On the Convergence of a Population Protocol When Population Goes to Infinity

Olivier Bournez[1] and Philippe Chassaing[2] and Johanne Cohen[1] and Lucas Gerin[2] and Xavier Koegler[3]

[1] LORIA/INRIA-CNRS, 615 Rue du Jardin Botanique, 54602 Villers-Lès-Nancy, FRANCE
{Olivier.Bournez,Johanne.Cohen}@loria.fr
[2] IECN/UHP, BP 239, 54506 Vandoeuvre-Lès-Nancy Cedex, FRANCE
{chassain,Lucas.Gerin}@iecn.u-nancy.fr
[3] Ecole Normale Supérieure, 45, rue d'Ulm 75230 Paris cedex 05, FRANCE
koegler@clipper.ens.fr

Abstract. Population protocols have been introduced as a model of sensor networks consisting of very limited mobile agents with no control over their own movement. A population protocol corresponds to a collection of anonymous agents, modeled by finite automata, that interact with one another to carry out computations, by updating their states, using some rules.

Their computational power has been investigated under several hypotheses but always when restricted to finite size populations. In particular, predicates stably computable in the original model have been characterized as those definable in Presburger arithmetic.

We study mathematically the convergence of several population protocols when the size of the population goes to infinity. We do so by giving general results, that we illustrate through the example of a particular population protocol for which we obtain a full asymptotic development. This example shows in particular that these protocols seem to have a rather different computational power when a huge population hypothesis is considered.

1 Motivation

The computational power of networks of finitely many anonymous resource-limited mobile agents has been investigated in several recent papers. In particular, the population protocol model, introduced in [1], consists of a population of finite-state agents that interact in pairs, where each interaction updates the state of both participants according to a transition based on the previous states of the participants. When all agents converge after some finite time to a common value, this value represents the result of the computation.

Several variants of the original model have been considered but with common features. See for example this ollowing survey [3] for some variant models: anonymous finite-state agents (the system consists of a large population of indistinguishable finite-state agents), computation by direct interaction (an interaction between two agents updates their states according to a joint transition table), unpredictable interaction patterns (the choice of interactions is made by an adversary, possibly limited to pairing only agents in an interaction graph), distributed input and outputs (the input to a population protocol is distributed across the initial state of the entire population, similarly the output is distributed to all agents), convergence rather than termination (the agent's output are required to converge after some time to a common correct value).

Typically, in the spirit of [1] and following papers (see again [3] for a survey), population protocols are assumed to (stably) compute predicates: a population protocols stably computes a predicate ϕ, if for any possible input x of ϕ, whenever $\phi(x)$ is true all agents of the population eventually stabilize to a state corresponding to 1, and whenever $\phi(x)$ is false, all agents of the population eventually stabilize to a state corresponding to 0.

Predicates stably computable by population protocols in this sense have been characterized as being precisely the semi-linear predicates, that is to say those predicates on counts of input agents definable in first-order Presburger arithmetic [9]. Semilinearity was shown to be sufficient in [1] and necessary in [2].

Here, we study a new variant: we assume a population close to infinity (we call this *a huge population hypothesis*), and we don't want to focus on protocols as predicate recognizers, but as computing functions. We assume outputs to correspond to proportions, which are clearly the analog of counts whenever the population is infinite or close to infinity.

We do so by providing general results that we illustrate by considering a particular population protocol, that we prove to converge to a fraction of $\frac{\sqrt{2}}{2}$ agents in a given state whatever its initial state is. We hence show that some algebraic irrational values can be computed in this sense. Then we show how the reasoning behind the proof of convergence of this particular protocol can be generalized to any such protocol to prove that it's behaviour can be analyzed through use of deterministic differential equations. We also give an asymptotic development of the convergence in the case of the protocol computing $\frac{\sqrt{2}}{2}$.

Our motivation is twofold. First, to prove formally that population protocol with a huge population hypothis can be mathematically studied using population models and ordinary differential equations. Second, to show that protocols considered with these two hypotheses (huge population, computing functions and not only predicates), have a rather different power.

We consider this work as a first step towards understanding which numbers can be computed by such protocols. Whereas we prove that $\frac{\sqrt{2}}{2}$ can be computed, and whereas this is easy to see that computable numbers in this sense must be algebraic numbers of $[0, 1]$, we didn't succeed yet to characterize precisely computable numbers.

In this more long term objective, the aim of this current work is first to discuss in which sense one can say that these protocols compute an irrational algebraic value such as $\frac{\sqrt{2}}{2}$, and second to study mathematically formally the convergence.

Our discussion is organized as follows. In Section 2, we present classical finite-size population protocols and related work. In Section 3, we recall our model of population protocols. In Section 4, we present a particular population protocol and we explain in which sense we would like to say that this protocol computes some irrational algebraic value, with a huge population hypothesis. We do so first by some informal study, that we justify mathematically in the rest of the paper. We first do some mathematical computations in Section 5, in order to use a general theorem presented in Section 6 from [10] about approximation of diffusions. This theorem yields the proof of convergence in Section 7. Then in Section 8 we show how the method used on this particular example can be used to prove that the study of such protocols can be reduced to the study of differential systems. The following two sections deal with additional results that can be given on restricted parts of the model. We prove in Section 9 that this is even possible to use the same theorem to go further and get an asymptotic development of the convergence on the example of $\frac{\sqrt{2}}{2}$. Section 10 gives, without proof, some first results on the type of algebraic numbers that can be computed in this model using only two possible states for all agents. Finally, Section 11 is devoted to a conclusion and a discussion.

2 Related Work

Population protocols have been introduced in [1]. In [1], the authors proved that all semi-linear predicates can be computed but left open the question of their exact power. This was solved in [2], where it has been proved that no-more predicates can be computed.

The population protocol model was inspired in part by the work by Diamadi and Fischer on trust propagation in social networks [5]. The model proposed in [1] was motivated by the study of sensor networks in which passive agents were carried along by other entities. The canonical example given in this latter paper was sensors attached to a flock of birds.

Most of the works so far on population protocols have concentrated on characterizing what predicates on the input configurations can be stably computed in different variants of the models and under various assumptions, such as bounded-degree interaction graphs and random scheduling [3].

Variants considered includes restriction to one-way communications, restriction to particular interaction graphs, random interactions, self-stabilizing solutions through population protocols to classical problems in distributed algorithmic, the taking into account of various kind of failures of agents, etc. See survey [3]. As far as we know, a huge population hypothesis in the sense of this paper, has not been considered yet.

Notice that we assume that interactions happen in probabilistic way, according to some uniform law. In the original population protocol model, only specific fairness hypotheses were assumed on possible adversaries [1]. When the size of the population goes to infinity, uniform sampling of agents seems to us the most natural way to extend the fairness hypothesis. This assumption is consistent with the interpretation of agents as autonomous biological entities moving at random. Notice that this notion of adversary has already been investigated for finite state systems [3].

The result proved in this paper can be considered as a macroscopic abstraction of a system given by microscopic rules of evolutions. See survey [7] for general discussions about extraction of macroscopic dynamics.

Whereas the ordinary differential equation (8) can be immediately abstracted in a physicist approach from the dynamic (1), the formal mathematical equivalence of the two approaches is not so trivial, and is somehow a strong motivation of this work.

Actually, these problems seem to arise in many macroscopic justifications of models from their microscopic description in experimental science: See for example the very instructive discussion in [8] about assumptions required for the justification of the Lotka-Volterra (predator-prey) model of population dynamics. In particular, observe that the fact that microscopic correlations must be neglected (i.e. $E[XY] = E[X]E[Y]$ is needed, where E is expectation). With a rather similar hypothesis (here assuming $E[p^2] = E[p]^2$), dynamic (8) is clear from rules (1). Somehow, we prove here that this hypothesis is not necessary for our system.

The techniques used in this paper are based on weak convergence techniques, introduced in [10], relating a stochastic differential equation (whose solutions are called diffusions) to approximations by a family of Markov processes. Refer also to [6] for an introduction to these techniques. The theorem used here is actually based on the presentation of [4] of a theorem from [10].

Moreover in [**?**], somes probabilistic population protocols, are studied using the differential equations approach. In this case, the population is finite and using the Markov Chain stationary distribution argument, the protocol population are always stable in terms of their eventual subpopulation percentages.

3 Population Protocols

We now recall definitions from [1]. A protocol is given by $(Q, \Sigma, \iota, \omega, \delta)$ with the following components. Q is a finite set of *states*. Σ is a finite set of *input symbols*. $\iota : \Sigma \to Q$ is the initial state mapping, and $\omega : Q \to \{0, 1\}$ is the individual output function. $\delta \subseteq Q^4$ is a joint transition relation that describes how pairs of agents can interact. Relation δ is sometimes described by listing all possible interactions using the notation $(q_1, q_2) \to (q'_1, q'_2)$, or even the notation $q_1 q_2 \to q'_1 q'_2$, for $(q_1, q_2, q'_1, q'_2) \in \delta$ (with the convention that $(q_1, q_2) \to (q_1, q_2)$ when no rule is specified with (q_1, q_2) in the left hand side).

Computations of a protocol proceed in the following way. The computation takes place among n *agents*, where $n \geq 2$. A *configuration* of the system can be described by a vector of all the agent's states. The state of each agent is an element of Q. Because agents with the same states are indistinguishable, each configuration can be summarized as an unordered multiset of states, and hence of elements of Q.

Each agent is given initially some input value from Σ: Each agent's initial state is determined by applying ι to its input value. This determines the initial configuration of the population.

An execution of a protocol proceeds from the initial configuration by interactions between pairs of agents. Suppose that two agents in state q_1 and q_2 meet and have an interaction. They can change into state q_1' and q_2' if (q_1, q_2, q_1', q_2') is in the transition relation δ. If C and C' are two configurations, we write $C \to C'$ if C' can be obtained from C by a single interaction of two agents: this means that C contains two states q_1 and q_2 and C' is obtained by replacing q_1 and q_2 by q_1' and q_2' in C, where $(q_1, q_2, q_1', q_2') \in \delta$. An *execution* of the protocol is an infinite sequence of configurations $C_0, C_1, C_2, \cdots$, where C_0 is an initial configuration and $C_i \to C_{i+1}$ for all $i \geq 0$. An execution is *fair* if for all configurations C that appears infinitely often in the execution, if $C \to C'$ for some configuration C', then C' appears infinitely often in the execution.

At any point during an execution, each agent's state determines its output at that time. If the agent is in state q, its output value is $\omega(q)$. The configuration output is 0 (respectively 1) if all the individual outputs are 0 (respectively 1). If the individual outputs are mixed 0s and 1s then the output of the configuration is undefined.

Let p be a predicate over multisets of elements of Σ. Predicate p can be considered as a function whose range is $\{0, 1\}$ and whose domain is the collection of these multisets. The predicate is said to be computed by the protocol if, for every multiset I, and every fair execution that starts from the initial configuration corresponding to I, the output value of every agent eventually stabilizes to $p(I)$.

The following was proved in [1, 2]

Theorem 1 ([1, 2]). *A predicate is computable in the population protocol model if and only if it is semilinear.*

Recall that semilinear sets are known to correspond to predicates on counts of input agents definable in first-order Presburger arithmetic [9].

4 A Simple Example

Consider the following population protocol, with $Q = \{+, -\}$, and the following joint transition relation.

$$\begin{cases} ++ \to +- \\ +- \to ++ \\ -+ \to ++ \\ -- \to +- \end{cases} \tag{1}$$

Using previous (classical) definition, this protocol does not stably compute anything. Indeed, if we put aside the special configuration where all agents are in state $-$ which is immediately left in any next round, any configuration is reachable from any configuration.

However, suppose that we want to discuss the limit of the proportion $p(k)$ of agents in state $+$ in the population at discrete time k. If $n_+(k)$ denotes the number of agents in state $+$, and $n_-(k) = n - n_+(k)$ the number of agents in state $-$,

$$p(k) = \frac{n_+(k)}{n}.$$

From now on, we suppose that at each time step, two different agents are sampled uniformly among the n particles, independently from the past. Since we are dealing with n indistinguishable agents, the population protocol is completely described by the number of agents in state $+$. We are then reduced to determine the evolution of the Markov chain

$$(p(k))_{k\in\mathbb{N}} \in \left\{ \frac{0}{n}, \frac{1}{n}, \dots, \frac{n}{n} \right\}.$$

The above discussion ensures that $(p(k))$ is an irreducible Markov chain in $\{\frac{1}{n}, \dots, \frac{n}{n}\}$. Let us now compute the transition probabilities of this irreducible Markov chain. We have

$$p(k+1) - p(k) \in \{-1, 1\}.$$

The, we have to determine for each $i = 1, 2, \dots, n$

$$\pi^{(n)}(\tfrac{i}{n} \to \tfrac{i-1}{n}) := \mathbb{P}\left(p(k+1) = \frac{i-1}{n} \mid p(k) = \frac{i}{n} \right),$$
$$\pi^{(n)}(\tfrac{i}{n} \to \tfrac{i+1}{n}) := \mathbb{P}\left(p(k+1) = \frac{i+1}{n} \mid p(k) = \frac{i}{n} \right).$$

Assume that $p(k) = i/n$, the only possibility for $p(k)$ to decrease is to fire 2 of the i agents in state $+$. That is,

$$\pi^{(n)}(\tfrac{i}{n} \to \tfrac{i-1}{n}) = \frac{\binom{i}{2}}{\binom{n}{2}} = \frac{i(i-1)}{n(n-1)}.$$

In any other case, $p(k)$ increases by one :

$$\begin{aligned}\pi^{(n)}(\tfrac{i}{n} \to \tfrac{i+1}{n}) &= 1 - \pi^{(n)}(\tfrac{i}{n} \to \tfrac{i-1}{n}) \\ &= 1 - \frac{i(i-1)}{n(n-1)}.\end{aligned}$$

A consequence of the ergodic theorem is that the chain $(p(k))$ admits an unique stationary distribution μ. By definition, it is the only application

$$\mu : \left\{ \frac{1}{n}, \dots, \frac{n}{n} \right\} \to [0, 1]$$

such that

1. $\sum_{i=1}^{n} \mu(i/n) = 1$.
2. μ satisfies the *balance equation*, *i.e.* for each i

$$\mu(\frac{i}{n}) = \mu(\frac{i-1}{n})\pi^{(n)}(\tfrac{i-1}{n} \to \tfrac{i}{n}) + \mu(\frac{i+1}{n})\pi^{(n)}(\tfrac{i+1}{n} \to \tfrac{i}{n})$$

We do not pay attention to the exact expression of μ. We only notice that, as the unique solution to a rational system, it is an element of $\mathbb{Q}^n$. Hence, its mean $\sum_i \mu(i/n)i/n$ is a rational number, that we denote $p^{(n)}$. The second consequence of the ergodic theorem is the following convergence :

$$\frac{p(1) + p(2) + ... + p(k)}{k} \overset{k\to\infty}{\to} p^{(n)}, \text{ almost surely.}$$

The purpose of the rest of the discussion is to show that however, when n goes to infinity, the mean value of $p(k)$ converges to the irrational number $\sqrt{2}/2$. To see why this is true, we write

$$\begin{aligned}
\mathbb{E}[n_+(k+1) - n_+(k) \mid n_+(k)] &= (n_+(k)+1)\,\pi^{(n)}\left(p(k) \to p(k) + \tfrac{1}{n}\right) \\
&\quad + (n_+(k)-1)\,\pi^{(n)}\left(p(k) \to p(k) - \tfrac{1}{n}\right) \\
&\quad - n_+(k) \\
\mathbb{E}[n_+(k+1) - n_+(k) \mid n_+(k)] &= (n_+(k)+1)\left(1 - \tfrac{n_+(k)}{n}\tfrac{n_+(k)-1}{n-1}\right) \\
&\quad + (n_+(k)-1)\,\tfrac{n_+(k)}{n}\tfrac{n_+(k)-1}{n-1} - n_+(k) \\
&= 1 - 2\tfrac{n_+(k)}{n}\tfrac{n_+(k)-1}{n-1} \\
&= 1 - 2p(k)\left(p(k)\tfrac{n-1}{n} + \tfrac{1}{n-1}\right).
\end{aligned}$$

From this, we can derive (not yet rigourously) the asymptotic behavior of $p(k)$. Take indeed n large, so that the right-hand term is close to $1 - 2p(k)^2$. Now, when k goes large, the system concentrates on configurations that does not create or destroy $+$, in mean. Thus, the left-hand side should vanish, and $p(k) \approx \sqrt{2}/2$.

The remaining problem is hence to justify and discuss mathematically the convergence.

5 Computing Expectation and Variance of Increments

We now justify mathematically this convergence.

We will first compute

$$\begin{aligned}
E[\Delta_n^2 | n_+(k)] &= 1 \times \pi_{+1} + 1 \times \pi_{-1} \\
&= 1.
\end{aligned} \tag{2}$$

It follows, from Equations (**??**) and (2), that we have

$$E[p(k+1) - p(k) | p(k)] = \frac{1}{n}(1 - 2p(k)^2 \frac{n}{n-1} + p(k)\frac{2}{n-1}), \tag{3}$$

which yields the equivalent

$$nE[p(k+1)-p(k)|p(k)] \approx 1-2p(k)^2 \tag{4}$$

when n goes to infinity, and

$$E[(p(k+1)-p(k))^2|p(k)] = \frac{1}{n^2}, \tag{5}$$

which yields the equivalent

$$nE[(p(k+1)-p(k))^2|p(k)] \approx \frac{1}{n}, \tag{6}$$

when n goes to infinity.

6 A General Theorem about Approximation of Diffusions

We will use the following theorem from [10]. We use here the formulation of it in [4] (Theorem 5.8 page 96).

Suppose that for all integers $n \geq 1$, we have an homogeneous Markov chain $(Y_k^{(n)})$ in $\mathbb{R}^d$ of transition $\pi^{(n)}(x,dy)$, that is to say so that the law of $Y_{k+1}^{(n)}$ conditioned by $Y_0^{(n)}, \cdots, Y_k^{(n)}$ depends only on $Y_k^{(n)}$ and is given, for all Borelian B, by

$$P(Y_{k+1}^{(n)} \in B | Y_k^{(n)}) = \pi^{(n)}(Y_k^{(n)}, B).$$

almost surely.

Define for $x \in \mathbb{R}^d$,

$$\begin{aligned} b^{(n)}(x) &= n\int (y-x)\pi^{(n)}(x,dy), \\ a^{(n)}(x) &= n\int (y-x)(y-x)^*\pi^{(n)}(x,dy), \\ K^{(n)}(x) &= n\int (y-x)^3\pi^{(n)}(x,dy), \\ \Delta_\epsilon^{(n)}(x) &= n\pi^{(n)}(x, B(x,\epsilon)^c), \end{aligned}$$

where $B(x,\epsilon)^c$ is the complement of the ball centered in x of radius ϵ.

In other words,

$$b^{(n)}(x) = n\mathbb{E}_x[(Y_1 - x)],$$

and

$$a^{(n)}(x) = n\mathbb{E}_x[(Y_1 - x)(Y_1 - x)*]$$

where $\mathbb{E}_x$ stands for "expectation starting from x", that is,

$$\mathbb{E}_x[(Y_1 - x)] = \mathbb{E}[(Y_1 - x)|Y_0 = x].$$

Define

$$X^{(n)}(t) = Y_{\lfloor nt \rfloor}^{(n)} + (nt - \lfloor nt \rfloor)(Y_{\lfloor nt+1 \rfloor}^{(n)} - Y_{\lfloor nt \rfloor}^{(n)}).$$

The coefficients $b^{(n)}$ and $a^{(n)}$ can be interpreted as the instantaneous drift and variance (or matrix of covariance) of $X^{(n)}$.

Theorem 2 (Theorem 5.8, page 96 of [4]). *Suppose that there exist some continuous functions a, b, such that for all $R < +\infty$,*

$$\lim_{n\to\infty} sup_{|x|\leq R}|a^{(n)}(x) - a(x)| = 0$$
$$\lim_{n\to\infty} sup_{|x|\leq R}|b^{(n)}(x) - b(x)| = 0$$
$$\lim_{n\to\infty} sup_{|x|\leq R}\Delta_\epsilon^{(n)} = 0, \forall\epsilon > 0$$
$$\sup_{|x|\leq R} K^{(n)}(x) < \infty.$$

With σ a matrix such that $\sigma(x)\sigma^*(x) = a(x)$, $x \in \mathbb{R}^d$, we suppose that the stochastic differential equation

$$dX(t) = b(X(t))dt + \sigma(X(t))dB(t), \qquad X(0) = x, \tag{7}$$

has an unique weak solution for all x. This is in particular the case, if it admits an unique strong solution.

Then for all sequences of initial conditions $Y_0^{(n)} \to x$, the sequence of random processes $X^{(n)}$ converges in law to the diffusion given by (7).

In other words, for all function $F : \mathcal{C}(\mathbb{R}^+, \mathbb{R}) \to \mathbb{R}$ bounded and continuous, one has

$$\lim_{n\to\infty} E[F(X^{(n)})] = E[F(X)].$$

7 Proving Convergence

Consider $Y_i^{(n)}$ as the homogeneous Markov chain corresponding to $p(k)$, when n is fixed. From previous discussions, $\pi^{(n)}(x, .)$ is a weighted sum of two Dirac that weight $x - \frac{1}{n}$ and $x + \frac{1}{n}$, with respective probabilities π_{-1} and π_{+1}, whenever x is of type $\frac{i}{n}$ for some i.

Set $a(x) = 1 - 2x^2$, and $b(x) = 0$. From equivalent Equations (4) and (6), we have clearly

$$\lim_{n\to\infty} sup_{|x|\leq R}|a^{(n)}(x) - a(x)| = 0$$
$$\lim_{n\to\infty} sup_{|x|\leq R}|b^{(n)}(x) - b(x)| = 0$$

for all $R < +\infty$.

Since the jumps of $Y^{(n)}$ are bounded in absolute value by $\frac{1}{n}$, $\Delta_\epsilon^{(n)}$ is null, as soon as $\frac{1}{n}$ is smaller than ϵ, and so

$$\lim_{n\to\infty} sup_{|x|\leq R}\Delta_\epsilon^{(n)} = 0, \forall\epsilon > 0$$

$$\sup_{|x|\leq R} K^{(n)}(x) < \infty$$

is easy to establish.

Now, (ordinary and deterministic) differential equation

$$dX(t) = (1 - 2X^2)dt \tag{8}$$

has an unique solution for any initial condition.

It follows from above theorem that the sequence of random processes $X^{(n)}$ defined by

$$X^{(n)}(t) = Y^{(n)}_{\lfloor nt \rfloor} + (nt - \lfloor nt \rfloor)(Y^{(n)}_{\lfloor nt+1 \rfloor} - Y^{(n)}_{\lfloor nt \rfloor})$$

converges in law to the unique solution of differential equation (8).

Clearly, all solutions of ordinary differential equation (8) converge to $\frac{\sqrt{2}}{2}$. Doing the change of variable $Z(t) = X(t) - \frac{\sqrt{2}}{2}$, we get

$$dZ(t) = (-2Z^2 + 2\sqrt{2}Z)dt, \tag{9}$$

that converges to 0.

Coming back to $p(k)$ using definition of $X^{(n)}(t)$, we hence get

Theorem 3. *We have for all t,*

$$p(\lfloor nt \rfloor) = \frac{\sqrt{2}}{2} + Z_n(t),$$

where $Z_n(t)$ converges in law when n goes to infinity to the (deterministic) solution of ordinary differential (9)*. Solutions of this ordinary differential equation go to* 0 *at infinity.*

This implies that $p(k)$ must converge to $\frac{\sqrt{2}}{2}$ when k and n go to infinity.

8 Generalization To General Population Protocols

We will now generalize the reasonning made on this particular example in order to prove that the behaviour of any such protocol can be approximated by a deterministic differential equation in a similar way.

To generalize our model, we shall consider the set of states possible for any one agent to be an arbitrary finite set Q and transition rules of the dynamic to be of the form :

$$q\ q' \to \delta_1(q, q')\ \delta_2(q, q')$$

for all $(q_1, q_2) \in Q^2$.

As previously, we consider pairwise interactions between two agents chosen randomly according to an uniform law in a population of size n.

Let us define the Markov chain $Y^{(n)}_i$ corresponding to the vector of $\mathbb{R}^Q$ whose components are the proportions of agents in the different states and

$$X^{(n)}(t) = Y^{(n)}_{\lfloor nt \rfloor} + (nt - \lfloor nt \rfloor)(Y^{(n)}_{\lfloor nt+1 \rfloor} - Y^{(n)}_{\lfloor nt \rfloor}).$$

Theorem 4. *Le b be the function defined by :*

$$b(x) = \sum_{(q,q')\in Q} x_q x_{q'} (-(e_q + e'_q) + e_{\delta_1(q,q')} + e_{\delta_2(q,q')})$$

where $(e_q)_{q\in Q}$ *is the canonical base of* $\mathbb{R}^Q$.

Then for all sequences of initial conditions $Y_0^{(n)} \to x$*, the sequence of random processes* $X^{(n)}$ *converges in law to the solution of the stochastic differential equation (with degenerated brownian motion) :*

$$dX(t) = b(X(t))dt, \qquad X(0) = x, \tag{10}$$

Remark 1. The stochastic differential Equation (10) being deterministic, we are sure that it has an unique weak solution for all x.

Proof. Y_i^n is of the form required by Theorem 2 with $pi^{(n)}(x, .)$ being the sum of $5^{|Q|}$ Dirac : the variation of the proportion of agents in any one given state is in $\{\frac{-2}{n}, \frac{-1}{n}, 0, \frac{1}{n}, \frac{2}{n},\}$ and the probabilities of any of these variations are clearly only dependant on the current state x.

Now let us define $a^{(n)}(x), b^{(n)}(x), K^{(n)}(x)$ and $\Delta_\epsilon^{(n)}$ as in Theorem 2. Let R be any finite non-negative real number.

As in the example above, since at any given time step at most two out of n agents change state, $\Delta_\epsilon^n = 0$ if $\epsilon > \frac{4}{n}$ and thus

$$\lim_{n\to\infty} sup_{|x|\le R} \Delta_\epsilon^{(n)} = 0, \forall \epsilon > 0.$$

$$\sup_{|x|\le R} K^{(n)}(x) < \infty$$

is also easy to establish.

Similarly

$$\forall x \in \mathbb{R}^{|Q|}, |x| \le R, |a^{(n)}(x)| \le \frac{4|Q|}{n}.$$

So if we take $a(x) = 0$, we have

$$\lim_{n\to\infty} sup_{|x|\le R} |a^{(n)}(x) - a(x)| = 0.$$

If we write, for all $(q, q') \in Q^2, q \neq q'$,

$$\Pi_{q,q'}^{(n)}(x) = x_q x_{q'} \frac{n}{n-1}$$

and

$$\Pi_{q,q}^{(n)}(x) = x_q x_q \frac{n}{n-1} - \frac{x_q}{n-1}.$$

Then $\Pi_{q,q'}^{(n)}(x)$ is exactly the probability of an encounter between an agent in state q and an agent in state q' to happen when the population is in configuration x. We then have :

$$b^{(n)}(x) = \sum_{(q,q')\in Q} \Pi^{(n)}_{q,q'}(x)(-(e_q + e'_q) + e_{\delta_1(q,q')} + e_{\delta_2(q,q')}),$$

or

$$b^{(n)}(x) = \frac{n}{n-1} b(x) - \frac{1}{n-1} \sum_{q\in Q} x_q(-2e_q + e_{\delta_1(q,q)} + e_{\delta_2(q,q)}).$$

Thus, finally,

$$\lim_{n\to\infty} sup_{|x|\leq R} |b^{(n)}(x) - b(x)| = 0.$$

We can now conclude by Theorem 2.

This means that to understand the asymptotical behaviour of any such protocol, we can study the associated differential equation. It is also of interest to note that the function b defined here is a quadratic form over $\mathbb{R}^Q$.

9 An Asymptotic Development of the Example Dynamic

It is actually possible to go further, at least in some cases like the example used here and prove the equivalent of a central limit theorem, or if one prefers, to do an asymptotic development of the convergence, in terms of stochastic processes. We shall do so for the example dynamic used before using the same notations as in previous sections.

In our prevous example, as $p(k)$ is expected to converge to $\frac{\sqrt{2}}{2}$, consider the following change of variable:

$$Y^{(n)}(k) = \sqrt{n}(p(k) - \frac{\sqrt{2}}{2}).$$

The subtraction of $\frac{\sqrt{2}}{2}$ is here to get something centered, and the $\sqrt{n}$ factor is here in analogy with classical central limit theorem.

Clearly, $Y^{(n)}(.)$, that we will also note $Y(.)$ in what follows when n is fixed, is still an homogeneous Markov Chain.

We have

$$E[Y(k+1) - Y(k)|Y(k)] = \sqrt{n}(E[p(k+1) - p(k)|p(k)]),$$

hence, from (3),

$$E[Y(k+1) - Y(k)|Y(k)] = \frac{1}{\sqrt{n}}(1 - 2p(k)^2 \frac{n}{n-1} + p(k)\frac{2}{n-1}).$$

Using $p(k) = \frac{\sqrt{2}}{2} + \frac{Y(k)}{\sqrt{n}}$, we get

$$\begin{aligned} E[Y(k+1) - Y(k)|Y(k)] = & \tfrac{\sqrt{2}-1}{\sqrt{n}(n-1)} + Y(k)(-\tfrac{2\sqrt{2}}{n-1} \\ & + \tfrac{2}{n(n-1)}) + Y(k)^2(-\tfrac{2}{\sqrt{n}(n-1)}) \end{aligned}$$

which yields the equivalent

$$nE[Y(k+1) - Y(k)|Y(k)] \approx -2\sqrt{2}Y(k)$$

when n goes to infinity.

We have

$$E[(Y(k+1) - Y(k))^2|Y(k)] = n(E[(p(k+1) - p(k))^2|p(k)]),$$

hence, from Equation (5),

$$nE[(Y(k+1) - Y(k))^2|Y(k)] = 1.$$

Set $a(x) = -2\sqrt{2}x$, $b(x) = 1$.

From the above calculations we have clearly

$$\lim_{n\to\infty} sup_{|x|\leq R}|a^{(n)}(x) - a(x)| = 0$$

$$\lim_{n\to\infty} sup_{|x|\leq R}|b^{(n)}(x) - b(x)| = 0$$

for all $R < +\infty$.

Since the jumps of $Y^{(n)}$ are bounded in absolute value by $\frac{1}{\sqrt{n}}$, $\Delta_\epsilon^{(n)}$ is null, as soon as $\frac{1}{\sqrt{n}}$ is smaller than ϵ, and so

$$\lim_{n\to\infty} sup_{|x|\leq R}\Delta_\epsilon^{(n)} = 0, \forall \epsilon > 0$$

$$\sup_{|x|\leq R} K^{(n)}(x) < \infty$$

is still easy to establish.

Now stochastic differential equation

$$dX(t) = -2\sqrt{2}X(t)dt + dB(t) \tag{11}$$

is of a well-known type. This is an Orstein-Uhlenbeck process, i.e. a stochastic differential equation of type

$$dX(t) = -bX(t)dt + \sigma dB(t).$$

Such an equation is known to have a unique solution for all initial conditions $X(0) = x$. This solution is given by (see e.g. [4])

$$X(t) = e^{-bt}X(0) + \int_0^t e^{-b(t-s)}\sigma dB(s).$$

It is known for these processes, that for all initial conditions $X(0)$, $X(t)$ converges in law when t goes to infinity to the Gaussian $\mathcal{N}(0, \frac{\sigma^2}{2b})$. This latter Gaussian is invariant. See for e.g. [4].

We have all the ingredients to apply Theorem 2 again, and get:

Theorem 5. *We have for all t,*

$$p(\lfloor nt \rfloor) = \frac{\sqrt{2}}{2} + \frac{1}{\sqrt{n}} A_n(t),$$

where $A_n(t)$ converges in law to the unique solution of stochastic differential equation (11)*, and hence to the Gaussian $\mathcal{N}(0, \frac{\sqrt{2}}{8})$ when t goes to infinity.*

10 Some Other Algebraic Numbers

We have treated in detail the case of $\sqrt{2}/2$. We present in this Section, without proofs, the extension of our result to 2-states protocols, with pairing of agents.

At each time step, two agents are fired and their states are possibly changed, according to the fixed rule δ. These protocols are completely described by the three mean increments

$$\begin{aligned}
\alpha &= \mathbb{E}[n_+(k+1) - n_+(k) | \{+,+\} \text{have been fired}], \\
\beta &= \mathbb{E}[n_+(k+1) - n_+(k) | \{+,-\} \text{have been fired}], \\
\gamma &= \mathbb{E}[n_+(k+1) - n_+(k) | \{-,-\} \text{have been fired}].
\end{aligned}$$

Thus, there are $27 = 3^3$ different rules, we denote them by the corresponding triplet (α, β, γ). For instance, the rule computing $\sqrt{2}/2$ is denoted by $(-1, +1, +1)$. We exclude the *identity* rule $(0, 0, 0)$.

We also set

$$\begin{aligned}
a &= \alpha - 2\beta + \gamma, \\
b &= 2\beta - 2\gamma, \\
c &= \gamma.
\end{aligned}$$

We associate then to each triplet (α, β, γ) the polynomial

$$P = aX^2 + bX + c.$$

The following Lemma, whose proof is omitted, is the basis of the next discussion.

Lemma 1 *The polynomial $P = aX^2 + bX + c$ admits at most one root in $(0, 1)$, which we denote by $p^\star$. Moreover,*

$$\begin{aligned}
q := (\alpha^2 - 2\beta^2 + \gamma^2)(p^\star)^2 + (2\beta^2 - 2\gamma^2)p^\star + \gamma^2 &> 0 \\
2ap^\star + b &< 0.
\end{aligned}$$

We will see that the computational power of a protocol population reads on the corresponding polynomial P.

Case 1: P has no root in (0,1). Monotonic convergence.

For 10 rules, P does not admit a root in $(0,1)$. In this case, the convergence of the corresponding protocol is easy to establish. Take for instance $(0,1,2)$:

$$\begin{cases} ++ & \mapsto ++ \\ +- & \mapsto ++ \\ -- & \mapsto ++ \end{cases}$$

It is clear that the protocol converges to the configuration $\{+\}^n$. We summarize the behaviors of the 9 remaining rules in the following table.

α	β	γ	Convergence
0	1	0	$\{+\}^n$ (or $\{-\}^n$ if it is the init. config.)
0	1	1	$\{+\}^n$
0	1	2	$\{+\}^n$
0	0	1	$\{-\}\{+\}^{n-1}$
0	0	2	$\{+\}^n$ or $\{-\}\{+\}^{n-1}$
0	-1	0	$\{-\}^n$ (or $\{+\}^n$ if it is the init. config.)
-1	0	0	$\{+\}\{-\}^{n-1}$
-1	-1	0	$\{-\}^n$
-2	0	0	$\{-\}^n$ ou $\{+\}\{-\}^{n-1}$
-2	-1	0	$\{-\}^n$

Case 2: P **has a unique root in (0,1). Approximation with a diffusion.**
According to α, β, γ, $p^\star$ has one of the three following expressions :

$$p^\star = \begin{cases} \frac{-b+\sqrt{b^2-4ac}}{2a}, \\ \frac{-b-\sqrt{b^2-4ac}}{2a}, \\ -\frac{c}{b}. \end{cases}$$

As in the previous section, we set

$$Y_k = Y_k^{(n)} := \sqrt{n}(p_k^{(n)} - p^\star),$$

and X is the linear interpolation of Y:

$$X^{(n)}(t) = Y_{\lfloor nt \rfloor}^{(n)} + (nt - \lfloor nt \rfloor)(Y_{\lfloor nt+1 \rfloor}^{(n)} - Y_{\lfloor nt \rfloor}^{(n)}).$$

Theorem 6. *Assume that $p_0^{(n)}$ converges to a r.v. X_0 in $(0,1)$. When n goes to infinity, the process $\left(X^{(n)}(t)\right)_{t\geq 0}$ converges to the unique (weak) solution X of the Stochastic Differential Equation*

$$dX_t = (2ap^\star + b)X_t dt + q dB_t. \tag{12}$$

By the previous Lemma, $2ap^\star + b < 0$ and $q > 0$. This solution X has the representation

$$X_t = X_0 e^{(2ap^\star+b)t} + q\int_0^t \exp^{(2ap^\star+b)(t-s)}\, dB_s.$$

Proof. The proof for the case of $\sqrt{2}/2$ extends easily, so we omit the proof.

In particular, Theorem 3 of Section 7 . There exists a random variable $Z_n(t)$, vanishing when $t \to \infty$, such that

$$p(\lfloor nt \rfloor) = p^\star + Z_n(t).$$

There are 16 rules for which P has a root in $(0,1)$. They compute 13 different algebraic numbers.

α	β	γ	Polynomial P	$p^\star$
0	−1	1	$3X^2 - 4X + 1$	$1/3$
0	−1	2	$4X^2 - 6X + 2$	$1/2$
−1	1	0	$-3X^2 + 2X$	$2/3$
−1	1	1	$-2X^2 + 1$	$\sqrt{2}/2$
−1	1	2	$-X^2 - 2X + 2$	$\sqrt{3} - 1$
−1	0	1	$-2X + 1$	$1/2$
−1	0	2	$X^2 - 4X + 2$	$2 - \sqrt{2}$
−1	−1	1	$2X^2 - 4X + 1$	$1 - \sqrt{2}/2$
−1	−1	2	$3X^2 - 6X + 2$	$1 - \sqrt{3}/3$
−2	1	0	$-4X^2 + 2X$	$1/2$
−2	1	1	$-3X^2 + 1$	$\sqrt{3}/3$
−2	1	2	$-2X^2 - 2X + 2$	$(\sqrt{5} - 1)/2$
−2	0	1	$-X^2 - 2X + 1$	$\sqrt{2} - 1$
−2	0	2	$-4X + 2$	$1/2$
−2	−1	1	$X^2 - 4X + 1$	$2 - \sqrt{3}$
−2	−1	2	$2X^2 - 6X + 2$	$(3 - \sqrt{5})/2$

11 Conclusion

In this paper we considered population protocols with a huge population hypothesis. These protocols have been introduced in [1] as a sensor network model. Whereas for original definitions of the latter paper some population protocols are not considered as (stably) convergent, we proved through an example that they sometime actually computes in some natural sense some irrational algebraic value: indeed, in a simple example, the proportion of agents in state + converges to $\frac{\sqrt{2}}{2}$, whatever the initial state of the system is.

One aim of this paper was to formalize the proof of convergence. We did it using a diffusion approximation technique, using a theorem due to [10]. We detailed fully the proof in order to convince our reader that our reasoning can be easily generalized to other kinds of rules of the same type. In particular, this is easy to derive from the protocol considered here another protocol that would compute $\sqrt{\sqrt{\frac{1}{2}}}$, by working with an alphabet made of pairs of states. Clearly, the arguments here would prove its convergence.

We consider this work as a first step towards understanding which numbers can be computed by such protocols. Whereas we prove in this paper that $\frac{\sqrt{2}}{2}$ can be computed and we have given a detailed description of , and whereas this is easy to see that computable numbers in this sense must be algebraic numbers of $[0, 1]$, we didn't succeed yet to characterize precisely computable numbers.

References

1. Dana Angluin, James Aspnes, Zoë Diamadi, Michael J. Fischer, and René Peralta. Computation in networks of passively mobile finite-state sensors. In *Twenty-Third ACM Symposium on Principles of Distributed Computing*, pages 290–299. ACM Press, July 2004.
2. Dana Angluin, James Aspnes, and David Eisenstat. Stably computable predicates are semilinear. In *PODC '06: Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*, pages 292–299, New York, NY, USA, 2006. ACM Press.
3. James Aspnes and Eric Ruppert. An introduction to population protocols. In *Bulletin of the EATCS*, volume 93, pages 106–125, 2007.
4. F. Comets and T. Meyre. *Calcul stochastique et modeles de diffusions.* Dunod Paris, 2006.
5. Z. Diamadi and M.J. Fischer. A simple game for the study of trust in distributed systems. *Wuhan University Journal of Natural Sciences*, 6(1-2):72–82, 2001.
6. R. Durrett. *Stochastic Calculus: A Practical Introduction.* CRC Press, 1996.
7. D. Givon, R. Kupferman, and A. Stuart. Extracting macroscopic dynamics: model problems and algorithms. *Nonlinearity*, 17(6):R55–R127, 2004.
8. Annick Lesne. Discrete vs continuous controversy in physics. *Mathematical Structures in Computer Science*, 2006. In print.
9. M. Presburger. Uber die Vollstandig-keit eines gewissen systems der Arithmetik ganzer Zahlen, in welchemdie Addition als einzige Operation hervortritt. *Comptes-rendus du I Congres des Mathematicians des Pays Slaves*, pages 92–101, 1929.
10. D.W. Stroock and SRS Varadhan. *Multidimensional Diffusion Processes.* Springer, 1979.