

Calculabilité distribuée

applications concrètes & puissance

Guillaume Seguin

15/01/2009

Plan

- 1 Introduction à la calculabilité distribuée
 - Concept général
 - Exemple concret
- 2 Modèle des protocoles de population
 - Protocole de population
 - Convergence
- 3 Puissance du modèle
 - Calculabilité
 - Complexité

Concept général

Réseau d'agents :

- Anonymes
- Passivement mobiles
- Disposant d'une quantité de mémoire bornée
- Pouvant communiquer entre eux quand ils sont proches, deux par deux

Pertinence du concept

- Composants de petite taille, peu coûteux
- Production de masse (sans identifiant unique)
- Communication sans fil (RFID)
- Mobiles, mais passifs (capteurs, *tags* électroniques...)

Exemple concret



Question

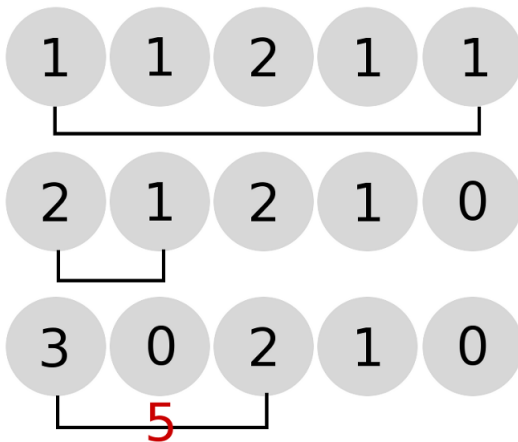
Y a-t-il au moins N (fixé) renards malades ?

Solution

Utiliser un protocole de population ! Chaque individu est muni d'un petit dispositif :

- Capteur médical déterminant si l'individu est malade
- Composant de communication sans fil de proximité
- Quelques bits de mémoire, réalisant un compteur
- Quand un compteur vaut 5, toute la population passe (de proche en proche) dans un état d'alerte

Algorithme



Autre exemple



Protocole de population, population

Définition

Un *protocole de population* est un uplet (X, Y, Q, I, O, δ) :

- X, Y : alphabets d'entrée et de sortie
- Q : ensemble des états
- $I : X \rightarrow Q$: fonction qui assigne l'état initial
- $O : Q \rightarrow Y$: fonction qui détermine la sortie
- $\delta : Q \times Q \rightarrow Q \times Q$: fonction de transition

Définition

Une *population* est un couple (A, E) :

- A : ensemble des agents
- E : graphe d'interaction

Configuration, transition, calcul

Définition

Une *configuration* est une fonction $C : A \rightarrow Q$ qui détermine l'état de chaque agent.

Définition

Il existe une *transition* $C_0 \rightarrow C_1$ entre des configurations C_0 et C_1 s'il existe une arête (u, v) du graphe d'interaction E telle que $(C'(u), C'(v)) = \delta(C(u), C(v))$ et $C' = C$ sinon.

Définition

Une *calcul* est une suite infinie de configurations C_0, C_1, \dots telle que pour toute transition $C \rightarrow C'$, si C apparaît un nombre infini de fois au cours de l'exécution, C' aussi (équité).

Configuration stable, convergence

Pas de *terminaison temporelle*, mais :

Définition

Une configuration C est dite *stable* si pour toute configuration C' *accessible* depuis C (c'est à dire qu'il existe une suite de transitions $C \rightarrow C_1 \rightarrow \dots \rightarrow C_n \rightarrow C'$), $O(C) = O(C')$

Définition

Un calcul *converge* si il contient une configuration stable.

Calcul stable d'une relation

Définition

Une relation R est calculée stablement par un protocole de population si le calcul sur toute entrée x converge et si pour tout (x, y) , on a $R(x, y)$ vrai si tout calcul sur l'entrée x se stabilise sur la sortie y .

Calculs réalisables

Déjà vu : les compteurs, les inégalités

Question

Plus généralement, quels calculs peut-on réaliser stablement avec les protocoles de population ?

Arithmétique de Presburger, prédicats calculables

Définition

L'arithmétique de Presburger est l'arithmétique de Peano de laquelle on a retiré les axiomes sur la multiplication.

Définition

Un prédicat $\phi : \mathbb{N}^n \rightarrow \{0, 1\}$ est calculable par un protocole de population si et seulement si ϕ est accepté pour toute entrée (x_1, x_2, \dots, x_k) telle que $\phi(x_1, x_2, \dots, x_k) = 1$ et refusé pour toute entrée (x_1, x_2, \dots, x_k) telle que $\phi(x_1, x_2, \dots, x_k) = 0$.

Prédicats calculables stablement

Théorème [Angluin *et al.*, 2004]

Tout prédicat définissable dans l'arithmétique de Presburger est calculable stablement par un protocole de population.

Et même :

Théorème [Angluin *et al.*, 2006]

L'ensemble des prédicats calculables stablement par les protocoles de population est exactement l'ensemble des prédicats définissable dans l'arithmétique de Presburger.

Automate conjuguant

Définition

Un *automate conjuguant* est un protocole de population dont le graphe d'interaction est complet (toutes les interactions sont possibles) et dont les interactions sont choisies indépendemment et uniformément dans l'ensemble des couples d'agents distincts.

Complexité probabiliste pour l'arithmétique de Presburger

Théorème

Pour tout prédicat ϕ définissable dans l'arithmétique de Presburger, il existe un automate conjuguant qui calcule ϕ avec une probabilité 1, et où la population des agents converge vers la réponse en, en moyenne, $O(n^2 \log(n))$ interactions.

Théorème

Soit une fonction f calculable en temps polynomial (en $O(n^d)$) dans le pire cas par une machine de Turing en espace mémoire logarithmique. Alors, pour tout $c > 0$, il existe un automate conjuguant qui calcule $f(x) \forall x \leq n$ avec une probabilité d'erreur en $O(n^{-c} \log(n))$ et en temps moyen polynomial (en $O(n^{d+2} \log(n) + n^{2d+c+1})$).