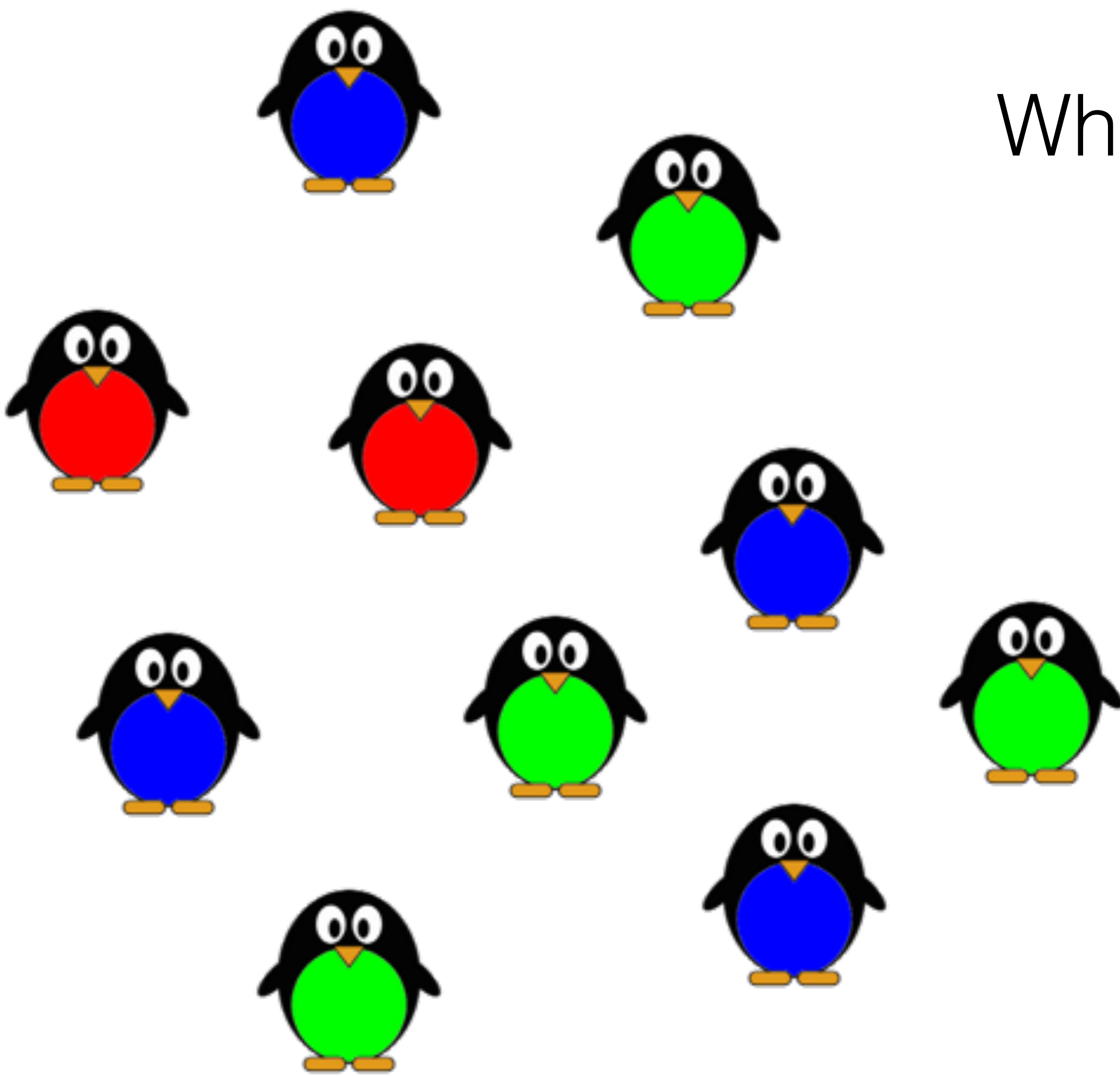
Protocol rule

a,b → c,d

What is computable ?

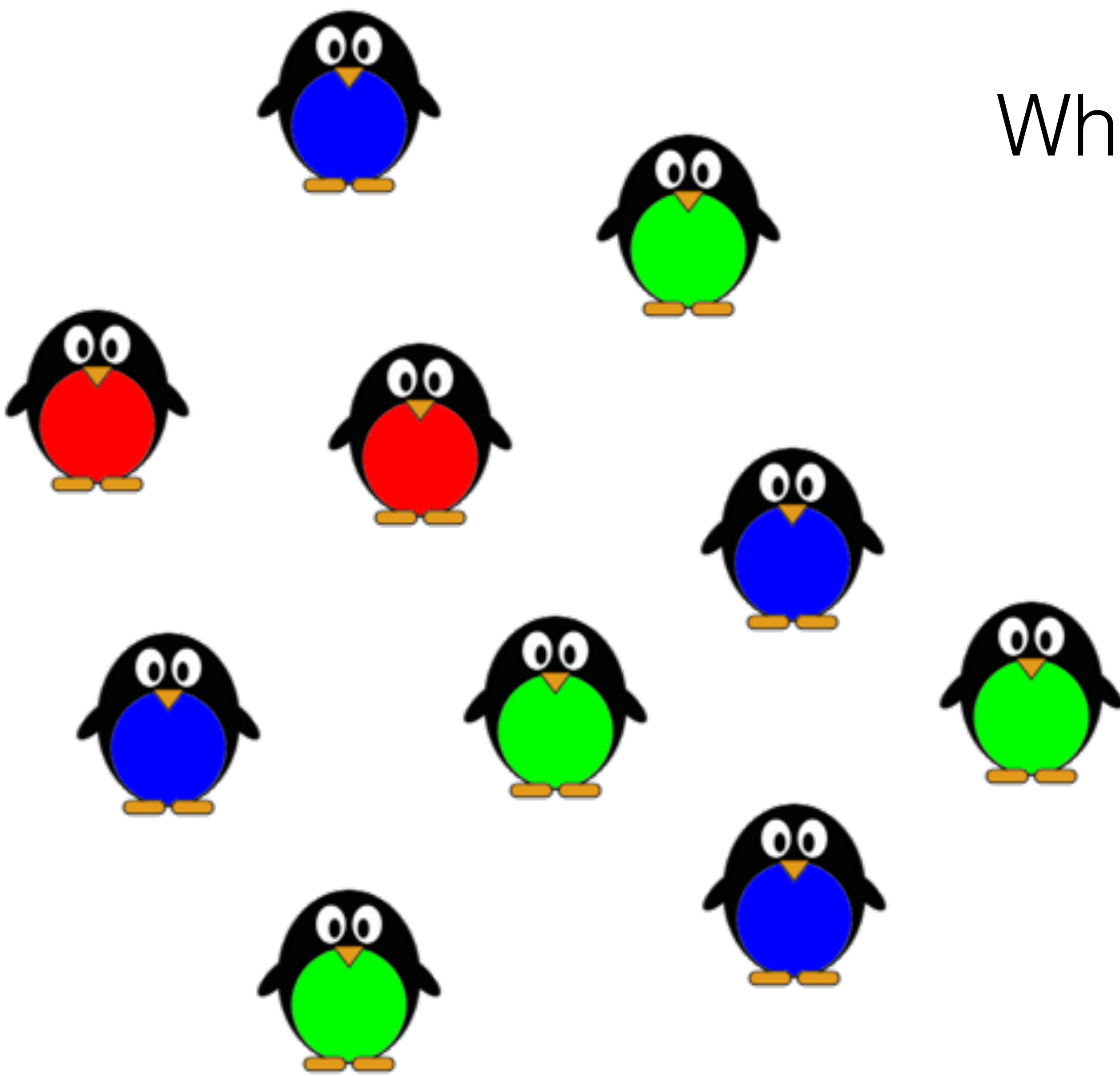


What is computable ?



What can the agents know about the initial configuration ?

What is computable ?



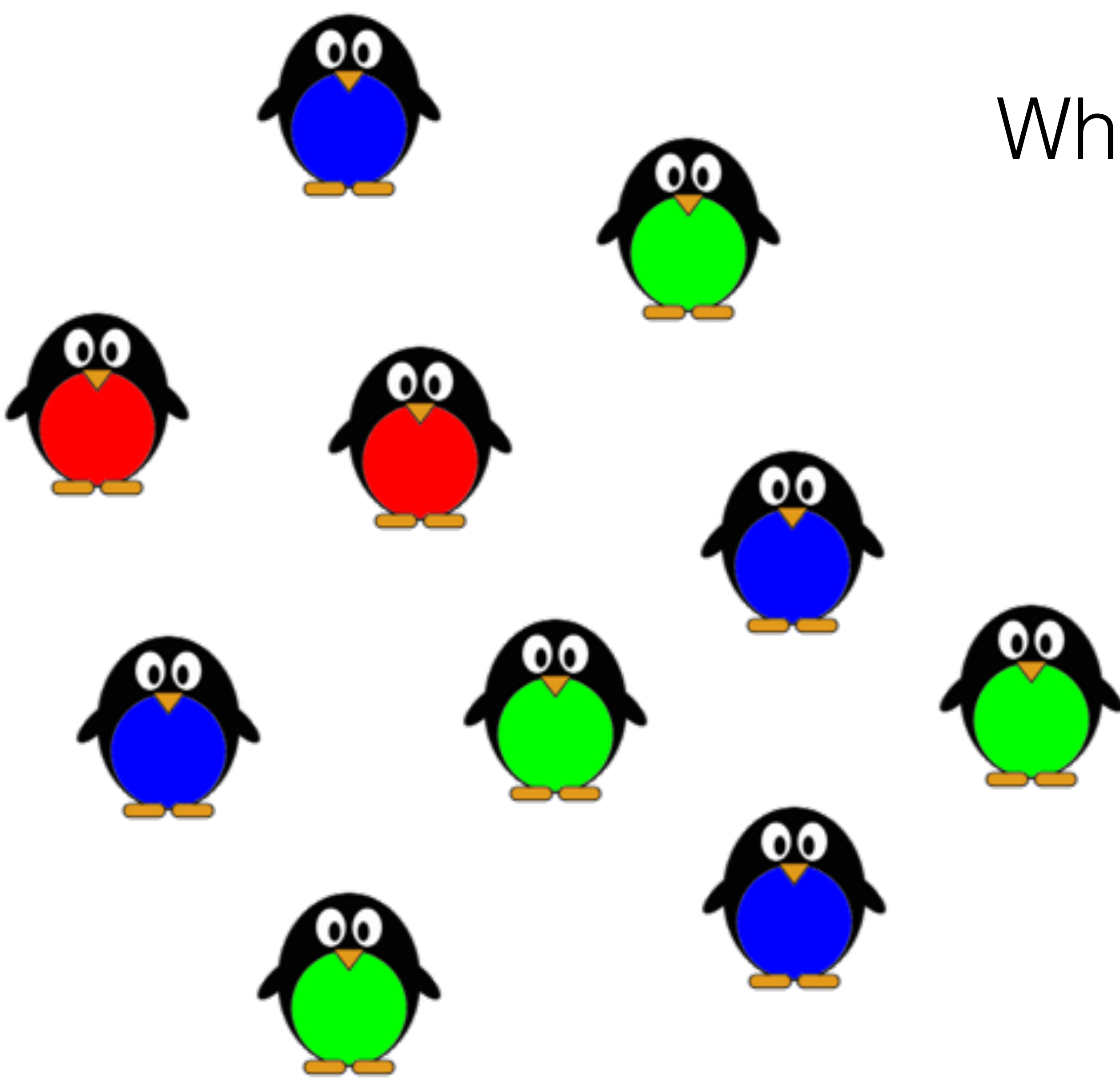
What can the agents know about the initial configuration ?

No id

$\Downarrow$

Only numbers of "species"

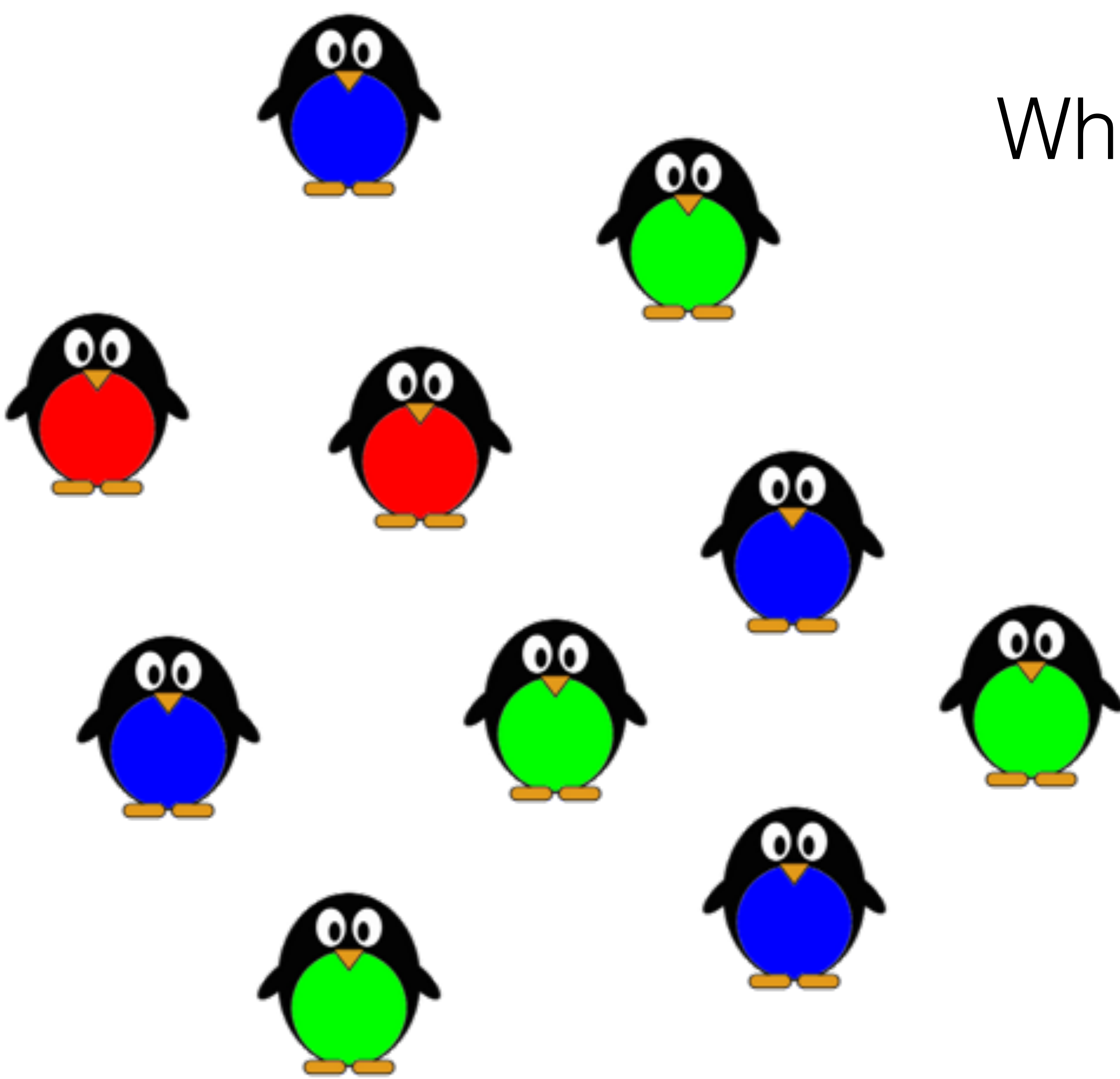
What is computable ?



What can the agents know about the initial configuration ?

#green $\leq$ 4

What is computable ?

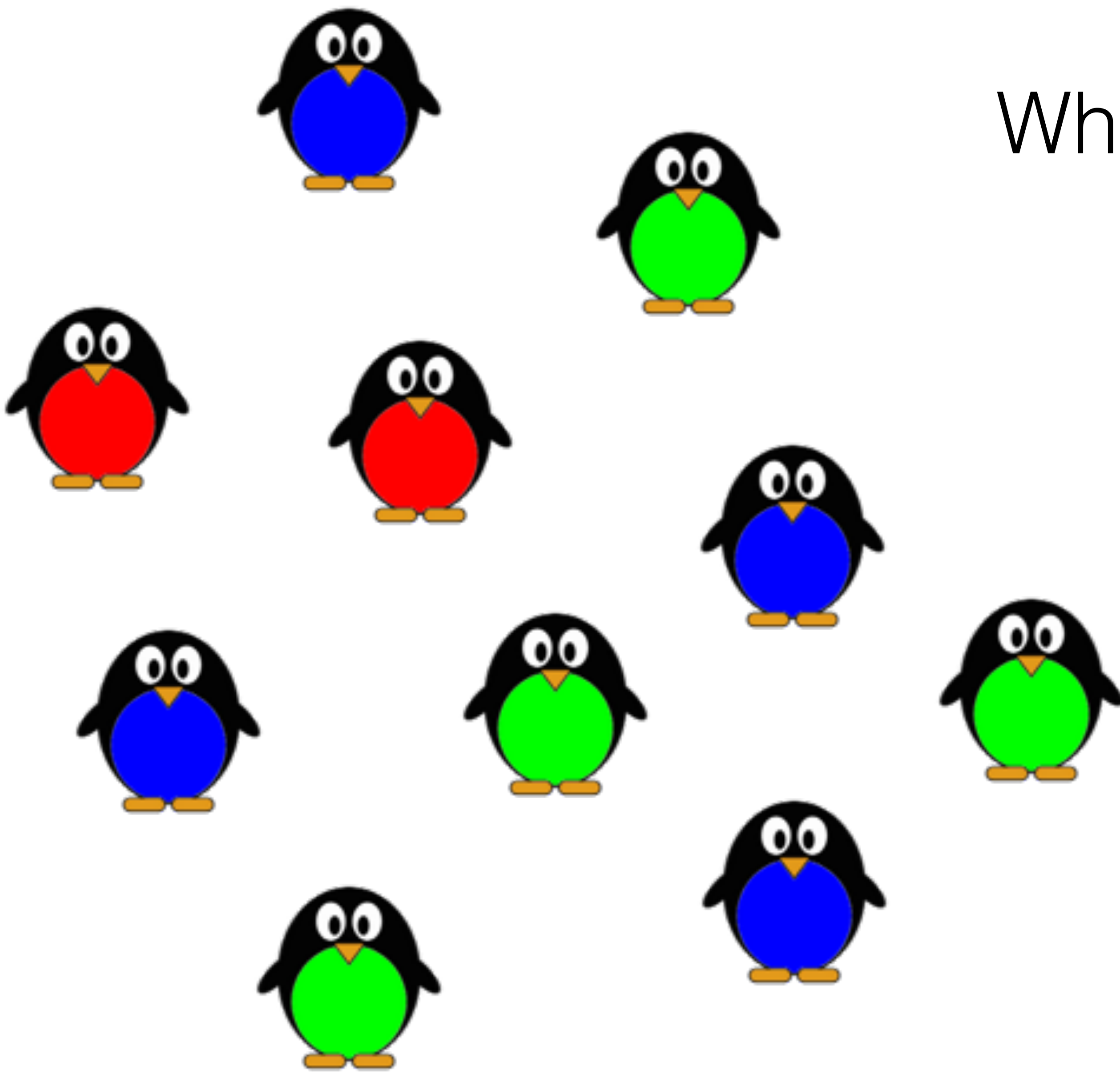


What can the agents know about the initial configuration ?

#green $\leq$ 4

#green $\leq$ #blue

What is computable ?



What can the agents know about the initial configuration ?

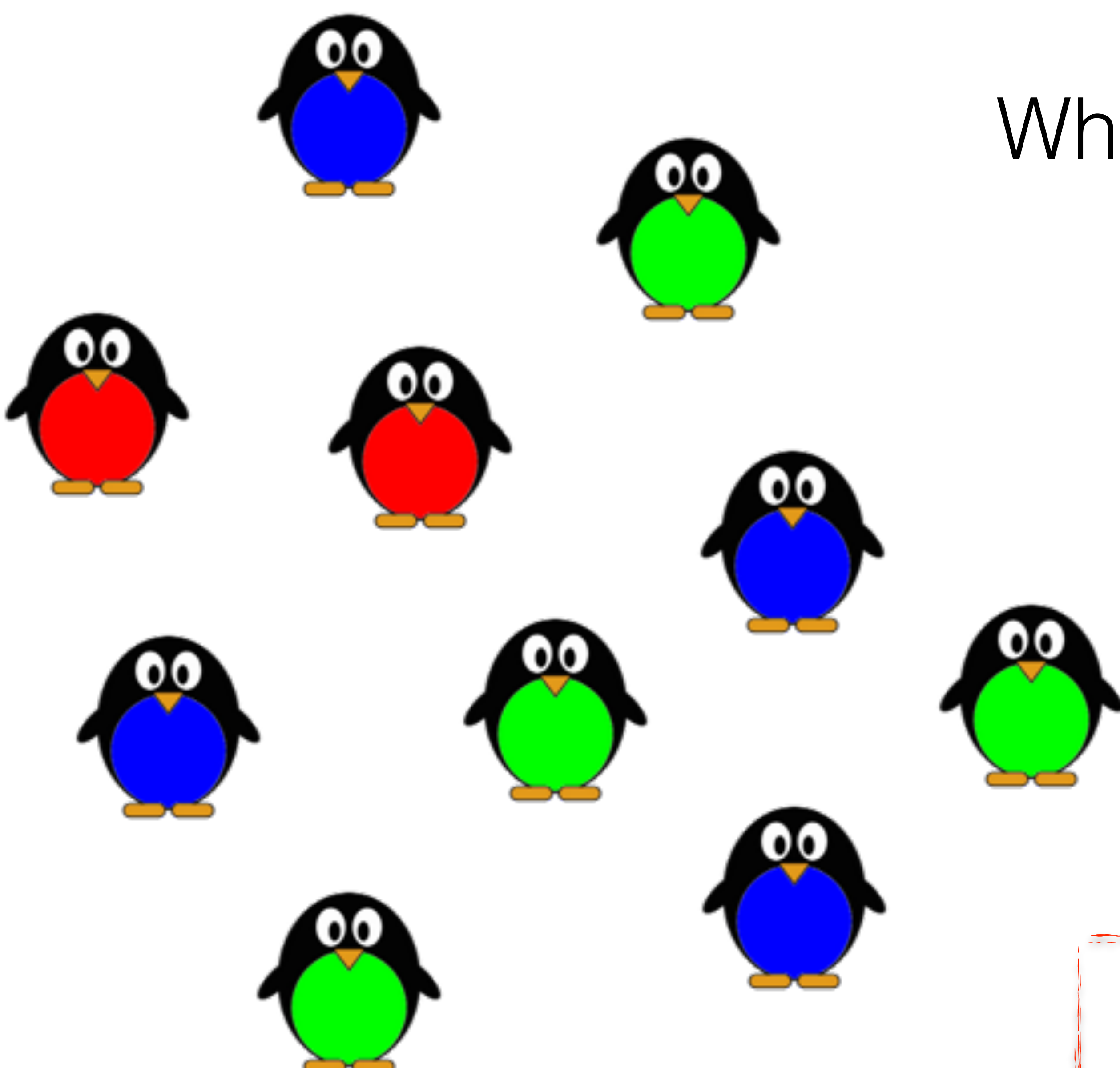
#green $\leq$ 4

#green $\leq$ #blue

#green $\leq$ #blue + 2#red

#green $\leq$ #blue x #red

What is computable ?



What can the agents know about the initial configuration ?

$\#green \leq 4$

$\#green \leq \#blue$

$\#green \leq \#blue + 2\#red$

OK

$\#green \leq \#blue \times \#red$

nok

$$X = \{\sigma_1, \ldots, \sigma_k\}$$

the "species" (red, green, blue, etc.)

$$X = \{\sigma_1, \ldots, \sigma_k\}$$

the "species" (red, green, blue, etc.)

$$a_1, \ldots, a_k, c$$

integer coefficients

$$X = \{\sigma_1, \ldots, \sigma_k\}$$

the "species" (red, green, blue, etc.)

$$a_1, \ldots, a_k, c$$

integer coefficients

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

$$X = \{\sigma_1, \ldots, \sigma_k\}$$

the "species" (red, green, blue, etc.)

$$a_1, \ldots, a_k, c$$

integer coefficients

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

Number of agents with input σ_1

$\ddots$

Number of agents with input σ_k

P computable

P computable

There exists a protocol A such that

P computable

There exists a protocol A such that

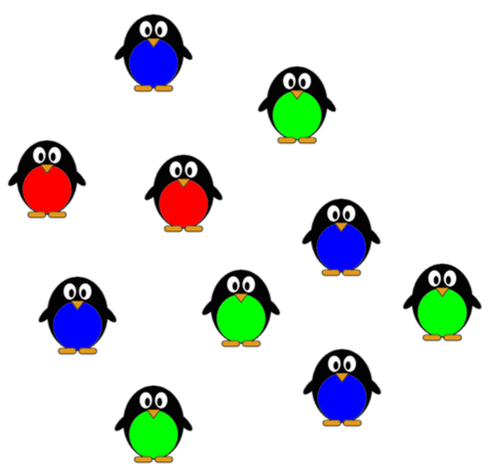
for any population size

P computable

There exists a protocol A such that

for any population size

for any input assignment

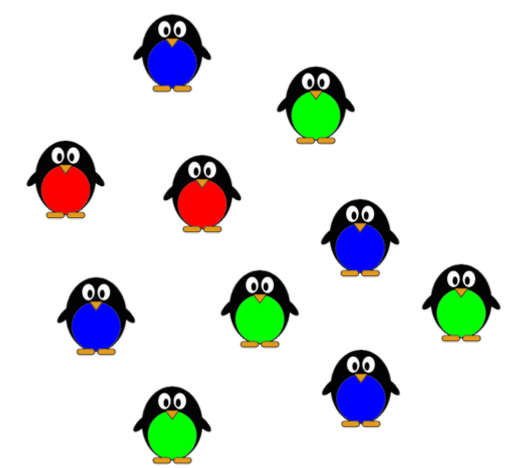


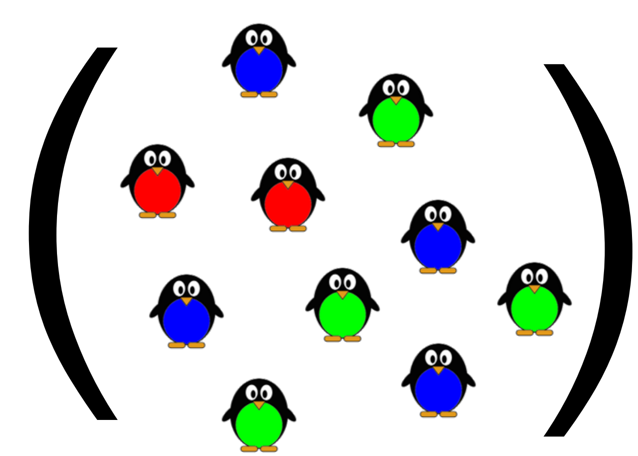
P computable

There exists a protocol A such that

for any population size

for any input assignment



eventually **all** agents output P 

Idea

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

Idea

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

- agent with input σ_i $\longrightarrow$ init. state with weight a_i

Idea

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

- agent with input σ_i $\longrightarrow$ init. state with weight a_i
- some leader collects the sum of weights

Idea

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

- agent with input σ_i $\longrightarrow$ init. state with weight a_i
- some leader collects the sum of weights
- leader can test the threshold

Idea

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

- agent with input σ_i $\longrightarrow$ init. state with weight a_i
- some leader collects the sum of weights
- leader can test the threshold

counter field

Idea

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

- agent with input σ_i ⟶ init. state with weight a_i
- some leader collects the sum of weights
- leader can test the threshold

leader bit

counter field

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

leader bit

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

leader bit

output bit

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

leader bit

output bit

counter

$$s = \max\{|c| + 1, |a_1|, \ldots, |a_k|\}$$

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

initial state : $\sigma_i \longrightarrow (1, 0, a_i)$

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

initial state : $\sigma_i \longrightarrow (1, 0, a_i)$

rules $(l \neq l')$

$$\begin{matrix} (l, \cdot, u) \\ (l', \cdot, u') \end{matrix} \longrightarrow \begin{matrix} (1, b(u,u'), q(u,u')) \\ (0, b(u,u'), r(u,u')) \end{matrix}$$

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

initial state : $\sigma_i \longrightarrow (1, 0, a_i)$

rules $(l \neq l')$

$$\begin{matrix} (l, \cdot, u) \\ (l', \cdot, u') \end{matrix} \longrightarrow \begin{matrix} (1, b(u,u'), q(u,u')) \\ (0, b(u,u'), r(u,u')) \end{matrix}$$

$$q(u,u') = \max\{-s, \min\{s, u+u'\}\}$$

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

initial state : $\sigma_i \longrightarrow (1, 0, a_i)$

rules $(l \neq l')$

$$\begin{matrix} (l, \cdot, u) \\ (l', \cdot, u') \end{matrix} \longrightarrow \begin{matrix} (1, b(u,u'), q(u,u')) \\ (0, b(u,u'), r(u,u')) \end{matrix}$$

truncated sum

$$q(u,u') = \max\{-s, \min\{s, u+u'\}\}$$

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s,\dots,s\}$

initial state : $\sigma_i \longrightarrow (1, 0, a_i)$

rules $(l \neq l')$ $\begin{matrix}(l, \cdot, u) \\ (l', \cdot, u')\end{matrix} \longrightarrow \begin{matrix}(1, b(u,u'), q(u,u')) \\ (0, b(u,u'), r(u,u'))\end{matrix}$

truncated sum

$$q(u,u') = \max\{-s, \min\{s, u+u'\}\}$$

$$r(u,u') = u + u' - q(u,u')$$

remainder

$$P : a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

State space $\{0,1\} \times \{0,1\} \times \{-s, \ldots, s\}$

initial state : $\sigma_i \longrightarrow (1, 0, a_i)$

rules $(l \neq l')$

$$\begin{matrix} (l, \cdot, u) \\ (l', \cdot, u') \end{matrix} \longrightarrow \begin{matrix} (1, b(u,u'), q(u,u')) \\ (0, b(u,u'), r(u,u')) \end{matrix}$$

test threshold

$$b(u,u') = \begin{cases} 1 & \text{if } q(u,u') < c \\ 0 & \text{otherwise} \end{cases}$$

Proof strategy

A. Eventually a single leader

B. Eventually, the leader collects the value

$$\max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

C. Eventually, the agents produce correct outputs

Proof strategy

A. Eventually a single leader

B. Eventually, the leader collects the value

$$\max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

C. Eventually, the agents produce correct outputs

Proof strategy

A. Eventually a single leader

$$(l \neq l') \quad \begin{matrix}(l, \cdot, u) \\ (l', \cdot, u')\end{matrix} \longrightarrow \begin{matrix}(1, b(u,u'), q(u,u')) \\ (0, b(u,u'), r(u,u'))\end{matrix}$$

Proof strategy

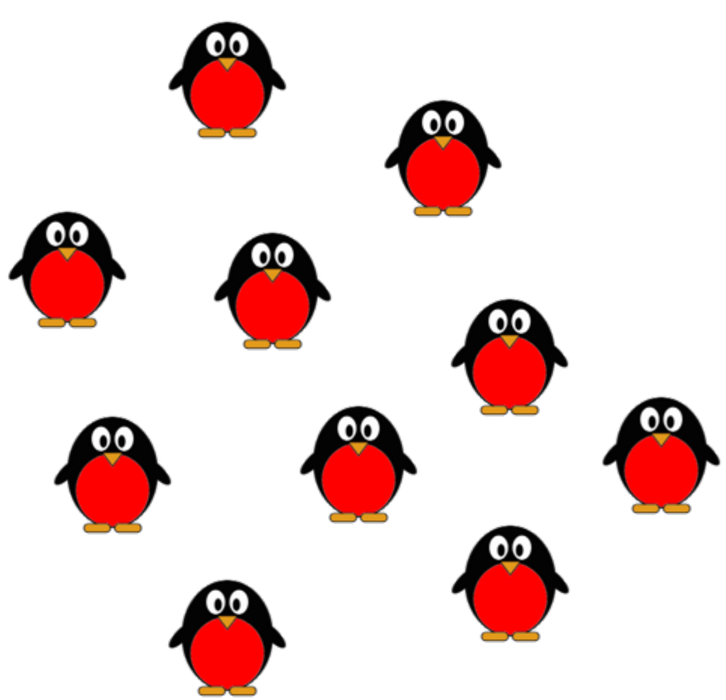
A. Eventually a single leader

leader, leader
leader, non-leader → leader, non-leader
non-leader, leader

Proof strategy

A. Eventually a single leader

leader, leader
leader, non-leader → leader, non-leader
non-leader, leader



init. all leaders

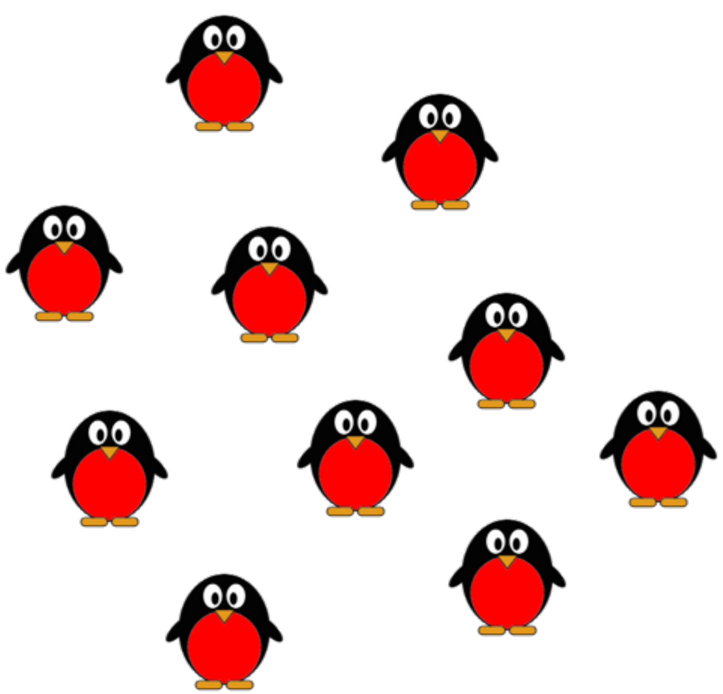
Proof strategy

A. Eventually a single leader

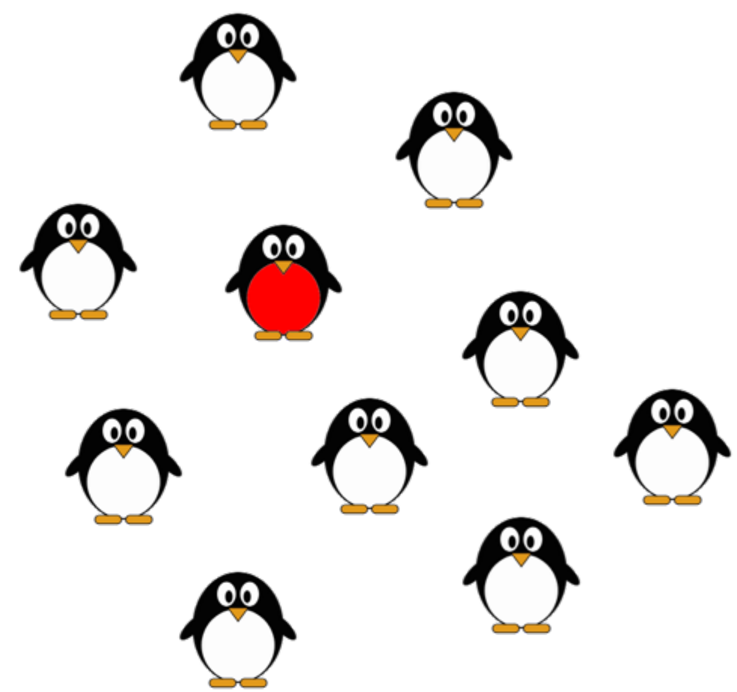
leader, leader
leader, non-leader
non-leader, leader

→

leader, non-leader



→



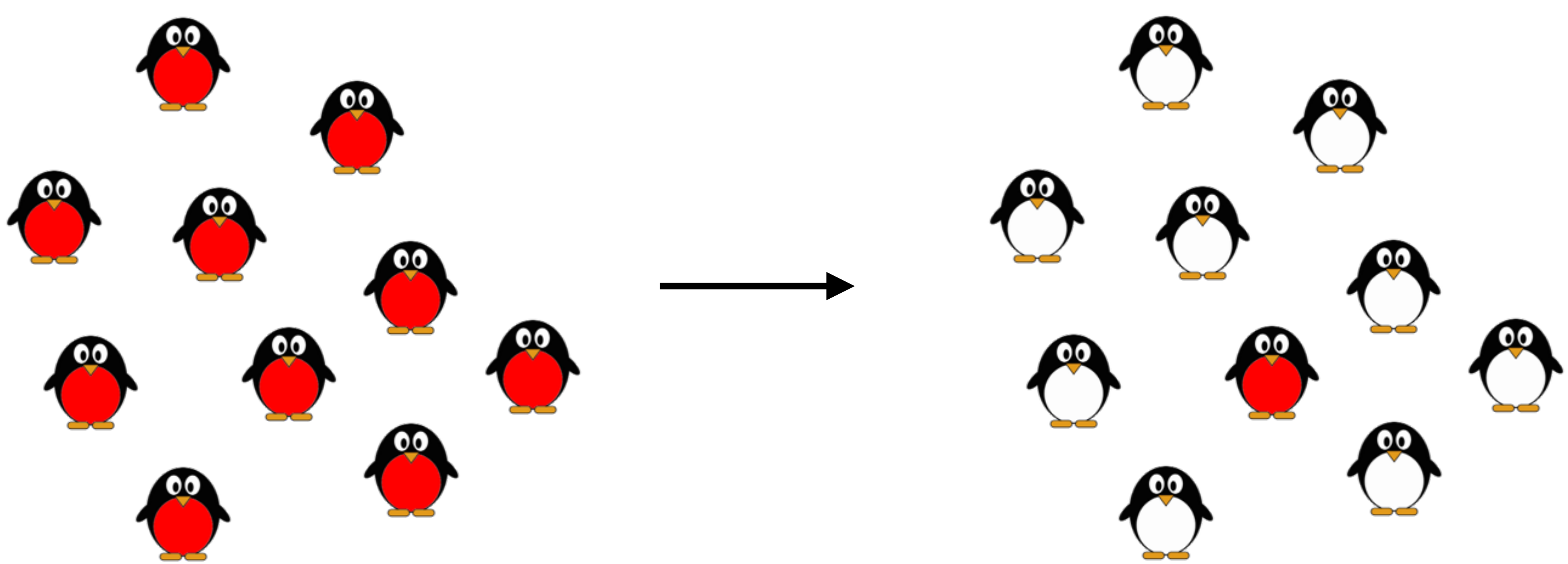
init. all leaders

one survivor

Proof strategy

A. Eventually a single leader

leader, leader
leader, non-leader → leader, non-leader
non-leader, leader



init. all leaders

one leader (which may change)

Proof strategy

A. Eventually a single leader

OK

B. Eventually, the leader collects the value

$$\max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

C. Eventually, the agents produce correct outputs

Proof strategy

B. Eventually, the leader ...

$$(l \neq l') \quad \begin{matrix} (l, \cdot, u) \\ (l', \cdot, u') \end{matrix} \longrightarrow \begin{matrix} (1, b(u, u'), q(u, u')) \\ (0, b(u, u'), r(u, u')) \end{matrix}$$

$$q(u, u') = \max\{-s, \min\{s, u + u'\}\}$$

$$r(u, u') = u + u' - q(u, u')$$

Proof strategy

B. Eventually, the leader ...

$$(l \neq l') \quad \begin{matrix} (l, \cdot, u) \\ (l', \cdot, u') \end{matrix} \longrightarrow \begin{matrix} (1, b(u,u'), q(u,u')) \\ (0, b(u,u'), r(u,u')) \end{matrix}$$

$$q(u,u') = \max\{-s, \min\{s, u+u'\}\}$$

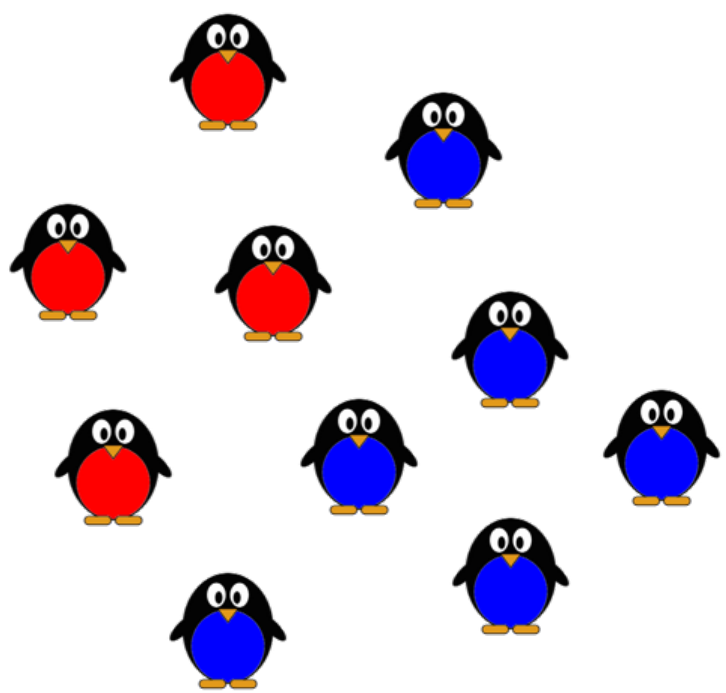
$$r(u,u') = u + u' - q(u,u')$$

$$\boxed{q(u,u') + r(u,u') = u + u'}$$

Proof strategy

B. Eventually, the leader ...

$$q(u, u') + r(u, u') = u + u'$$

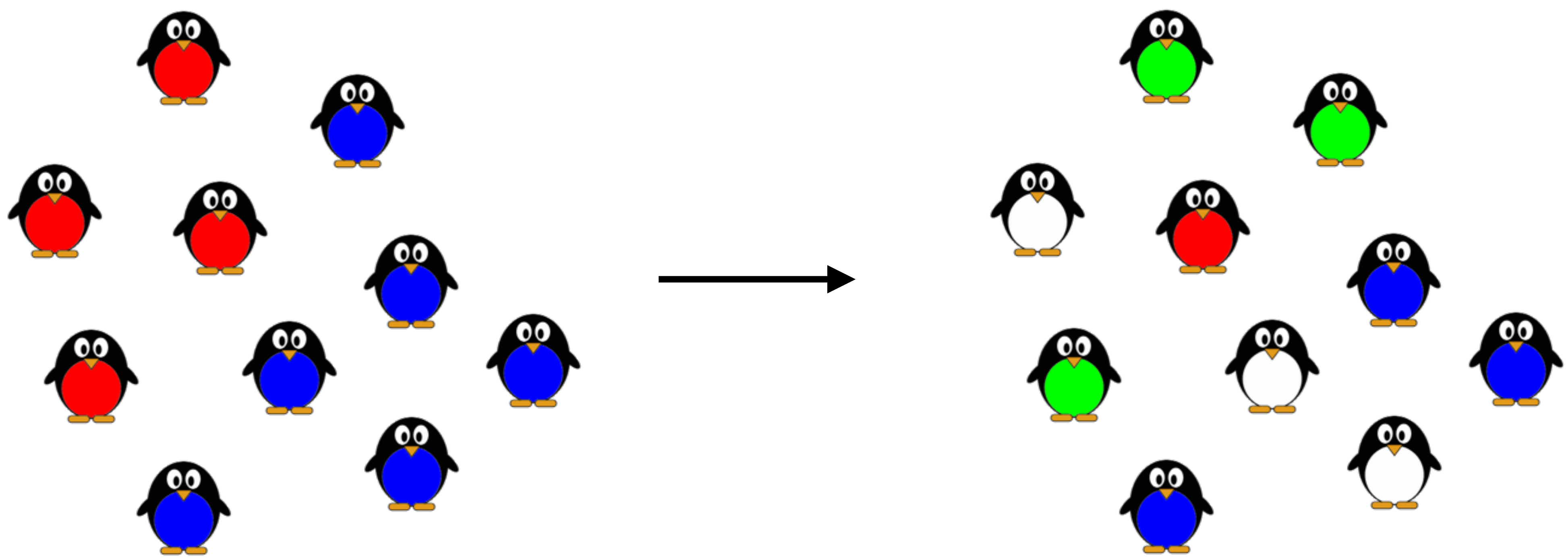


$$\sum a_i \cdot \#\sigma_i$$

Proof strategy

B. Eventually, the leader ...

$$q(u,u') + r(u,u') = u + u'$$

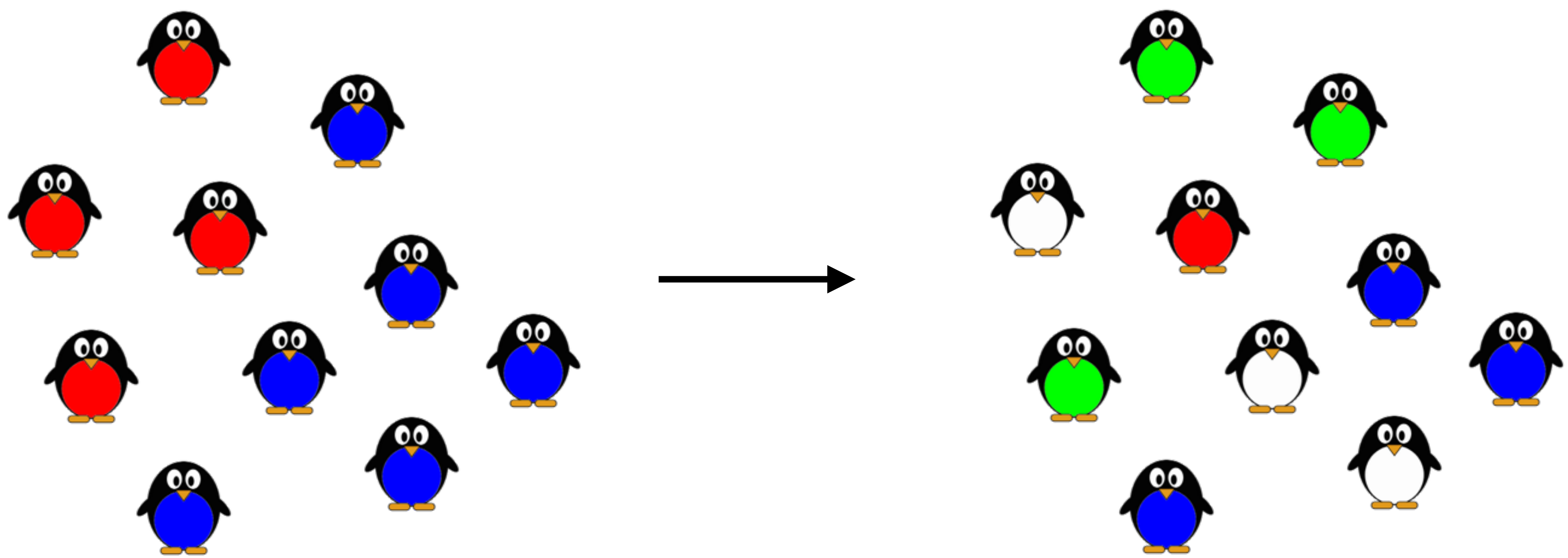


$$\sum a_i \cdot \#\sigma_i$$

Proof strategy

B. Eventually, the leader ...

$$q(u, u') + r(u, u') = u + u'$$



$$\sum a_i \cdot \#\sigma_i \quad = \quad \sum u_i$$

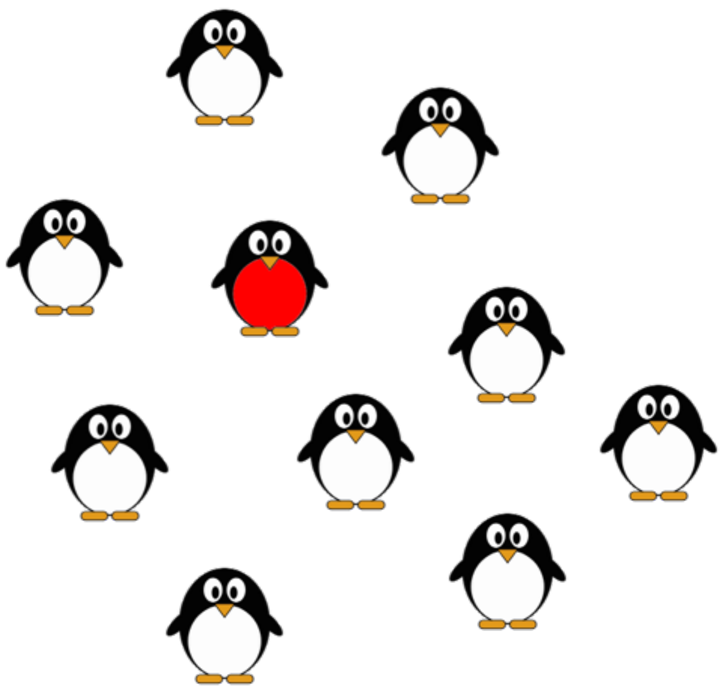
counter of agent i

Proof strategy

B. Eventually, the leader ...

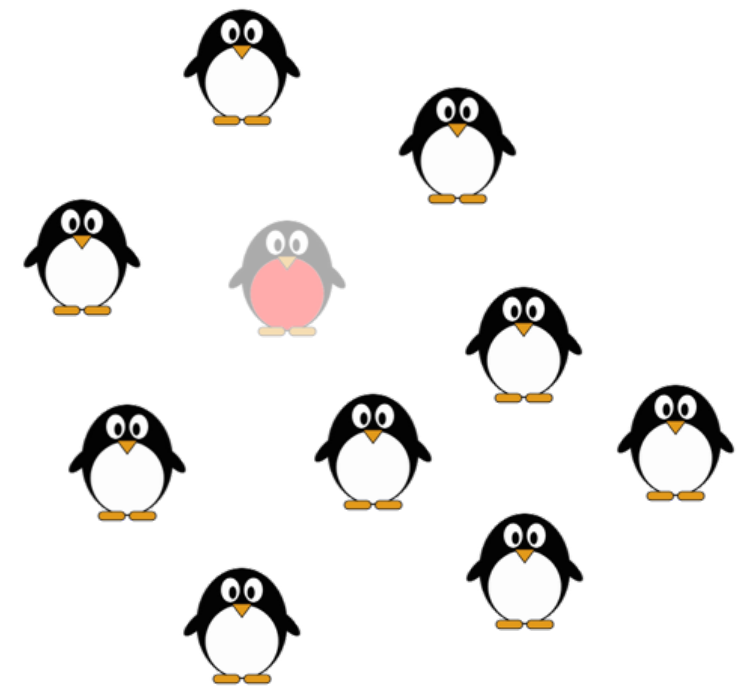
Focus on suffix of execution

in each config C, a unique leader L



Proof strategy

B. Eventually, the leader ...



Focus on suffix of execution

in each config C, a unique leader L

$$p(C) = \sum_{j \neq L} |u_j(C)|$$

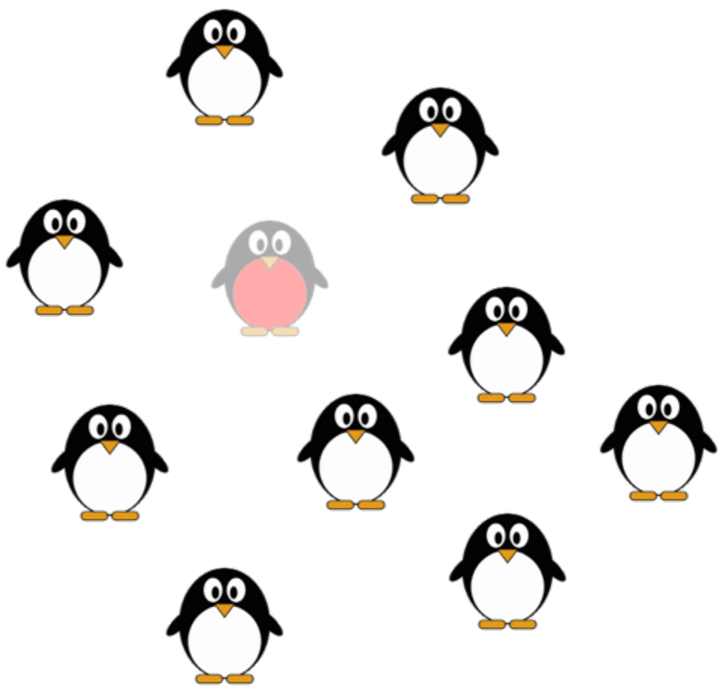
measures the "mass" of the non-leaders

Proof strategy

B. Eventually, the leader ...

Focus on suffix of execution

in each config C, a unique leader L



$$p(C) = \sum_{j \neq L} |u_j(C)|$$

measures the "mass" of the non-leaders

show that p decreases
& eventually cst

Proof strategy

B. Eventually, the leader ...

u_L $\to$ $\max\{-s, \min\{s, u_L + u_j\}\}$

u_j $\to$ $u_L + u_j -$ above

$$p(C) = \sum_{j \neq L} |u_j(C)|$$

case 1: $-s \leq u_L \leq s$ and $u_j \geq 0$

u_L $\to$ $\min\{u_L + u_j, s\} = u_L + \min\{u_j, s - u_L\}$

u_j $\to$ $u_j - \min\{u_j, s - u_L\}$

Proof strategy

B. Eventually, the leader ...

$u_L \rightarrow \max\{-s, \min\{s, u_L + u_j\}\}$

$u_j \rightarrow u_L + u_j -$ above

$$p(C) = \sum_{j \neq L} |u_j(C)|$$

case 1: $-s \leq u_L \leq s$ and $u_j \geq 0$

$u_L \rightarrow \min\{u_L + u_j, s\} = u_L + \min\{u_j, s - u_L\}$

$u_j \rightarrow u_j - \min\{u_j, s - u_L\}$

$|u_j|$ does not increase

p does not increase

Proof strategy

B. Eventually, the leader ...

$$u_L \rightarrow \max\{-s, \min\{s, u_L + u_j\}\}$$

$$u_j \quad u_L + u_j - \text{ above}$$

$$p(C) = \sum_{j \neq L} |u_j(C)|$$

case 2: $-s \leq u_L \leq s$ and $u_j \leq 0$

$$u_L \rightarrow \max\{u_L + u_j, -s\} = u_L - \min\{-u_j, s + u_L\}$$

$$u_j \rightarrow u_j + \min\{-u_j, s + u_L\}$$

Proof strategy

B. Eventually, the leader ...

u_L → $\max\{-s, \min\{s, u_L + u_j\}\}$

u_j → $u_L + u_j -$ above

$$p(C) = \sum_{j \neq L} |u_j(C)|$$

case 2: $-s \leq u_L \leq s$ and $u_j \leq 0$

u_L → $\max\{u_L + u_j, -s\} = u_L - \min\{-u_j, s + u_L\}$

u_j → $u_j + \min\{-u_j, s + u_L\}$

$|u_j|$ does not increase

p does not increase

Proof strategy

Thus, eventually, p is constant

Proof strategy

Thus, eventually, p is constant

Analyzing the previous equations

Proof strategy

Thus, eventually, p is constant

Analyzing the previous equations

It is impossible from C to decrease p

iff

Proof strategy

Thus, eventually, p is constant

Analyzing the previous equations

It is impossible from C to decrease p

iff

$$p = 0$$

or $u_L = s$ and $\forall j \neq L, u_j \geq 0$

or $u_L = -s$ and $\forall j \neq L, u_j \leq 0$

Proof strategy

Thus, eventually, p is constant

Analyzing the previous equations

It is impossible from C to decrease p

iff

In all cases

$p = 0$

$$u_L = \max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

or $u_L = s$ and $\forall j \neq L, u_j \geq 0$

or $u_L = -s$ and $\forall j \neq L, u_j \leq 0$

Proof strategy

A. Eventually a single leader

OK

B. Eventually, the leader collects the value

OK

$$\max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

C. Eventually, the agents produce correct outputs

Proof strategy

C. Eventually, correct outputs

$$u_L = \max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

Proof strategy

C. Eventually, correct outputs

$$u_L = \max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

If $\sum a_i \cdot \#\sigma_i < c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ -s \end{cases}$

If $\sum a_i \cdot \#\sigma_i \geq c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ s \end{cases}$

Proof strategy

C. Eventually, correct outputs

$$u_L = \max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

If $\sum a_i \cdot \#\sigma_i < c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ -s \end{cases}$

If $\sum a_i \cdot \#\sigma_i \geq c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ s \end{cases}$

Leader gets correct output

Proof strategy

C. Eventually, correct outputs

$$u_L = \max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

If $\sum a_i \cdot \#\sigma_i < c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ -s \end{cases}$

If $\sum a_i \cdot \#\sigma_i \geq c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ s \end{cases}$

Leader gets correct output

Others get correct output on meeting the leader

Proof strategy

C. Eventually, correct outputs

$$u_L = \max\{-s, \min\{s, \sum a_i \cdot \#\sigma_i\}\}$$

If $\sum a_i \cdot \#\sigma_i < c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ -s \end{cases}$

If $\sum a_i \cdot \#\sigma_i \geq c$ then $u_L = \begin{cases} \sum a_i \cdot \#\sigma_i \\ s \end{cases}$

QED

Leader gets correct output

Others get correct output on meeting the leader

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k = c \mod m$$

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k = c \mod m$$

boolean combinations

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k = c \mod m$$

boolean combinations

Presburger arithmetics

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k < c$$

$$a_1 \cdot \#\sigma_1 + \cdots + a_k \cdot \#\sigma_k = c \mod m$$

boolean combinations

Presburger arithmetics

(beware: integer coefficients)