Задача проверки бисимулярности. Разрешимость и неразрешимость

Techniques for Decidability and Undecidability of Bisimilarity

Petr Jančar, Faron Moller

17 ноября 2017 г.

Игра в бисимуляцию

- ***Игровое поле*** — (вообще говоря, бесконечный) ориентированный мультиграф с пометками на рёбрах (далее, граф), такой, что:
  - число различных пометок конечно;
  - граф обладает свойством ***конечного ветвления по пометке:*** для любой вершины E и любой пометки a множество $\{F : E \xrightarrow{a} F\}$ конечно.
- Игра $G_n(E_0, F_0)$ определяется двумя вершинами E_0 и F_0 и ограничением на число ходов $n \in \mathbb{N} \cup \{\omega\}$.
- Два игрока:
  - ***Алиса*** пытается показать, что E_0 и F_0 — в некотором смысле *различны*;
  - ***Боб*** пытается показать, что E_0 и F_0 — в некотором смысле *одинаковы*.

Игра в бисимуляцию

- ***Партия*** — это последовательность пар вершин

$$(E_0, F_0)\ (E_1, F_1)\ (E_2, F_2)\ldots$$

длины $\leqslant 1 + n$, в которой пара (E_{i+1}, F_{i+1}) получается следующим образом:

  - ***Алиса*** выбирает дугу $E_i \xrightarrow{a} E_{i+1}$ или $F_i \xrightarrow{a} F_{i+1}$;
  - ***Боб*** выбирает соответствующую дугу $F_i \xrightarrow{a} F_{i+1}$ или $E_i \xrightarrow{a} E_{i+1}$.

- ***Алиса*** выигрывает партию, если в какой-либо момент оказывается, что ***Боб*** не может сделать ход.
- ***Боб*** выигрывает партию, если в какой-либо момент оказывается, что ***Алиса*** не может сделать ход, а также любую партию длины n.

Бисимулярность

- У ***Боба*** есть ***выигрышная стратегия*** в игре $G_n(E_0, F_0)$, если он может выиграть любую партию в $G_n(E_0, F_0)$, независимо от действий ***Алисы.***
- $E_0 \sim_n F_0$, если у ***Боба*** есть выигрышная стратегия в игре $G_n(E_0, F_0)$, для $n \in \mathbb{N}$;
- $E_0 \sim F_0$, если у ***Боба*** есть выигрышная стратегия в игре $G_\omega(E_0, F_0)$.

Отношение $\sim$ называется ***бисимуляционной эквивалентностью*** или ***бисимулярностью***.

Бисимулярность

Факт (1)

Отношения $\sim_n$ и $\sim$ — это отношения эквивалентности.

Факт (2)

$$\sim_0 \supseteq \sim_1 \supseteq \sim_2 \supseteq \sim_3 \supseteq \ \ldots \ \supseteq \sim$$

Факт (3)

«Ограниченная бисимулярность»

1. $E \sim_0 F$ *для любых* E *и* F.
2. $E \sim_{n+1} F$ *тогда и только тогда, когда*
   - 2.1 *если* $E \xrightarrow{a} E'$, *то* $F \xrightarrow{a} F'$, *причём* $E' \sim_n F'$;
   - 2.2 *если* $F \xrightarrow{a} F'$, *то* $E \xrightarrow{a} E'$, *причём* $E' \sim_n F'$.

Бисимулярность

Факт (4)

«Бисимулярность»

Отношение $\sim$ — это наибольшее отношение $\equiv$, удовлетворяющее свойству: если $E \equiv F$, то

1. *если $E \xrightarrow{a} E'$, то $F \xrightarrow{a} F'$, причём $E' \equiv F'$;*
2. *если $F \xrightarrow{a} F'$, то $E \xrightarrow{a} E'$, причём $E' \equiv F'$.*

Факт (5)

*Для графов с **конечным ветвлением по пометкам***

$$\sim \;=\; \bigcap_{n \in \mathbb{N}} \sim_n .$$

Бисимулярность

Для графов с конечным ветвлением по пометкам проблема $E \not\sim F$ ***полуразрешима***.

Бисимулярность

Выигрышная стратегия ***Боба*** в игре $G_\omega(E_0, F_0)$ может быть представлена в виде множества $\mathcal{B}$ пар вершин, такого, что $(E_0, F_0) \in \mathcal{B}$, и для любой пары $(E, F) \in \mathcal{B}$:

1. если $E \xrightarrow{a} E'$, то $F \xrightarrow{a} F'$, причём $(E', F') \in \mathcal{B}$;
2. если $F \xrightarrow{a} F'$, то $E \xrightarrow{a} E'$, причём $(E', F') \in \mathcal{B}$.

Множество $\mathcal{B}$ называется ***отношением бисимуляции***.

Факт (6)

*Отношение $\sim$ — это объединение всех отношений бисимуляции (т. е. выигрышных стратегий **Боба**).*

Разрешимость. Деревья сдвигов

$E_0 \sim F_0$ тогда и только тогда, когда существует отношение бисимуляции, содержащее (E_0, F_0).

Разрешимость. Деревья сдвигов

Сдвиг множества пар вершин B — это *минимальное по включению* множество пар вершин A, такое, что для любой пары $(E, F) \in B$

1. если $E \xrightarrow{a} E'$, то $F \xrightarrow{a} F'$, причём $(E', F') \in A$;
2. если $F \xrightarrow{a} F'$, то $E \xrightarrow{a} E'$, причём $(E', F') \in A$.

Разрешимость. Деревья сдвигов

- непустое множество не имеет сдвига тогда и только тогда, когда оно содержит такую пару (E', F'), что $E' \not\sim_1 F'$;
- непустое множество имеет единственный пустой сдвиг $\varnothing$ тогда и только тогда, когда в каждой паре из этого множества обе вершины не имеют исходящих дуг;
- в условиях конечного ветвления по пометкам, конечное множество пар вершин имеет лишь конечное число конечных сдвигов;
- отношение бисимуляции, содержащее B, содержит также некоторый его сдвиг A.

Разрешимость. Деревья сдвигов

Факт (7)

Если $A \subseteq B$, и A является сдвигом B, то B — это отношение бисимуляции, и, таким образом, $B \subseteq \sim$.

Разрешимость. Деревья сдвигов

Дерево сдвигов — это (вообще говоря, бесконечное) дерево, у которого:

- узлы — это множества пар вершин графа, причём узлы-потомки представляют собой в точности все сдвиги родительского узла;
- пустые узлы — это листья, называемые ***правильными***;
- остальные (непустые) листья – ***неправильные***;
- ветвь (путь из корня) называется *правильной*, если она бесконечная или заканчивается правильным листом;

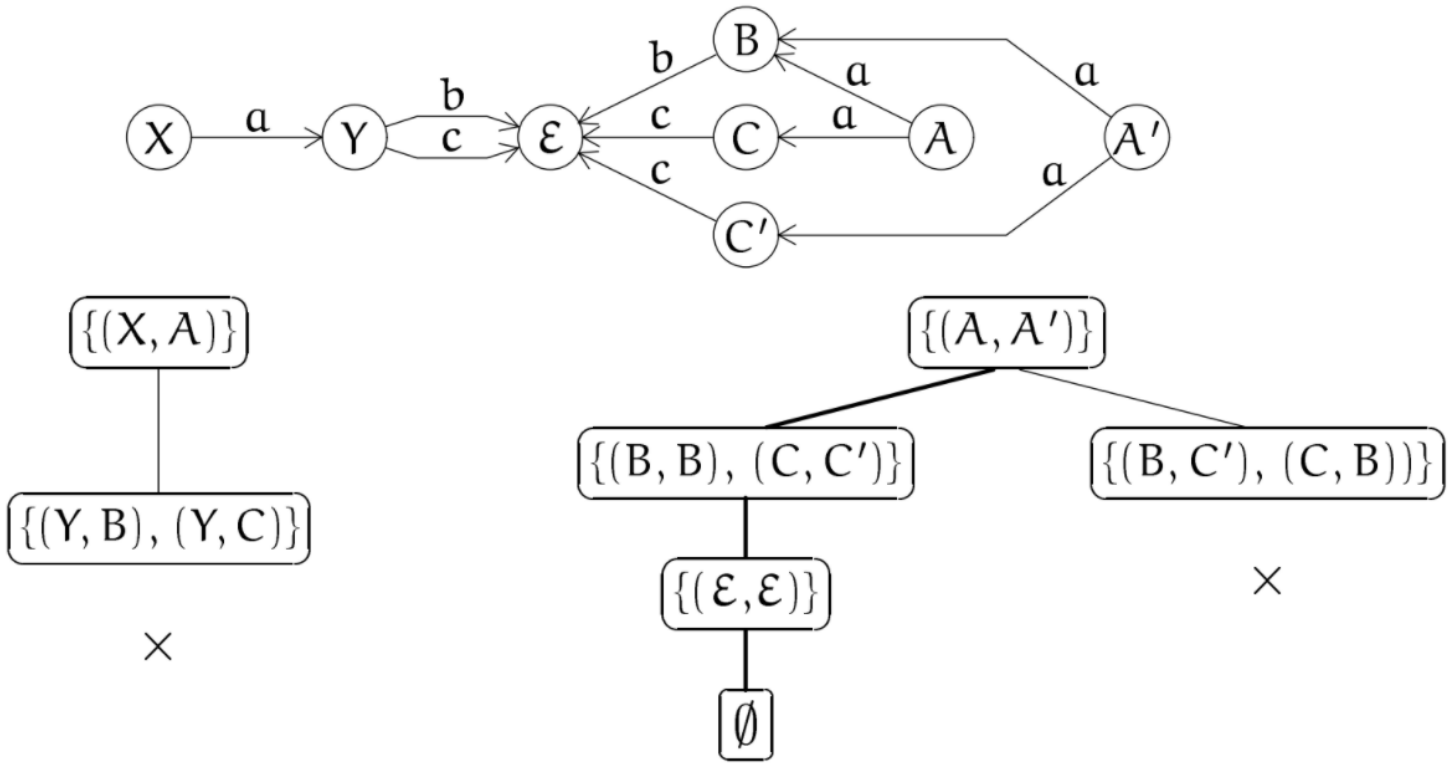
Разрешимость. Деревья сдвигов

Факт (8)

$E_0 \sim F_0 \iff$ *в дереве сдвигов с корнем в* $\{(E_0, F_0)\}$ *существует правильная ветвь.*

Если $E_0 \not\sim F_0$, то дерево сдвигов с корнем в $\{(E_0, F_0)\}$ обязательно конечное, что снова приводит к полуразрешимости проблемы $E_0 \not\sim F_0$.

Разрешимость. Деревья сдвигов



Разрешимость. Деревья сдвигов

Факт (9)

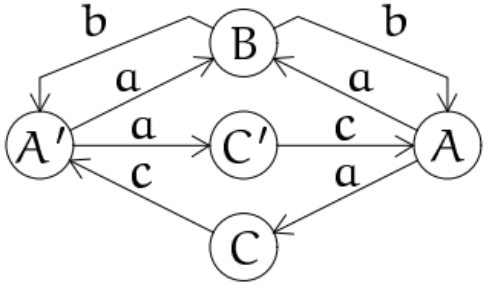
Для любого непустого узла A и любого $n \in \mathbb{N}$ верно, что $A \subseteq \sim_{n+1} \iff$ у A есть потомок $C \subseteq \sim_n$.

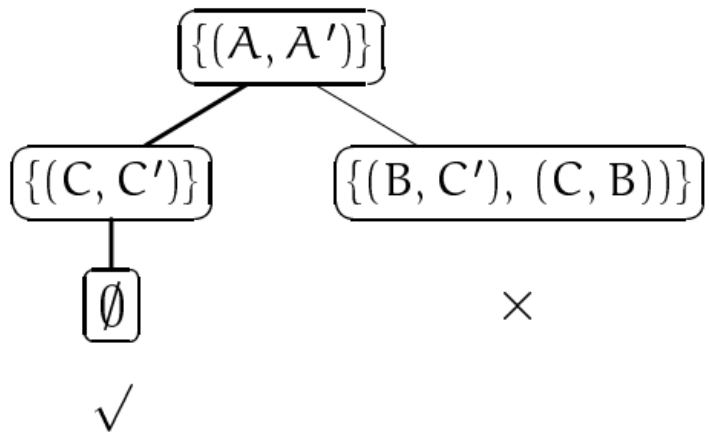
Таким образом, $A \subseteq \sim \iff$ у A есть потомок $C \subseteq \sim$.

Разрешимость. Деревья сдвигов

- $A^{\Uparrow}$ — это множество всех предков узла A;
- ***Правило исключения:*** из узла A можно удалить пару (E, F), если существует $B \subseteq A^{\Uparrow}$, такое, что, для любого $n \in \mathbb{N}$, если $B \subseteq \sim_n$, то $E \sim_n F$;
- ***Правило эквивалентности:*** из узла A можно удалить пару (E, F), если она принадлежит наименьшему отношению эквивалентности, содержащему $A^{\Uparrow}$.

Разрешимость. Деревья сдвигов





Разрешимость. Деревья сдвигов

Теперь объединение узлов на правильной ветви дерева — это множество B, для которого обязательно существует сдвиг A, такой, что, для всех $n \in \mathbb{N}$, если $B \subseteq \sim_n$, то $A \subseteq \sim_n$, откуда $B \subseteq \sim$.

Разрешимость. Алгебры процессов

- ***Граф алгебры процессов (PA-граф)*** определяется набором *правил вывода* вида $\mathcal{X} \xrightarrow{a} \alpha$, где
  - $\mathcal{X}$ принадлежит множеству переменных V;
  - a — множеству пометок Σ;
  - α — множеству термов свободной алгебры над V, порождённой некоммутативным ассоциативным оператором $\cdot$ и коммутативным ассоциативным оператором $|$.
- Вершины графа — это термы.
- Дуги графа определяются продолжением правил вывода на термы:
  - если $\alpha \xrightarrow{a} \beta$, то $\alpha \cdot \gamma \xrightarrow{a} \beta \cdot \gamma$;
  - если $\alpha \xrightarrow{a} \beta$, то $\alpha | \gamma \xrightarrow{a} \beta | \gamma$.

Разрешимость. Алгебры процессов

Различные виды *PA*-графов:

- *BPA*-графы (используется только оператор $\cdot$);
- *BPP*-графы (используется только оператор $|$);

Все *PA*-графы — конечно ветвящиеся по пометкам.

Разрешимость. Алгебры процессов

Отношения $\sim_n$ и $\sim$ — конгруэнции относительно операторов $\cdot$ и $|$

Разрешимость. Алгебры процессов

- ***Правило конгруэнтности:*** из узла A можно удалить пару (α, β), если она принадлежит наименьшей конгруэнции, содержащей $A^{\Uparrow}$.
- Термы в *BPP* можно рассматривать как векторы в $\mathbb{N}^k$, $k = |V|$. То есть, множество термов в *BBP* можно рассматривать как конечно порождённую коммутативную полугруппу (КПКП).
- Все конгруэнции в КПКП являются конечно порождёнными.

Разрешимость. Алгебры процессов

Пусть все пары (α, β) в узлах дерева лексикографически упорядоченны: $\alpha <_L \beta$.

- ***Правило BPP:*** пару $(\alpha', \beta|\gamma)$ можно не включать в узел A, если существует $(\alpha, \beta) \in A^{\Uparrow}$; вместо неё можно рассмотреть пару $(\alpha', \alpha|\gamma)$ (или симметричную, в зависимости от $<_L$).
- ***Лемма Диксона:*** каждая бесконечная последовательность в $\mathbb{N}^k$ содержит бесконечно возрастающую подпоследовательность.

Разрешимость. Алгебры процессов

Конечная порождённость $\sim$ даёт ещё одний полурешающий алгоритм для проблемы $\alpha \sim \beta$: нужно «угадать» (систематически построить) конечное множество пар B, включающее (α, β), а также его сдвиг A, такие, что A входит в наименьшую конгруэнцию, содержащую B.

Разрешимость. Алгебры процессов

В *BPA* существуют конгруэнции, не являющиеся конечно порождёнными.

:(

Разрешимость. Алгебры процессов

- ***Правило замены:*** к узлу A можно добавить братский узел, в котором пара (E, F) заменяется конечным множеством пар $\mathcal{S}$, если существует $B \subseteq A^{\Uparrow}$, такое, что, для всех $n \in \mathbb{N}$, если $B \subseteq \sim_n$ и $\mathcal{S} \subseteq \sim_n$, то $E \sim_n F$.

Разрешимость. Алгебры процессов

- Терм α — *нормированный*, если в графе существует путь из α в ε, $norm(\alpha)$ — длина самого короткого из таких путей.
- Если α — ненормированный терм, то $\alpha \sim \alpha\beta$.
- Любой терм представим в виде α или $\alpha\mathcal{X}$, где α — нормированный терм, а $\mathcal{X}$ — ненормированный.

Разрешимость. Алгебры процессов

***Правила** BPA:*

1. Если $(\mathcal{X}\alpha, \mathcal{Y}\beta) \in A$, а $(\mathcal{X}\alpha', \mathcal{Y}\beta') \in A^{\Uparrow}$, то можно добавить братский узел, содержащий (α, α') и (β, β') вместо $(\mathcal{X}\alpha, \mathcal{Y}\beta)$.
2. Если $(\mathcal{X}\alpha, \mathcal{Y}\beta) \in A$, $\mathcal{X}$, $\mathcal{Y}$ — нормированны, то можно добавить братский узел, содержащий «декомпозиционные пары» $(\mathcal{X}, \mathcal{Y}\gamma)$, $(\gamma\alpha, \beta)$, вместо $(\mathcal{X}\alpha, \mathcal{Y}\beta)$, где $norm(\mathcal{X}) = norm(\mathcal{Y}\gamma)$ (таких пар конечное число).

Разрешимость. Алгебры процессов

Эти правила приводят к дереву с хотя бы одной конечной правильной ветвью.

Разрешимость. Алгебры процессов

Но в общем случае, для *PA* почти ничего не известно.

- Для *нормированных термов* в *PA* разработана похожая техника. В этом случае узлы дерева сдвигов содержат не только конечное число пар вершин, но и *схемы*, представляющие бесконечные множества пар вершин.
- Для всех (ненормированных) *PA* вообще ничего неизвестно.

Разрешимость. Алгебры процессов с состояниями

Усложнение модели: теперь у алгебры процессов есть конечное множество *состояний*, причём

- правила вывода имеют вид $p\mathcal{X} \xrightarrow{a} q\alpha$, где p и q — состояния;
- правила вывода распространяются на термы с учётом состояний:
  - если $p\alpha \xrightarrow{a} q\beta$, то $p(\alpha \cdot \gamma) \xrightarrow{a} q(\beta \cdot \gamma)$;
  - если $p\alpha \xrightarrow{a} q\beta$, то $p(\alpha|\gamma) \xrightarrow{a} q(\beta|\gamma)$;

Разрешимость. Алгебры процессов с состояниями

Графы, порождаемые односчётчиковыми машинами:

- все вершины имеют вид $p\mathcal{X}\mathcal{X}\ldots\mathcal{X}\mathcal{Z}$;
- число символов $\mathcal{X}$ интерпретируется как значение счётчика;
- символ $\mathcal{Z}$ — символ «дна стека», используется для проверки на ноль;
- будем записывать $p(m)$ вместо $p\mathcal{X}^m\mathcal{Z}$.

Разрешимость. Алгебры процессов с состояниями

Здесь используется альтернативный (по сравнению с предыдущими случаями) подход:

- последовательно генерируются конечные описания (вообще говоря, бесконечных) отношений бисимуляции;
- для каждого отношения проверяется, не содержит ли оно пару (E_0, F_0);
- если пара (E_0, F_0) бисимулярна, то алгоритм остановится и даст положительный ответ.

Разрешимость. Алгебры процессов с состояниями

Раскраска — это отображение $: \mathbb{N} \times \mathbb{N} \to \mathcal{C}$, где $\mathcal{C}$ — конечное множество *цветов*.

Разрешимость. Алгебры процессов с состояниями

- Раскраской для односчётчиковой машины $\mathcal{M}$ назовём раскраску

$$c = \prod_{p,q \in Q} c_{pq},$$

где $c_{pq} : \mathbb{N} \times \mathbb{N} \to \{black, white\}$.

- Раскраска c задаёт отношение

$$\mathcal{R}_c : p(m)\mathcal{R}_c q(n) \iff c_{pq}(m,n) = black$$

Разрешимость. Алгебры процессов с состояниями

Раскраска, порождающая отношение бисимуляции

$$c^{\mathcal{M}} = \prod_{p,q \in Q} c^{\mathcal{M}}_{pq},$$

где

$$c^{\mathcal{M}}_{pq}(i,j) = \mathit{black} \iff p(i) \sim q(j),$$

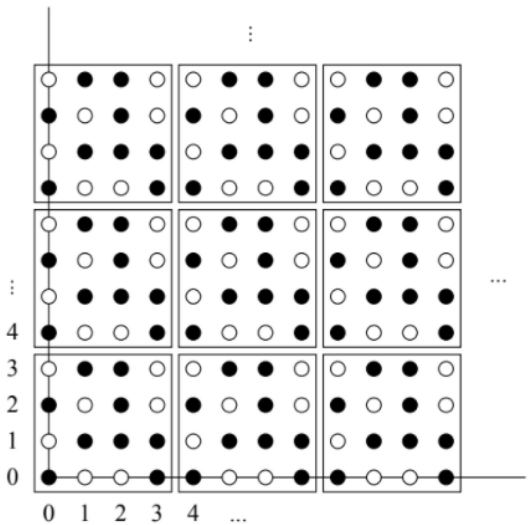
$$c^{\mathcal{M}}_{pq}(i,j) = \mathit{white} \iff p(i) \not\sim q(j)$$

Разрешимость. Алгебры процессов с состояниями

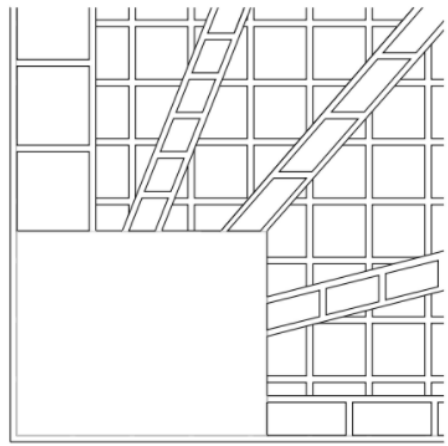
Регулярная раскраска — это раскраска, получающаяся из периодической раскраски путём изменения цветов в конечном числе полос (коэффициент наклона которых — неотрицательное рациональное число или ∞), так, чтобы в каждой полосе раскраска оставалась периодической, и, затем, перекрашивания начального квадрата.

Разрешимость. Алгебры процессов с состояниями

Эти картинки, по мнению авторов, иллюстрируют понятие регулярной раскраски.



A periodic colouring.



Scheme of a regular colouring.

Разрешимость. Алгебры процессов с состояниями

Факт (10)

Для односчётчиковой машины $\mathcal{M}$ раскраска $c^{\mathcal{M}}$ регулярна.

Таким образом, можно последовательно генерировать все регулярные раскраски c и проверять, что $\mathcal{R}_c$ — отношение бисимуляции, содержащее (E_0, F_0).

Неразрешимость

- Нельзя ожидать разрешимость для графов, моделирующих универсальные вычислительные устройства (например, двухсчётчиковые машины (Минского)).
- Алгебры процессов с состояниями могут моделировать двухсчётчиковую машину Минского с помощью термов вида $(\mathcal{X}\mathcal{X}\ldots\mathcal{X}\mathcal{Z})|(\mathcal{Y}\mathcal{Y}\ldots\mathcal{Y}\mathcal{Z})$.
- Алгебры *BPP* с состояниями могут *слабо* (но достаточно для неразрешимости) моделировать двухсчётчиковую машину Минского.

Неразрешимость

Машина Минского $\mathcal{M}$ (с двумя счётчиками) — это последовательность помеченных команд:

$$X_0 : comm_0;\ X_1 : comm_1;\ \ldots X_n : comm_n,$$

где для $0 \leqslant s \leqslant n-1$ команды имеют вид $(b = 0, 1)$

$$X_s : c_b := c_b + 1;\ goto\ X_j$$

или вид

$$X_s : if\ c_b = 0\ then\ goto\ X_j\ else\ c_b = c_b - 1;\ goto\ X_k$$

Неразрешимость

- Машина начинает работу со значениями счётчиков $c_0 = c_1 = 0$.
- Выполнение начинается с команды с меткой X_0.
- Машина последовательно выполняет команды.
- Машина останавливается, достигая команды X_n: *halt*.

Неразрешимость

Построим *BPP*-граф, слабо моделирующий машину Минского:

- множество пометок $\Sigma = \{i, d, z, h\}$;
- множество состояний $Q = \{p_0, p_1, \ldots, p_n, q_0, q_1, \ldots, q_n\}$;
- множество переменных $V = \{\mathcal{Z}, 0, 1\}$;

Неразрешимость

- для каждой команды

$$X_s : c_b = c_b + 1;\ goto\ X_j$$

создаём правила вывода

$$p_s\mathcal{Z} \xrightarrow{i} p_j(b|\mathcal{Z}) \qquad q_s\mathcal{Z} \xrightarrow{i} q_j(b|\mathcal{Z});$$

Неразрешимость

- для каждой команды

$$X_s\colon \mathit{if}\ c_b = 0\ \mathit{then}\ \mathit{goto}\ X_j\ \mathit{else}\ c_b = c_b - 1;\ \mathit{goto}\ X_k$$

создаём правила вывода

$$p_s b \xrightarrow{d} p_k \qquad p_s \mathcal{Z} \xrightarrow{z} p_j \mathcal{Z} \qquad p_s b \xrightarrow{z} q_j b$$

$$q_s b \xrightarrow{d} q_k \qquad q_s \mathcal{Z} \xrightarrow{z} q_j \mathcal{Z} \qquad q_s b \xrightarrow{z} p_j b$$

Неразрешимость

- создаём единственное финальное правило вывода

$$p_n \mathcal{Z} \xrightarrow{h} p_n$$

Неразрешимость

Факт (11)

$p_0\mathcal{Z} \sim q_0\mathcal{Z} \Longleftrightarrow$ *машина* $\mathcal{M}$ *не останавливается.*

Факт (12 и последний)

Задача проверки бисимулярности неразрешима в классе BPP-алгебр с состояниями.

Наконец-то

Спасибо за внимание!