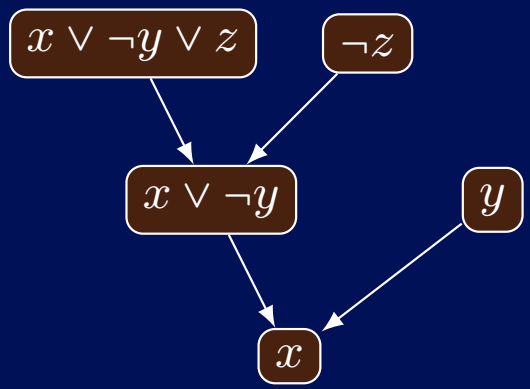
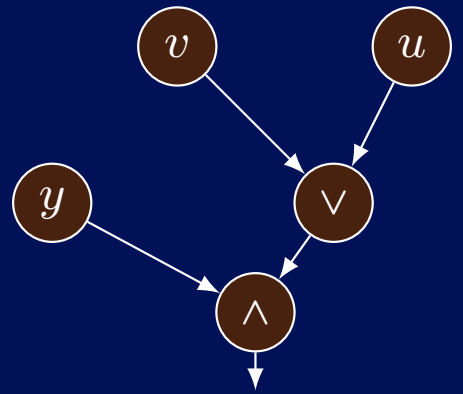
Несколько слов о сложности доказательств





Дмитрий Соколов

Тверь 2021
Декабрь 6

St Petersburg University

PDMI

RAS

Немного о «теории сложности»

$f\colon X^n \to Y$

Есть ли простое описание у функции f?

Немного о «теории сложности»

$f\colon X^n \to Y$

Есть ли простое описание у функции f? $\Leftrightarrow$ Выразима ли функция f, как композиция «простых»?

Немного о «теории сложности»

$f: X^n \to Y$

Есть ли простое описание у функции f? $\Leftrightarrow$ Выразима ли функция f, как композиция «простых»?

- [Теорема Абеля] Корни многочленов степени 5 невыразимы в виде композиции «простых» функций.

Немного о «теории сложности»

$f: X^n \to Y$

Есть ли простое описание у функции f? $\Leftrightarrow$ Выразима ли функция f, как композиция «простых»?

- [Теорема Абеля] Корни многочленов степени 5 невыразимы в виде композиции «простых» функций.
- [13-я проблема Гильберта] Можно ли выразить корни многочленов степени 7 в виде композиции функций от двух переменных?

Немного о «теории сложности»

$f: X^n \to Y$

Есть ли простое описание у функции f? $\Leftrightarrow$ Выразима ли функция f, как композиция «простых»?

- [Теорема Абеля] Корни многочленов степени 5 невыразимы в виде композиции «простых» функций.
- [13-я проблема Гильберта] Можно ли выразить корни многочленов степени 7 в виде композиции функций от двух переменных?
- [Теорема Колмогорова – Арнольда] Любую непрерывную функцию, можно выразить в виде композиции функций от двух переменных.

Немного о «теории сложности»

$f\colon X^n \to Y$

Есть ли простое описание у функции f? $\Leftrightarrow$ Выразима ли функция f, как композиция «простых»?

- [Теорема Абеля] Корни многочленов степени 5 невыразимы в виде композиции «простых» функций.
- [13-я проблема Гильберта] Можно ли выразить корни многочленов степени 7 в виде композиции функций от двух переменных?
- [Теорема Колмогорова – Арнольда] Любую непрерывную функцию, можно выразить в виде композиции функций от двух переменных.

$X \coloneqq \{0, 1\}$

- Интерполяционный полином.

Немного о «теории сложности»

$f\colon X^n \to Y$

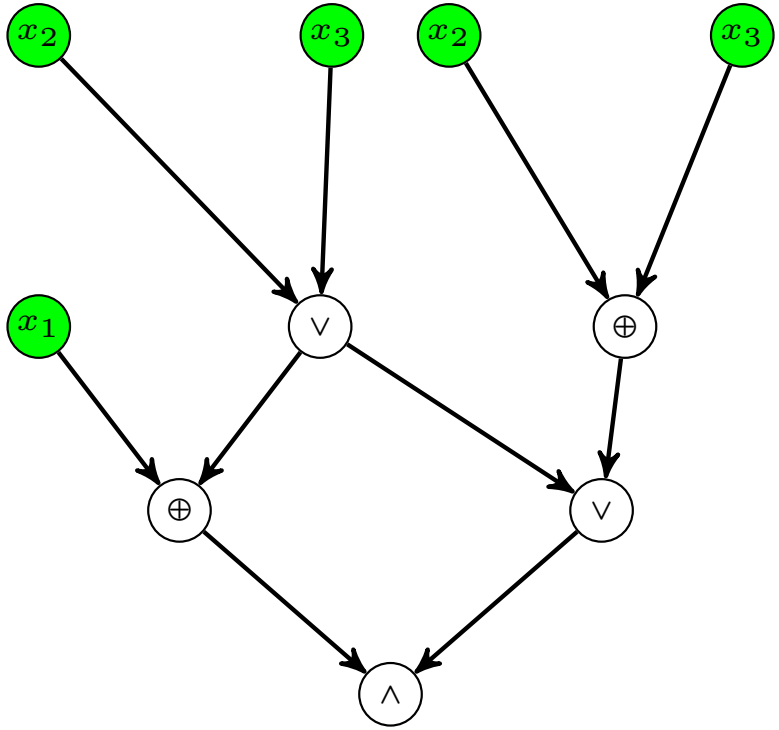
Есть ли простое описание у функции f? $\Leftrightarrow$ Выразима ли функция f, как композиция «простых»?

- [Теорема Абеля] Корни многочленов степени 5 невыразимы в виде композиции «простых» функций.
- [13-я проблема Гильберта] Можно ли выразить корни многочленов степени 7 в виде композиции функций от двух переменных?
- [Теорема Колмогорова – Арнольда] Любую непрерывную функцию, можно выразить в виде композиции функций от двух переменных.

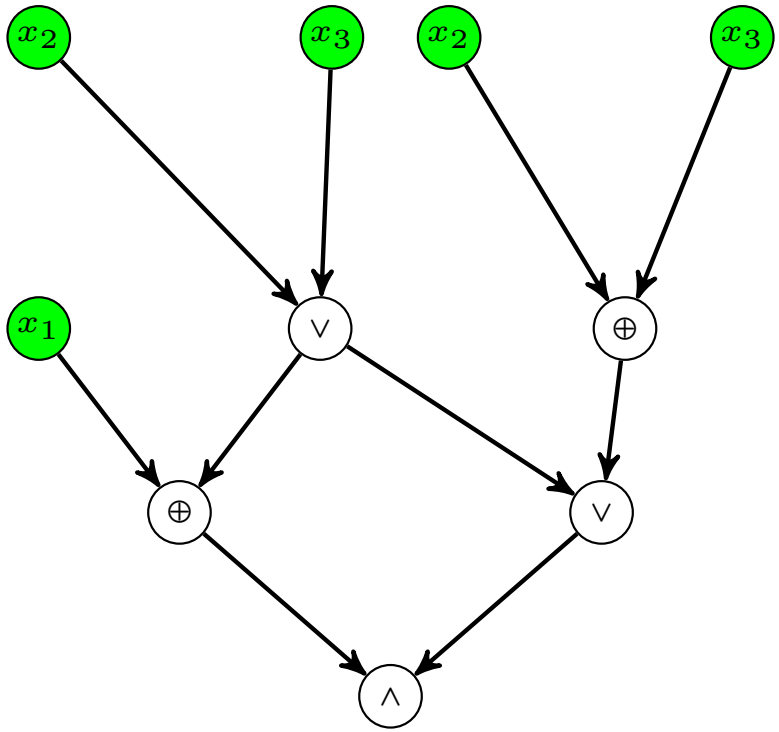
$X \coloneqq \{0, 1\}$

- Интерполяционный полином.
- «Можно ли выразить?» $\Rightarrow$ «Насколько сложно выразить?»

Схемы



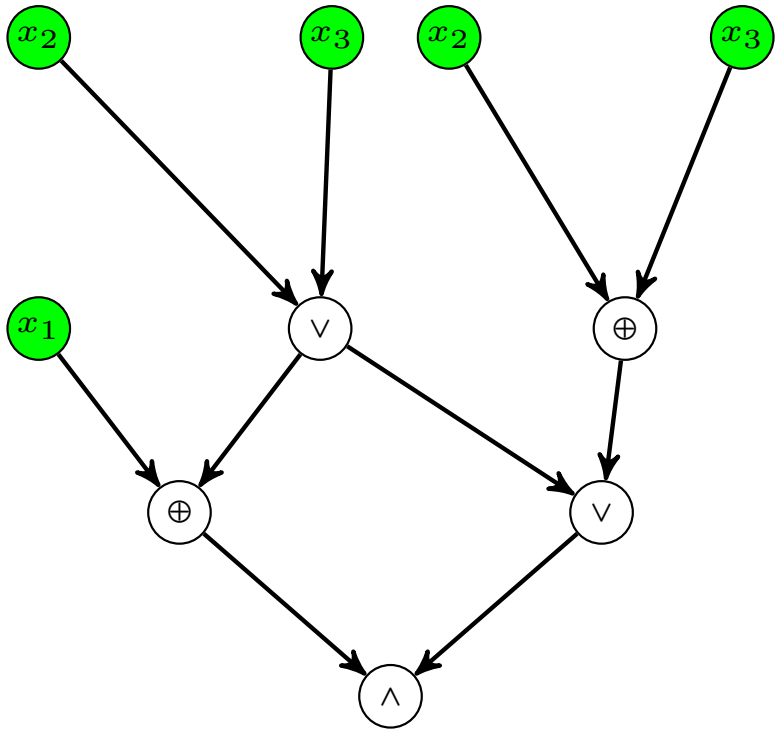
Схемы



Теорема

Если алгоритм может посчитать функцию за время t, то есть и схема для функции размера $\mathcal{O}(t \log t)$.

Схемы



Теорема

Если алгоритм может посчитать функцию за время t, то есть и схема для функции размера $\mathcal{O}(t \log t)$.

- Криптография;
- классификация вычислительных задач;
- ...

Системы доказательств

Язык: $L \subseteq \{0,1\}^*$. UNSAT: язык невыполнимых пропозициональных формул в КНФ.

Системы доказательств

Язык: $L \subseteq \{0,1\}^*$. UNSAT: язык невыполнимых пропозициональных формул в КНФ.

Определение[Cook, Reckhow 79]

Система доказательств для языка L — такой полиномиальный по времени алгоритм Π: $\{0,1\}^* \times \{0,1\}^* \to \{0,1\}$, что:

- (полнота) $x \in L \Rightarrow \exists w\ \Pi(x,w) = 1$;
- (корректность) $\exists w\ \Pi(x,w) = 1 \Rightarrow x \in L$.

Мера сложности — длина $|w|$.

Системы доказательств

Язык: $L \subseteq \{0,1\}^*$. UNSAT: язык невыполнимых пропозициональных формул в КНФ.

Определение[Cook, Reckhow 79]

Система доказательств для языка L — такой полиномиальный по времени алгоритм Π: $\{0,1\}^* \times \{0,1\}^* \to \{0,1\}$, что:

- (полнота) $x \in L \Rightarrow \exists w\ \Pi(x,w) = 1$;
- (корректность) $\exists w\ \Pi(x,w) = 1 \Rightarrow x \in L$.

Мера сложности — длина $|w|$.

Программа Кука

Будем доказывать оценки для все более сильных систем, пока не удастся обобщить методы на произвольную систему доказательств.
Цель: показать, что язык UNSAT сложный ($\mathbf{NP} \neq \mathbf{coNP}, \mathbf{P} \neq \mathbf{NP}$).

Примеры

$$\varphi \coloneqq (x \vee y \vee \neg z) \wedge (\neg w \wedge u) \wedge (\neg x \wedge \neg u) \wedge \dots$$

Примеры

$$\varphi \coloneqq (x \vee y \vee \neg z) \wedge (\neg w \wedge u) \wedge (\neg x \wedge \neg u) \wedge \dots$$

- Резолюция. A, B — дизъюнкты.
  - $\dfrac{A \vee x \quad B \vee \neg x}{A \vee B} \qquad \dfrac{A}{A \vee z}$

  Доказательство: вывод пустого дизъюнкта из дизъюнктов исходной формулы.

Примеры

$$\varphi \coloneqq (x \vee y \vee \neg z) \wedge (\neg w \wedge u) \wedge (\neg x \wedge \neg u) \wedge \ldots$$

- Резолюция. A, B — дизъюнкты.
  - $\frac{A \vee x \quad B \vee \neg x}{A \vee B} \qquad \frac{A}{A \vee z}$

  Доказательство: вывод пустого дизъюнкта из дизъюнктов исходной формулы.
- Cutting Planes. $(x \vee y \vee \neg z) \Rightarrow x + y + (1 - z) \geq 1$.
  - $\frac{A \geq a \quad B \geq b}{\alpha A + \beta B \geq \alpha a + \beta b} \qquad \frac{k a_1 x_1 + k a_2 x_2 + \cdots \geq c}{a_1 x_1 + a_2 x_2 + \cdots \geq \lceil \frac{c}{k} \rceil}$

  Доказательство: вывод неравенства $0 \geq 1$ из неравенств, кодирующих дизъюнкты формулы.

Примеры

$$\varphi \coloneqq (x \vee y \vee \neg z) \wedge (\neg w \wedge u) \wedge (\neg x \wedge \neg u) \wedge \dots$$

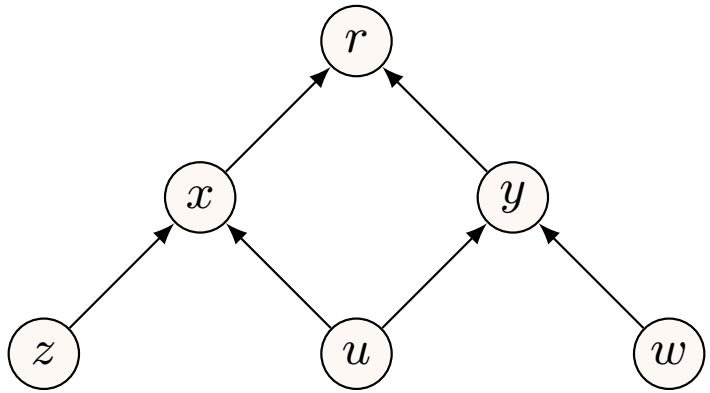
- Резолюция. A, B — дизъюнкты.
  - $\frac{A \vee x \quad B \vee \neg x}{A \vee B} \qquad \frac{A}{A \vee z}$

  Доказательство: вывод пустого дизъюнкта из дизъюнктов исходной формулы.
- Cutting Planes. $(x \vee y \vee \neg z) \Rightarrow x + y + (1 - z) \geq 1$.
  - $\frac{A \geq a \quad B \geq b}{\alpha A + \beta B \geq \alpha a + \beta b} \qquad \frac{k a_1 x_1 + k a_2 x_2 + \dots \geq c}{a_1 x_1 + a_2 x_2 + \dots \geq \lceil \frac{c}{k} \rceil}$

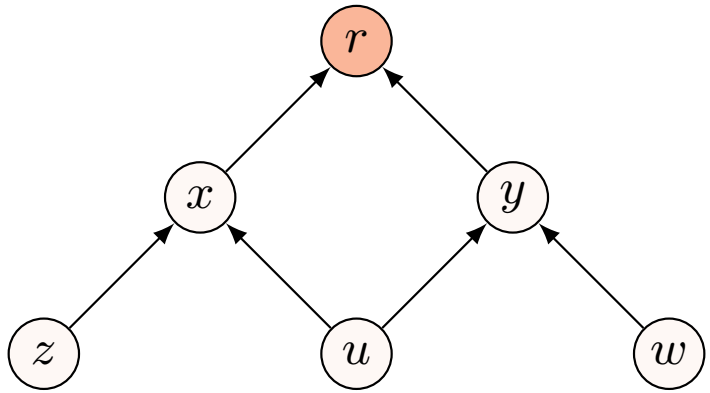
  Доказательство: вывод неравенства $0 \geq 1$ из неравенств, кодирующих дизъюнкты формулы.
- Nullstellensatz.
  - $\mathbb{F}$ — поле;
  - $(x \vee y \vee \neg z) \Rightarrow f_i \coloneqq (1 - x)(1 - y)z = 0$;
  - $x^2 - x = 0$.

  Доказательство: такой набор полиномов h_i, что $\sum\limits_i h_i f_i = 1$.

Pebbling

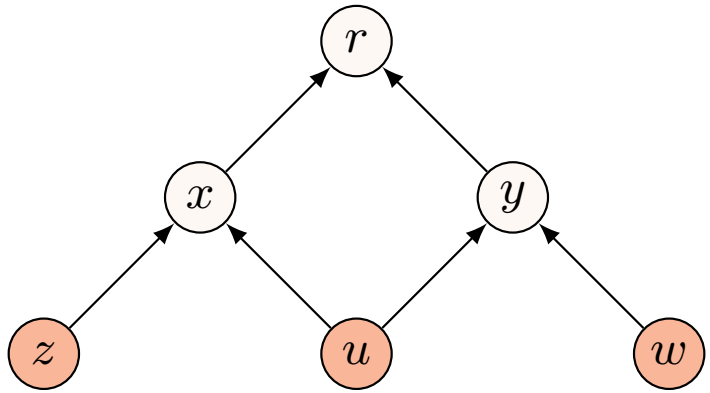


Pebbling



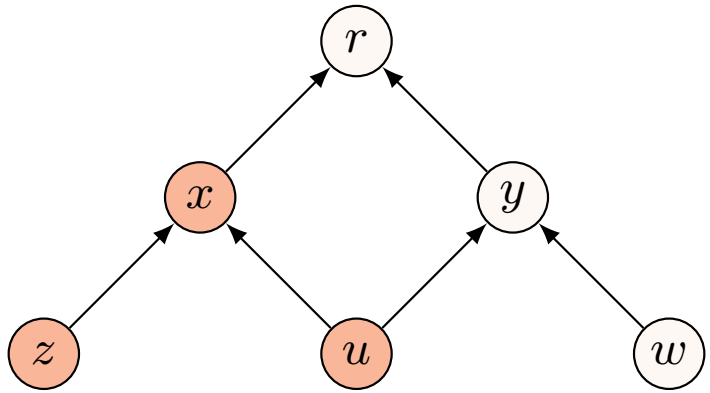
- $(\neg r)$;

Pebbling



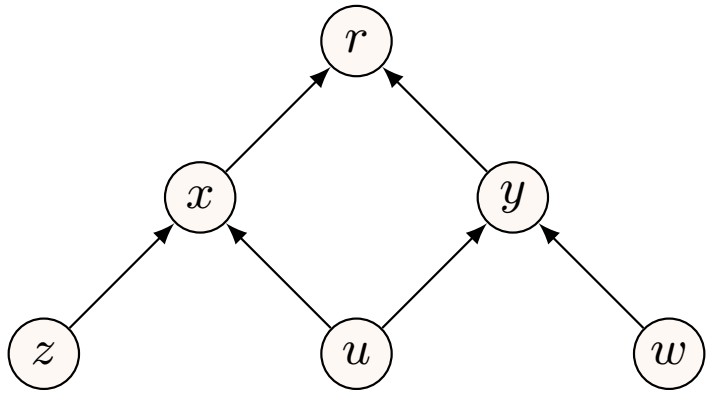
- $(\neg r)$;
- $(z), (u), (w)$;

Pebbling



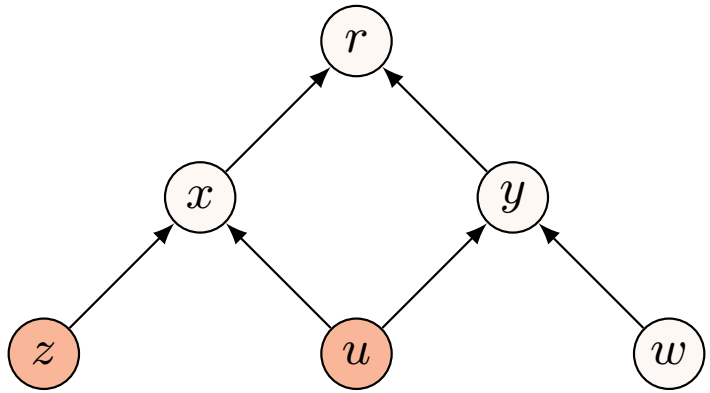
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x), (\neg w \vee \neg u \vee y), (\neg x \vee \neg y \vee r)$.

Pebbling



- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x), (\neg w \vee \neg u \vee y), (\neg x \vee \neg y \vee r)$.

Pebbling



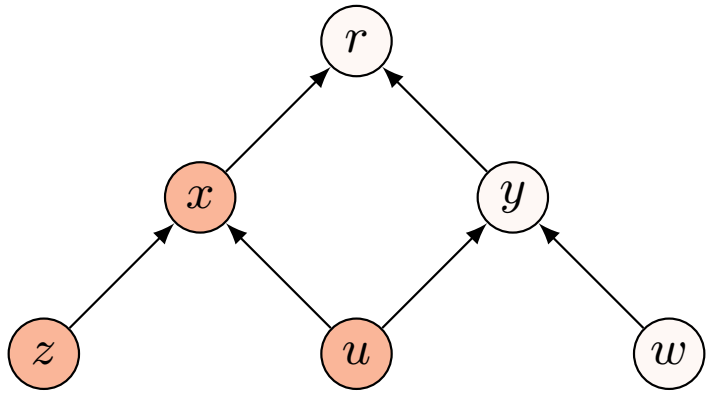
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x), (\neg w \vee \neg u \vee y), (\neg x \vee \neg y \vee r)$.

u

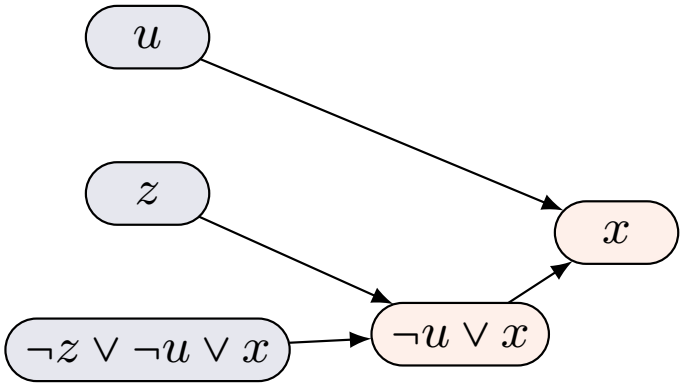
z

$\neg z \vee \neg u \vee x$

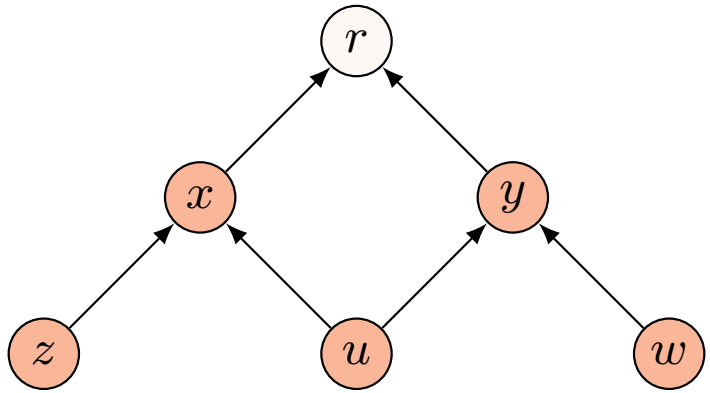
Pebbling



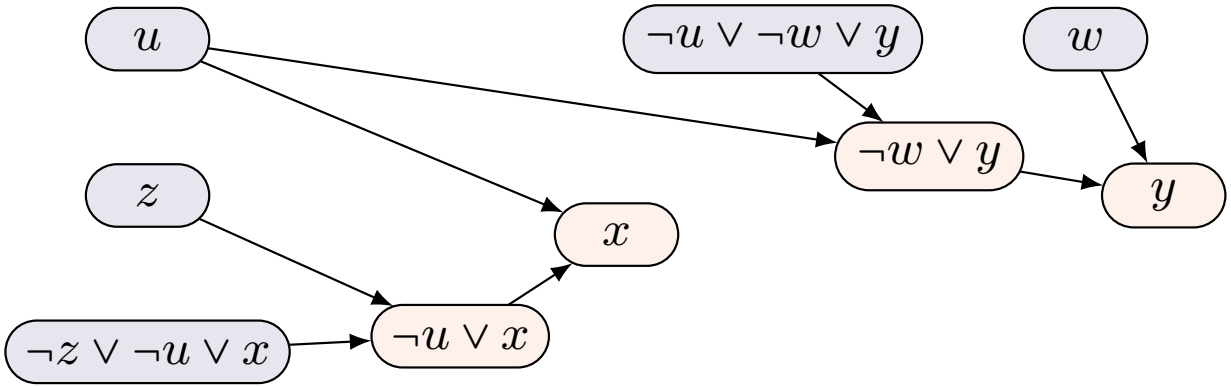
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x), (\neg w \vee \neg u \vee y), (\neg x \vee \neg y \vee r)$.



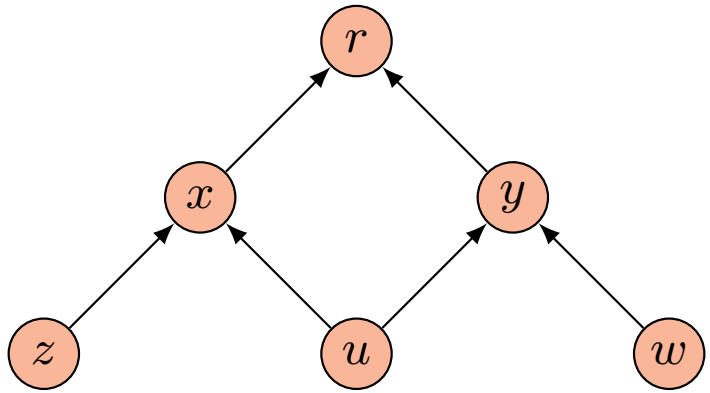
Pebbling



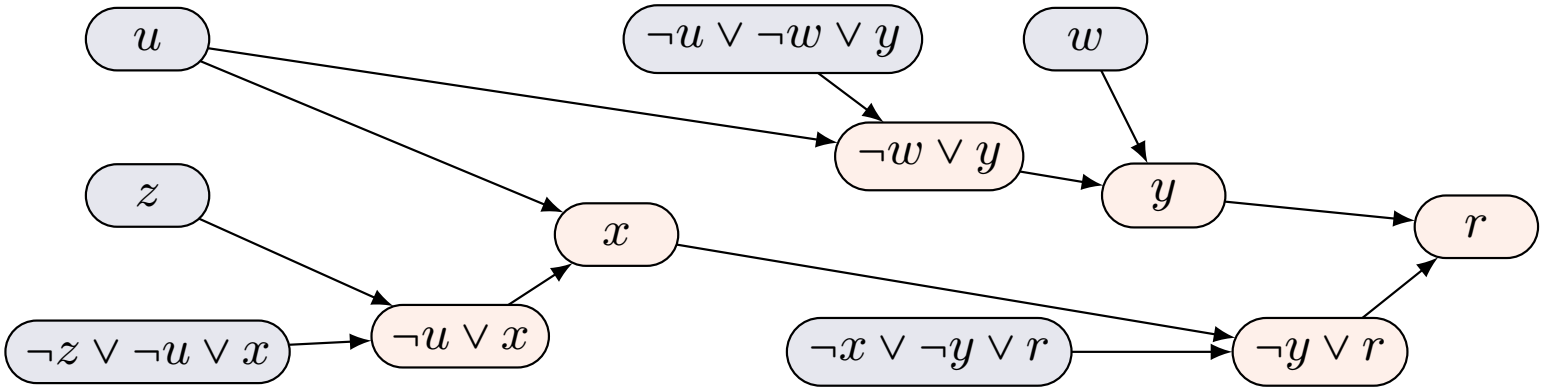
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x), (\neg w \vee \neg u \vee y), (\neg x \vee \neg y \vee r)$.



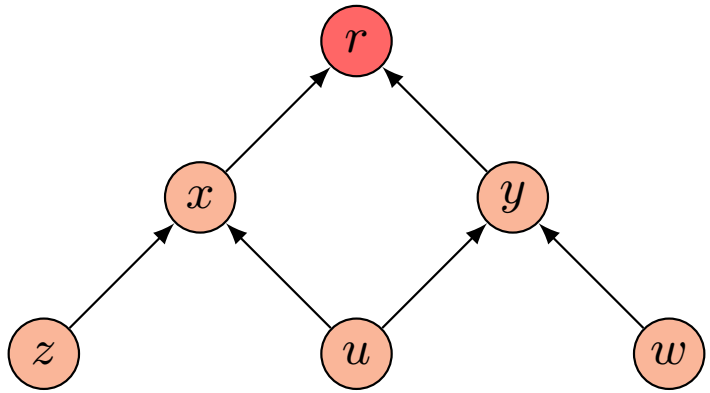
Pebbling



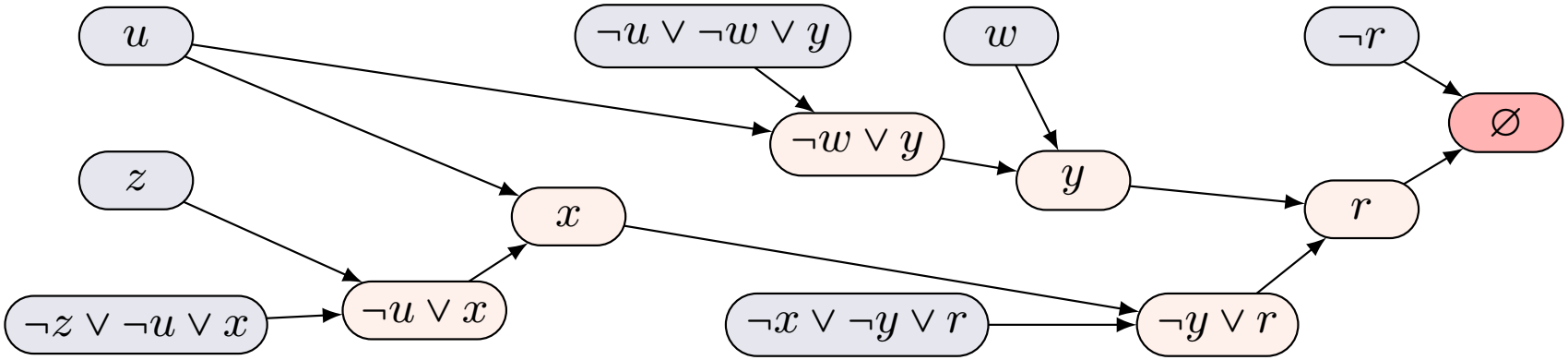
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x), (\neg w \vee \neg u \vee y), (\neg x \vee \neg y \vee r)$.



Pebbling



- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x), (\neg w \vee \neg u \vee y), (\neg x \vee \neg y \vee r)$.



Принцип Дирихле (Pigeonhole Principle), PHP_n^m

Переменные: $x_{i,j}$, $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$.

Принцип Дирихле (Pigeonhole Principle), PHP_n^m

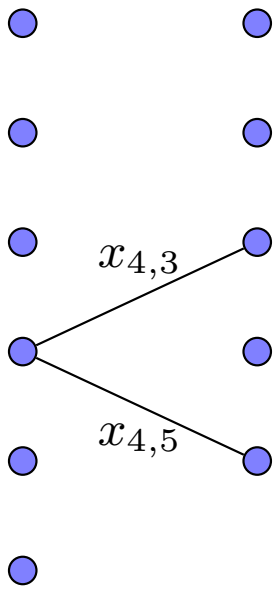
Переменные: $x_{i,j}$, $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$.

- $\bigvee_{j=1}^{n} x_{i,j}$;
- $\neg x_{i,j} \vee \neg x_{i',j}$.

Принцип Дирихле (Pigeonhole Principle), PHP_n^m

Переменные: $x_{i,j}$, $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$.

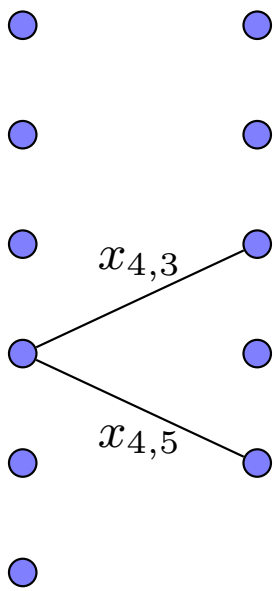
- $\bigvee_{j=1}^{n} x_{i,j}$;
- $\neg x_{i,j} \vee \neg x_{i',j}$.



Принцип Дирихле (Pigeonhole Principle), PHP_n^m

Переменные: $x_{i,j}$, $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$.

- $\bigvee_{j=1}^{n} x_{i,j}$;
- $\neg x_{i,j} \vee \neg x_{i',j}$.



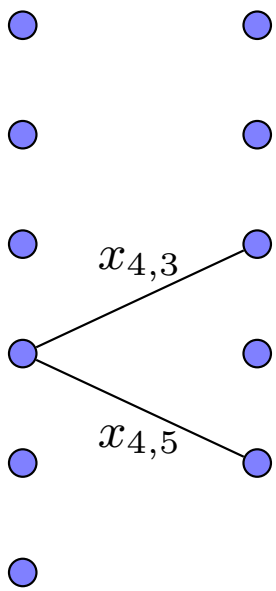
Теорема[Haken 85]

Любое резолюционное доказательство PHP_n^{n+1} имеет размер $2^{\Omega(n)}$.

Принцип Дирихле (Pigeonhole Principle), PHP_n^m

Переменные: $x_{i,j}$, $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$.

- $\bigvee_{j=1}^{n} x_{i,j}$;
- $\neg x_{i,j} \vee \neg x_{i',j}$.



Теорема[Haken 85]

Любое резолюционное доказательство PHP_n^{n+1} имеет размер $2^{\Omega(n)}$.

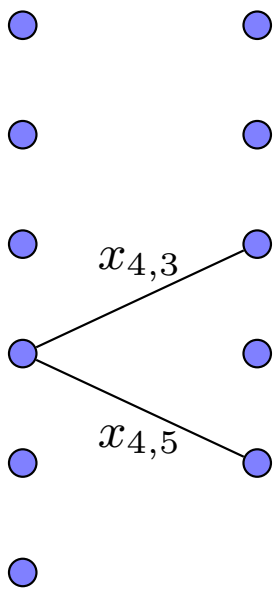
Теорема[Raz 04; Razborov 03]

Любое резолюционное доказательство PHP_n^{∞} имеет размер $2^{\Omega(n^{1/3})}$.

Принцип Дирихле (Pigeonhole Principle), PHP_n^m

Переменные: $x_{i,j}$, $i \in \{1, 2, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$.

- $\bigvee_{j=1}^{n} x_{i,j}$;
- $\neg x_{i,j} \vee \neg x_{i',j}$.

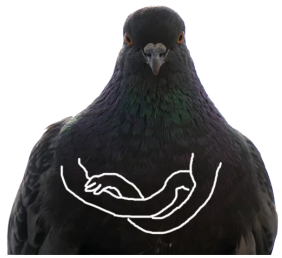


Теорема[Haken 85]

Любое резолюционное доказательство PHP_n^{n+1} имеет размер $2^{\Omega(n)}$.

Теорема[Raz 04; Razborov 03]

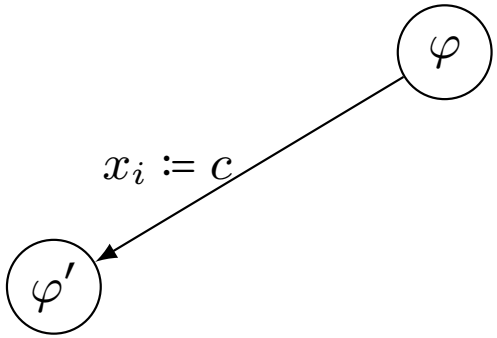
Любое резолюционное доказательство PHP_n^{∞} имеет размер $2^{\Omega(n^{1/3})}$.



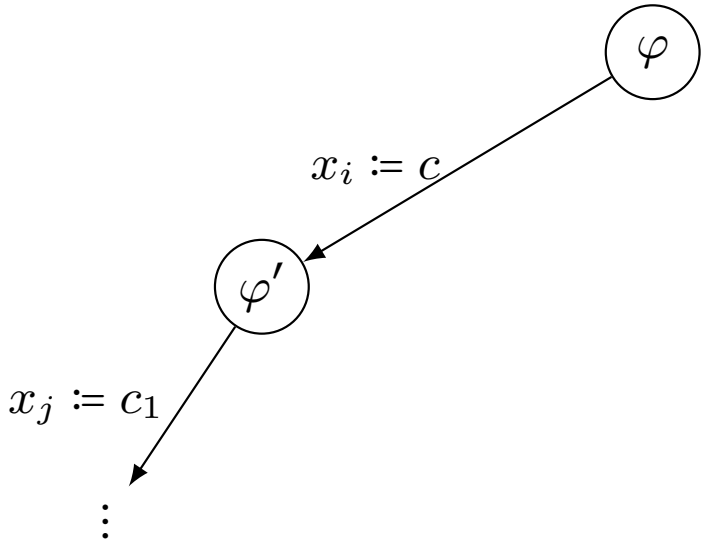
Открытый вопрос: улучшить нижнюю оценку на размер доказательств PHP_n^{∞} до $2^{\Omega(n^{1/2})}$.

DPLL **алгоритмы**

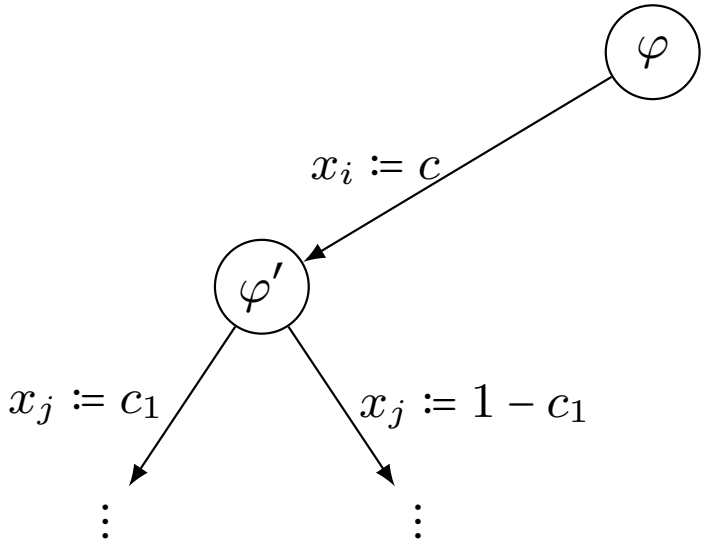
DPLL **алгоритмы**



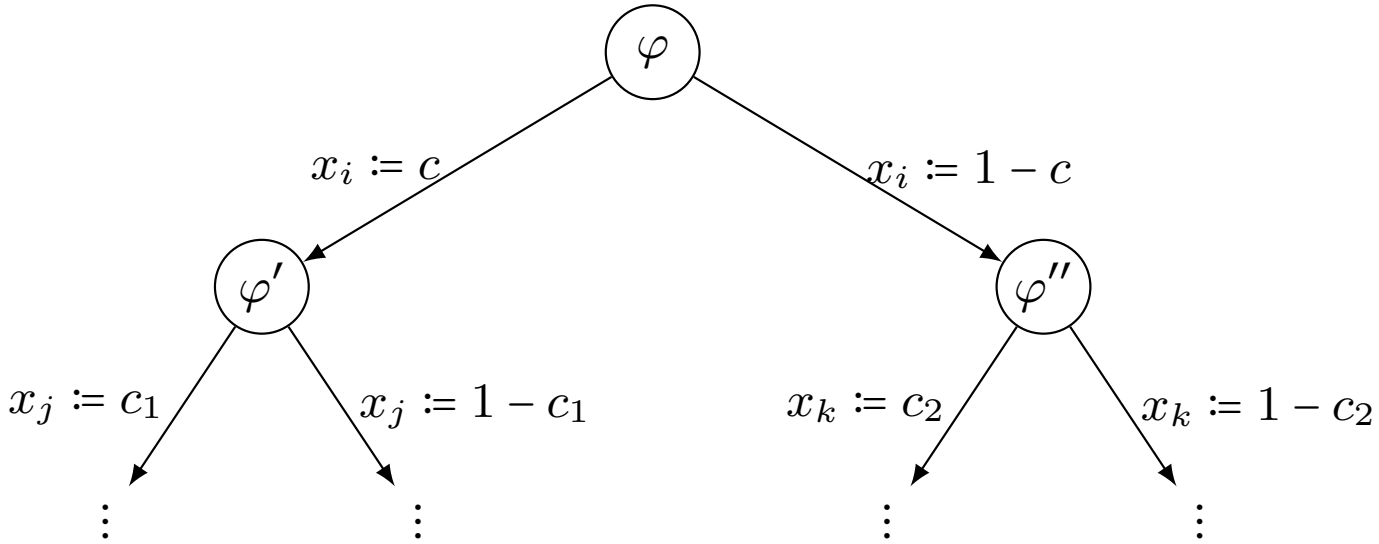
DPLL **алгоритмы**



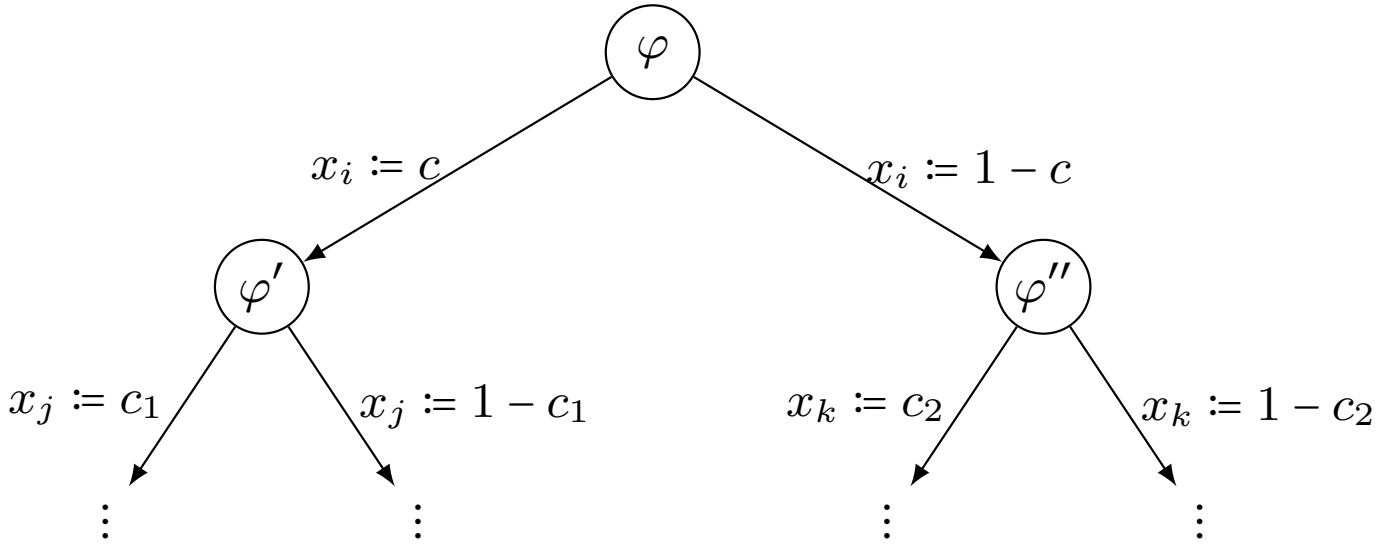
DPLL **алгоритмы**



DPLL **алгоритмы**

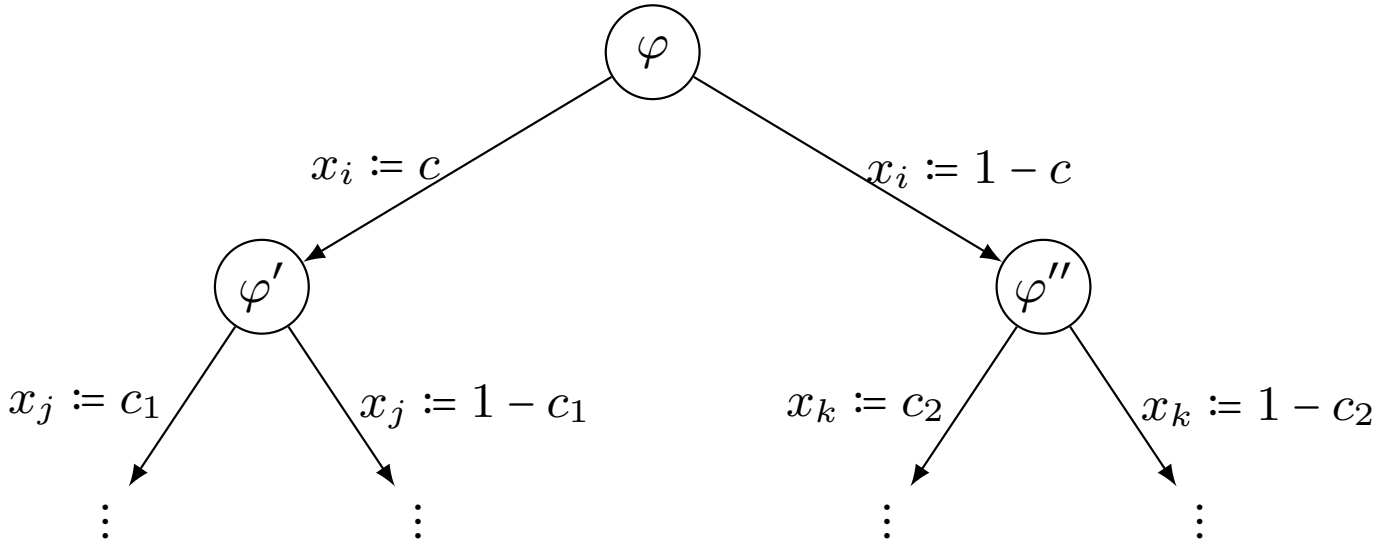


DPLL **алгоритмы**



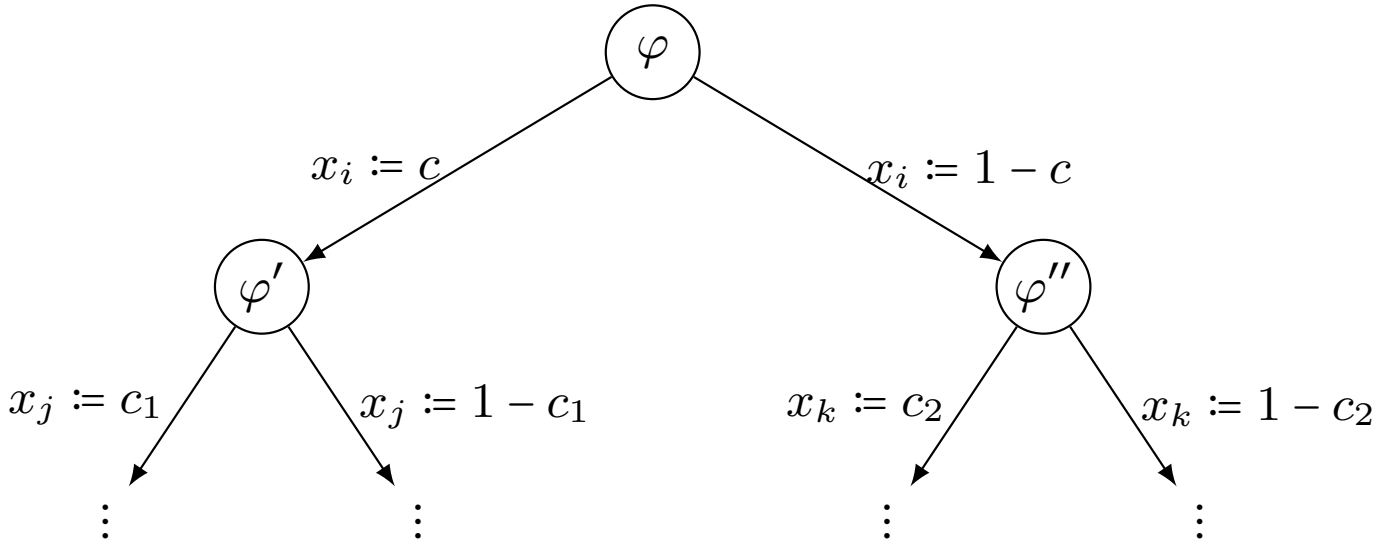
- Эвристика **A** выбирает переменную для расщепления.

DPLL **алгоритмы**



- Эвристика **A** выбирает переменную для расщепления.
- Эвристика **B** выбирает значения.

DPLL **алгоритмы**



- Эвристика **A** выбирает переменную для расщепления.
- Эвристика **B** выбирает значения.
- Правила упрощения: предположим, что их нет.

DPLL и резолюция

Теорема

DPLL алгоритм делает t расщеплений на невыполнимой формуле

$$\varphi := \bigvee_i C_i$$

$\Rightarrow$ существует резолюционное доказательство φ размера $2t$.

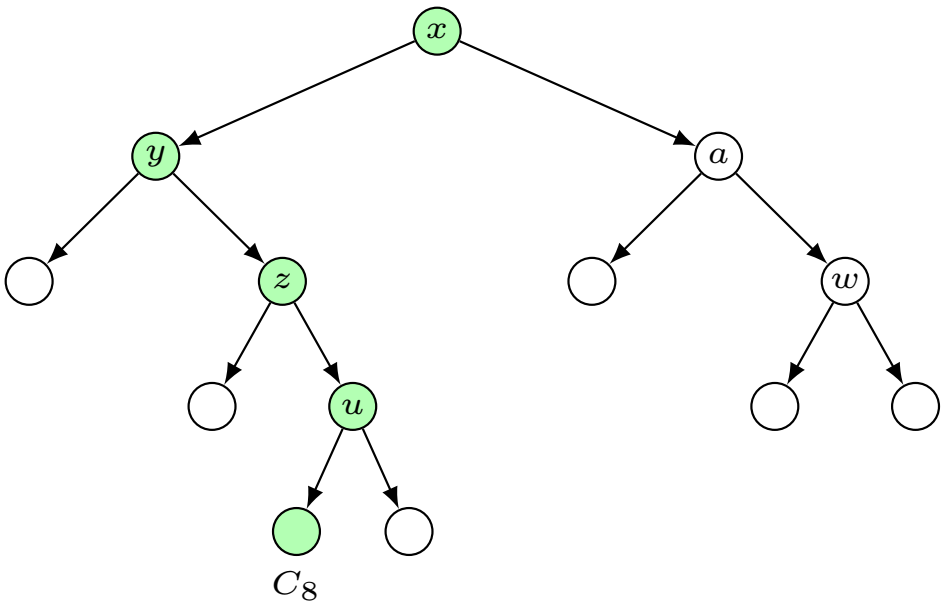
DPLL **и резолюция**

Теорема

DPLL алгоритм делает t расщеплений на невыполнимой формуле

$$\varphi := \bigvee_i C_i$$

$\Rightarrow$ существует резолюционное доказательство φ размера $2t$.



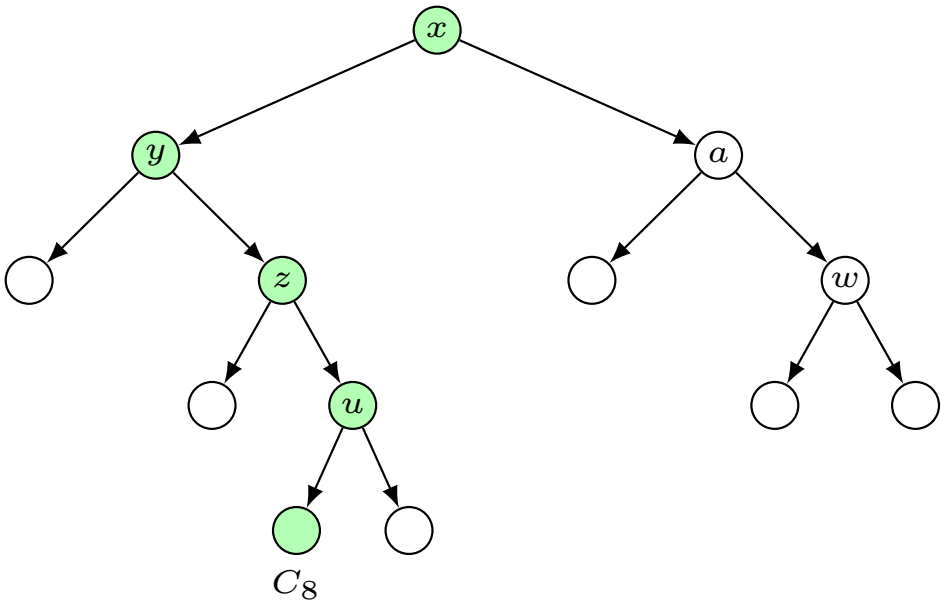
DPLL и резолюция

Теорема

DPLL алгоритм делает t расщеплений на невыполнимой формуле

$$\varphi := \bigvee_i C_i$$

$\Rightarrow$ существует резолюционное доказательство φ размера $2t$.



$$\frac{A \vee x \quad B \vee \neg x}{A \vee B} \qquad \frac{A}{A \vee z}$$

- Вершина $\Rightarrow$ дизъюнкция отраций запросов.
- $(x \vee \neg y \vee \neg z \vee u)$.

Следствия

- [Следствие из Haken 85] DPLL алгоритмы будут работать не менее $2^{\Omega(n)}$ шагов на формулах PHP_n^{n+1}.

Следствия

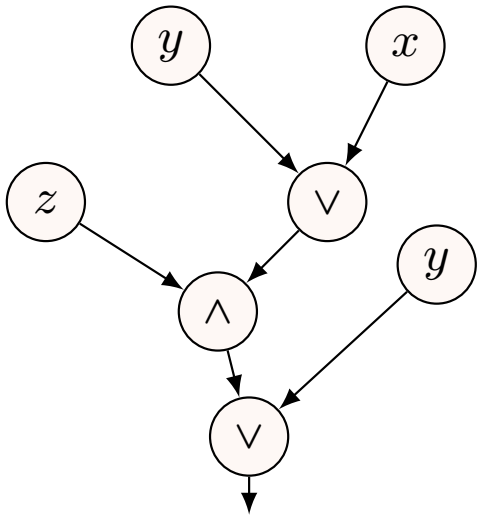
- [Следствие из Haken 85] DPLL алгоритмы будут работать не менее $2^{\Omega(n)}$ шагов на формулах PHP_n^{n+1}.
- [Алехнович, Гирш, Ицыксон 05; неформально] На выполнимых формулах «ограниченные» DPLL алгоритмы требуют экспоненциального времени.

Следствия

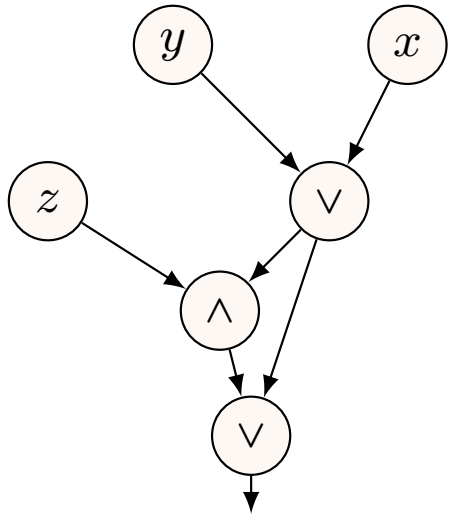
- [Следствие из Haken 85] DPLL алгоритмы будут работать не менее $2^{\Omega(n)}$ шагов на формулах PHP_n^{n+1}.
- [Алехнович, Гирш, Ицыксон 05; неформально] На выполнимых формулах «ограниченные» DPLL алгоритмы требуют экспоненциального времени.
- [Ицыксон, С 11; неформально] «В среднем» на выполнимых формулах «ограниченные» DPLL алгоритмы требуют экспоненциального времени.

Монотонные вычисления

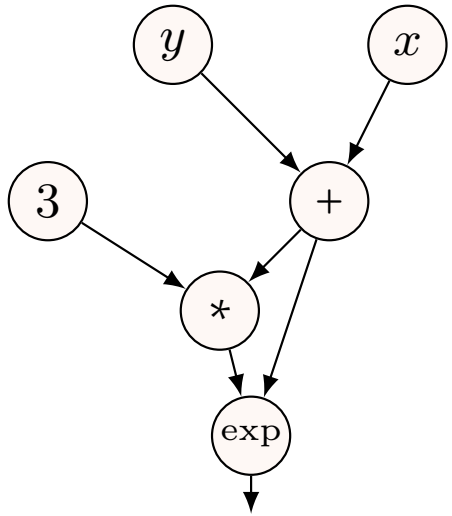
Формулы



Схемы

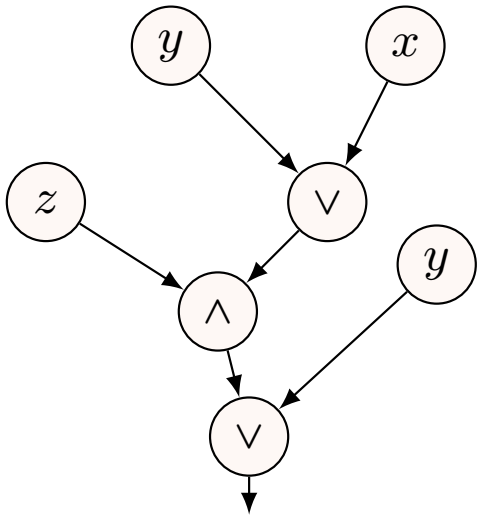


Еще схемы

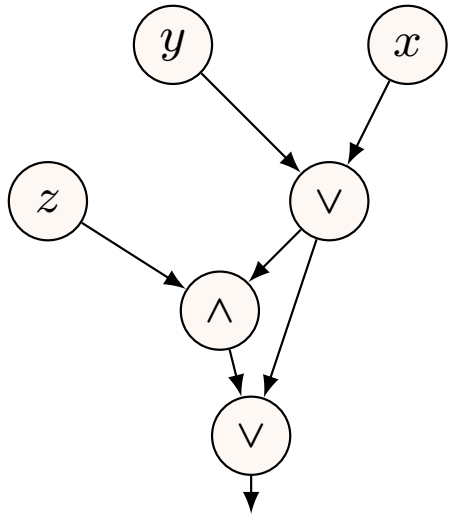


Монотонные вычисления

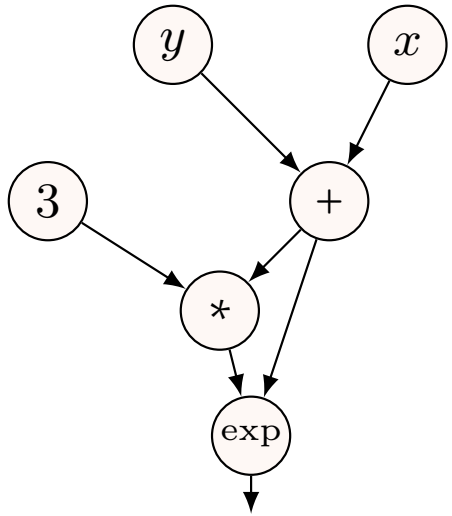
Формулы



Схемы



Еще схемы

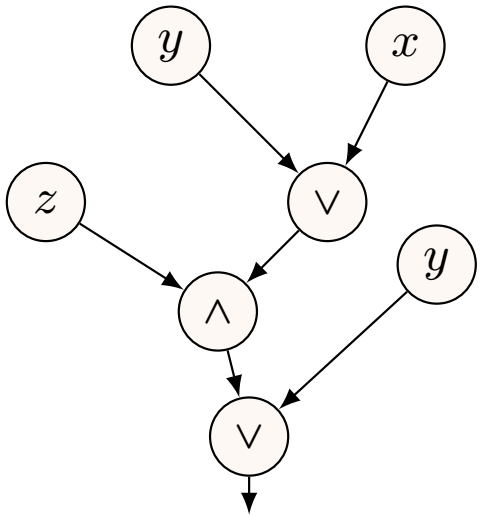


Почему монотонные вычисления это важно?

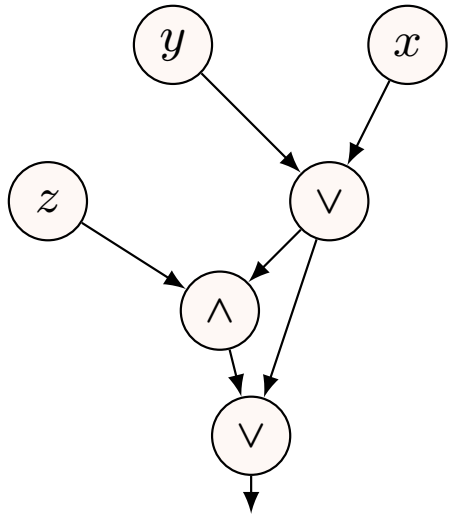
- У нас получается что-то доказать ([Разборов 85; Alon, Boppana 87] Функция клики в графе на n вершинах требует монотонных схем размера $2^{\Omega(n^{1/4})}$)!

Монотонные вычисления

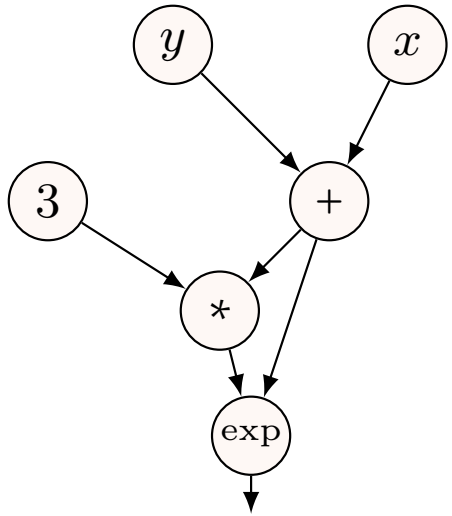
Формулы



Схемы



Еще схемы

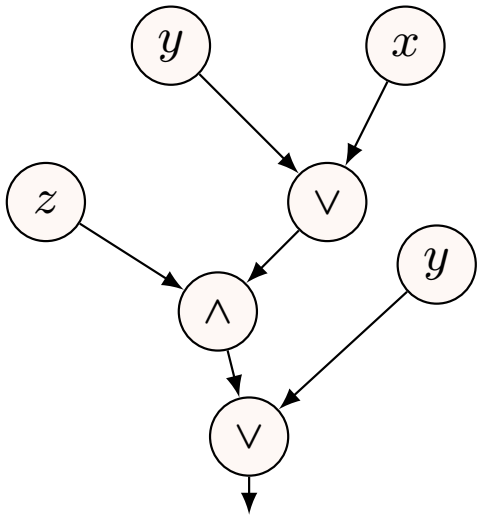


Почему монотонные вычисления это важно?

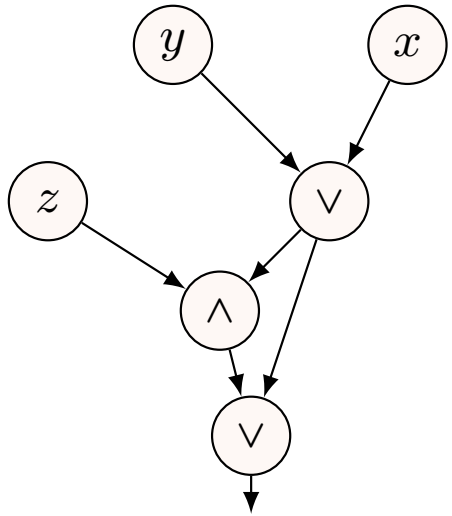
- У нас получается что-то доказать ([Разборов 85; Alon, Boppana 87] Функция клики в графе на n вершинах требует монотонных схем размера $2^{\Omega(n^{1/4})}$)!
- Монотонные вычисления дают контроль над погрешностью вычислений.

Монотонные вычисления

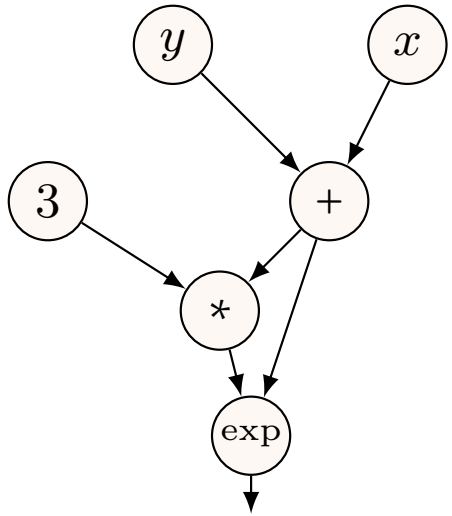
Формулы



Схемы



Еще схемы

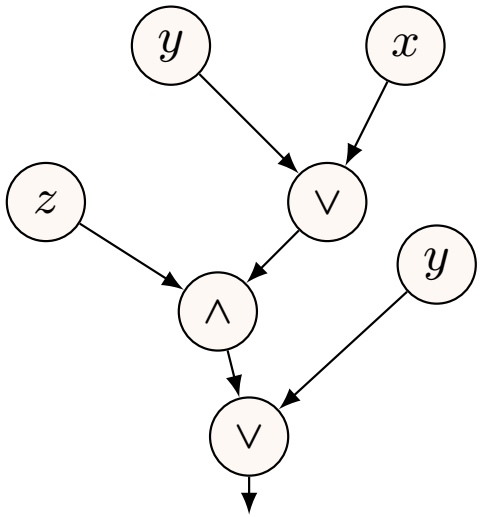


Почему монотонные вычисления это важно?

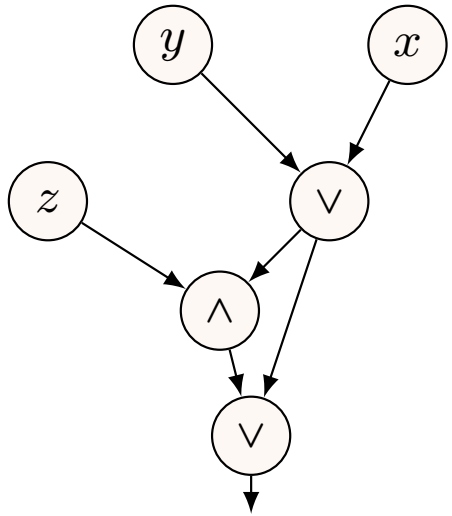
- У нас получается что-то доказать ([Разборов 85; Alon, Boppana 87] Функция клики в графе на n вершинах требует монотонных схем размера $2^{\Omega(n^{1/4})}$)!
- Монотонные вычисления дают контроль над погрешностью вычислений.
- Сильные нижние оценки на монотонные схемы $\Rightarrow$ нижние оценки на общие схемы.

Монотонные вычисления

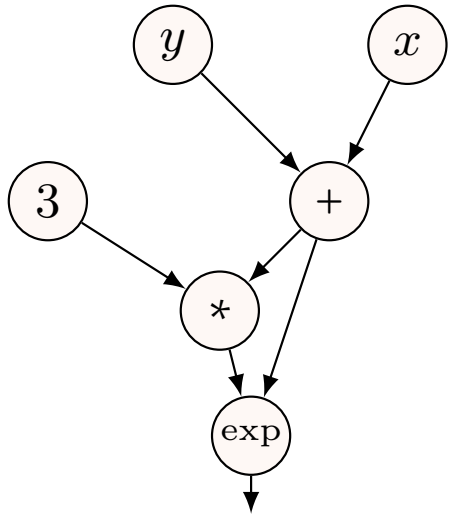
Формулы



Схемы



Еще схемы



Почему монотонные вычисления это важно?

- У нас получается что-то доказать ([Разборов 85; Alon, Boppana 87] Функция клики в графе на n вершинах требует монотонных схем размера $2^{\Omega(n^{1/4})}$)!
- Монотонные вычисления дают контроль над погрешностью вычислений.
- Сильные нижние оценки на монотонные схемы $\Rightarrow$ нижние оценки на общие схемы.
- Протоколы разделения секрета/криптография.

«Лифтинг» 

«Слабые» системы доказательств простая модель, а схемы «сложная».

«Лифтинг»

«Слабые» системы доказательств простая модель, а схемы «сложная».

Теорема[Raz, McKenzie 99; Göös, Pitassi, Watson 16]

Формула φ сложна для «древесной» резолюции $\Rightarrow$ функция F_φ сложна для монотонных формул.

Следствие: нижния оценка на монотонные формулы 2^{n^ε}.

«Лифтинг»

«Слабые» системы доказательств простая модель, а схемы «сложная».

Теорема[Raz, McKenzie 99; Göös, Pitassi, Watson 16]

Формула φ сложна для «древесной» резолюции $\Rightarrow$ функция F_φ сложна для монотонных формул.

Следствие: нижния оценка на монотонные формулы 2^{n^ε}.

Теорема[Garg, Göös, Kamath, S 18]

Формула φ сложна для резолюции $\Rightarrow$ функция F_φ сложна для монотонных схем.

Следствие: нижния оценка на монотонные схемы 2^{n^ε}.

«Лифтинг»

«Слабые» системы доказательств простая модель, а схемы «сложная».

Теорема[Raz, McKenzie 99; Göös, Pitassi, Watson 16]

Формула φ сложна для «древесной» резолюции $\Rightarrow$ функция F_φ сложна для монотонных формул.

Следствие: нижния оценка на монотонные формулы 2^{n^ε}.

Теорема[Garg, Göös, Kamath, S 18]

Формула φ сложна для резолюции $\Rightarrow$ функция F_φ сложна для монотонных схем.

Следствие: нижния оценка на монотонные схемы 2^{n^ε}.

Теорема[Pitassi, Robere 16; Robere, Pitassi 18]

Nullstellensatz $\Leftrightarrow$ функция F_φ сложна для монотонных «span programs».

Формулы и функции

Формулы и функции

- $\varphi(x) \coloneqq \bigvee C_j$ — формула от n переменных;
- $g\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}$;

Формулы и функции

- $\varphi(x) \coloneqq \bigvee C_j$ — формула от n переменных;
- $g\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}$;
- $\varphi \circ g \coloneqq \varphi(g(y_1, z_1), g(y_2, z_2), g(y_3, z_3), \dots)$.

Формулы и функции

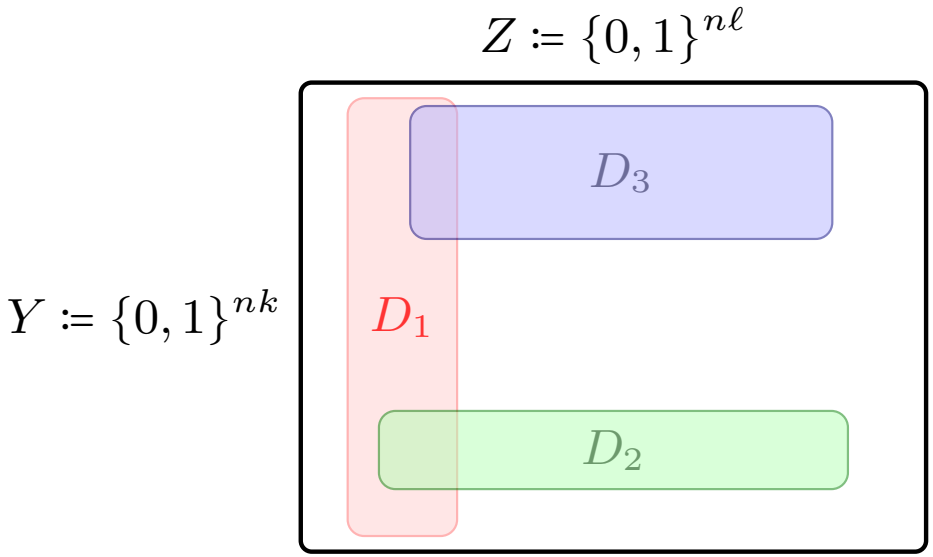
- $\varphi(x) \coloneqq \bigvee C_j$ — формула от n переменных;
- $g\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}$;
- $\varphi \circ g \coloneqq \varphi(g(y_1, z_1), g(y_2, z_2), g(y_3, z_3), \dots)$.

$\psi(y, z) \coloneqq \varphi \circ g = \bigvee\limits_{j=1}^{m} D_j$, определим функцию $F_\psi\colon \{0,1\}^m \to \{0,1\}$.

Формулы и функции

- $\varphi(x) \coloneqq \bigvee C_j$ — формула от n переменных;
- $g\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}$;
- $\varphi \circ g \coloneqq \varphi(g(y_1, z_1), g(y_2, z_2), g(y_3, z_3), \dots)$.

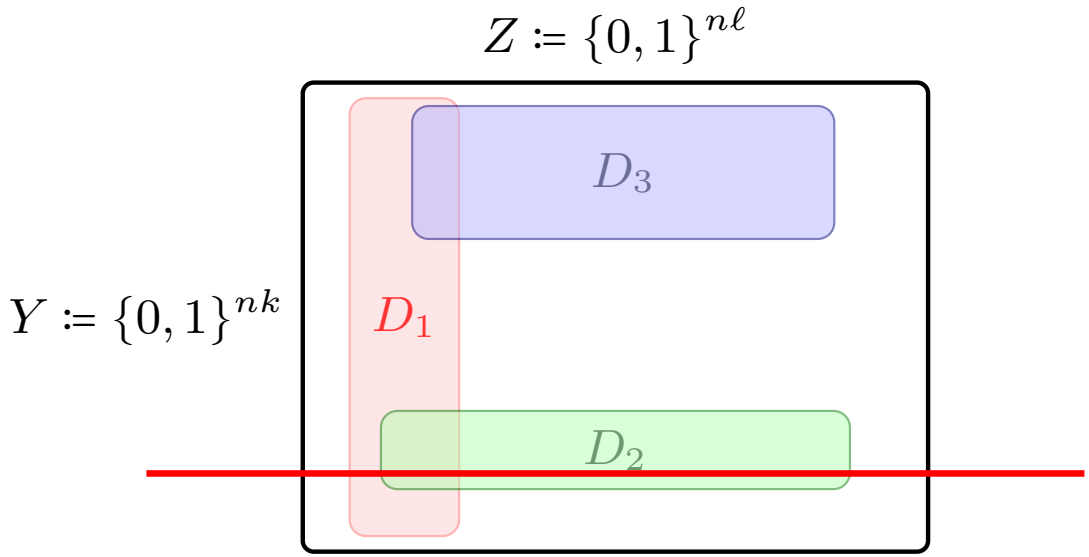
$\psi(y,z) \coloneqq \varphi \circ g = \bigvee\limits_{j=1}^{m} D_j$, определим функцию $F_\psi\colon \{0,1\}^m \to \{0,1\}$.



Формулы и функции

- $\varphi(x) \coloneqq \bigvee C_j$ — формула от n переменных;
- $g\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}$;
- $\varphi \circ g \coloneqq \varphi(g(y_1, z_1), g(y_2, z_2), g(y_3, z_3), \dots)$.

$\psi(y,z) \coloneqq \varphi \circ g = \bigvee\limits_{j=1}^{m} D_j$, определим функцию $F_\psi\colon \{0,1\}^m \to \{0,1\}$.

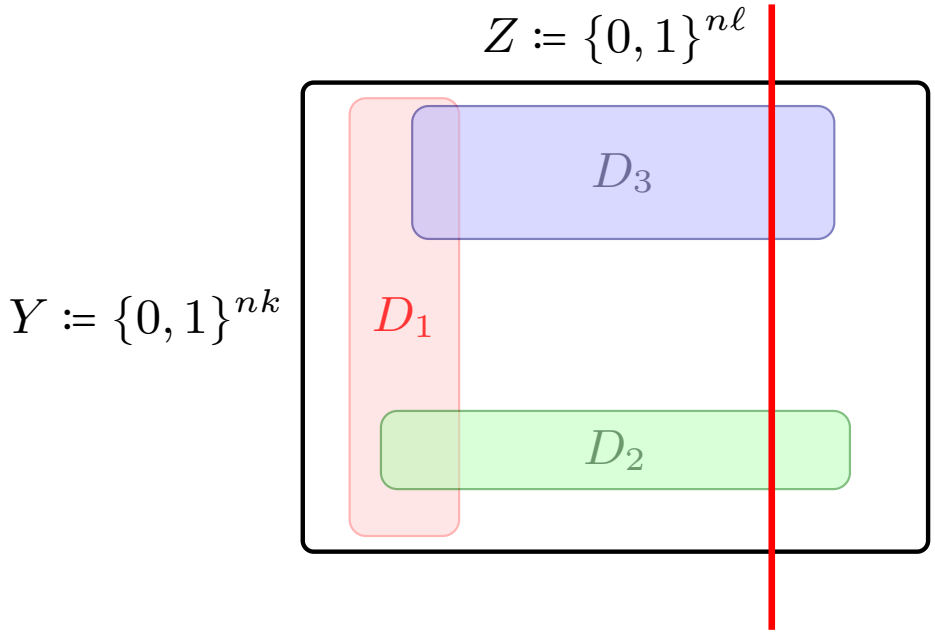


$F_\psi(1,1,0,\dots) \coloneqq 1$

Формулы и функции

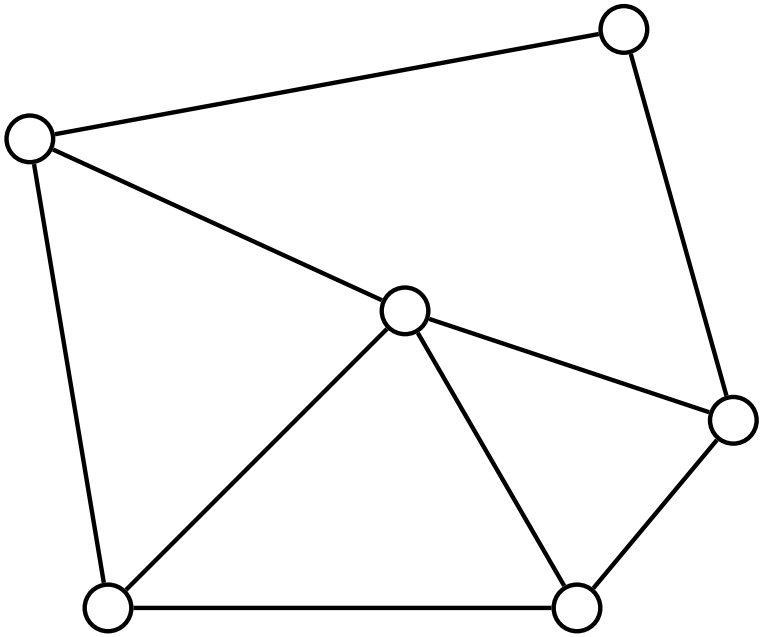
- $\varphi(x) \coloneqq \bigvee C_j$ — формула от n переменных;
- $g\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}$;
- $\varphi \circ g \coloneqq \varphi(g(y_1, z_1), g(y_2, z_2), g(y_3, z_3), \dots)$.

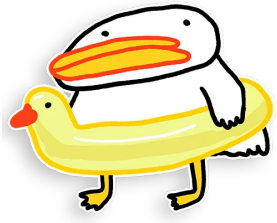
$\psi(y,z) \coloneqq \varphi \circ g = \bigvee\limits_{j=1}^{m} D_j$, определим функцию $F_\psi\colon \{0,1\}^m \to \{0,1\}$.



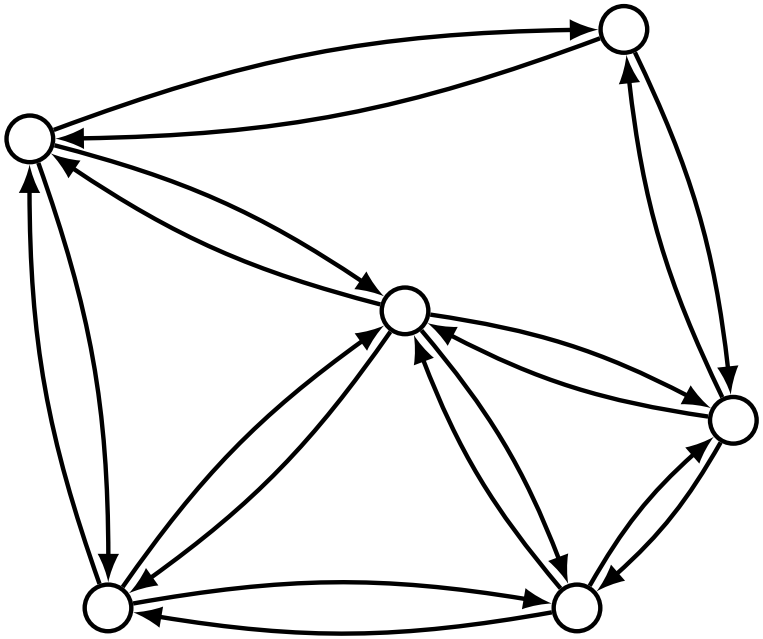
$F_\psi(1,1,0,\dots) \coloneqq 1, \quad F_\psi(1,0,0,\dots) \coloneqq 0$

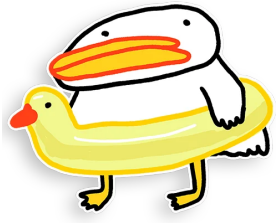
Простые функции?



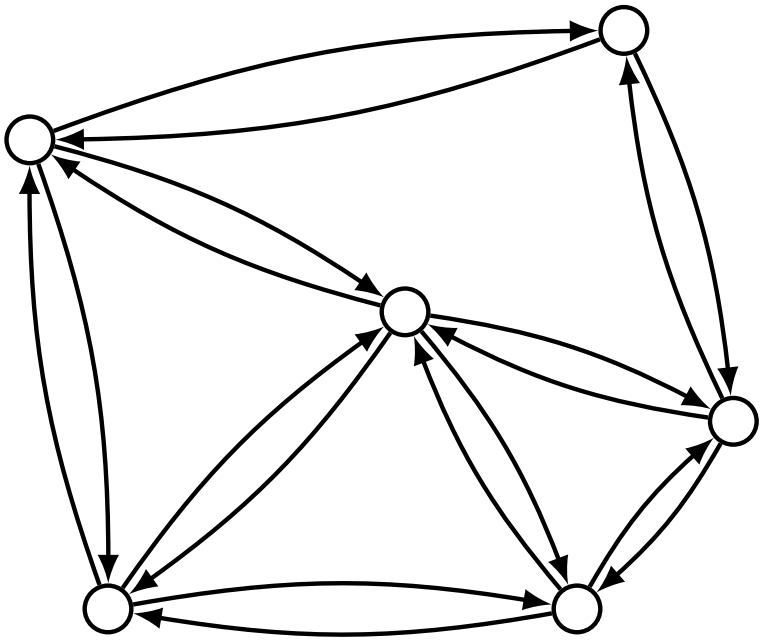


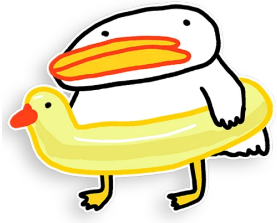
Простые функции?





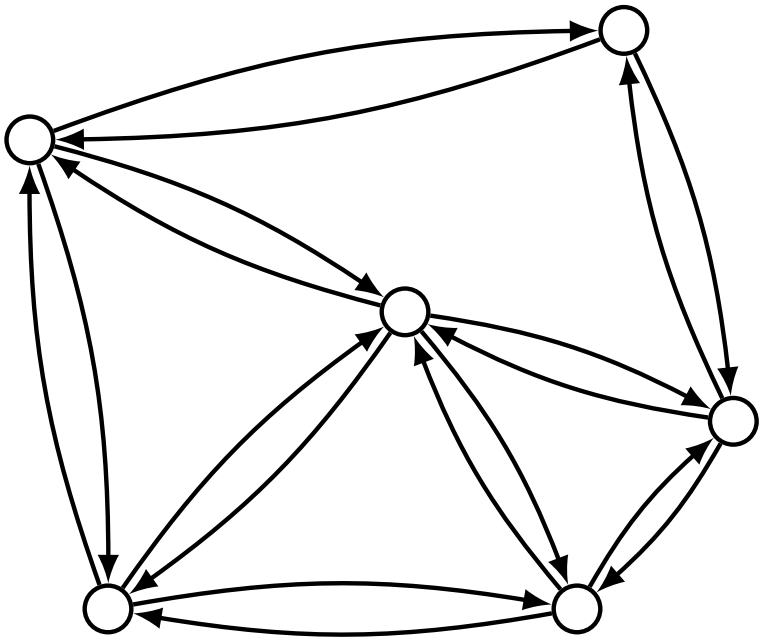
Простые функции?

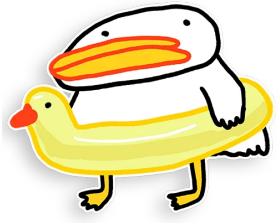




- v: $\sum\limits_{e \in E_v^{\text{in}}} x_e - \sum\limits_{e \in E_v^{\text{out}}} x_e = c(v)$ ($\mathbb{R}$);
- $\sum\limits_v c(v) = 1$ ($\mathbb{R}$);
- степень графа: d.

Простые функции?





- v: $\sum\limits_{e \in E_v^{\text{in}}} x_e - \sum\limits_{e \in E_v^{\text{out}}} x_e = c(v)$ ($\mathbb{R}$);
- $\sum\limits_v c(v) = 1$ ($\mathbb{R}$);
- степень графа: d.

- Flow эффективно доказывается в системе Nullstellensatz.
- [Alekhnovich, Razborov 03] Если G — (n, d, α)-экспандер $\Rightarrow$ любое резолюционное доказательство Flow имеет размер $2^{\Omega(n)}$.

Простые функции?

$f\colon \{0,1\}^{2n^3} \to \{0,1\}$

- Занумеруем равенства $z_i \oplus z_j \oplus z_k = c$ (не более $2n^3$ равенств);
- $x_i = 1 \Leftrightarrow$ добавляем равенство в систему;
- $f(x) = 1 \Leftrightarrow$ система несовместна.

Простые функции?

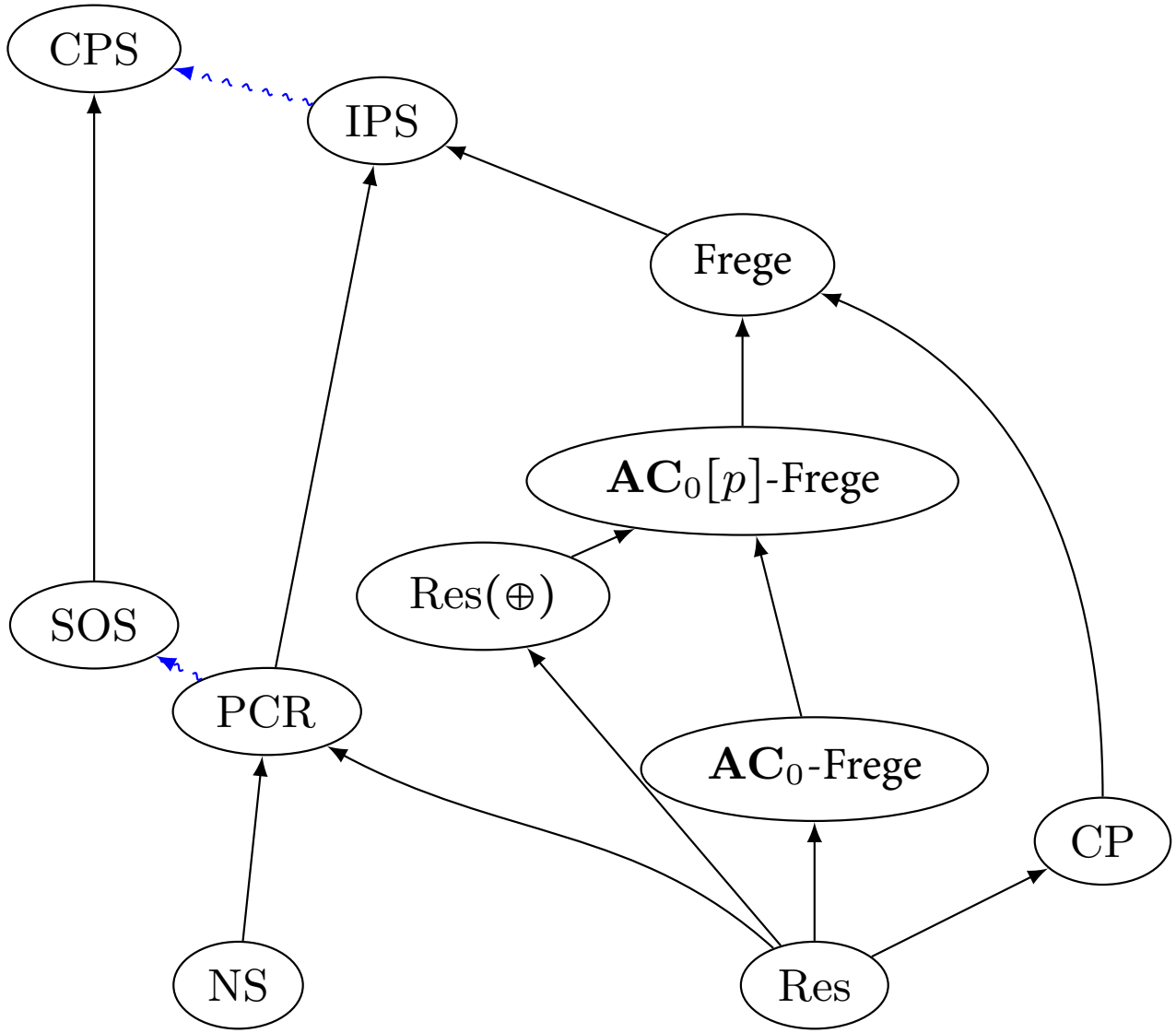
$f\colon \{0,1\}^{2n^3} \to \{0,1\}$

- Занумеруем равенства $z_i \oplus z_j \oplus z_k = c$ (не более $2n^3$ равенств);
- $x_i = 1 \Leftrightarrow$ добавляем равенство в систему;
- $f(x) = 1 \Leftrightarrow$ система несовместна.

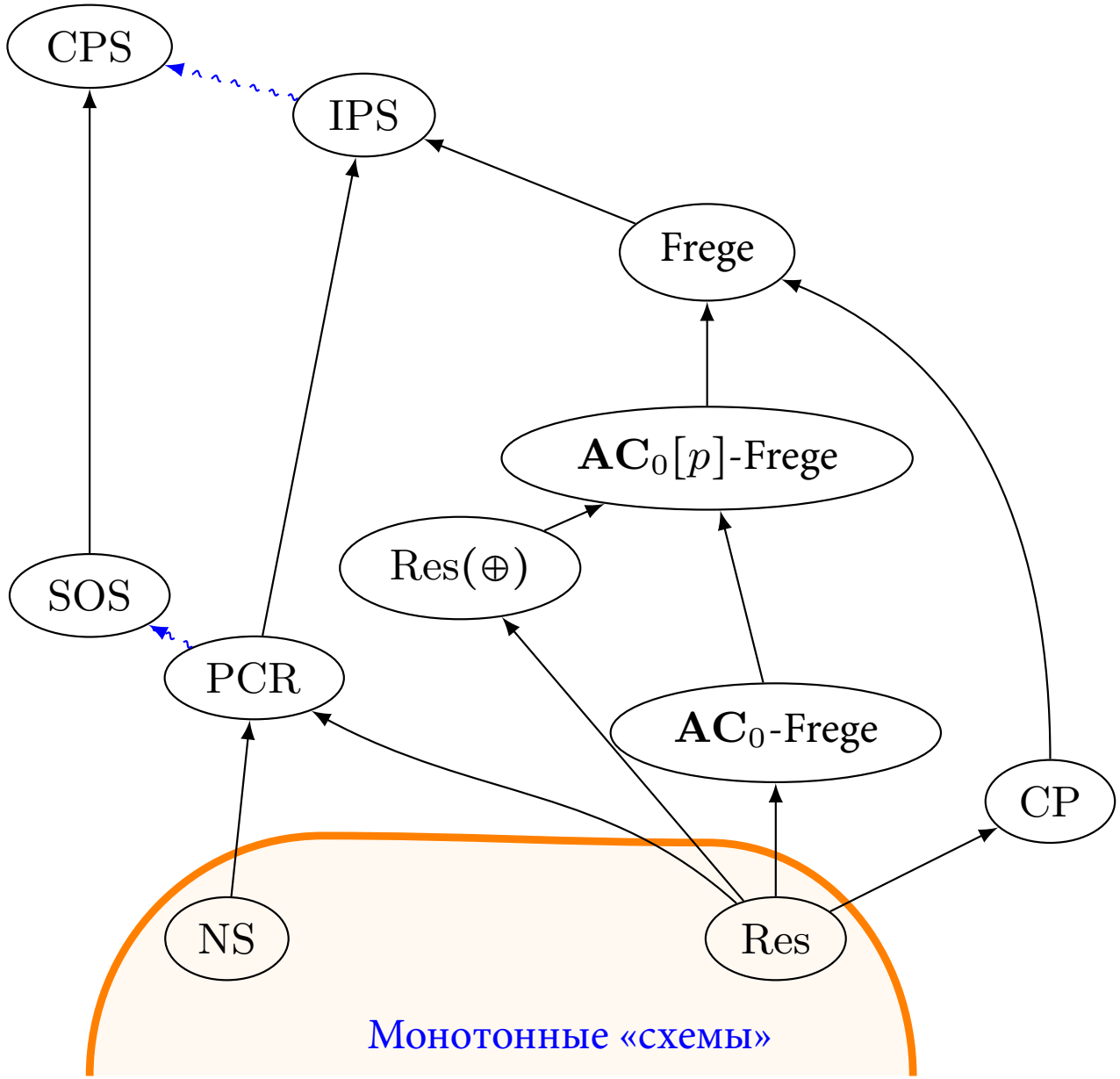
Факты о функции f:

- $f \in \mathbf{NC}^2$;
- F_{Flow} может быть вложена в f (поскольку есть эффективное Nullstellensatz доказательство Flow!);
- нет маленьких монотонных схем для f (поскольку нет эффективного резолюционного доказательства Flow).

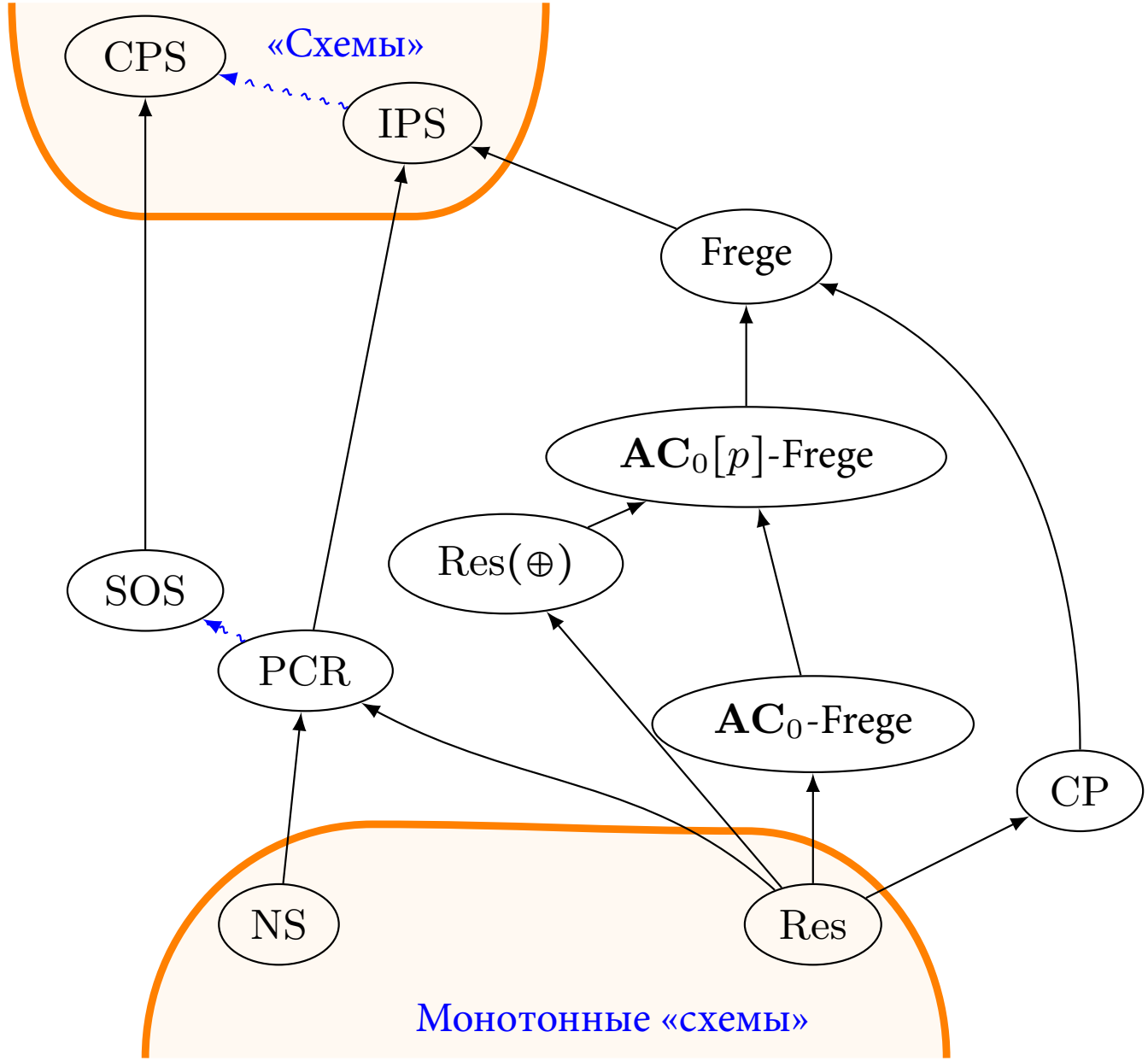
Иерархия


CPS
IPS
Frege
$\mathbf{AC}_0[p]$-Frege
Res($\oplus$)
SOS
PCR
$\mathbf{AC}_0$-Frege
CP
NS
Res

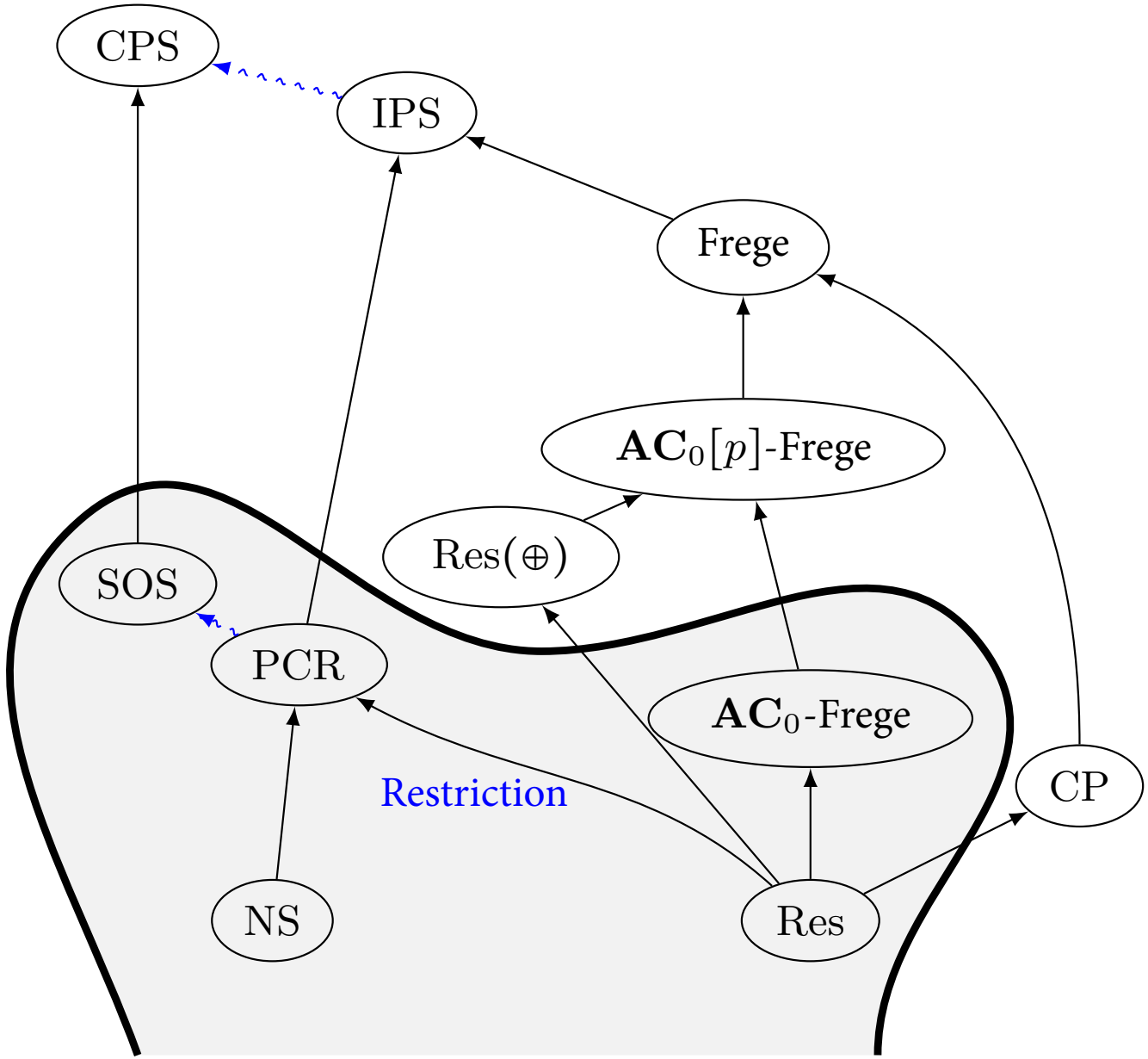
Иерархия


CPS
IPS
Frege
$\mathbf{AC}_0[p]$-Frege
Res(⊕)
SOS
PCR
$\mathbf{AC}_0$-Frege
CP
NS
Res
Монотонные «схемы»

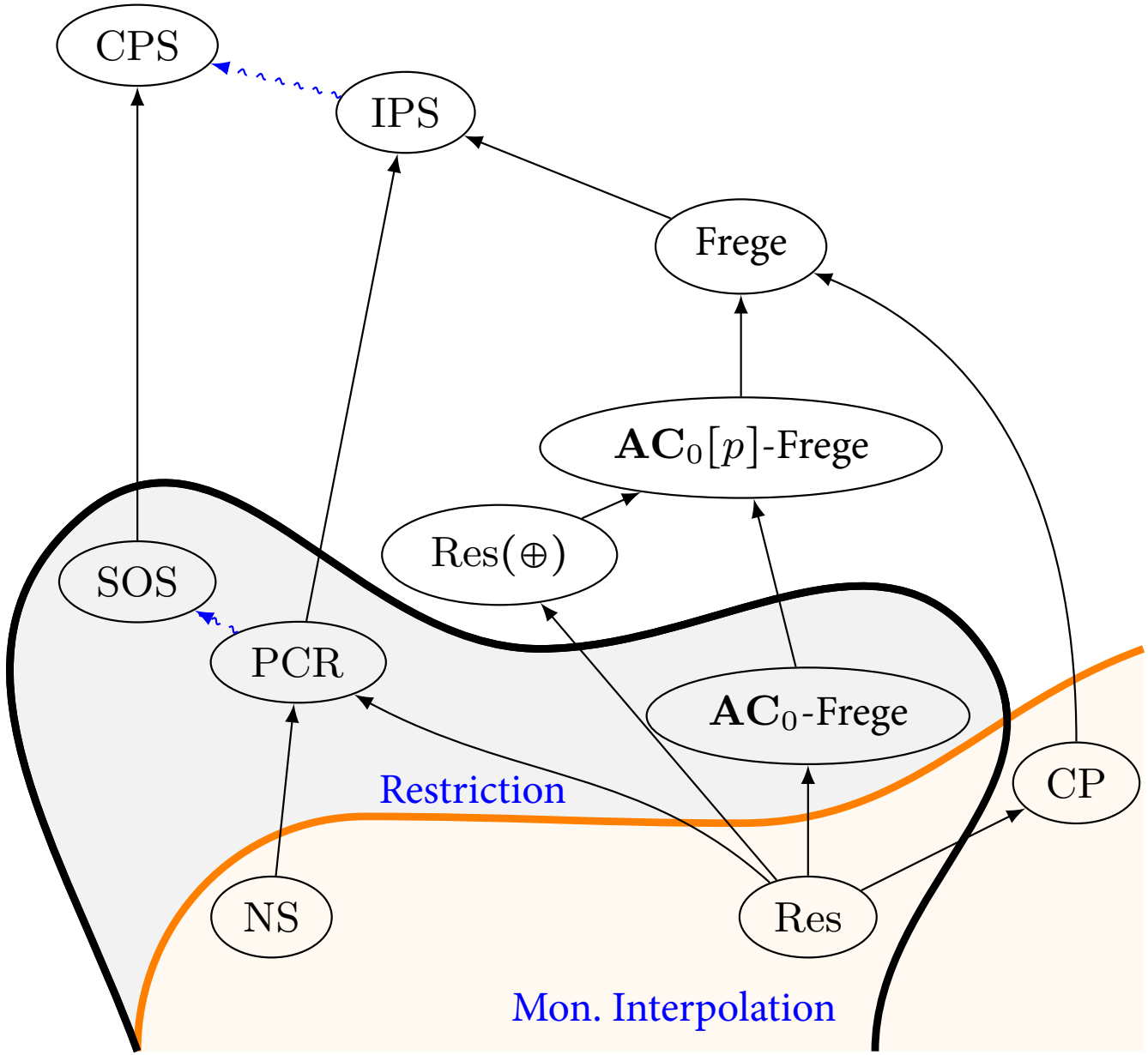
Иерархия


CPS
«Схемы»
IPS
Frege
$\mathbf{AC}_0[p]$-Frege
Res(⊕)
SOS
PCR
$\mathbf{AC}_0$-Frege
CP
NS
Res
Монотонные «схемы»

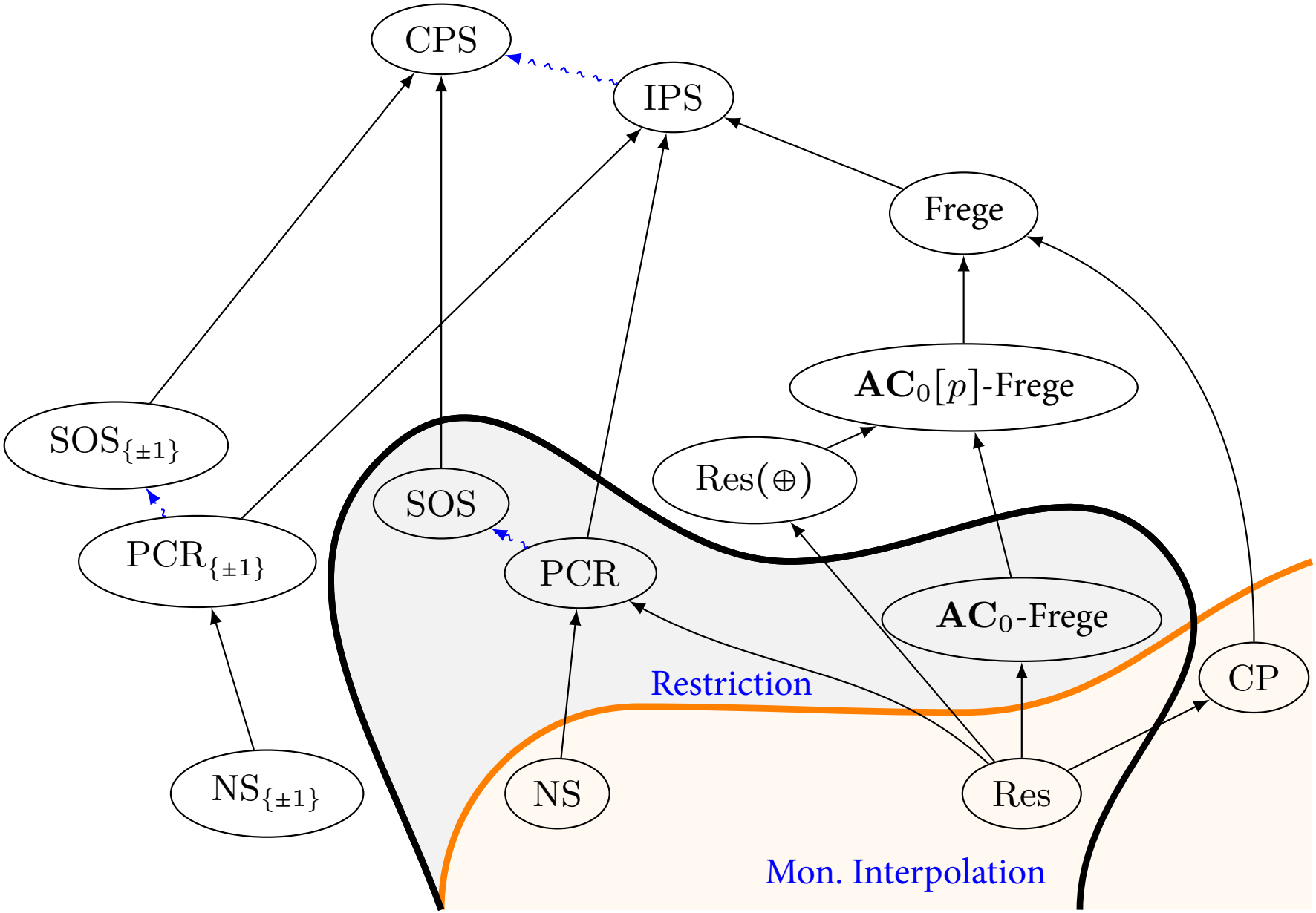
Иерархия


CPS
IPS
Frege
$\mathbf{AC}_0[p]$-Frege
Res(⊕)
SOS
PCR
$\mathbf{AC}_0$-Frege
CP
Restriction
NS
Res

Иерархия


CPS
IPS
Frege
$\mathbf{AC}_0[p]$-Frege
Res(⊕)
SOS
PCR
$\mathbf{AC}_0$-Frege
CP
Restriction
NS
Res
Mon. Interpolation

Иерархия


CPS
IPS
Frege
$\mathbf{AC}_0[p]$-Frege
$\mathrm{SOS}_{\{\pm1\}}$
Res($\oplus$)
SOS
$\mathrm{PCR}_{\{\pm1\}}$
PCR
$\mathbf{AC}_0$-Frege
Restriction
CP
$\mathrm{NS}_{\{\pm1\}}$
NS
Res
Mon. Interpolation

Иерархия

Mod_p

CPS

IPS

Frege

$\mathbf{AC}_0[p]$-Frege

$\mathrm{SOS}_{\{\pm 1\}}$

$\mathrm{Res}(\oplus)$

SOS

$\mathrm{PCR}_{\{\pm 1\}}$

PCR

$\mathbf{AC}_0$-Frege

Restriction

CP

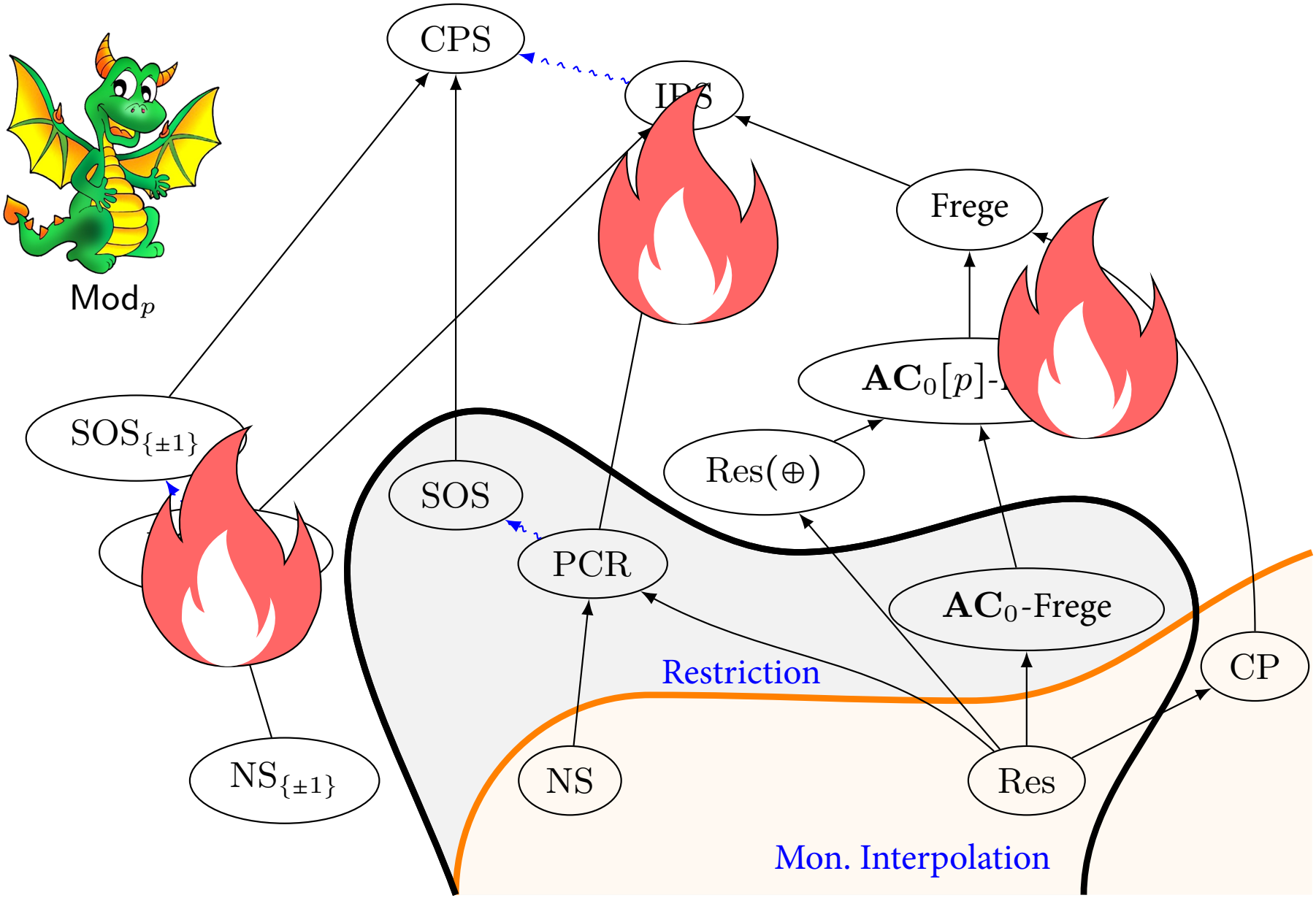
$\mathrm{NS}_{\{\pm 1\}}$

NS

Res

Mon. Interpolation

Иерархия


CPS
IPS
Frege
Mod$_p$
$\mathbf{AC}_0[p]$-
SOS$_{\{\pm1\}}$
Res($\oplus$)
SOS
PCR
$\mathbf{AC}_0$-Frege
Restriction
CP
NS$_{\{\pm1\}}$
NS
Res
Mon. Interpolation

Поиск доказательств

Система доказательств Π автоматизируема $\Rightarrow$ существует алгоритм A:

- $\varphi \in \mathsf{UNSAT}, A(\varphi) = w \Rightarrow \Pi(\varphi, w) = 1$;
- A полиномиален от $|\varphi|$ и $\min\limits_{|w'|}\{w' \mid \Pi(\varphi, w') = 1\}$.

Поиск доказательств

Система доказательств Π автоматизируема $\Rightarrow$ существует алгоритм A:

- $\varphi \in \mathsf{UNSAT}, A(\varphi) = w \Rightarrow \Pi(\varphi, w) = 1$;
- A полиномиален от $|\varphi|$ и $\min\limits_{|w'|}\{w' \mid \Pi(\varphi, w') = 1\}$.

Некоторые результаты:

- [Алехнович, Разборов 08] $\mathbf{FPT} \neq \mathsf{W}[1] \Rightarrow$ резолюция неавтоматизируема.

Поиск доказательств

Система доказательств Π автоматизируема $\Rightarrow$ существует алгоритм A:

- $\varphi \in \mathsf{UNSAT}, A(\varphi) = w \Rightarrow \Pi(\varphi, w) = 1$;
- A полиномиален от $|\varphi|$ и $\min\limits_{|w'|}\{w' \mid \Pi(\varphi, w') = 1\}$.

Некоторые результаты:

- [Алехнович, Разборов 08] $\mathbf{FPT} \neq \mathrm{W}[1] \Rightarrow$ резолюция неавтоматизируема.
- [Atserias, Müller 19] $\mathbf{P} \neq \mathbf{NP} \Rightarrow$ резолюция неавтоматизируема.

Поиск доказательств

Система доказательств Π автоматизируема $\Rightarrow$ существует алгоритм A:

- $\varphi \in \mathsf{UNSAT}, A(\varphi) = w \Rightarrow \Pi(\varphi, w) = 1$;
- A полиномиален от $|\varphi|$ и $\min\limits_{|w'|}\{w' \mid \Pi(\varphi, w') = 1\}$.

Некоторые результаты:

- [Алехнович, Разборов 08] $\mathbf{FPT} \neq \mathrm{W}[1] \Rightarrow$ резолюция неавтоматизируема.
- [Atserias, Müller 19] $\mathbf{P} \neq \mathbf{NP} \Rightarrow$ резолюция неавтоматизируема.
- [de Rezende et al. 21] $\mathbf{P} \neq \mathbf{NP} \Rightarrow$ Nullstellensatz и ряд других алгебраических систем неавтоматизируемы.

Некоторые открытые вопросы

Polynomial Calculus ($\mathrm{PCR}^{\mathbb{F}}$) доказательство несовместности системы равенств $\mathcal{F} \coloneqq \{f_1 = 0, f_2 = 0, \ldots, f_m = 0\}$ — это последовательность полиномов $(p_1, p_2, p_3, \ldots, p_\ell)$:

Некоторые открытые вопросы

Polynomial Calculus ($\mathrm{PCR}^{\mathbb{F}}$) доказательство несовместности системы равенств $\mathcal{F} \coloneqq \{f_1 = 0, f_2 = 0, \ldots, f_m = 0\}$ — это последовательность полиномов $(p_1, p_2, p_3, \ldots, p_\ell)$:

1. $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{x_i^2 - x_i\}$;

Некоторые открытые вопросы

Polynomial Calculus ($\mathrm{PCR}^{\mathbb{F}}$) доказательство несовместности системы равенств $\mathcal{F} \coloneqq \{f_1 = 0, f_2 = 0, \ldots, f_m = 0\}$ — это последовательность полиномов $(p_1, p_2, p_3, \ldots, p_\ell)$:

1. $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{x_i^2 - x_i\}$;
2. $p_i = x_j p_k$ для некоторого j и $k < i$;

Некоторые открытые вопросы

Polynomial Calculus ($\mathrm{PCR}^{\mathbb{F}}$) доказательство несовместности системы равенств $\mathcal{F} \coloneqq \{f_1 = 0, f_2 = 0, \ldots, f_m = 0\}$ — это последовательность полиномов $(p_1, p_2, p_3, \ldots, p_\ell)$:

1. $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{x_i^2 - x_i\}$;
2. $p_i = x_j p_k$ для некоторого j и $k < i$;
3. $p_i = \alpha p_k + \beta p_s$ для некоторых $k, s < i$ и $\alpha, \beta \in \mathbb{F}$;

Некоторые открытые вопросы

Polynomial Calculus ($\mathrm{PCR}^{\mathbb{F}}$) доказательство несовместности системы равенств $\mathcal{F} \coloneqq \{f_1 = 0, f_2 = 0, \ldots, f_m = 0\}$ — это последовательность полиномов $(p_1, p_2, p_3, \ldots, p_\ell)$:

1. $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{x_i^2 - x_i\}$;
2. $p_i = x_j p_k$ для некоторого j и $k < i$;
3. $p_i = \alpha p_k + \beta p_s$ для некоторых $k, s < i$ и $\alpha, \beta \in \mathbb{F}$;
4. $p_\ell = 1$.

- Какова сложность $\mathsf{PHP}_n^{n^3}$ в системе $\mathrm{PCR}^{\mathbb{F}}$.

Некоторые открытые вопросы

Polynomial Calculus ($\mathrm{PCR}^{\mathbb{F}}$) доказательство несовместности системы равенств $\mathcal{F} \coloneqq \{f_1 = 0, f_2 = 0, \ldots, f_m = 0\}$ — это последовательность полиномов $(p_1, p_2, p_3, \ldots, p_\ell)$:

1. $p_i \in \mathcal{F} \cup \bigcup_{j=1}^{n} \{x_i^2 - x_i\}$;
2. $p_i = x_j p_k$ для некоторого j и $k < i$;
3. $p_i = \alpha p_k + \beta p_s$ для некоторых $k, s < i$ и $\alpha, \beta \in \mathbb{F}$;
4. $p_\ell = 1$.

- Какова сложность $\mathsf{PHP}_n^{n^3}$ в системе $\mathrm{PCR}^{\mathbb{F}}$.
- Нижние оценки на систему Frege.
- Какова сложность случайных Δ-КНФ формул в системах CP и $\mathbf{AC}[0]$-Frege.

Коммуникационные протоколы. $f: U \times V \to T$

$$f(x, y) = ?$$

$x \in U$

$y \in V$

Коммуникационные протоколы. $f: U \times V \to T$

$$f(x, y) = ?$$

$x \in U$

$y \in V$

$$r_1 = a(x)$$

Коммуникационные протоколы. $f: U \times V \to T$

$$f(x, y) = ?$$

$x \in U$ $\qquad$ $y \in V$

$$r_1 = a(x)$$

$$r_2 = b(y, r_1)$$

Коммуникационные протоколы. $f: U \times V \to T$

$$f(x, y) = ?$$

$x \in U$ $\qquad$ $y \in V$

$r_1 = a(x)$

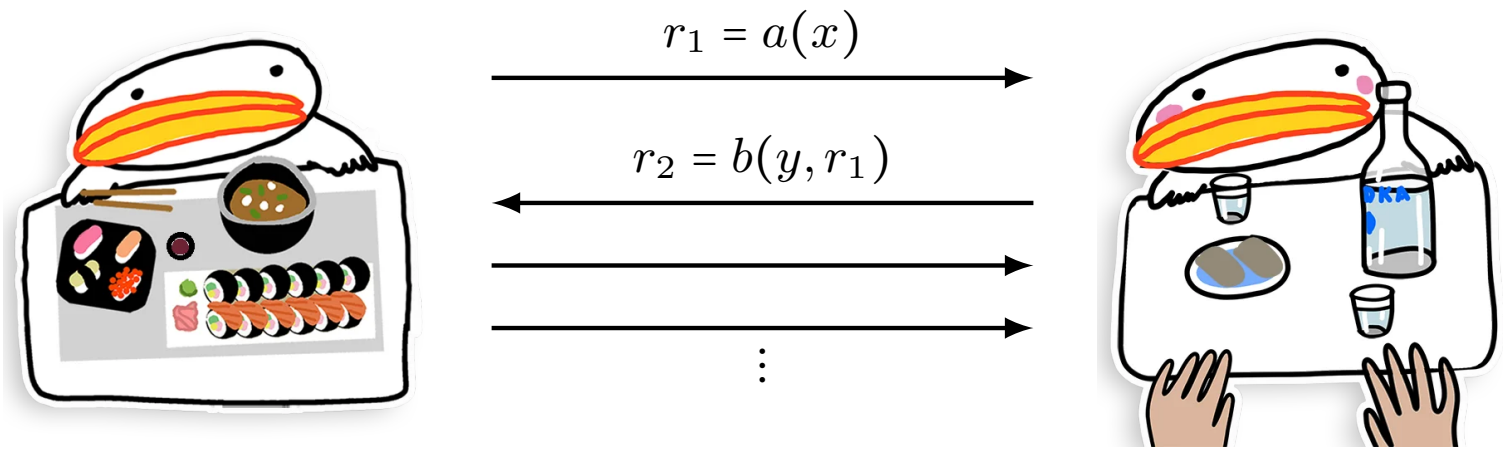
$r_2 = b(y, r_1)$

$\vdots$

Коммуникационные протоколы. $f: U \times V \to T$

$$f(x, y) = ?$$

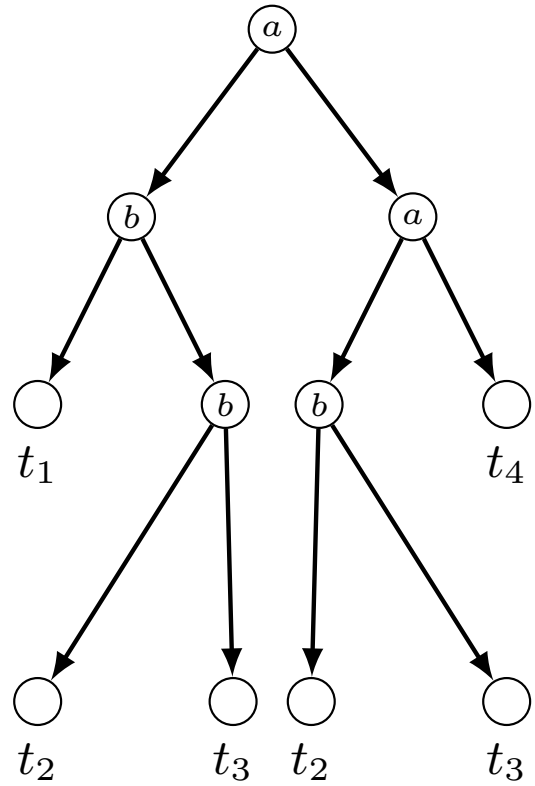
$x \in U$ $\qquad$ $y \in V$



- Глубина — число раундов (в худшем случае).
- $\mathrm{D}(f) = \min\limits_{P \in \mathcal{P}} \mathrm{depth}(P)$, где $\mathcal{P}$ — множество протоколов для f.

Протоколы и деревья

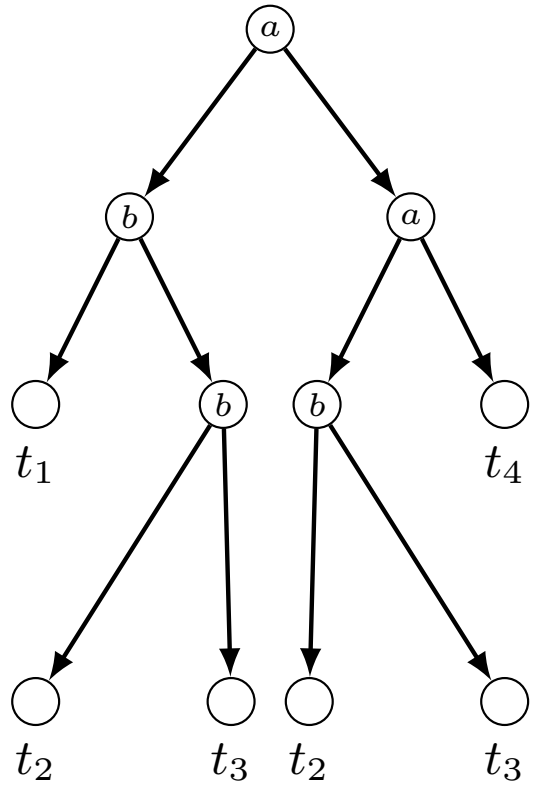
Алиса полуает $u \in U$, Боб $v \in V$. Протокол — это дерево:



Протоколы и деревья

Алиса полуает $u \in U$, Боб $v \in V$. Протокол — это дерево:

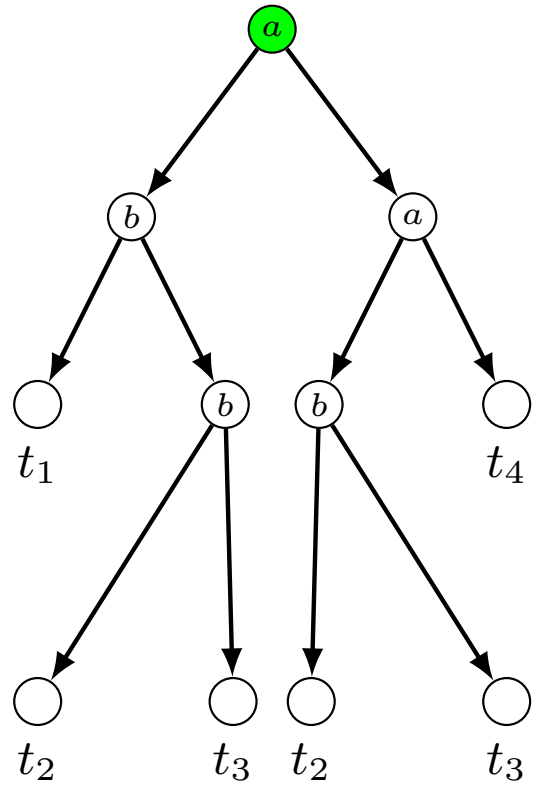
- вершины помечены игроками;



Протоколы и деревья

Алиса полуает $u \in U$, Боб $v \in V$. Протокол — это дерево:

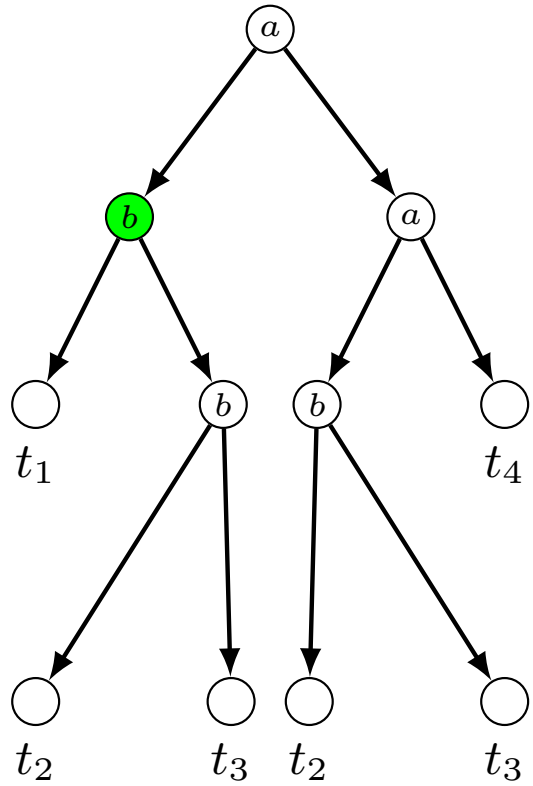
- вершины помечены игроками;



Протоколы и деревья

Алиса полуает $u \in U$, Боб $v \in V$. Протокол — это дерево:

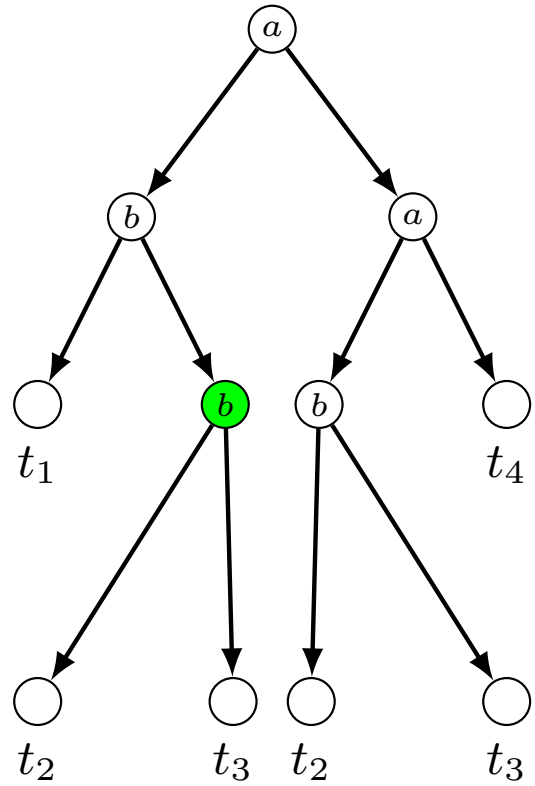
- вершины помечены игроками;



Протоколы и деревья

Алиса полуает $u \in U$, Боб $v \in V$. Протокол — это дерево:

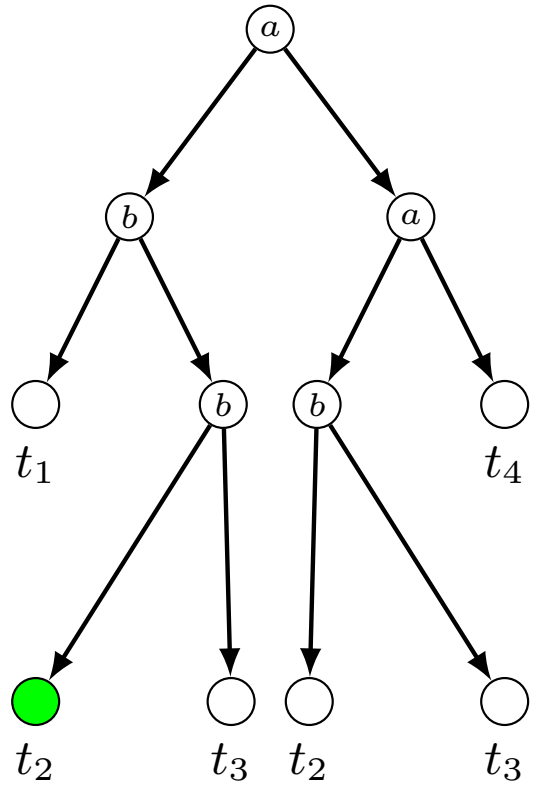
- вершины помечены игроками;



Протоколы и деревья

Алиса полуает $u \in U$, Боб $v \in V$. Протокол — это дерево:

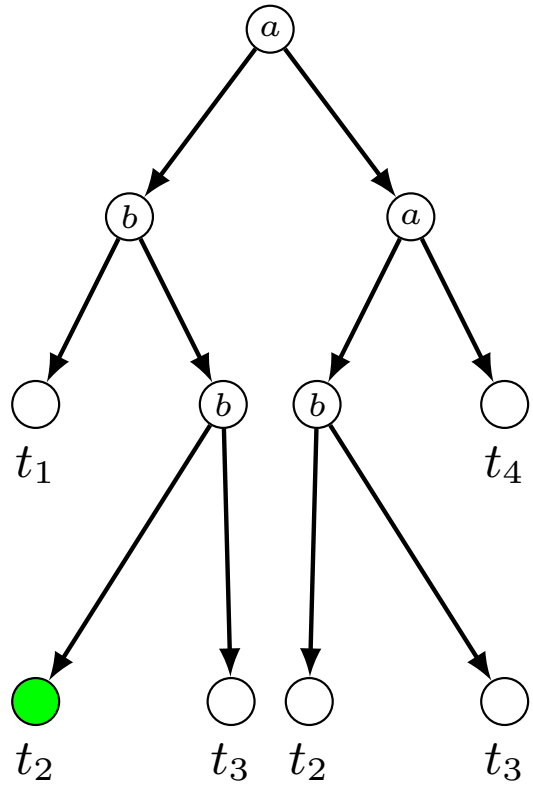
- вершины помечены игроками;



Протоколы и деревья

Алиса полуает $u \in U$, Боб $v \in V$. Протокол — это дерево:

- вершины помечены игроками;
- листья ответами.



Отношение KW [Karchmer, Wigderson 90]

$U, V \subseteq \{0,1\}^n$ и $U \cap V = \varnothing$.

KW:

- Алиса получает $u \in U$, Боб получает $v \in V$;
- цель: найти такой i, что $u_i \neq v_i$.

Отношение KW [Karchmer, Wigderson 90]

$U, V \subseteq \{0,1\}^n$ и $U \cap V = \varnothing$.

KW:

- Алиса получает $u \in U$, Боб получает $v \in V$;
- цель: найти такой i, что $u_i \neq v_i$.

Монотонная версия KW^{m}:

- цель: найти такой i, что $u_i = 1 \wedge v_i = 0$.

Отношение KW [Karchmer, Wigderson 90]

$U, V \subseteq \{0,1\}^n$ и $U \cap V = \varnothing$.

KW:

- Алиса получает $u \in U$, Боб получает $v \in V$;
- цель: найти такой i, что $u_i \neq v_i$.

Монотонная версия KW^{m}:

- цель: найти такой i, что $u_i = 1 \wedge v_i = 0$.

Теорема[Karchmer, Wigderson 90]

Монотонная формула для f размера $S \Leftrightarrow$ коммуникационный протокол для KW^{m} KW размера S, где $U \coloneqq f^{-1}(1), V \coloneqq f^{-1}(0)$.

Search_φ [Lovász, Naor, Newman, Wigderson et al. 94]

$\varphi(z) \coloneqq \bigvee_{i=1}^{m} C_i$ невыполнимая КНФ формула.

Search_φ [Lovász, Naor, Newman, Wigderson et al. 94]

$\varphi(z) \coloneqq \bigvee_{i=1}^{m} C_i$ невыполнимая КНФ формула.

$\mathsf{Search}_\varphi \subseteq \{0,1\}^n \times [m]$:

- $(\alpha, i) \in \mathsf{Search}_\varphi \Leftrightarrow C_i(\alpha) = 0$.

Search_φ [Lovász, Naor, Newman, Wigderson et al. 94]

$\varphi(z) \coloneqq \bigvee_{i=1}^{m} C_i$ невыполнимая КНФ формула.

$\mathsf{Search}_\varphi \subseteq \{0,1\}^n \times [m]$:

- $(\alpha, i) \in \mathsf{Search}_\varphi \Leftrightarrow C_i(\alpha) = 0$.

Коммуникационная версия:

- "gadget" $g\colon X \times Y \to \{0,1\}$;
- $\mathsf{Ind}\colon [k] \times \{0,1\}^k \to \{0,1\}$, $\mathsf{Ind}(x, y) = y_x$.

Search_φ [Lovász, Naor, Newman, Wigderson et al. 94]

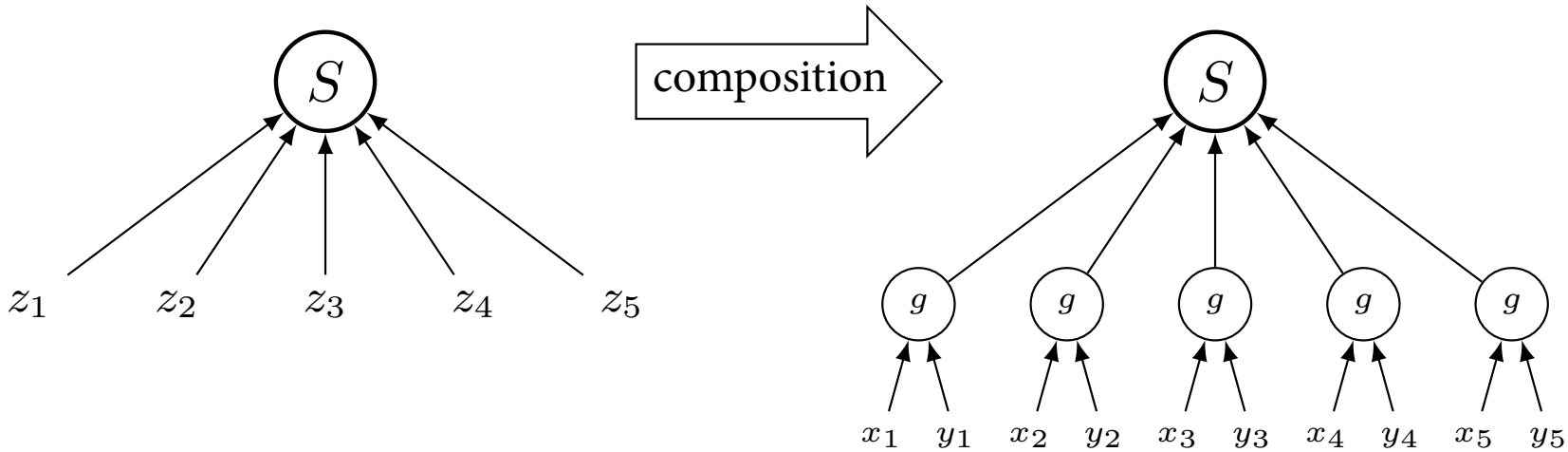
$\varphi(z) \coloneqq \bigvee_{i=1}^{m} C_i$ невыполнимая КНФ формула.

$\mathsf{Search}_\varphi \subseteq \{0,1\}^n \times [m]$:

- $(\alpha, i) \in \mathsf{Search}_\varphi \Leftrightarrow C_i(\alpha) = 0$.

Коммуникационная версия:

- "gadget" $g\colon X \times Y \to \{0,1\}$;
- $\mathsf{Ind}\colon [k] \times \{0,1\}^k \to \{0,1\}$, $\mathsf{Ind}(x, y) = y_x$.



$\mathsf{Search}_\varphi \circ g \equiv \mathsf{Search}_{\varphi \circ g}$.

Lifting

Теорема[Raz, McKenzie 99; Göös, Pitassi, Watson 16]

Резолюционная глубина φ не менеее $d \Rightarrow \mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \geq n^{\mathcal{O}(d)}$, где $m \coloneqq \mathsf{poly}(n)$. $\mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \approx \mathrm{D}(\mathsf{Ind}) \cdot \text{res-depth}(\varphi)$.

Следствие: нижние оценки на монотонные формулы 2^{n^ε}.

Lifting

Теорема[Raz, McKenzie 99; Göös, Pitassi, Watson 16]

Резолюционная глубина φ не менеее $d \Rightarrow \mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \geq n^{\mathcal{O}(d)}$, где $m \coloneqq \mathsf{poly}(n)$. $\mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \approx \mathrm{D}(\mathsf{Ind}) \cdot \text{res-depth}(\varphi)$.

Следствие: нижние оценки на монотонные формулы 2^{n^ε}.

Теорема[Garg, Göös, Kamath, S 18]

Резолюционный размер φ не менее $S \Rightarrow$ размер dag-like протокола для $\mathsf{Search}_\varphi \circ \mathsf{Ind}_m$ не менее $\Omega(S)$, where $m \coloneqq \mathsf{poly}(n)$.

Следствие: нижние оценки на монотонные схемы 2^{n^ε}.

Lifting

Теорема[Raz, McKenzie 99; Göös, Pitassi, Watson 16]

Резолюционная глубина φ не менеее $d \Rightarrow \mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \geq n^{\mathcal{O}(d)}$, где $m \coloneqq \mathsf{poly}(n)$. $\mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \approx \mathrm{D}(\mathsf{Ind}) \cdot \text{res-depth}(\varphi)$.

Следствие: нижние оценки на монотонные формулы 2^{n^ε}.

Теорема[Garg, Göös, Kamath, S 18]

Резолюционный размер φ не менее $S \Rightarrow$ размер dag-like протокола для $\mathsf{Search}_\varphi \circ \mathsf{Ind}_m$ не менее $\Omega(S)$, where $m \coloneqq \mathsf{poly}(n)$.

Следствие: нижние оценки на монотонные схемы 2^{n^ε}.

Теорема[Pitassi, Robere 16; Robere, Pitassi 18, informal]

Nullstellensatz $\Leftrightarrow$ algebraic tiling для $\mathsf{Search}_\varphi \circ g$.