Computing Real Numbers with Large-Population Protocols Having a Continuum of Equilibria

Xiang Huang
(xhuan5@uis.edu)
xianghuang.org

Rachel Huls
(rhuls2@uis.edu)

University of Illinois Springfield

August 8, 2022

OUTLINE

1. Background
2. The Proof of the main theorem
3. Future work

OUTLINE

1. **Background**
2. The Proof of the main theorem
3. Future work

WHY COMPUTING REAL NUMBERS?

- Theoretical benchmark. (Turing 1936, computable numbers. We now consider analog models.)

WHY COMPUTING REAL NUMBERS?

- Theoretical benchmark. (Turing 1936, computable numbers. We now consider analog models.)
- Complicated systems not based on concrete bio-chemical problems.

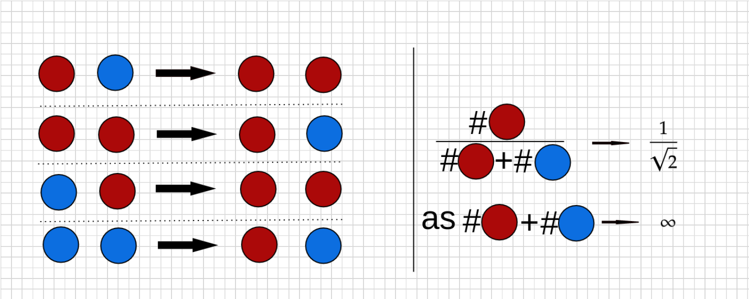
WHY COMPUTING REAL NUMBERS?

- Theoretical benchmark. (Turing 1936, computable numbers. We now consider analog models.)
- Complicated systems not based on concrete bio-chemical problems.
- Guide algorithm design.

REAL NUMBERS BY POPULATION PROTOCOLS?

What do we mean by saying a real number is computable by a PP?

Example (Bournez et. al., 2011[1].)



[1] Guillaume Aupy, Olivier Bournez. On the number of binary-minded individuals required to compute $\frac{1}{\sqrt{2}}$

BASIC PROPERTIES OF COMPUTABLE NUMBERS

Some basic properties:

1. They are the *expected* proportion of some species and hence are between 0 and 1.
2. Total population goes to infinity. We call such population protocols “large-population protocols” or LPPs.
3. Although all proportions are rationals, but the limits might not be so.

BASIC PROPERTIES OF COMPUTABLE NUMBERS

Some basic properties:

1. They are the *expected* proportion of some species and hence are between 0 and 1.
2. Total population goes to infinity. We call such population protocols "large-population protocols" or LPPs.
3. Although all proportions are rationals, but the limits might not be so.

Extra requirement and property:

- They systems must have finitely many equilibria.
- The computing result does not depend on initial values.

THE POWER OF LPPS WITH FINITE EQUILIBRIA

Question: Can we compute $\frac{\pi}{4}$?

[2] Olivier Bournez, Pierre Fraigniaud, and Xavier Koegler. Computing with large populations using interactions.

THE POWER OF LPPS WITH FINITE EQUILIBRIA

Question: Can we compute $\frac{\pi}{4}$?

Theorem (Bournez et. al., 2016. (with a gap)[2])

A number α is computable by a large-population protocol if and only if α is algebraic.

[2] Olivier Bournez, Pierre Fraigniaud, and Xavier Koegler. Computing with large populations using interactions.

THE POWER OF LPPS WITH FINITE EQUILIBRIA

Question: Can we compute $\frac{\pi}{4}$?

Theorem (Bournez et. al., 2016. (with a gap)[2])

A number α is computable by a large-population protocol if and only if α is algebraic.

So only numbers like $\frac{1}{\sqrt{7}}$ and $\sqrt{3}-\sqrt{2}$; no $\frac{\pi}{4}$ and e^{-1}.

[2] Olivier Bournez, Pierre Fraigniaud, and Xavier Koegler. Computing with large populations using interactions.

BUT ON THE OTHER HAND ...

The General Purpose Analog Computer (GPAC) and Chemical Reaction Networks (CRNs) are not so boring.

Theorem (Huang, Klinge and Lathrop 2019)

Transcendental numbers such as π, e, and Euler's γ can be computed by GPAC/CRN in real time.

- Roughly, α is computable if there is a species x such that $\lim_{t\to\infty} x(t) = \alpha$.
- "In real time" simply means we can do it quick. We are not talking about real-time computation today.

AN ANALOG CHURCH-TURING THESIS

Church-Turing thesis: All powerful enough models are equivalent (in some sense).

Question

Are large-population protocols as powerful as GPACs/CRNs (in terms of computing real numbers)?

Or can LPPs "compute" at least some transcendental numbers in some way?

EXAMPLE OF A SYSTEM WITH A CONTINUUM OF EQUILIBRIA

Example (Titus Klinge)

Let $F(t) = \frac{1}{2}e^{e^{-t}-1}$, $E(t) = \frac{1}{2}e^{-t}$, and $G(t)$ be a function such that its derivative "cancels" with E and F's derivative.

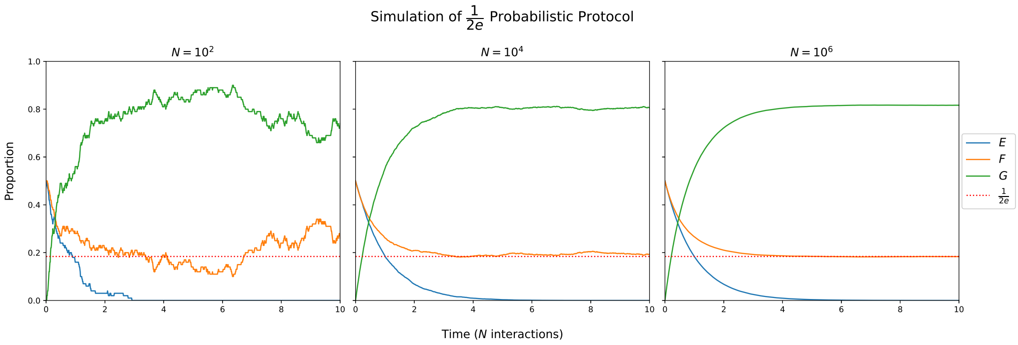
ODE: $$\begin{cases} F' = -2FE \\ E' = -E \\ G' = 2FE + E \end{cases}$$ CRN/PP: $$\begin{cases} F + E \xrightarrow{2} G + E \\ E \to G. \end{cases}$$

with initial values $F(0) = \frac{1}{2}$, $E(0) = \frac{1}{2}$, and $G(0) = 0$. Clearly, $F(t) \to \frac{1}{2e}$

The system has all the F-G plan as equilibria.

SIMULATION

Simulation (by ppsim[3])



[3] David Doty and Eric Severson. Ppsim: A software package for efficiently simulating and visualizing population protocols.

TODAY

Today's Theorem (Huang and Huls)

LPPs compute the same set of numbers in [0,1] as GPACs and CRNs.

TODAY

Today's Theorem (Huang and Huls)

LPPs compute the same set of numbers in [0,1] as GPACs and CRNs.

- We achieve this by lifting the finitary requirement on equilibria. Now we allow systems with a continuum of equilibria.
- The computation results now critically depend on initial values.

TODAY

Today's Theorem (Huang and Huls)

LPPs compute the same set of numbers in [0,1] as GPACs and CRNs.

- We achieve this by lifting the finitary requirement on equilibria. Now we allow systems with a continuum of equilibria.
- The computation results now critically depend on initial values.

Byproducts:

1. fixes Bournez et. al.'s algebraic number proof.
2. gives an algorithm turning CRNs into PPs.

OUTLINE

1. Background
2. **The Proof of the main theorem**
3. Future work

A BRIDGE BETWEEN STOCHASTIC AND CONTINUOUS MODEL

Kurtz Theorem (Kurtz,1972[4].)

Stochastic CRNs agree with their continuous model almost surely when population goes to infinity.

To simplify our discussion in this talk, we treat population protocols as two-input two output CRNs with deterministic mass-action semantic, under large population assumption.

[4] Thomas G. Kurtz. The relationship between stochastic and deterministic models for chemical reactions.

LPP-COMPUTABLE NUMBER: FORMAL DEFINITION

Definition

A real number ν is said to be computable by an LPP if there exists an LPP such that $\mathbf{x}(t) = (x_1(t), x_2(t), \cdots, x_n(t)) \in [0,1]^n$ and

$$\lim_{t\to\infty} \sum_{i\in M} x_i(t) = \nu,$$

where $M \subseteq \{1, \cdots, n\}$ represents the subset of states marked in $\mathbf{x}$. Moreover, all the states x_i must be initialized to some positive rational $r_i \in \mathbb{Q} \cap [0,1]$, in the sense that $\lim_{N\to\infty} x_i^{(N)}(0) = r_i$, when $x_i^{(N)}(0)$ is the initial fraction of state i at the stage when the population is N.

POLYNOMIAL CHARACTERIZATION OF GPAC AND CRN

GPAC/ODE

$$x_i' = p_i(x_1, \cdots, x_n),$$

for $i = 1, 2, \cdots, n$,

where p_i's are polynomials.

CRN/ODE[5]

$$x_i' = p_i(x_1, \cdots, x_n) - q_i(x_1, \cdots, x_n)x_i,$$

for $i = 1, 2, \cdots, n$,

where p_i's and q_i's are polynomials with **positive** coefficients.

The idea: A reaction cannot destroy a non-reactant, so x must appear as a reactant in the reaction.

[1] Vera Hars and János Tóth: On the Inverse Problem of Reaction Kinetics, 1979.

POLYNOMIAL CHARACTERIZATION OF PP

1. Must first be CRN. $x_i{}' = p_i(x_1, \cdots, x_n) - q_i(x_1, \cdots, x_n)x_i,$
2. Must preserve population. $\sum_i x_i{}'$ = 0.
3. p_i does not have x_i^2 term.

The third bullet is because a two-input-two-output reaction like

$$X_i + X_i \to Y + W$$

can not increase X_i anymore.

GPAC EXAMPLE

$$\begin{cases} f' = w, \\ g' = -pqv, \\ w' = -w + u + v, \\ u' = -u + rv, \\ v' = -v, \\ r' = -r^2, \\ p' = pv, \\ q' = v - q, \end{cases}$$

with $f(0) = g(0) = u(0) = w(0) = q(0) = 0$ and $v(0) = r(0) = p(0) = 1$.

CRN AND PP EXAMPLE

Example (CRN/ODE)

$$x' = 1 - x$$

Example (PP/ODE)

$$\begin{aligned} x' &= 2xy + y^2 - x^2 \\ y' &= x^2 - (2x + y)y \end{aligned}$$

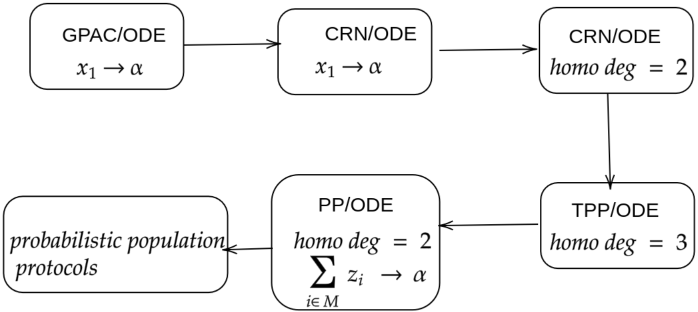
This one is the PP that computes $\frac{1}{\sqrt{2}}$ in the beginning of the talk.

THE BAG OF TRICKS

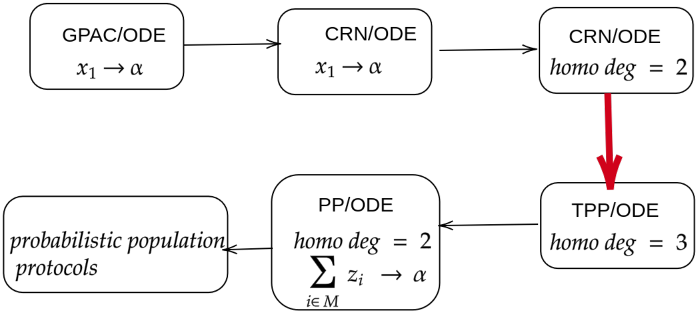
Given an ODE system $\mathbf{x}' = p(\mathbf{x})$ with $\lim_x x_1 \to \alpha$, where α is a targeting number.

1. Rewrite the system with a new set of auxiliary variables.
2. Rewrite the system with $\sum_i x_i = 1$.
3. Dilate the system by a new time function.
4. Taking product of the system.
5. ...

THE OVERVIEW OF THE PROOF



THE OVERVIEW OF THE PROOF



A STRAIGHTFORWARD IDEA

A PP preserves population/mass.

Question

Given a CRN $\mathbf{x} = (x_1, \cdots, x_n)$*, how could we make it preserves population/mass to begin with?*

A STRAIGHTFORWARD IDEA

A PP preserves population/mass.

Question

Given a CRN $\mathbf{x} = (x_1, \cdots, x_n)$*, how could we make it preserves population/mass to begin with?*

- add a new variable x_0.

A STRAIGHTFORWARD IDEA

A PP preserves population/mass.

Question

Given a CRN $\mathbf{x} = (x_1, \cdots, x_n)$*, how could we make it preserves population/mass to begin with?*

- add a new variable x_0.
- make the derivative of the new variable cancel all other change!

$$x_0' = \sum_{i=1}^{n} x_i'$$

A DECENT IDEA, BUT NOT WORK

$$S = \begin{cases} dx_1 = \epsilon(a_0 + a_1 x_1 + \sum_{i=1}^{\delta-1} \frac{a_{i+1}}{\lambda^{i-1}} x_1 x_i) \\ \\ dx_i = \lambda x_1 x_{i-1} - x_i \quad \text{for } i = 2, \ldots, \delta - 1 \\ \\ dx_\delta = -\sum_{i=1}^{\delta-1} dx_i \end{cases}$$

A DECENT IDEA, BUT NOT WORK

$$S = \begin{cases} dx_1 = \epsilon(a_0 + a_1 x_1 + \sum_{i=1}^{\delta-1} \frac{a_{i+1}}{\lambda^{i-1}} x_1 x_i) \\ \\ dx_i = \lambda x_1 x_{i-1} - x_i \quad \text{for } i = 2, \ldots, \delta - 1 \\ \\ dx_\delta = -\sum_{i=1}^{\delta-1} dx_i \end{cases}$$

Bournez et. al. use this system to compute arbitrary *algebraic* number. But the last summation bring in all the terms in the system, which is usually not implementable by PP.
For example, $\sqrt{3} - \sqrt{2}$ with minimal polynomial $x^4 - 10x^2 + 1$ is a counterexample of their construction.

$\sqrt{3} - \sqrt{2}$

Let $(x_1, x_2, x_2, x_4) = (x, x^2, x^3, x^4)$. To encode the minimal polynomial, we have

$$\begin{Bmatrix} x_1' & = & (x_4+1) - 10x_1x_1 \\ x_2' & = & 2x_1(x_4+1) - 20x_1x_2 \\ x_3' & = & 3x_2(x_4+1) - 30x_1x_3 \\ x_4' & = & 4x_3(x_4+1) - 40x_1x_4 \end{Bmatrix}$$

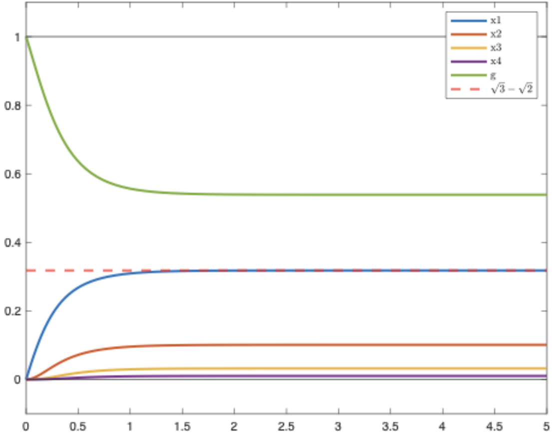
SECOND ATTEMPT: TPP

~~We~~ *multiply* the variable we are going to introduce to the system.

$$\begin{cases} x_1' = x_0\left[(x_4+1) - 10x_1x_1\right] \\ x_2' = x_0\left[2x_1(x_4+1) - 20x_1x_2\right] \\ x_3' = x_0\left[3x_2(x_4+1) - 30x_1x_3\right] \\ x_4' = x_0\left[4x_3(x_4+1) - 40x_1x_4\right] \\ x_0' = -\sum_{i=1}^{4} x_i' \end{cases}$$

- every negative terms of x_0' now always has x_0.
- but now the system is of degree 3 (termolecular system)!
- x_0' does not have positive x_0^3 term.

TPP



TIME DILATION / CHAIN RULE

But what is x_0 doing here?
Let $\mathbf{x}(t)$ be the solution of $\mathbf{x}' = p(\mathbf{x})$, where $\mathbf{x} = (x_1, \cdots, x_n)$ be a vector of variables, p a multivariable polynomial.

Example (Constant Dilation)

Then x(2t) is the solution of the ODE:

$$\mathbf{x}'(t) = p(\mathbf{x}) \cdot 2$$

Example (with a known function)

Then x(F(t)) is the solution of the ODE:

$$\mathbf{x}'(t) = p(\mathbf{x}) \cdot f(t),$$

where $F(t)' = f(t)$.
In our setting $F(t) = \int_0^t f(t)dt$

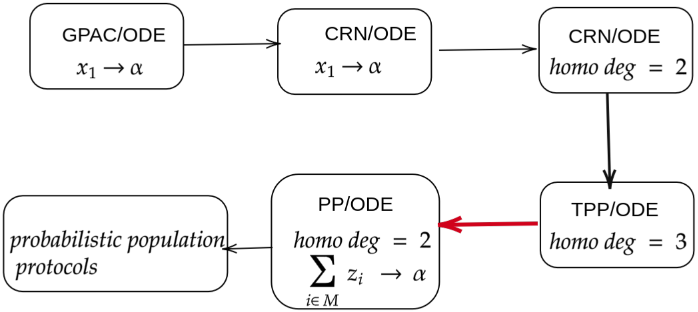
BALANCING DILATION

$$\begin{cases} x_i' = (p_i - q_i \cdot x_i) \cdot x_0, & \text{for } i \in \{1, \cdots, n\} \\ x_0' = -\sum_{i=1}^{n} x_i'. \end{cases}$$

- The function x_0 is not known in advance.
- It is determined by the ODE above.
- How time dilates depends on / customizes to the original system $\mathbf{x}$.

TO POPULATION PROTOCOLS

We now turn the TPP into PP.



CALCULUS I AGAIN

We introduce

$$z_{i,j} = x_i \cdot x_j$$

Then

$$z'_{i,j} = x'_i \cdot x_j + x_i \cdot x'_j$$

- The z-system is now of degree 4, homogeneously.
- Each term has the form such $x_1 x_2 x_4 x_5$, carefully assign the z-variable can make the system population-protocol implementable.
  - Make sure it is CRN implementable first.
  - Then avoid $z_{i,j}^2$ term in $z'_{i,j}$.

$x_1 x_2 x_4 x_5 = z_{1,2} \cdot z_{4,5}$ = $z_{2,4} \cdot z_{1,5}$, etc.

OUTLINE

1. Background
2. The Proof of the main theorem
3. Future work

HIERARCHY DOWN

GPAC/CRN/PP compute roughly the same set of real numbers. How about weaker models?

Example (One-side protocols)

The model with all the reactions in the form of:

$$Y + X \to Z + X$$

HIERARCHY UP

$$\vdots$$
$$R_2 = CRN(R_1)$$
$$R_1 = CRN(R_0)$$
$$R_0 = CRN(\mathbb{Q}) = GPAC(\mathbb{Q}) = PP(\mathbb{Q}).$$

We begin with allowing rational number as initial values and rate constants. Then build a new hierarchy on top the the previous level.

HIERARCHY UP

$$\vdots$$

$$R_2 = CRN(R_1)$$

$$R_1 = CRN(R_0)$$

$$R_0 = CRN(\mathbb{Q}) = GPAC(\mathbb{Q}) = PP(\mathbb{Q}).$$

We begin with allowing rational number as initial values and rate constants. Then build a new hierarchy on top the the previous level.

Question: Do we really have a tower, or all layers collapse to $\mathbb{R}_0$? Or

$$R_0 \stackrel{?}{=} \bigcup_{i=0}^{\infty} R_i.$$