

# Протоколы на популяциях и вычислительная сложность

М.А. Раскин

Технический университет Мюнхена (TUM)

31.03.2021



# Понятие протокола на популяциях

## Определение

**Протокол на популяциях** задаётся множеством состояний  $Q$  и правилами взаимодействия

$$\delta : Q \times Q \rightarrow Q \times Q.$$

**Популяция (конфигурация)** — мультимножество состояний

**Шаг протокола** — выбор двух состояний  $q_1, q_2$  из популяции и их замена на состояния  $\delta(q_1, q_2)$

**Исполнение протокола** — последовательность шагов

Определение:

Dana Angluin, James Aspnes, Zoë Diamadi, Michael J. Fischer, René Peralta. Computation in networks of passively mobile finite-state sensors. 2004.

Понятие близко к сетям Петри (упрощённым) и системам прибавления векторов, отличие: ровно два входа и два выхода у каждого взаимодействия

Определение:

[AADFP2004] Computation in networks of passively mobile finite-state sensors.

Понятие близко к сетям Петри (упрощённым) и системам прибавления векторов, отличие: ровно два входа и два выхода у каждого взаимодействия

Определение:

[AADFP2004] Computation in networks of passively mobile finite-state sensors.

Ряд родственных понятий:

Dana Angluin, James Aspnes, David Eisenstat, Eric Ruppert:  
The computational power of population protocols. Distributed Computing. 2007

- В исходной статье — вычисления минимальными средствами для сетей сенсоров (вычислительные возможности нереалистично занижены)
- Распределённые вычисления, где хоть что-то разрешимо
- Взаимодействующие агенты с фиксированным объёмом памяти

# Вопросы о протоколах

- В сетях Петри типичные вопросы — достижимость, покрытие
- В протоколах на популяциях принято изучать вычисление предикатов

Вычисление предиката: участники с какого-то момента всегда согласны

Зависит от порядка взаимодействий

Случайный порядок или детерминированный аналог

# Вопросы о протоколах

- В сетях Петри типичные вопросы — достижимость, покрытие
- В протоколах на популяциях принято изучать вычисление предикатов

Вычисление предиката: участники с какого-то момента всегда согласны

Зависит от порядка взаимодействий

Случайный порядок или детерминированный аналог



# Вопросы о протоколах

- В сетях Петри типичные вопросы — достижимость, покрытие
- В протоколах на популяциях принято изучать вычисление предикатов

Вычисление предиката: участники с какого-то момента всегда согласны

Зависит от порядка взаимодействий

Случайный порядок или детерминированный аналог

# Вычисления с помощью протоколов: честные исполнения

## Определение

*Бесконечное исполнение называется **честным**, если всякая конфигурация, всегда остающаяся доступной во время исполнения, достигается бесконечно много раз*

Случайное исполнение является честным почти наверное

## Определение

Протокол  $(Q, \delta)$  с исходными состояниями  $\{i_1, \dots, i_k\}$  и функцией ответов  $o : Q \rightarrow \{\perp, \top\}$  **вычисляет** предикат  $\varphi : \mathbb{N}^k \rightarrow \{\perp, \top\}$ , если каждое честное исполнение из всякой конфигурации  $\{a_1 \otimes i_1, \dots, a_k \otimes i_k\}$  с какого-то места содержит только конфигурации, где все состояния дают правильный ответ, то есть лежат в  $o^{-1}(\{\varphi(a_1, \dots, a_k)\})$ .

# Вычисления с помощью протоколов

Пример протокола:

$$Q = \{Y, N, y, n\} \qquad i_0 = Y, i_1 = N$$
$$Y, N \mapsto n, n \qquad y, n \mapsto n, n \qquad Y, n \mapsto Y, y \qquad N, y \mapsto N, n$$

Протокол вычисляет  $\varphi(a_0, a_1) := a_0 > a_1$

# Сложность вопросов о протоколах

Вопросы про конкретную популяцию лежат в PSPACE

Полнота: симуляция машин Тьюринга

Достижимость: PSPACE-полна

Корректность вычисления на одном входе: PSPACE-полна

Многое эквивалентно свойствам сетей Петри

# Сложность вопросов о протоколах

Вопросы про конкретную популяцию лежат в PSPACE

Полнота: симуляция машин Тьюринга

Достижимость: PSPACE-полна

Корректность вычисления на одном входе: PSPACE-полна

Многое эквивалентно свойствам сетей Петри

W. Czerwinski, S. Lasota, R. Lazic, J. Leroux, F. Mazowiecki. The reachability problem for Petri nets is not elementary. 2019

# Сложность вопросов о протоколах

Вопросы про конкретную популяцию лежат в PSPACE

Полнота: симуляция машин Тьюринга

Достижимость: PSPACE-полна

Корректность вычисления на одном входе: PSPACE-полна

Многое эквивалентно свойствам сетей Петри

[CLLLM2019] Reachability for Petri nets is not elementary

Корректность вычисления предиката неэлементарна

# Сложность вопросов о протоколах

Корректность вычисления предиката неэлементарна

Корректность вычисления предиката сводится к  
достижимости в сетях Петри

J. Esparza, P. Ganty, J. Leroux, R. Majumdar: Verification of  
population protocols. 2017

Jérôme Leroux, Sylvain Schmitz. Reachability in Vector  
Addition Systems is Primitive-Recursive in Fixed Dimension.  
2019



# Сложность вопросов о протоколах

Достижимость: PSPACE-полна

Корректность вычисления на одном входе: PSPACE-полна

Корректность вычисления предиката неэлементарна

Достижимость между бесконечными множествами  
неэлементарна

# Сложность вопросов о протоколах

Достижимость между бесконечными множествами  
неэлементарна

Какие бесконечные множества?

Вычислимые протоколами предикаты — полулинейны  
выразимы в арифметике Пресбургера:  $+$ ,  $>$ ,  $\equiv \pmod{}$

Параллелепипеды ( $a_j \geq c$ )

Достижимость между параллелепипедами уже  
неэлементарна

# Сложность вопросов о протоколах

Достижимость между параллелепипедами уже  
неэлементарна

Достижимость между полулинейными множествами  
разрешима

Неэлементарная сложность корректности и достижимости между бесконечными множествами

- Ограничение возможных протоколов
- Другие вопросы (время работы)
- Более удобные вопросы про достижимость

## Определение

*Протоколы с непосредственным наблюдением:  
протоколы, в которых при взаимодействии первое  
состояние сохраняется ( $\delta(p, q) = (p, q')$ )*

- Вычислимые предикаты: параллелепипеды [AAER2007]
- Достижимость PSPACE-полна
- Достижимость между параллелепипедами PSPACE-полна, корректность PSPACE-полна

## Протоколы с непосредственным наблюдением

- Вычислимые предикаты: параллелепипеды [AAER2007]
- Достижимость PSPACE-полна
- Достижимость между параллелепипедами PSPACE-полна, корректность PSPACE-полна  
J. Esparza, M. Raskin, C. Weil-Kennedy. Parameterized Analysis of Immediate Observation Petri Nets. 2019

# Ограниченные протоколы

## Протоколы с непосредственным наблюдением

- Вычислимые предикаты: параллелепипеды [AAER2007]
- Достижимость между параллелепипедами PSPACE-полна, корректность PSPACE-полна [ERWK2019]
- Отношение достижимости полулинейно  
M. Raskin, C. Weil-Kennedy, J. Esparza. Flatness and Complexity of Immediate Observation Petri Nets. 2020

# Ограниченные протоколы

## Протоколы с непосредственным наблюдением

- Вычислимые предикаты: параллелепипеды [AAER2007]
- Достижимость между параллелепипедами PSPACE-полна, корректность PSPACE-полна [ERWK2019]
- «Необратимые» наблюдения делают достижимость NP-полной

M. Raskin, C. Weil-Kennedy. Efficient Restrictions of Immediate Observation Petri Nets. 2020



# Время работы

Сложность вычислений в модели протоколов на популяциях

Задача большинства,  $a_0 > a_1$

При случайном исполнении:  $n \cdot O(\log n \log s + \frac{\log n}{s\varepsilon})$

взаимодействий (время  $O(\log n \log s + \frac{\log n}{s\varepsilon})$ )

$\varepsilon$  — исходный перевес

$s$  — число состояний

$\Omega(\frac{1}{\varepsilon})$  для четырёх состояний

$\Omega(n \log n)$  взаимодействий в любом случае

# Время работы

Сложность вычислений в модели протоколов на популяциях

Задача большинства,  $a_0 > a_1$

При случайном исполнении:  $n \cdot O(\log n \log s + \frac{\log n}{s\varepsilon})$

взаимодействий (время  $O(\log n \log s + \frac{\log n}{s\varepsilon})$ )

$\varepsilon$  — исходный перевес

$s$  — число состояний

D. Alistarh, R. Gelashvili, M. Vojnović. Fast and Exact Majority in Population Protocols. 2015

## Другие вопросы про достижимость

Достижимость между популяциями, содержащими только одно состояние

«Для всех достаточно больших размеров» — в P

Граница «достаточно большого» —  $\exp(\text{poly}(|Q|))$

«Для всех» — PSPACE-полная задача

A. R. Balasubramanian, J. Esparza, M. Raskin. Finding Cut-Offs in Leaderless Rendez-Vous Protocols is Easy. 2021

## Другие вопросы про достижимость

Что должно быть «достаточно большим» для упрощения достижимости в протоколах с непосредственным наблюдением?

Разница между разными суммами кратностей состояний

За полиномиальное время можно либо проверить

достижимость  $C'$  из  $C$ , либо найти

$X, Y \subseteq Q : 0 < |C'(Y) - C(X)| < |Q|^3$  [RWK2020]

# Заключение

Протоколы на популяциях — модель распределённых вычислений, в которой проверка корректности ещё вычислима

В максимальной общности большинство задач имеют неэлементарную сложность

Различные ограничения или упрощения приводят к значительному снижению сложности