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

Olivier Bournez [a] Philippe Chassaing [b] Johanne Cohen [a]
Lucas Gerin [b] Xavier Koegler [c]

[a]LORIA/INRIA-CNRS, *615 Rue du Jardin Botanique, 54602 Villers-Lès-Nancy, FRANCE*

[b]IECN/UHP, *BP 239, 54506 Vandoeuvre-Lès-Nancy Cedex, FRANCE*

[c] Ecole Normale Supérieure, *45, rue d'Ulm, 75230 Paris cedex 05, FRANCE*

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.

In this paper, we study mathematically a particular population protocol that we show to compute in some natural sense some algebraic irrational number, whenever the population goes to infinity. Hence we show that these protocols seem to have a rather different computational power when considered as computing functions, and 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 partic-

Email addresses: `bournez@loria.fr` (Olivier Bournez), `chassain@iecn.u-nancy.fr` (Philippe Chassaing), `jcohen@loria.fr` (Johanne Cohen), `Lucas.Gerin@iecn.u-nancy.fr` (Lucas Gerin), `koegler@clipper.ens.fr` (Xavier Koegler).

ular, 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. Following survey [3]: 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 agents' 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].

In this paper, we want to 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.

Indeed, we consider a particular population protocol, that we prove to converge, whatever its initial state is, to a fraction of $\frac{\sqrt{2}}{2}$ agents in a given state. We hence show that some algebraic irrational values can be computed in this sense. We also give an asymptotic development of the convergence.

Our motivation is 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 paper 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 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 paper 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 present the considered system. In Section 4, as a preliminary discussion, we discuss what can be said when population is assumed to be finite. The rest of the paper is devoted to consider the case of an infinite population. To do so, 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. We prove in Section 8 that this is even possible to use the same theorem to go further and get an asymptotic development of the convergence. Section 9 is devoted to a conclusion and a discussion.

2 Related Work

Population protocols have been introduced in [1]. In the paper, 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.

Much of the work so far on population protocols has 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]. Somehow our notion of adversary is stronger: for finite state systems, this satisfies the fairness hypotheses of the original model, but for infinite state systems, we think that this becomes more natural to expect such a notion, since fairness hypotheses in the sense [1] become problematic to generalize. Notice that this notion of adversary has already be considered for finite state systems [3], in order to study speed of convergence of specific algorithms.

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 (9) can be immediately abstracted in a physicist approach from the dynamic (1), the formal mathematical equivalence of the two is not so immediate, and is somehow a strong motivation of this paper.

Actually, these problems seem to arise in many macroscopic justification 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 (9) 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].

3 The Considered System

We now present our system, in a self-contained manner, to avoid to redefine formally population protocols. However, the reader can check that this is indeed a (non-stably-converging in the sense of [1]) population protocol.

We consider a set of n anonymous agents. Each agent can be in state $+$ or in state $-$. A configuration hence corresponds to an element of $S = \{+, -\}^n$. There are 2^n such configurations.

Suppose that time is discrete.

At each discrete round, two agents are paired. These two agents are chosen according to a uniform law (without choosing twice the same). The effect of a pairing is given by the following rules:

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

These rules must be interpreted as follows: if an agent in state $+$ is paired with an agent in state $+$, then the second becomes $-$. If an agent in state $+$ is paired with an agent in state $-$, then the second becomes $+$, and symmetrically. If an agent in state $-$ is paired with an agent in state $-$, then the first becomes in state $+$.

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 $-$,

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

The object of the rest of this paper is to show the convergence of p to $\frac{\sqrt{2}}{2}$ whenever k goes to infinity, and n goes to infinity.

4 A Preliminary Discussion: The Case of Finite Size Populations

Let us first restate what we are considering by discussing the case of a fixed n. Clearly, the previous rules of interactions can be considered as a description of a discrete time homogeneous Markov chain. This Markov chain has 2^n states corresponding to all configurations. Special configuration $s^- = (-, -, \cdots, -)$ where all agents are in state $-$ is immediately left with probability 1 to a configuration of $S^* = S - \{s^-\}$. Now, any configuration $s' \in S^*$ is clearly reachable from any configuration $s \in S^*$ with positive probability.

Hence, the sequence $p(k)_{k\geq 1}$ is an irreducible Markov chain on S^*.

Let us discuss the basic transition probabilities of this irreducible Markov chain.

At any time step, when selecting an agent in the soup uniformly, it will be in state $+$ with probability $p(k)$, and in state $-$ with probability $1 - p(k)$.

The other agent with whom it will be paired is selected in the rest of the population:

- if the first agent was in state $+$, then the other will be in state $+$ with probability $\frac{n_+(k)-1}{n-1} = p(k)\frac{n}{n-1} - \frac{1}{n-1}$, and in state $-$ with probability $\frac{n_-(k)}{n-1} = \frac{n}{n-1} - p(k)\frac{n}{n-1}$.

  Hence the probability that two agents in state $+$ are paired, and that an agent in state $+$ is paired to an agent in state $-$ are given respectively by

$$\pi_{++} = p(k)^2\frac{n}{n-1} - p(k)\frac{1}{n-1}$$

  and

$$\pi_{+-} = p(k)\frac{n}{n-1} - p(k)^2\frac{n}{n-1}.$$

- Otherwise, the first agent is in state $-$. In this case, the other will be in state $+$ with probability $\frac{n_+(k)}{n-1} = p(k)\frac{n}{n-1}$, and in state $-$ with probability $\frac{n_-(k)-1}{n-1} = 1 - p(k)\frac{n}{n-1}$.

  Hence the probability that an agent in state $-$ is paired with an agent in state $+$, and that an agent in state $-$ is paired with an agent in state $-$ are given respectively by

$$\pi_{-+} = p(k)\frac{n}{n-1} - p(k)^2\frac{n}{n-1}$$

  and

$$\pi_{--} = 1 + p(k)\frac{1-2n}{n-1} + p(k)^2\frac{n}{n-1}.$$

To any state $s \in S^*$ of the Markov chain is associated some proportion $p(k) = \frac{n_+}{n}$ of agents in state $+$, that takes value in $V = \{\frac{1}{n}, \frac{2}{n}, \frac{n-1}{n}, \cdots, 1\}$. Clearly, from above discussions, the Markov chain on S^* can be abstracted on an irreducible Markov chain on this latter set V. As it evolves on finite set V, it is positive recurrent.

The number of agents in state $+$ is increased by one by the second, third and fourth rule, hence with probability

$$\pi_{+1} = \pi_{+-} + \pi_{-+} + \pi_{--} = 1 - \pi_{++},$$

and is decreased by one by the first rule, hence with probability

$$\pi_{-1} = \pi_{++}.$$

By ergodic theorem whatever the initial distribution of probability on states is, the sequence $p(k)$ will ultimately converge in law to the unique stationary distribution π of the Markov chain on V. Distribution π is given by the unique solution with $\sum_{i=1}^{n} \pi(\frac{i}{n}) = 1$ to the global balance equations

$$\pi(\frac{i}{n}) = \pi(\frac{i-1}{n})\pi_{+1} + \pi(\frac{i+1}{n})\pi_{-1},$$

for $i = 1, 2, \cdots, n$ (interpreting $\pi(0)$ and $\pi(\frac{n+1}{n})$ as 0).

As the unique solution to a rational system of equations is rational, the probabilities $\pi(\frac{i}{n})$ are rational, and hence expectation $E[p]$ on the stationary distribution, that can be computed from this stationary distribution by

$$E[p] = \sum_{i=1}^{n} \frac{i}{n}\pi(\frac{i}{n})$$

is rational.

Hence, when the population is finite, this is clear that the proportion of agents in state + converges in law to some rational value, that can be computed as above.

The purpose of the rest of the discussion, is to see that when n goes to infinity, the mean value of $p(k)$ converges to some irrational algebraic value, i.e. to $\frac{\sqrt{2}}{2}$.

Notice also that it follows from the fact that the chain restricted to S^* is irreducible that all configurations of S^* are visited with some positive probability. Hence, in the classical model of [1] this protocol cannot stably compute any non-trivial predicate. Our notion of convergence is different, and based on convergence towards limit distributions on proportions, which is a natural notion when considering huge populations.

5 Computing Expectation and Variance of Increments

As all rules increase or decrease by 1 the number of agents in state +, given $n_+(k)$, one knows that the increment $\Delta_n = n_+(k+1) - n_+(k)$ takes its value in $\{-1, 1\}$.

From previous discussions, we have:

$$\pi_{+1} = 1 - p(k)^2 \frac{n}{n-1} + p(k) \frac{1}{n-1}$$

and

$$\pi_{-1} = p(k)^2 \frac{n}{n-1} - p(k) \frac{1}{n-1}.$$

We get

$$E[\Delta_n | n_+(k)] = 1 \times \pi_{+1} - 1 \times \pi_{-1},$$

from which we get the fundamental equation at the source of the following discussion:

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

Remark 1 *When n goes to infinity, this converges to $1 - 2p(k)^2$.*

Assuming that limit commutes, and that the limit p^* of $p(k)$ when k goes to infinity exists, it must cancel this quantity. Indeed, the system must converge to configuration(s) when one doesn't create nor destroy + in mean.

We get clearly that the limit can only be $p^* = \frac{\sqrt{2}}{2}$.

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

We will first compute

$$\begin{aligned} E[\Delta_n^2 | n_+(k)] &= 1 \times \pi_{+1} + 1 \times \pi_{-1} \\ &= 1. \end{aligned} \tag{3}$$

It follows, from Equations (2) and (3), that we have

$$E[p(k+1) - p(k) | p(k)] = \frac{1}{n}(1 - 2p(k)^2 \frac{n}{n-1} + p(k) \frac{2}{n-1}), \tag{4}$$

which yields the equivalent

$$nE[p(k+1) - p(k) | p(k)] \approx 1 - 2p(k)^2 \tag{5}$$

when n goes to infinity, and

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

which yields the equivalent

$$nE[(p(k+1)-p(k))^2|p(k)] \approx \frac{1}{n}, \tag{7}$$

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 we have for all integer $n \geq 1$, 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 $x \in \mathbb{R}^d$,

$$b^{(n)}(x) = n\int (y-x)\pi^{(n)}(x,dy),$$

$$a^{(n)}(x) = n\int (y-x)(y-x)^*\pi^{(n)}(x,dy),$$

$$K^{(n)}(x) = n\int (y-x)^3\pi^{(n)}(x,dy),$$

$$\Delta_\epsilon^{(n)}(x) = n\pi^{(n)}(x, B(x,\epsilon)^c),$$

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

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

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

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

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

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

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

$$dX(t) = b(X(t))dt + \sigma(X(t))dB(t), \qquad X(0) = x, \tag{8}$$

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

Then for all sequence of initial conditions $Y_0^{(n)} \to x$, the sequence of random processes $X^{(n)}$ converges in law to the diffusion given by (8).

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 the equivalent (5) and (7), we have clearly

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

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

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

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

is easy to establish.

Now, (ordinary and deterministic) differential equation

$$dX(t) = (1 - 2X^2)dt \tag{9}$$

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 (9).

Clearly, all solutions of ordinary differential equation (9) converge to $\frac{\sqrt{2}}{2}$. Doing the change of variable $Z(t) = X(t) - \frac{\sqrt{2}}{2}$, we get

$$dZ(t) = (-2Z^2 + 2\sqrt{2}Z)dt, \tag{10}$$

that converges to 0.

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

Theorem 2 *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 (10)*. 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 An Asymptotic Development of the Dynamic

This is actually possible to go further 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.

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 (4),

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

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 (6),

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

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 condition $X(0) = x$. 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 condition $X(0)$, $X(t)$ 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 1 again, and get:

Theorem 3 *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.*

9 Conclusion

In this paper we considered a particular system of rules. This system describes a particular population protocol. These protocols have been introduced in [1] as a sensor network model. Whereas for original definitions of the latter paper it is not considered as (stably) convergent, we proved that it actually computes in some natural sense some irrational algebraic value: indeed, 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 paper 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 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.

10 Acknoledgements

This work has been partially supported by French Ministry of Research through ANR Project SOGEA.

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.