# **Playing With Population Protocols**

Olivier Bournez<sup>1</sup> Jérémie Chalopin<sup>2,5</sup> Johanne Cohen<sup>3,5</sup> Xavier Koegler<sup>4</sup>

<sup>1</sup>Ecole Polytechnique, France

<sup>2</sup>University of Marseille, France

<sup>3</sup>University of Versailles, France

<sup>4</sup>Paris VII University, France

<sup>5</sup>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 : Final result

















































































































































































































































































































































































































































































































































# 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 is strictly greater than the initial population of •.

#### Alternative statement

• A configuration can be seen as an element of  $\mathbb{N}^4$ .

- ►  $(n_b, n_r, n_g, n_{bl})$  if there is  $n_b \bullet$ ,  $n_r \bullet$ ,  $n_g \bullet$  and  $n_{bl} \bullet$
- $n_b + n_r + n_g + n_{bl}$  is preserved.
- An initial configuration is of type  $(n_b, n_r, 0, 0)$ .
- This protocol computes predicates  $n_r > n_b$ , i.e. MAJORITY

# General Case : Algorithm

An algorithm consists of

- a finite set of states  $Q = \{q_1, q_2, \cdots, q_k\}$ .
- transition rules, mapping pairs of states to pairs of states

Executions are given by :

- instantaneous configuration : a multiset of states = an element of N<sup>k</sup>.
- 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 :  $\bullet \bullet \rightarrow \bullet \bullet$ 

Output of an agent is its state.

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

# 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  $C \rightarrow C'$  for some configuration *C'*, then *C'* 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 •

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 •.



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



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

### 40%

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

# **40%**

- Each agent is initially or •
- Determine whether at least 5% of the inputs are •
- A bit trickier (exercice).

# How to Compute $\sum_{i=1}^{k} c_i x_i \ge a$

Input convention : each agent with ith input symbol starts in state  $c_i$ .

Each agent has a **leader bit** governed by  $\bullet \to \bullet \bullet$ . Let  $m = \max(|a| + 1, |c_1|, ..., |c_k|)$ . Each agent also stores a value from -m, -m + 1, ..., 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. ©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  $-m \Rightarrow Output$  No. If  $-m \le sum \le m$ , leader's value is the actual sum  $\Rightarrow Output$  depends on sum.

In each case, leader knows output and tells everyone else. ©Eric Ruppert

# **Computable Predicates**

#### Theorem (Angluin et al. 2006)

A predicate is computable iff it is on the following list.

$$\sum_{i=1}^{k} c_i x_i \ge a, \text{ where } a, c_i \text{ 's are integer constants'}$$

- $\sum_{i=1}^{k} c_i x_i \equiv a \pmod{b}$  where  $a_i$ ,  $b_i$  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  $+, 0, 1, \lor, \land, \neg, \forall, \exists, =, <, (, )$  and variables.

(This system is known as Presburger Arithmetic [1929].)

Note : no multiplication.

**Examples :** majority :  $x_0 < x_1$ divisible by 3 :  $\exists y : y + y + y = x_1$ at least 40% : $x_0 + x_0 < x_1 + x_1 + x_1$ 

©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  $\vec{x} = (x_1, x_2, ..., x_k) \in \mathbb{N}^k$  is **linear** if it is of the form  $\{\vec{v_0} + c_1\vec{v_1} + c_2\vec{v_2} + c_m\vec{v_m} : c_1, ..., c_m \in \mathbb{N}\}$ 

A set of vectors is **semilinear** if it is a finite union of linear sets. ©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

#### Plan

**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, Strat(I) and Strat(II).
- Denote by  $A_{i,j}$  (respectively :  $B_{i,j}$ ) the score for player I (resp. II) when I uses strategy  $i \in Strat(I)$  and II uses strategy  $j \in Strat(II)$ .
- The game is termed *symmetric* if A is the transpose of B.

Famous prisonner's dilemma :



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

#### Best response

A strategy x ∈ Strat(I) is said to be a best response to strategy y ∈ Strat(II), denoted by x ∈ BR(y) if

$$A_{z,y} \le A_{x,y} \tag{1}$$

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

In the prisonner's dilemma,

$$BR(ullet)=BR(ullet)=ullet,$$

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

• We write  $\mathbf{x} \in BR_{\neq \mathbf{x}'}(\mathbf{y})$  for

$$A_{z,y} \le A_{x,y} \tag{2}$$

for all strategy  $z \in Strat(I), z \neq x'$ .

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

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

The protocol associated to the game is a population protocol whose set of states is Q = Strat(I) = Strat(II) and whose transition rules δ are given as follows :

$$q_1,q_2 
ightarrow q_1',q_2'$$

where

- $q'_1 = q_1$  when  $A_{q_1,q_2} \ge \Delta$ •  $q'_1 \in BR_{\neq q_1}(q_2)$  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  $q_1, q_2 \rightarrow q'_1, q'_2$  in the program, one has also  $q_2, q_1 \rightarrow q'_2, q'_1$ .

Pavlovian implies symmetric.

#### Theorem

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

### Symmetric $\neq$ Pavlovian

Write any rule of the protocol

$$q_1q_2 \rightarrow \delta_1(q_1,q_2)\delta_1(q_2,q_1)$$

- Consider a 3-states population protocol with set of states  $Q = \{\bullet, \bullet, \bullet\}$  and a joint transition function  $\delta$  such that  $\delta_1(\bullet, \bullet) = \bullet$ ,  $\delta_1(\bullet, \bullet) = \bullet$ .
- 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 :  $\bullet \bullet \rightarrow \bullet \bullet$  is not symmetric.
- Proposition : The following Pavlovian protocol solves the leader election problem, as soon as the population is of size ≥ 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 

   and 
   determine whether there are more 
   than 
   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.