State Complexity of Population Protocols

Javier Esparza

Joint work with Michael Blondin, Philipp Czerner, Blaise Genest, Roland Guttenberg, Martin Helfrich, Stefan Jaax, and Jérôme Leroux

Technical University of Munich

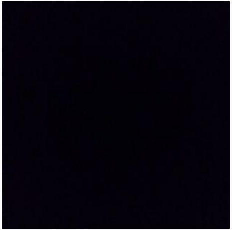
European Research Council
Established by the European Commission

An example: Deaf Black Ninjas in the Dark

- Deaf Black Ninjas meet at a Zen garden in the dark to attack a castle
- They’ll only attack if at least 100 ninjas show up

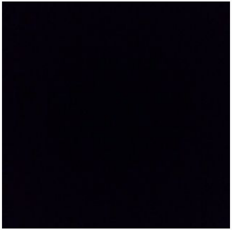
An example: Deaf Black Ninjas in the Dark

- Deaf Black Ninjas meet at a Zen garden in the dark to attack a castle
- They’ll only attack if at least 100 ninjas show up



An example: Deaf Black Ninjas in the Dark

- Deaf Black Ninjas meet at a Zen garden in the dark to attack a castle
- They'll only attack if at least 100 ninjas show up
- How can they find out?



An example: Deaf Black Ninjas in the Dark

Ninjas are told to carry a purse with one pebble, start wandering randomly around the garden, and proceed as follows:

An example: Deaf Black Ninjas in the Dark

Ninjas are told to carry a purse with one pebble, start wandering randomly around the garden, and proceed as follows:

- When two ninjas bump into each other, one of them gives the other all their pebbles.

An example: Deaf Black Ninjas in the Dark

Ninjas are told to carry a purse with one pebble, start wandering randomly around the garden, and proceed as follows:

- When two ninjas bump into each other, one of them gives the other all their pebbles.

  If at least 100 ninjas, some ninja eventually collects at least 100 pebbles $\rightarrow$ knows that at least 100 ninjas.

An example: Deaf Black Ninjas in the Dark

Ninjas are told to carry a purse with one pebble, start wandering randomly around the garden, and proceed as follows:

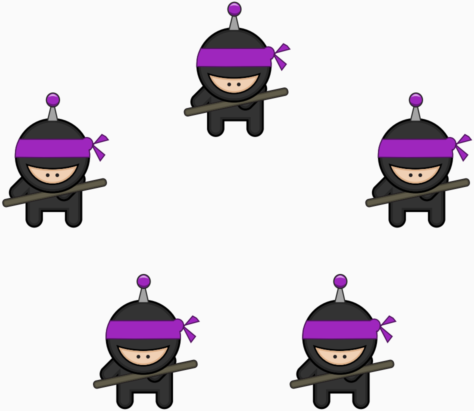
- When two ninjas bump into each other, one of them gives the other all their pebbles.

  If at least 100 ninjas, some ninja eventually collects at least 100 pebbles $\rightarrow$ knows that at least 100 ninjas.

- Ninjas who know they are at least 100 spread the word.

An example: Deaf Black Ninjas in the Dark

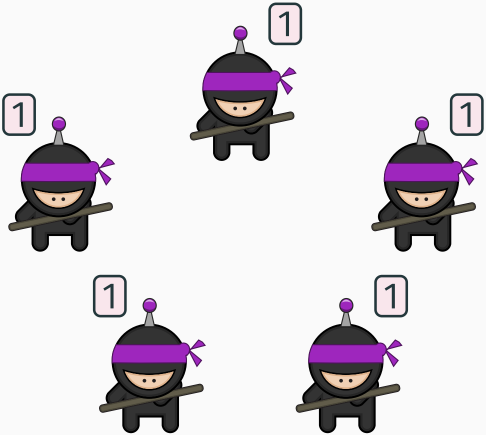
Protocol for: At least 4 ninjas?



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

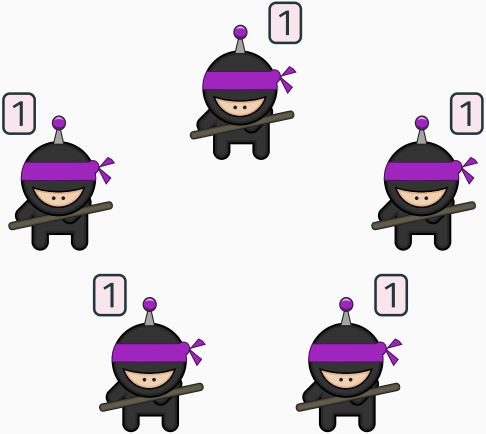
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

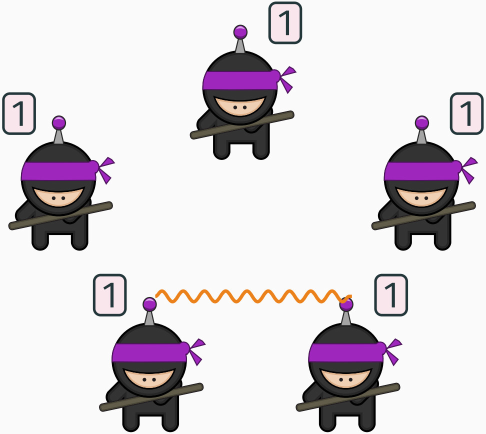
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

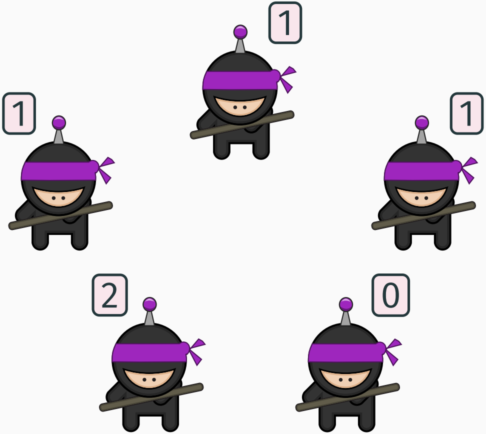
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

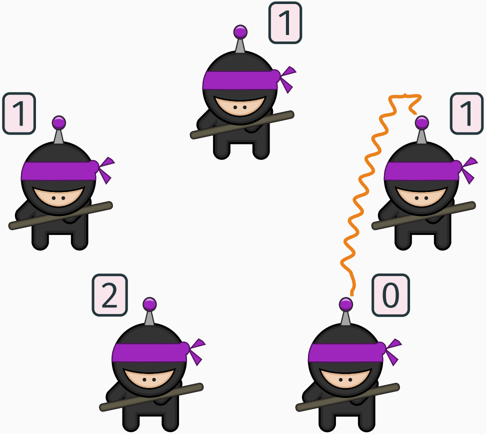
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

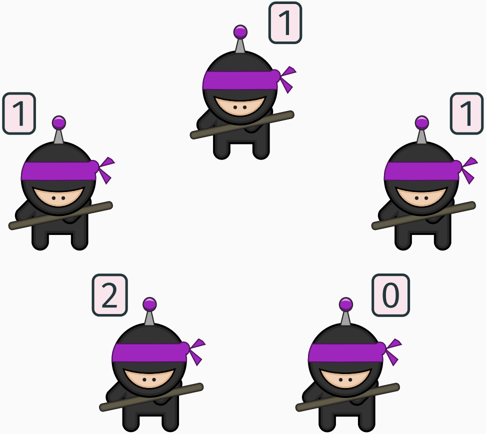
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

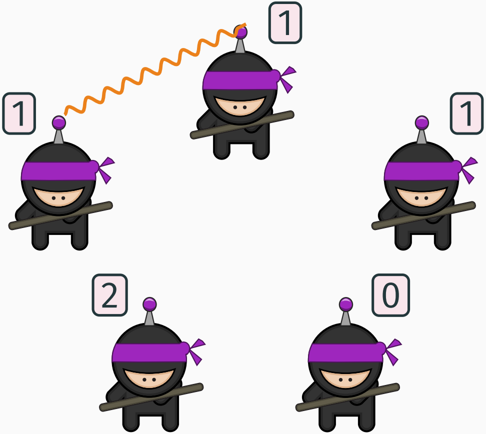
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

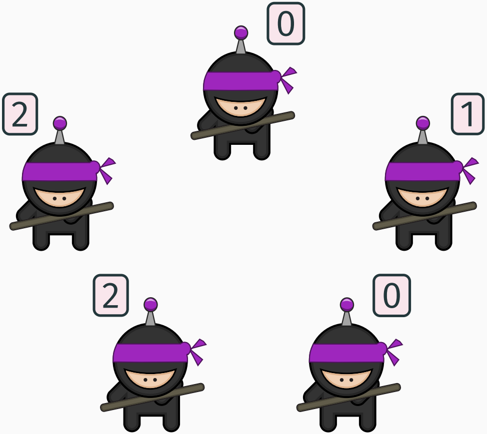
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

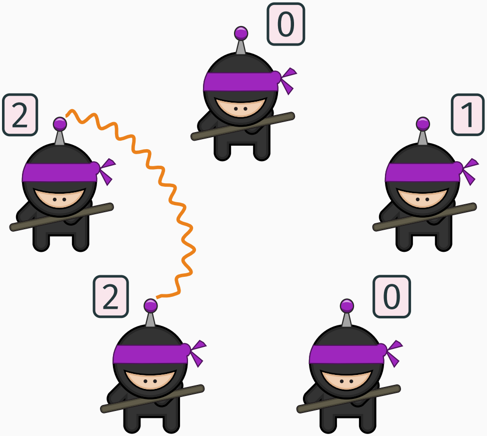
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

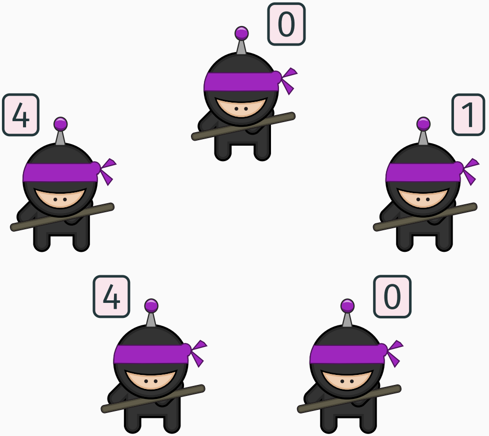
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

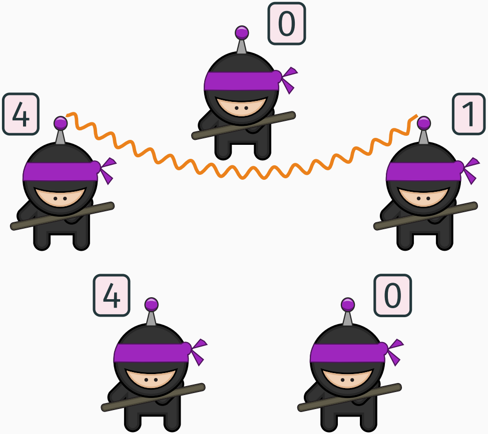
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

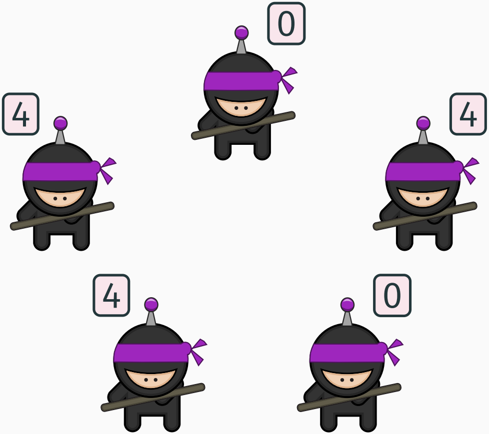
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

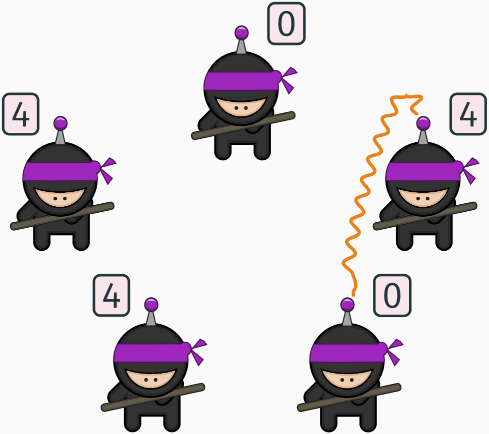
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

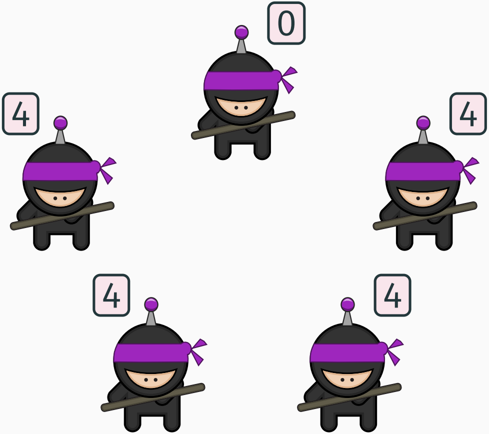
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

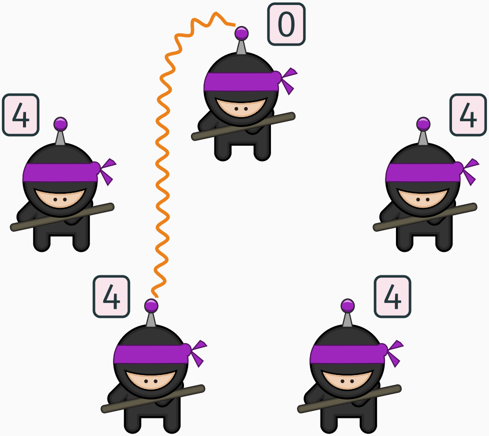
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

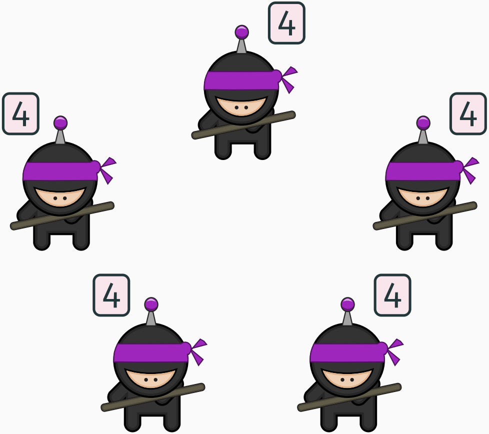
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

Protocol for: At least 4 ninjas?

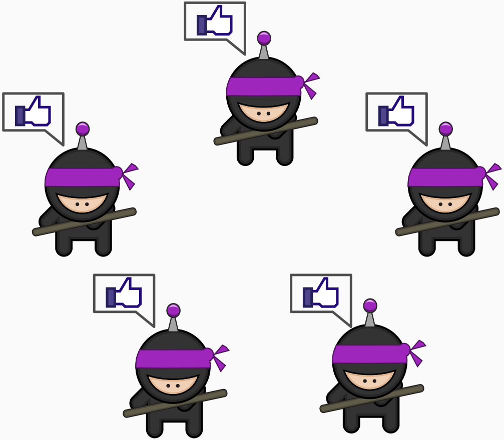
- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



An example: Deaf Black Ninjas in the Dark

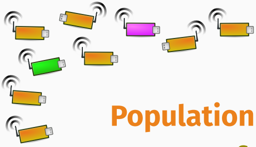
Protocol for: At least 4 ninjas?

- Each ninja is in a state of $\{0, 1, 2, 3, 4\}$
- Initially all ninjas in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 4$
- $(m, n) \mapsto (4, 4)$
  if $m + n \geq 4$



Population protocols

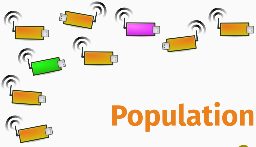
Angluin, Aspnes *et al.* PODC'04



Population protocols: formal model to describe **swarms of mobile agents** that interact randomly to decide a property of their initial configuration

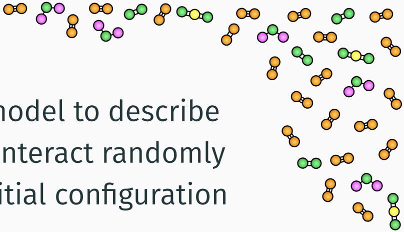
Population protocols

Angluin, Aspnes *et al.* PODC'04



Population protocols: formal model to describe **swarms of mobile agents** that interact randomly to decide a property of their initial configuration

Examples of properties: Does the initial configuration ...
...contain at least 100 agents?
...contain more agents in state A than in state B ?



Population protocols: formal model to describe **swarms of mobile agents** that interact randomly to decide a property of their initial configuration

Since the late 00s: model of natural computation.

Agents $\rightarrow$ atoms/molecules

Chemical Reaction Networks

$$CH_4 + 2\ O_2 \rightarrow CO_2 + 2\ H_2O$$

An NSF Expedition in Computing (2008-2018)

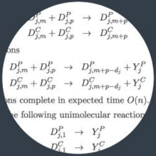
Molecular Programming Project

Computer science and engineering has mastered complexity for electronic computation — can we do the same for engineering molecular devices and systems?

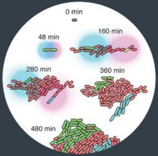
Learn More

Example works

NUPACK:
nucleic acid package



Leaderless deterministic
chemical reaction networks



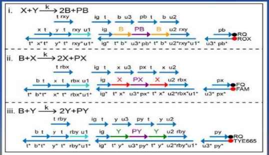
gro: the cell
programming language

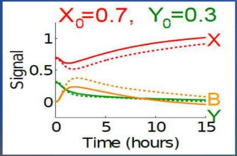
DNA Implementation of the Approximate Majority algorithm

nature nanotechnology

Programmable chemical controllers made from DNA

Yuan-Jyue Chen, Neil Dalchau, Niranjan Srinivas, Andrew Phillips, Luca Cardelli, David Soloveichik & Georg Seelig





Population protocols: formal model

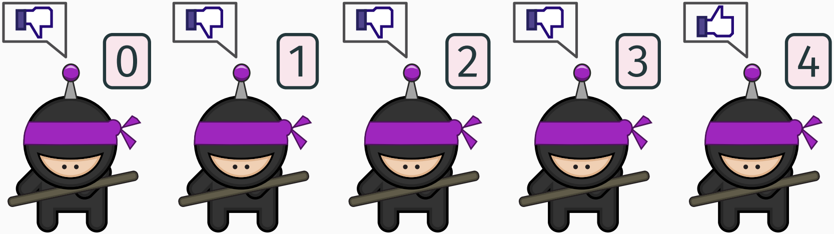
Angluin, Aspnes *et al.* PODC'04

- States: finite set Q
- Opinions: $O : Q \to \{$  ,  $\}$
- Initial states: $I \subseteq Q$
- Transitions: $T \subseteq Q^2 \times Q^2$

Population protocols: formal model

Angluin, Aspnes *et al.* PODC'04

- States: finite set Q
- Opinions: $O : Q \to \{$  ,  $\}$
- Initial states: $I \subseteq Q$
- Transitions: $T \subseteq Q^2 \times Q^2$



Population protocols: formal model

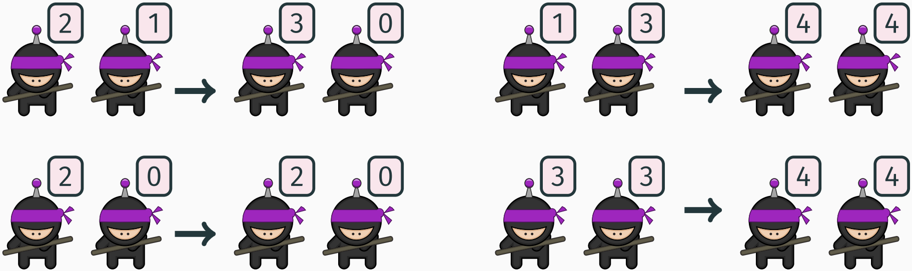
Angluin, Aspnes *et al.* PODC'04

- States: finite set Q
- Opinions: $O : Q \to \{$  ,  $\}$
- Initial states: $I \subseteq Q$
- Transitions: $T \subseteq Q^2 \times Q^2$

Population protocols: formal model

Angluin, Aspnes *et al.* PODC'04

- States: finite set Q
- Opinions: $O : Q \to \{$  ,  $\}$
- Initial states: $I \subseteq Q$
- Transitions: $T \subseteq Q^2 \times Q^2$



Population protocols: formal model

- States: finite set Q
- Opinions: $O : Q \to \{$  ,  $\}$
- Initial states: $I \subseteq Q$
- Transitions: $T \subseteq Q^2 \times Q^2$
- Configurations: $Q \to \mathbb{N}$

$$(\; 9 \quad 1 \quad 2 \quad 1 \quad 1 \;)$$

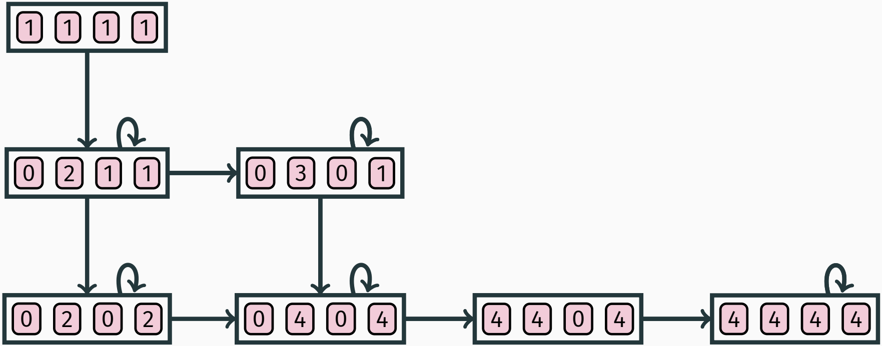
Population protocols: formal model

- States: finite set Q
- Opinions: $O : Q \to \{$  ,  $\}$
- Initial states: $I \subseteq Q$
- Transitions: $T \subseteq Q^2 \times Q^2$
- Configurations: $Q \to \mathbb{N}$
- Initial configurations: $I \to \mathbb{N}$

$$(\ 0 \quad 15 \quad 0 \quad 0 \quad 0\ )$$

Reachability graph for an initial configuration

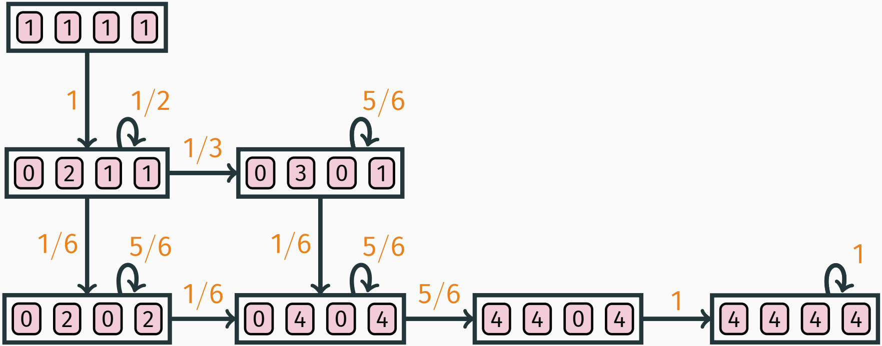
Reachability graph for  :



Markov chain for an initial configuration

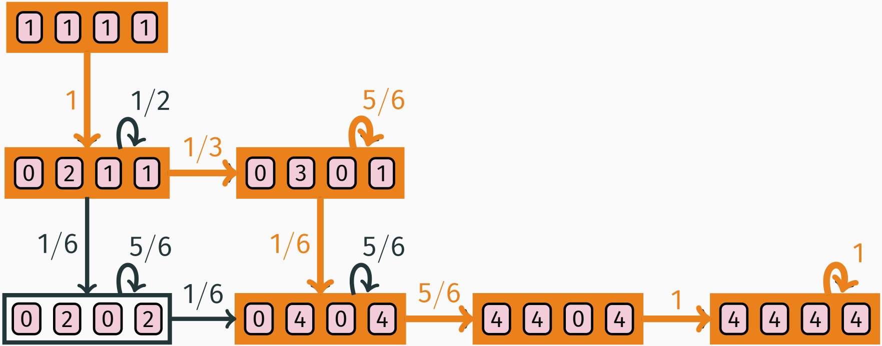
Underlying Markov chain:

(pairs of agents are picked uniformly at random)



Runs

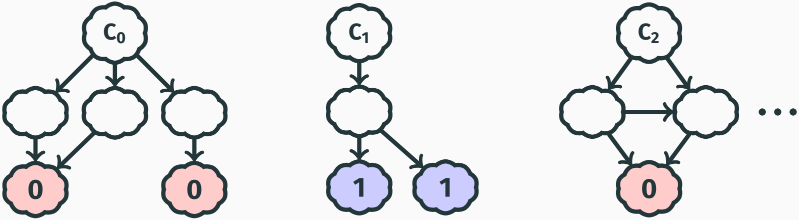
Run : infinite path from initial configuration



Predicate decided (computed) by a protocol

Protocol decides φ : InitC $\to \{0, 1\}$:

for every $C \in$ InitC, the runs starting at C reach **stable consensus** $\varphi(C)$ with probability 1.



All agree to 

All agree to 

All agree to 

Predicate decided (computed) by a protocol

Protocol decides φ: InitC $\to \{0, 1\}$:
for every $C \in$ InitC, the runs starting at C reach **stable consensus** $\varphi(C)$ with probability 1.

Our protocol decides the predicate $\boldsymbol{x \geq 4}$

The quest for succinct protocols

Protocol for $\boldsymbol{x \geq c}$

- States: $\{0, 1, 2, \ldots, c\}$
  $\rightarrow \boldsymbol{c + 1}$ states
- Initially, all agents
  in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < c$
- $(m, n) \mapsto (c, c)$
  if $m + n \geq c$

The quest for succinct protocols

Protocol for $\boldsymbol{x} \geq \boldsymbol{c}$

- States: $\{0, 1, 2, \ldots, c\}$
  $\rightarrow$ $\boldsymbol{c} + \mathbf{1}$ states
- Initially, all agents
  in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < c$
- $(m, n) \mapsto (c, c)$
  if $m + n \geq c$

Exponentially many states
in $\log c$, the length of $\mathbf{x} \geq \mathbf{c}$

The quest for succinct protocols

Protocol for $\boldsymbol{x \geq c}$

- States: $\{0, 1, 2, \ldots, c\}$
  $\rightarrow \boldsymbol{c + 1}$ states
- Initially, all agents
  in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < c$
- $(m, n) \mapsto (c, c)$
  if $m + n \geq c$

Exponentially many states
in $\log c$, the length of $\mathbf{x} \geq \mathbf{c}$

Can we do better?

The quest for succinct protocols

Protocol for $\boldsymbol{x \geq c}$

- States: $\{0, 1, 2, \ldots, c\}$
  $\rightarrow \boldsymbol{c + 1}$ states
- Initially, all agents
  in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < c$
- $(m, n) \mapsto (c, c)$
  if $m + n \geq c$

Exponentially many states
in $\log c$, the length of $\mathbf{x} \geq \mathbf{c}$

Can we do better?

State complexity of $\boldsymbol{x \geq c}$:

minimal number of states

of a protocol deciding it.

Why care about state complexity?

PPs as a model for natural computing (**chemical reaction networks**):

Why care about state complexity?

PPs as a model for natural computing (**chemical reaction networks**):

- Agent $\rightarrow$ molecule

Why care about state complexity?

PPs as a model for natural computing (**chemical reaction networks**):

- Agent $\rightarrow$ molecule
- State $\rightarrow$ current **species** of the molecule

Why care about state complexity?

PPs as a model for natural computing (**chemical reaction networks**):

- Agent $\rightarrow$ molecule
- State $\rightarrow$ current **species** of the molecule
- Transition $\rightarrow$ chemical reaction

$$CH_4 + 2\,O_2 \quad \rightarrow \quad CO_2 + 2\,H_2O$$

Why care about state complexity?

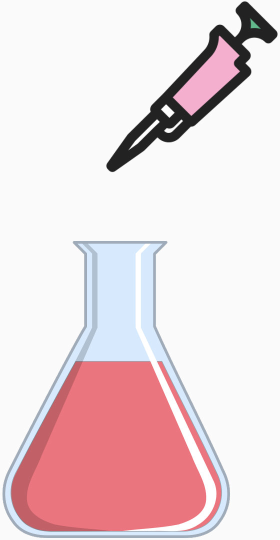
PPs as a model for natural computing (**chemical reaction networks**):

- Agent $\rightarrow$ molecule
- State $\rightarrow$ current **species** of the molecule
- Transition $\rightarrow$ chemical reaction

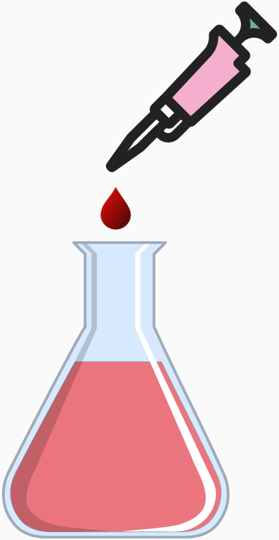
$$CH_4 + 2\,O_2 \quad \rightarrow \quad CO_2 + 2\,H_2O$$

$$(A, B, B) \quad \mapsto \quad (C, D, D)$$

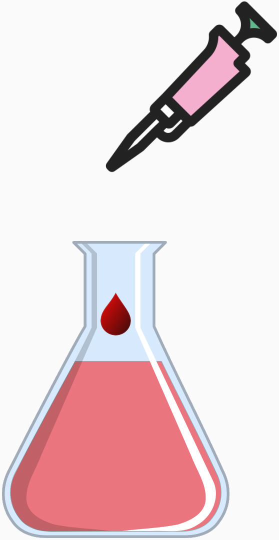
Why care about state complexity?



Why care about state complexity?

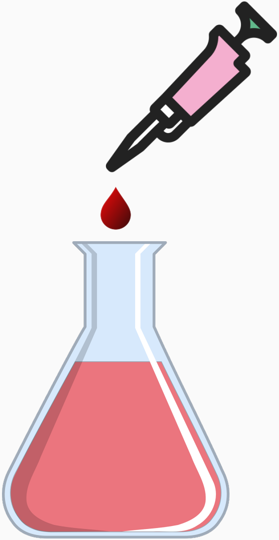


Why care about state complexity?

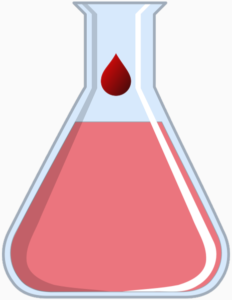


Why care about state complexity?

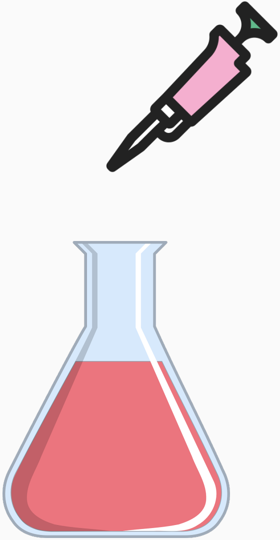
Why care about state complexity?



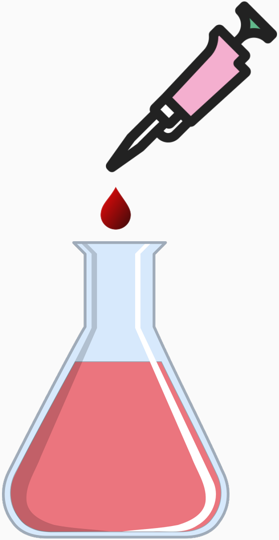
Why care about state complexity?



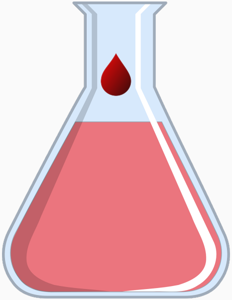
Why care about state complexity?



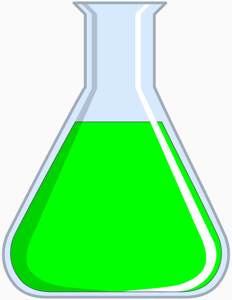
Why care about state complexity?



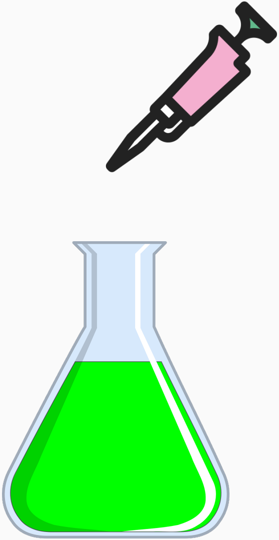
Why care about state complexity?



Why care about state complexity?



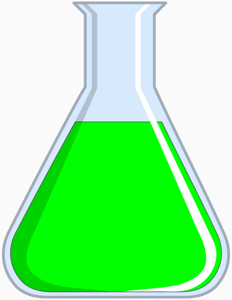
Why care about state complexity?



Color should change when the number of molecules in the flask reaches c.

We need to implement a protocol for $x \geq c$.

Why care about state complexity?

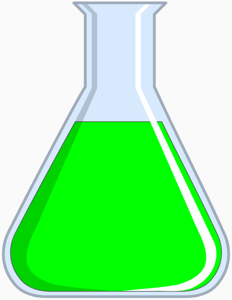


Color should change when the number of molecules in the flask reaches $\boldsymbol{c}$.

We need to implement a protocol for $\boldsymbol{x} \geq \boldsymbol{c}$.

Avogadro's number is $\sim 6 \times 10^{23}$, so we need the protocol for $\boldsymbol{c} \sim \boldsymbol{2^{60}}$.

Why care about state complexity?



Color should change when the number of molecules in the flask reaches $\boldsymbol{c}$.

We need to implement a protocol for $\boldsymbol{x} \geq \boldsymbol{c}$.

Avogadro's number is $\sim 6 \times 10^{23}$, so we need the protocol for $\boldsymbol{c} \sim \mathbf{2^{60}}$.

But in chemical reaction networks

 # states = # chemical species

We need **2^{60} species**.

The quest for succinct protocols

Protocol for $\boldsymbol{x \geq 2^k}$

- States: $\{0, 1, 2, \ldots, 2^k\}$
  $\rightarrow \mathbf{2^k + 1}$ states
- Initially, all agents
  in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 2^k$
- $(m, n) \mapsto (2^k, 2^k)$
  if $m + n \geq 2^k$

The quest for succinct protocols

Protocol for $\boldsymbol{x \geq 2^k}$

- States: $\{0, 1, 2, \ldots, 2^k\}$
  $\rightarrow \mathbf{2^k + 1}$ states
- Initially, all agents
  in state 1
- $(m, n) \mapsto (m + n, 0)$
  if $m + n < 2^k$
- $(m, n) \mapsto (2^k, 2^k)$
  if $m + n \geq 2^k$

Protocol for $\boldsymbol{x \geq 2^k}$

- States: $\boldsymbol{\{0, 2^0, \ldots, 2^{k-1}, 2^k\}}$
  $\rightarrow \mathbf{k + 2}$ states
- Initially, all agents
  in state $\mathbf{2^0}$
- $(\mathbf{2^\ell}, \mathbf{2^\ell}) \mapsto (\mathbf{2^{\ell+1}}, \mathbf{0})$
  if $\ell + \mathbf{1} \leq \boldsymbol{k}$
- $(\mathbf{2^k}, \boldsymbol{n}) \mapsto (\mathbf{2^k}, \mathbf{2^k})$

The quest for succinct protocols

Extensible to arbitrary $\mathbf{x} \geq \mathbf{c}$ predicates: $\mathcal{O}(\log \mathbf{c})$ states (not totally trivial).

Protocol for $\boldsymbol{x} \geq \mathbf{2}^{\boldsymbol{k}}$

- States: $\{\mathbf{0}, \mathbf{2}^{\mathbf{0}}, \ldots, \mathbf{2}^{\boldsymbol{k}-\mathbf{1}}, \mathbf{2}^{\boldsymbol{k}}\}$
  $\rightarrow \mathbf{k} + \mathbf{2}$ states
- Initially, all agents
  in state $\mathbf{2}^{\mathbf{0}}$
- $(\mathbf{2}^{\ell}, \mathbf{2}^{\ell}) \mapsto (\mathbf{2}^{\ell+\mathbf{1}}, \mathbf{0})$
  if $\ell + \mathbf{1} \leq \boldsymbol{k}$
- $(\mathbf{2}^{\boldsymbol{k}}, \boldsymbol{n}) \mapsto (\mathbf{2}^{\boldsymbol{k}}, \mathbf{2}^{\boldsymbol{k}})$

The quest for succinct protocols

Extensible to arbitrary **x ≥ c** predicates: $\mathcal{O}(\log \mathbf{c})$ states (not totally trivial).

Can we do even better?

Is $O(\log\log \mathbf{c})$ possible?

Protocol for $\boldsymbol{x} \geq \mathbf{2}^{\boldsymbol{k}}$

- States: $\{\mathbf{0}, \mathbf{2}^{\mathbf{0}}, \ldots, \mathbf{2}^{\boldsymbol{k}-\mathbf{1}}, \mathbf{2}^{\boldsymbol{k}}\}$
  $\rightarrow \mathbf{k} + \mathbf{2}$ states
- Initially, all agents in state $\mathbf{2}^{\mathbf{0}}$
- $(\mathbf{2}^{\ell}, \mathbf{2}^{\ell}) \mapsto (\mathbf{2}^{\ell+\mathbf{1}}, \mathbf{0})$ if $\ell + \mathbf{1} \leq \boldsymbol{k}$
- $(\mathbf{2}^{\boldsymbol{k}}, \boldsymbol{n}) \mapsto (\mathbf{2}^{\boldsymbol{k}}, \mathbf{2}^{\boldsymbol{k}})$

Not for every $\mathbf{c}$ ...

Blondin, E., Jaax STACS'18

There exist infinitely many $\mathbf{c}$ such that every protocol for $\mathbf{x} \geq \mathbf{c}$ has at least $(\log \mathbf{c})^{1/4}$ states

Not for every **c** …

Blondin, E., Jaax STACS'18

There exist infinitely many **c** such that every protocol for $\mathbf{x} \geq \mathbf{c}$ has at least $(\log \mathbf{c})^{1/4}$ states

…but for infinitely many **c**, if we allow **leaders**.

A protocol with a leader for $x = y$

Initially ninjas are blue or red.

Question to be decided: same number of blue and red ninjas?

One leader helps the ninjas. Leader searches for pairs of blue-red ninjas, “neutralizing them”, until no such pairs left.

A protocol with a leader for $x = y$

Initially ninjas are blue or red.

Question to be decided: same number of blue and red ninjas?

One leader helps the ninjas. Leader searches for pairs of blue-red ninjas, “neutralizing them”, until no such pairs left.

Leader states:  = More blue  = Tie  = More red

Ninja states: 

A protocol with a leader for $x = y$

Initially ninjas are blue or red.

Question to be decided: same number of blue and red ninjas?

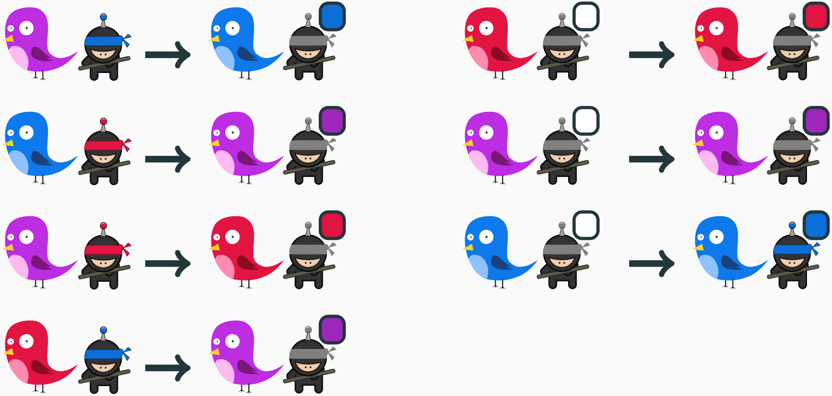
One leader helps the ninjas. Leader searches for pairs of blue-red ninjas, “neutralizing them”, until no such pairs left.

Leader states:  = More blue  = Tie  = More red

Ninja states: 

A protocol with a leader for $x = y$

Transitions:



The quest for succinct protocols

Blondin, E., Jaax STACS'18

For infinitely many $\mathbf{c}$ there is a protocol with a leader and $\mathcal{O}(\log\log \mathbf{c})$ states that computes $\mathbf{x} \geq \mathbf{c}$

The quest for succinct protocols

Blondin, E., Jaax STACS'18

For infinitely many $\mathbf{c}$ there is a protocol with a leader and $\mathcal{O}(\log \log \mathbf{c})$ states that computes $\mathbf{x} \geq \mathbf{c}$

Proof:

Mayr and Meyer '82: For every n there is a reversible Petri net of size $O(n)$ and two places $\boldsymbol{s}$, $\boldsymbol{t}$ such that the shortest firing sequence leading from $\boldsymbol{s}$ to $\boldsymbol{t}$ has length $\boldsymbol{\Theta}(\mathbf{2}^{\mathbf{2}^{n}})$

The quest for succinct protocols

Blondin, E., Jaax STACS'18

For infinitely many **c** there is a protocol with a leader and $\mathcal{O}(\log \log \mathbf{c})$ states that computes $\mathbf{x} \geq \mathbf{c}$

Proof:

For every n there is a reversible protocol with a leader and $O(n)$ states and transitions s.t.

- ,  are two states of the leader,
-  is the initial state of the normal agents, and
- The leader may move from  to  iff the number of  is at least 2^{2^n}

The quest for succinct protocols

Blondin, E., Jaax STACS'18

For infinitely many **c** there is a protocol with a leader and $\mathcal{O}(\log\log \mathbf{c})$ states that computes $\mathbf{x} \geq \mathbf{c}$

Proof:

For every n there is a <u>reversible</u> protocol with a leader and $O(n)$ states and transitions s.t.

- ,  are two states of the leader,
-  is the initial state of the normal agents, and
- The leader <u>may</u> move from  to  iff the number of  is at least 2^{2^n} $\rightarrow$ **by reversibility it eventually will!**

The quest for succinct protocols

Blondin, E., Jaax STACS'18

For infinitely many **c** there is a protocol with a leader and $\mathcal{O}(\log\log \mathbf{c})$ states that computes $\mathbf{x} \geq \mathbf{c}$

Proof:

Add transitions  $, q \mapsto$  ,  for every state q

allowing leader to "attract" all other agents to  .

Make  the only  state.

The quest for succinct protocols

Blondin, E., Jaax STACS'18

For infinitely many **c** there is a protocol with a leader and $\mathcal{O}(\log \log \mathbf{c})$ states that computes $\mathbf{x} \geq \mathbf{c}$

Proof:

Add transitions  $, q \mapsto$  ,  for every state q

allowing leader to "attract" all other agents to  .

Make  the only  state.

At least 2^{2^n}  : leader eventually reaches  w.p.1 and attracts everyone to  , and so to  .

The quest for succinct protocols

Blondin, E., Jaax STACS'18

For infinitely many **c** there is a protocol with a leader and $\mathcal{O}(\log\log \mathbf{c})$ states that computes $\mathbf{x} \geq \mathbf{c}$

Proof:

Add transitions  , $q \mapsto$  ,  for every state q

allowing leader to "attract" all other agents to  .

Make  the only  state.

At least 2^{2^n}  : leader eventually reaches  w.p.1 and attracts everyone to  , and so to  .

Less than 2^{2^n}  : leader never reaches  .

How far can we go?

How far can we go?

Czerner, E., PODC'21

Every protocol for $\boldsymbol{x} \geq \boldsymbol{c}$, with or without leaders, has $\Omega(\alpha(\boldsymbol{c}))$ states, where α is the inverse of (some variant of) the Ackermann function.

How far can we go?

Czerner, E., PODC’21

Every protocol for $\boldsymbol{x} \geq \boldsymbol{c}$, with or without leaders, has $\Omega(\alpha(\boldsymbol{c}))$ states, where α is the inverse of (some variant of) the Ackermann function.

Proof technique for all bounds:

Find numbers $\boldsymbol{a}, \boldsymbol{b}$ such that

- protocol outputs  for $\boldsymbol{a}$; and
- if protocol outputs  for $\boldsymbol{a} + \boldsymbol{b}$, then it outputs  for $\boldsymbol{a} + \boldsymbol{\lambda b}$ for every $\boldsymbol{\lambda} \in \mathbb{N}$.

Then protocol outputs  for $\boldsymbol{a}$ and  for $\boldsymbol{a} + \boldsymbol{b}$, which implies $\boldsymbol{a} < \boldsymbol{c} \leq \boldsymbol{a} + \boldsymbol{b}$.

How far can we go?

Czerner, E., PODC'21

Every protocol for $\boldsymbol{x} \geq \boldsymbol{c}$, with or without leaders, has $\Omega(\alpha(\boldsymbol{c}))$ states, where α is the inverse of (some variant of) the Ackermann function.

Proof technique for all bounds:

Find numbers $\boldsymbol{a}, \boldsymbol{b}$ such that

- protocol outputs  for $\boldsymbol{a}$; and
- if protocol outputs  for $\boldsymbol{a} + \boldsymbol{b}$, then it outputs  for $\boldsymbol{a} + \boldsymbol{\lambda b}$ for every $\boldsymbol{\lambda} \in \mathbb{N}$.

Then protocol outputs  for $\boldsymbol{a}$ and  for $\boldsymbol{a} + \boldsymbol{b}$, which implies $\boldsymbol{a} < \boldsymbol{c} \leq \boldsymbol{a} + \boldsymbol{b}$.

Existence of $\boldsymbol{a}$ and $\boldsymbol{a} + \boldsymbol{b}$ derived from **Dickson's lemma**.

How far can we go?

Czerner, E., PODC'21

Every leaderless protocol for $\boldsymbol{x} \geq \boldsymbol{c}$ has $\Omega(\log\log\log \boldsymbol{c})$ states.

How far can we go?

Czerner, E., PODC'21

Every leaderless protocol for $\boldsymbol{x} \geq \boldsymbol{c}$ has $\Omega(\log\log\log \boldsymbol{c})$ states.

Czerner, E., Leroux 21, Submitted

Every leaderless protocol for $\boldsymbol{x} \geq \boldsymbol{c}$ has $\Omega(\log\log \boldsymbol{c})$ states.

How far can we go?

Czerner, E., PODC'21

Every leaderless protocol for $x \geq c$ has $\Omega(\log\log\log c)$ states.

Czerner, E., Leroux 21, Submitted

Every leaderless protocol for $x \geq c$ has $\Omega(\log\log c)$ states.

Bound on $a + b$ derived from

- **Rackoff's theorem** (used to obtain a clover of the set of configurations that are a stable consensus whose elements have double exponential norm).
- **Pottier's small basis theorem** for systems of Diophantine equations.

How far can we go?

Leroux 21, arXiv

Every protocol for $\boldsymbol{x} \geq \boldsymbol{c}$, with or without leaders, has $\Omega((\log \log \mathbf{c})^{1/3})$ states.

How far can we go?

Leroux 21, arXiv

Every protocol for $\boldsymbol{x} \geq \boldsymbol{c}$, with or without leaders, has $\Omega((\log\log \mathbf{c})^{1/3})$ states.

Bound uses all of the above, plus some stuff I'll leave to Jérôme ...

This far we've come

Summary

For every $\boldsymbol{c}$, there is a leaderless protocol with $\mathcal{O}(\log \boldsymbol{c})$ states.

For every $\boldsymbol{c}$, every protocol, with or without a leader, has $\Omega((\log \log \boldsymbol{c})^{1/3})$ states.

For infinitely many $\boldsymbol{c}$, there is a protocol with a leader with $\mathcal{O}(\log \log \boldsymbol{c})$ states.

Open question: Are there leaderless protocols with $\mathcal{O}(\log \log \boldsymbol{c})$ states for infinitely many $\boldsymbol{c}$?

State complexity of general Presburger predicates

Angluin, Aspnes, Eisenstat Dist. Comp.'07

Population protocols decide precisely the predicates definable in Presburger arithmetic, i.e. $\mathrm{FO}(\mathbb{N}, +, <)$

State complexity of general Presburger predicates

Angluin, Aspnes, Eisenstat Dist. Comp.'07

Population protocols decide precisely the predicates definable in Presburger arithmetic, i.e. $\mathrm{FO}(\mathbb{N}, +, <)$

PPs for all Presburger predicates

Using that Presburger arithmetic has quantifier elimination, Angluin et al. proceed as follows:

1) Exhibit PPs for **threshold** and **modulo** predicates

$$a_1x_1 + \cdots + a_kx_k \leq b \qquad a_1x_1 + \cdots + a_kx_k \equiv b \bmod c$$

2) Show that predicates decidable by PPs are closed under negation and conjunction

State complexity of general Presburger predicates

Angluin, Aspnes, Eisenstat Dist. Comp.'07

Population protocols decide precisely the predicates definable in Presburger arithmetic, i.e. FO($\mathbb{N}, +, <$)

Exponential state complexity in both

- the number of bits of the coefficients, and
- the number of threshold and modulo predicates.

State complexity of general Presburger predicates

Angluin, Aspnes, Eisenstat Dist. Comp.'07

Population protocols decide precisely the predicates definable in Presburger arithmetic, i.e. $\mathrm{FO}(\mathbb{N}, +, <)$

Can polynomial state complexity be achieved ?

A protocol for $x - y \geq 2^k$ with $O(k)$ states

Protocol for $x \geq 2^k$

States: $\{0, 2^0, \ldots, 2^k\}$

Initially: all ninjas in state 1

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$

A protocol for $x - y \geq 2^k$ with $O(k)$ states

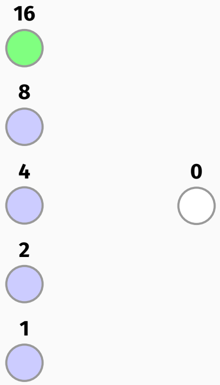
Protocol for $x \geq 2^k$

States: $\{0, 2^0, \ldots, 2^k\}$

Initially: all ninjas in state 1

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$



A protocol for $x - y \geq 2^k$ with $O(k)$ states

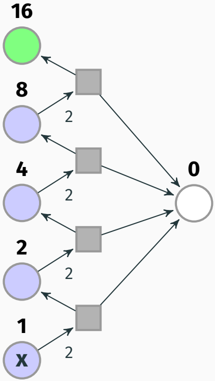
Protocol for $x \geq 2^k$

States: $\{0, 2^0, \ldots, 2^k\}$

Initially: all ninjas in state 1

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$



A protocol for $x - y \geq 2^k$ with $O(k)$ states

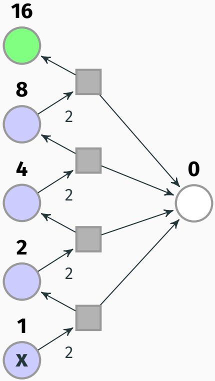
Protocol for $x \geq 2^k$

States: $\{0, 2^0, \ldots, 2^k\}$

Initially: all ninjas in state 1

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$



A ninja that
"climbs the ladder"
attracts all others to
the top

A protocol for $x - y \geq 2^k$ with $O(k)$ states

Protocol for $x - y \geq 2^k$

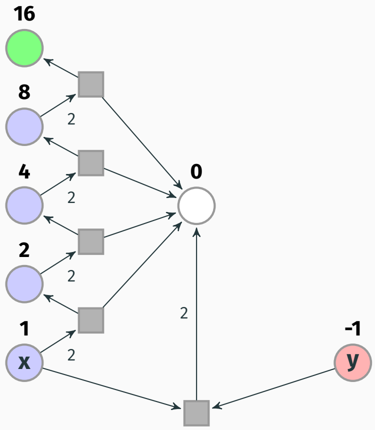
States: $\{-1, 0, 2^0, \ldots, 2^k\}$

Initially: x, y ninjas in 1, -1

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$

$(1, -1) \mapsto (0, 0)$



A protocol for $x - y \geq 2^k$ with $O(k)$ states

Protocol for $x - y \geq 2^k$

States: $\{-1, 0, 2^0, \ldots, 2^k\}$

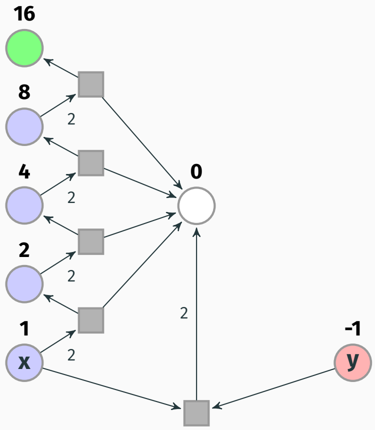
Initially: x, y ninjas in 1, -1

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$

$(1, -1) \mapsto (0, 0)$

Not yet correct!



A protocol for $x - y \geq 2^k$ with $O(k)$ states

Protocol for $x - y \geq 2^k$

States: $\{-1, 0, 2^0, \ldots, 2^k\}$

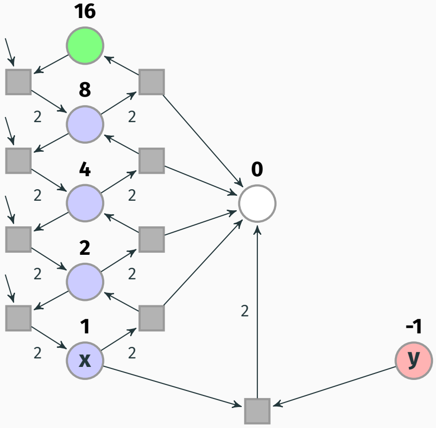
Initially: x, y ninjas in 1, -1

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$

$(1, -1) \mapsto (0, 0)$

$(2^\ell, 0) \mapsto (2^{\ell-1}, 2^{\ell-1})$
if $\ell \leq 1$



All predicates have polynomial state complexity

Blondin, E., Genest, Helfrich, Jaax STACS'20

Every predicate φ of quantifier-free Presburger arithmetic can be decided by a leaderless protocol with a polynomial number of states in $|\varphi|$.

All predicates have polynomial state complexity

Blondin, E., Genest, Helfrich, Jaax STACS'20

Every predicate φ of quantifier-free Presburger arithmetic can be decided by a leaderless protocol with a polynomial number of states in $|\varphi|$.

Construction

Quite sophisticated "protocol engineering" !

1) Use "up and down" ladders plus other constructions to give PPs for threshold and modulo predicates with polynomial number of states.

2) Given protocols with sets of states n_1 and n_2 for φ_1 and φ_2, construct a protocol for $\varphi_1 \wedge \varphi_2$ with $\mathcal{O}(n_1 + n_2)$ states using protocols with *reversible dynamic initialization*.

But are they fast ... ?

Protocol for $x - y \geq 2^k$

States: $\{-1, 0, 2^0, \ldots, 2^k\}$

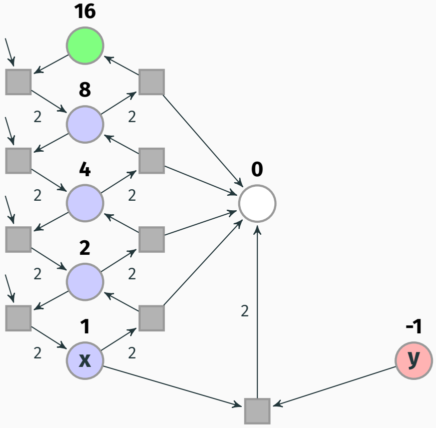
Initially: $x, y)$ ninjas in $1, -1$

$(2^\ell, 2^\ell) \mapsto (2^{\ell+1}, 0)$
if $\ell + 1 \leq k$

$(2^k, n) \mapsto (2^k, 2^k)$

$(1, -1) \mapsto (0, 0)$

$(2^\ell, 0) \mapsto (2^{\ell-1}, 2^{\ell-1})$
if $\ell \leq 1$

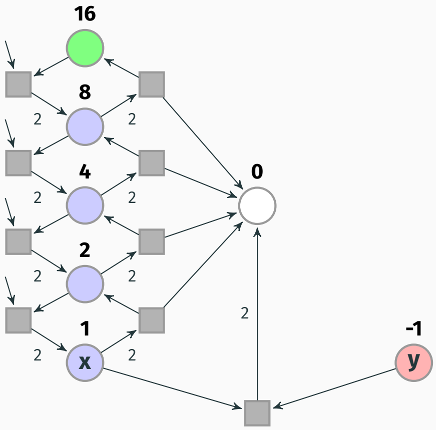


But are they fast ... ?

Very slow!

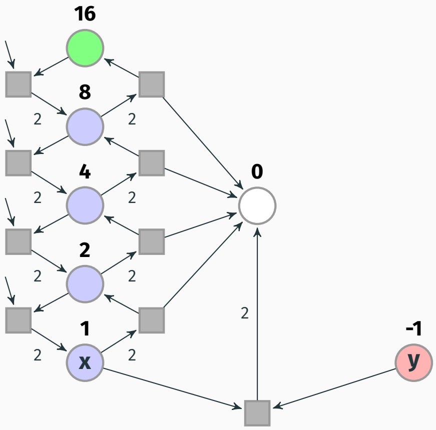
Exponential expected time to convergence in the number of ninjas.

Protocols of Angluin et al. run in $\mathcal{O}(n \log n)$ time.



But are they fast ... ?

Are there fast and succinct protocols for all Presburger predicates ?



Two years and 50 pages later ...

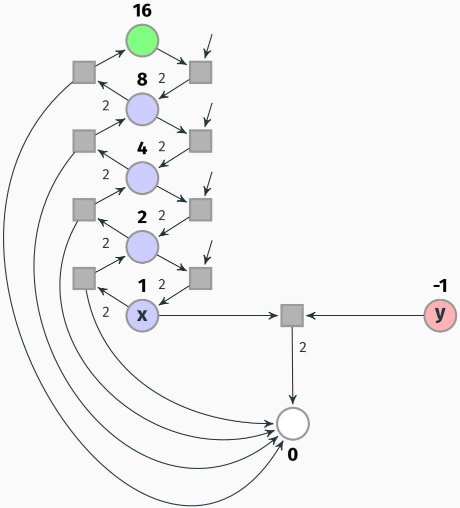
Czerner, Guttenberg, Helfrich, E. Submitted

Every predicate φ of quantifier-free Presburger arithmetic can be decided by a leaderless protocol

- with $|\varphi|$ states,
- running in $\mathcal{O}(n)$ expected time for all inputs of size $\Omega(|\varphi|)$.

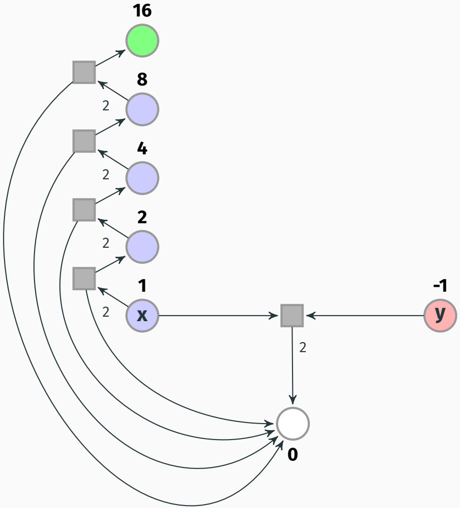
Two years and 50 pages later ...

One of the ideas ...



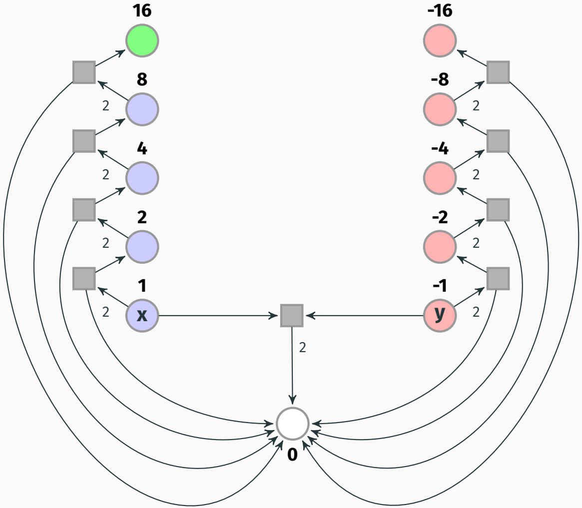
Two years and 50 pages later ...

One of the ideas ...



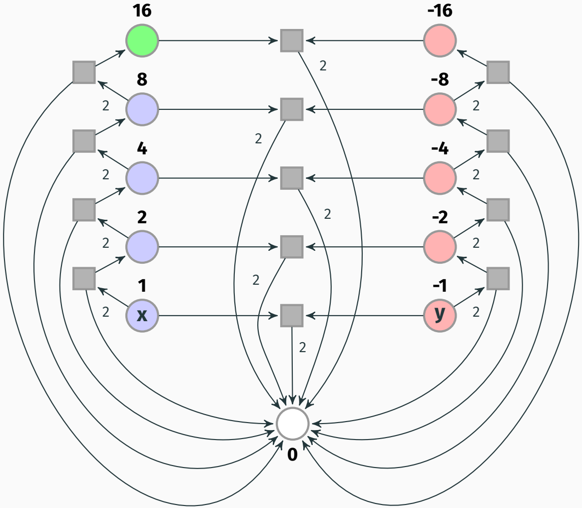
Two years and 50 pages later ...

One of the ideas ...



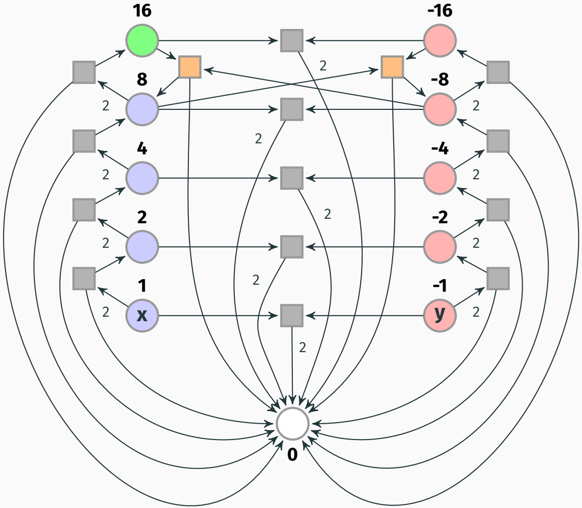
Two years and 50 pages later ...

One of the ideas ...



Two years and 50 pages later ...

One of the ideas ...



State complexity of population protocols is a fundamental question of distributed computation:

- Crucial for applications in natural computing
- Limits of collective knowledge
- Role of leaders

Conclusion

State complexity of counting predicates $x \geq c$

Leaderless protocols

- $\Omega((\log \log c)^{1/3})$ and $\mathcal{O}(\log c)$ states.
- Not known if $\Theta((\log \log c)^{1/3})$ achievable for some family of c.

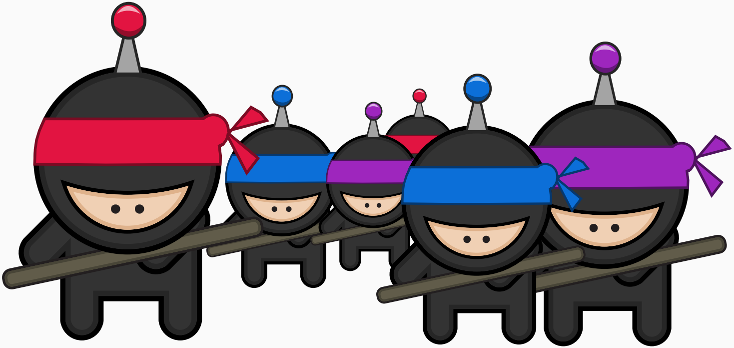
State complexity of counting predicates $x \geq c$

Protocols with a leader

- $\Omega((\log\log c)^{1/3})$ and $\mathcal{O}(\log c)$ states.
- $\Theta(\log\log c)$ for infinitely many c.

Succint protocols for Presburger predicates:

	States	Expected time
Angluin et al. ‘04	$2^{\Theta(\lvert\varphi\rvert)}$	$\Theta(n \log n)$
Blondin et al. ‘20	$\mathrm{poly}(\lvert\varphi\rvert)$	$2^{\Omega(n)}$
Czerner et al. ‘21	$\Theta(\lvert\varphi\rvert)$	$\Theta(n)$
		for inputs of size $\Omega(\lvert\varphi\rvert)$



THANK YOU!