## Playing With Population Protocols

Olivier Bournez ${ }^{1}$ Jérémie Chalopin ${ }^{2,5}$ Johanne Cohen ${ }^{3,5}$ Xavier Koegler ${ }^{4}$<br>${ }^{1}$ Ecole Polytechnique, France<br>${ }^{2}$ University of Marseille, France<br>${ }^{3}$ University of Versailles, France<br>${ }^{4}$ Paris VII University, France<br>${ }^{5}$ Centre National de la Recherche Scientifique

## Réunion SHAMAN.

Tuesday January 27th 2009.

Plan

Population Protocols

## Variants

Population Protocols and Games

## Population protocols

■ Introduced by [Angluin,Aspnes,Diamadi,Fischer,Peralta 2004] in the context of distributed systems.

- A model of sensor networks, with absolutely minimal assumptions about
- sophistication of mobile units :
- finite state machines.
- infrastructure : none
- no topology,
- not even unique ids.
- synchrony :
- totally asynchronous.
- communications :
- communications are occasionally possible between pairs of agents.

Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


Example 1 : starting with 3 blues, 2red


## Example 1 : Final result



Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3 red


Example 2 : starting with 2 blues, 3red


Example 2 : starting with 2 blues, 3red


Example 2 : Final result


## What is computed?

## Let's interpret

-     - and by yes.
-     - and by no.

■ Whatever the initial state is, ultimately, all agents will agree.

■ They agree on yes iff the initial population of $\bullet$ is strictly greater than the initial population of $\bullet$.

## Alternative statement

- A configuration can be seen as an element of $\mathbb{N}^{4}$.
- $\left(n_{b}, n_{r}, n_{g}, n_{b}\right)$ if there is $n_{b} \bullet, n_{r} \bullet, n_{g}$ and $n_{b}$
- $n_{b}+n_{r}+n_{g}+n_{b l}$ is preserved.
- An initial configuration is of type $\left(n_{b}, n_{r}, 0,0\right)$.
- This protocol computes predicates $n_{r}>n_{b}$, i.e. MAJORITY


## General Case: Algorithm

An algorithm consists of

- a finite set of states $Q=\left\{q_{1}, q_{2}, \cdots, q_{k}\right\}$.

■ transition rules, mapping pairs of states to pairs of states

Executions are given by :

- instantaneous configuration : a multiset of states $=$ an element of $\mathbb{N}^{k}$.
- transitions between configuration : two agents are picked, and updated according to the rules of the algorithm.
- output interpretation : mapping states to $\{0,1\}$.
- a computation is over when all agents agree on 0 or 1 .

Remark : Algorithm are assumed independent of size of population!

## Simplest example : Computing OR of input bits

States: •,॰

One transition rule

Output of an agent is its state.

If all inputs are •, all agents will remain in state $\bullet$ If some agent is $\bullet$, eventually all will have state $\bullet$

## A remark: Fairness

- One need to guarantee that all possible interactions happen eventually
- an execution is fair if for all configurations $C$ that appear infinitely often in the execution, if $C \rightarrow C^{\prime}$ for some configuration $C^{\prime}$, then $C^{\prime}$ appears infinitely often in the execution.
- can be seen as capturing the idea of probabilistic adversary : there is some (unknown) underlying probability distribution on interactions such that events are independent.
- True notion of computation : For any input I, for any fair sequence of executions starting from I agents ultimately agree on 0 or 1 .


## Leader Election

Initially, all agents in same state $\bullet$

Eventually, exactly one agent is in a special leader state •


## Threshold Predicate

- Suppose each agent starts with input • or •
- Determine whether at least five agents have input $\bullet$.


## 5\%

- Each agent is initially $\bullet$ or $\bullet$
- Determine whether at least $5 \%$ of the inputs are $\bullet$


## $5 \%$

- Each agent is initially $\bullet$ or
- Determine whether at least $5 \%$ of the inputs are $\bullet$
- Similar to majority, except each • can cancel 19 •'s.


## 40\%

- Each agent is initially $\bullet$ or $\bullet$
- Determine whether at least $5 \%$ of the inputs are -


## 40\%

- Each agent is initially $\bullet$ or $\bullet$

■ Determine whether at least $5 \%$ of the inputs are •

- A bit trickier (exercice).


## How to Compute $\sum_{i=1}^{k} c_{i} x_{i} \geq a$

Input convention : each agent with ith input symbol starts in state $c_{i}$.
Each agent has a leader bit governed by $\bullet \bullet \bullet \bullet$.
Let $m=\max \left(|a|+1,\left|c_{1}\right|, \ldots,\left|c_{k}\right|\right)$.
Each agent also stores a value from $-m,-m+1, \ldots, m-1, m$.
If a leader meets a non-leader, their values change as follows :

$$
\begin{array}{ll}
x, y \rightarrow x+y, 0 & \text { if } 0 \leq x+y \leq m \\
x, y \rightarrow m, x+y-m & \text { if } x+y>m \\
x, y \rightarrow-m, x+y+m & \text { if } x+y<-m
\end{array}
$$

(In each case first agent on right hand side is the leader.)
Each agent also remembers output of last leader it met.
(c) Eric Ruppert

## Correctness

Sum of agents' values is invariant.

Sum is eventually gathered into the unique leader (up to maximum absolute value of $m$ ) :

If sum $>m$, leader has value $m \Rightarrow$ Output Yes.
If sum $<-m$, leader has value $-\mathrm{m} \Rightarrow$ Output No.
If $-m \leq$ sum $\leq m$, leader's value is the actual sum $\Rightarrow$ Output depends on sum.

In each case, leader knows output and tells everyone else.
(c) Eric Ruppert

## Computable Predicates

Theorem (Angluin et al. 2006)
A predicate is computable iff it is on the following list.

- $\sum_{i=1}^{k} c_{i} x_{i} \geq a$, where $a, c_{i}$ 's are integer constants
- $\sum_{i=1}^{k} c_{i} x_{i} \equiv a(\bmod b)$ where $a, b$ and $c_{i}$ 's are constants
- Boolean combinations of the above predicates


## Alternate Characterization : Presburger Arithmetic

A predicate is computable iff it can be expressed in first-order logic using the symbols $+, 0,1, \vee, \wedge, \neg, \forall, \exists,=,<,($,$) and variables.$
(This system is known as Presburger Arithmetic [1929].)

Note : no multiplication.

```
Examples:
majority: x0 < x1
divisible by 3: \existsy:y+y+y=\mp@subsup{x}{1}{}
at least 40% :x0 + x0<x1+x1+x1
```

(c)Eric Ruppert

## Alternate Characterization : Semilinear Sets

A predicate is computable iff it the set of inputs with output yes is semilinear.

A set of vectors $\vec{x}=\left(x_{1}, x_{2}, \ldots, x_{k}\right) \in \mathbb{N}^{k}$ is linear if it is of the form $\left\{\overrightarrow{v_{0}}+c_{1} \overrightarrow{v_{1}}+c_{2} \overrightarrow{v_{2}}+c_{m} \overrightarrow{v_{m}}: c_{1}, \ldots, c_{m} \in \mathbb{N}\right\}$

A set of vectors is semilinear if it is a finite union of linear sets.
(C)Eric Ruppert

## Variants of the model

The basic classical model is now already understood pretty well.

Variants considered in literature :

- Limited interaction graph
- One-way communication
- Failures

Dana Angluin, James Aspnes, Melody Chan, Carole Delporte-Gallet, Zoë Diamadi, David Eisenstat, Michael J. Fischer, Hugues Fauconnier, Rachid Guerraoui, Hong Jiang, René Peralta, Eric Ruppert

## Population Protocols

Variants

## Population Protocols and Games

## One-way communication

- Classical model assumes an interaction can update the state of both agents simultaneously.
- One-way interactions :
- Information can flow from sender to receiver, but not vice-versa.


## Variants

- Is sender aware that it has sent a message?
- Does the information flow instantaneously?
- Immediate transmission : message delivered instantly
- Immediate observation : receiver sees sender's current state
- Delayed transmission : unpredictable delay in delivery
- Delayed observation : receiver sees an old state of sender
- Can incoming message be queued?


## Overview

Exact characerizations exist :

- Delayed observation : can count up to 2.

■ Immediate observation : can count up to any constant.

- Immediate and delayed transmission : characterization exists
- strictly stronger than observation (can compute mods)
- strictly weaker than two-way (cannot compute majority)
- Queued transmission is equivalent to two-way interactions.
(C)Eric Ruppert


## Plan

## Population Protocols

## Variants

Population Protocols and Games

## Our question

- Can one say that all protocols are games?

■ What is the power of protocols that correspond to games?

## Basic of Game theory

- Two players games : I and II, with a finite set of pure strategies, $\operatorname{Strat}(I)$ and $\operatorname{Strat}(I I)$.
- Denote by $A_{i, j}$ (respectively: $B_{i, j}$ ) the score for player I (resp. II) when I uses strategy $i \in \operatorname{Strat}(I)$ and II uses strategy $j \in \operatorname{Strat}(I I)$.
- The game is termed symmetric if $A$ is the transpose of $B$.
- Famous prisonner's dilemma :


## Opponent

Player

with $T>R>P>S$ and $2 R>T+S$, where $\operatorname{Strat}(I)=\operatorname{Strat}(I I)=\{\bullet, \bullet\}$.

## Best response

- A strategy $x \in \operatorname{Strat}(I)$ is said to be a best response to strategy $y \in \operatorname{Strat}(I I)$, denoted by $x \in B R(y)$ if

$$
\begin{equation*}
A_{z, y} \leq A_{x, y} \tag{1}
\end{equation*}
$$

for all strategies $z \in \operatorname{Strat}(I)$.

- In the prisonner's dilemma,

$$
B R(\bullet)=B R(\bullet)=\bullet,
$$

hend $\bullet$ is the best rational choice, but $\bullet$ would be the better social choice.

- We write $\mathbf{x} \in B R_{\neq \mathbf{x}^{\prime}}(\mathbf{y})$ for

$$
\begin{equation*}
A_{z, y} \leq A_{x, y} \tag{2}
\end{equation*}
$$

for all strategy $\mathbf{z} \in \operatorname{Strat}(I), \mathbf{z} \neq \mathbf{x}^{\prime}$.

## Turing a Game into a Dynamic : Pavlovian's behavior

Assume a symmetric two-player game is given. Let $\Delta$ be some threshold.

- The protocol associated to the game is a population protocol whose set of states is $Q=\operatorname{Strat}(I)=\operatorname{Strat}(I I)$ and whose transition rules $\delta$ are given as follows:

$$
q_{1}, q_{2} \rightarrow q_{1}^{\prime}, q_{2}^{\prime}
$$

where

- $q_{1}^{\prime}=q_{1}$ when $A_{q_{1}, q_{2}} \geq \Delta$
- $q_{1}^{\prime} \in B R_{\neq q_{1}}\left(q_{2}\right)$ when $A_{q_{1}, q_{2}}<\Delta$
and symmetrically.
- A population protocol is Pavlovian if it can be obtained from a game as above.


## Example: The Prisonner's Dilemma

$T>R>\Delta>P>S$

- Several studies of this dynamic over various graphs: see e.g. [Dyer et al. 02], [Fribourg et al. 04].
- Somehow, our question is: can any dynamic be termed "a game", or "pavlovian".


## First observation : Pavlovian $=>$ Symmetric

- We say that a population protocol is symmetric if, whenever $q_{1}, q_{2} \rightarrow q_{1}^{\prime}, q_{2}^{\prime}$ in the program, one has also $q_{2}, q_{1} \rightarrow q_{2}^{\prime}, q_{1}^{\prime}$.
- Pavlovian implies symmetric.

Theorem
Any symmetric deterministic 2-states population protocol is Pavlovian.

## Symmetric $\neq$ Pavlovian

- Write any rule of the protocol

$$
q_{1} q_{2} \rightarrow \delta_{1}\left(q_{1}, q_{2}\right) \delta_{1}\left(q_{2}, q_{1}\right)
$$

- Consider a 3-states population protocol with set of states $Q=\{\bullet, \bullet, \bullet\}$ and a joint transition function $\delta$ such that $\delta_{1}(\bullet, \bullet)=\bullet, \delta_{1}(\bullet, \bullet)=\bullet, \delta_{1}(\bullet, \bullet)=\bullet$.
- One can not find a matrix of a game that would lead to this dynamic.
- Corollary : Not all protocols are Pavlovian.


## Basic Pavlovian Protocols

- OR is computed by 2-state protocol :

- AND is computed by 2-state protocol :


■ Remark: XOR is not computed by 2-state protocol :


## Electing a Leader

- Classical solution : $\bullet \rightarrow \bullet$ is not symmetric.
- Proposition: The following Pavlovian protocol solves the leader election problem, as soon as the population is of size $\geq 3$.

- Indeed, ultimately there will be exactly one leader, that is one agent in state - or

- Taking $\Delta=4$, this corresponds to matrix



## Majority

- The majority problem (given some population of $\bullet$ and $\bullet$, determine whether there are more $\bullet$ than $\bullet$ ) can be solved by a Pavlovian population protocol.
- Proof :


This corresponds to the following matrix.


## Dicussions and conclusions

- We are still far from understanding the power of Pavlovian population protocols.
- Simple protocols become rather complicated (and hard to explain).
- We don't even know how to compute mod 2.

■ We don't even know how to compute $\geq k$, for a fixed $k$.

- Nor have a proof that this is not possible.


## Some Side Effects of this Study

■ Conclusion 1 : Not all distributed algorithms are games!!!

- A contribution? :


## Proposition

Any population protocol can be simulated by a symmetric population protocol, as soon as the population is of size $\geq 3$.

Corollary
A predicate is computable by a symmetric population protocol if and only if it is semilinear.

