Зачем нужна сложность доказательств

$$\sum_{u=1}^{a} p_u f_u + \sum_{w=1}^{n} r_w (x^2 - 1) + \sum_{v=1}^{b} q_v^2 h_v = -1$$

Дмитрий Соколов

СПбГУ 2022
Апрель 5-7

St Petersburg University

PDMI

RAS

Немного о задачах

Как понять, что объект достоен изучения?

Немного о задачах

Как понять, что объект достоен изучения?

- Объект интересен лично вам.

Немного о задачах

Как понять, что объект достоен изучения?

- Объект интересен лично вам.
- Объект появился хотя бы дважды в различных задачах независимым образом.

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»

$f\colon X^n \to Y$

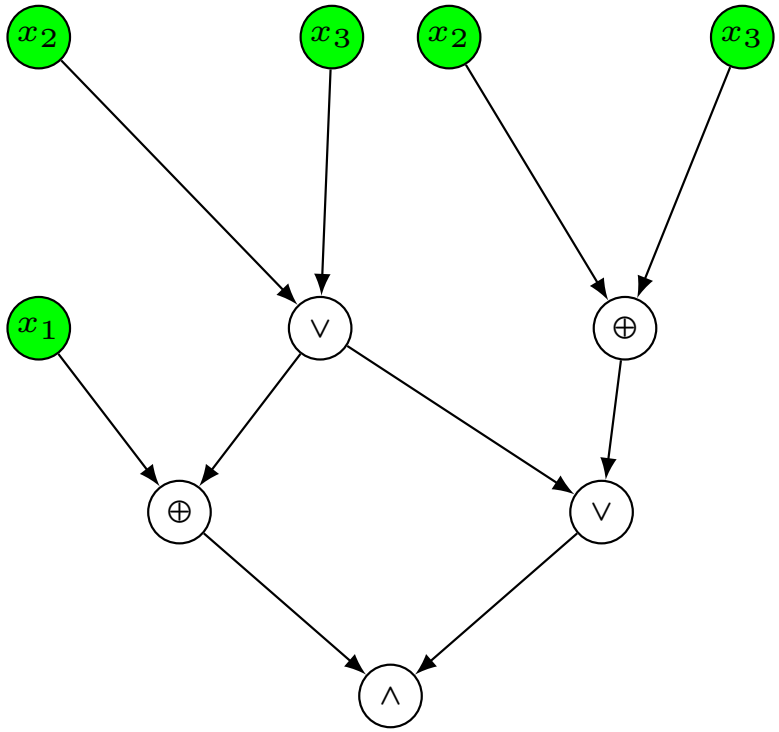
Есть ли простое описание у функции f? $\Leftrightarrow$ Выразима ли функция f, как композиция «простых»?

- [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.

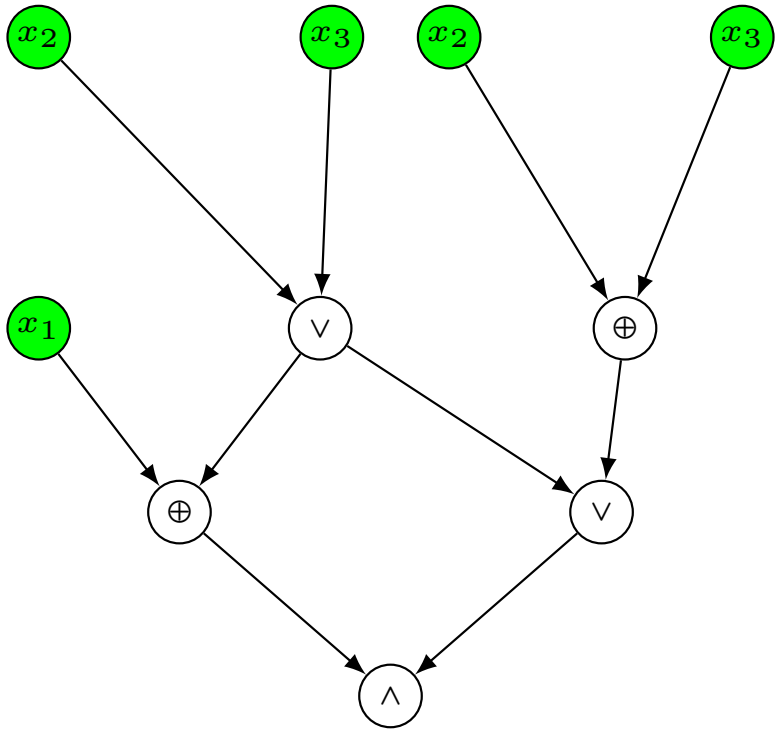
$X \coloneqq \{0, 1\}$

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

Схемы



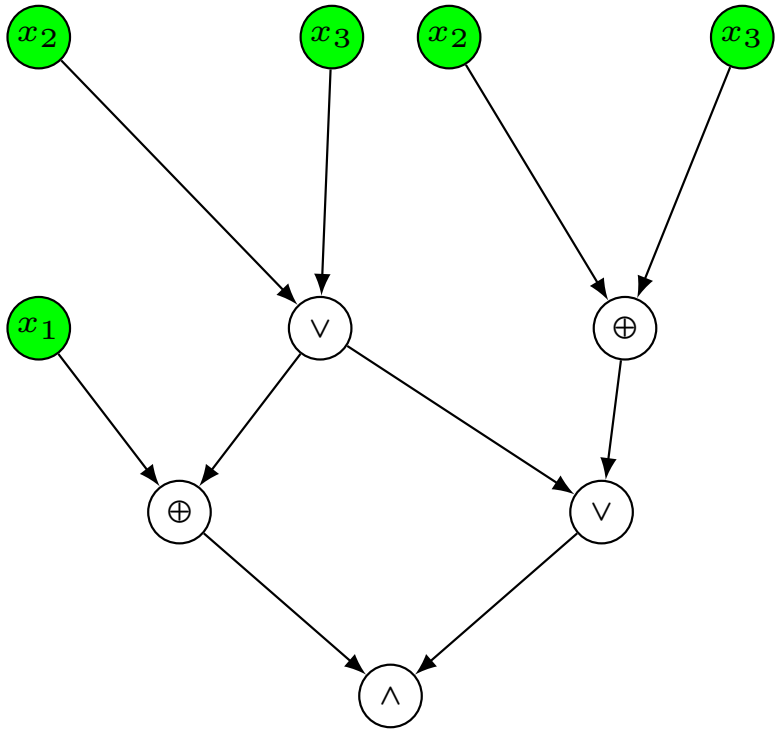
Схемы



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.

Примеры

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

Примеры

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

- 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

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

- 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.

Примеры

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

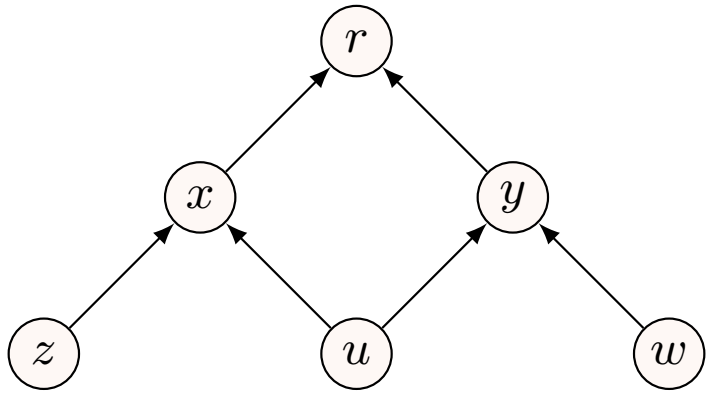
- Резолюция. A, B — дизъюнкты.
  - $\frac{A \vee x \quad B \vee \neg x}{A \vee B} \qquad \frac{A}{A \vee z}$

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

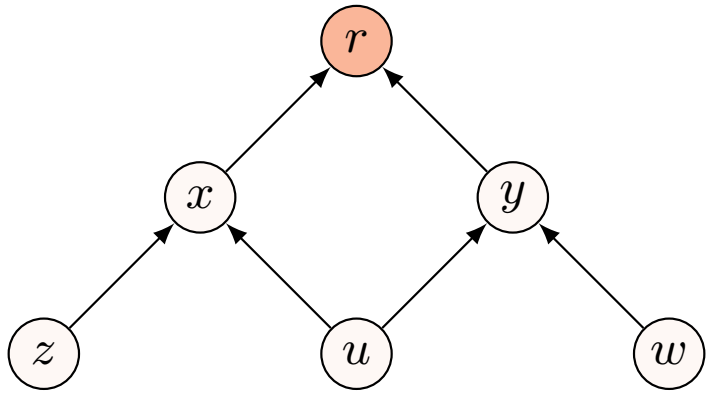
  Доказательство: вывод неравенства $0 \geq 1$ из неравенств, кодирующих дизъюнкты формулы.
- Nullstellensatz. $\{f_1 = 0, f_2 = 0, \dots, f_m = 0\}$
  - $\mathbb{F}$ — поле;
  - $(x \vee y \vee \neg z) \Rightarrow f_i := xy\bar{z}$;
  - $x^2 - x = 0, x + \bar{x} - 1 = 0$.

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

Pebbing

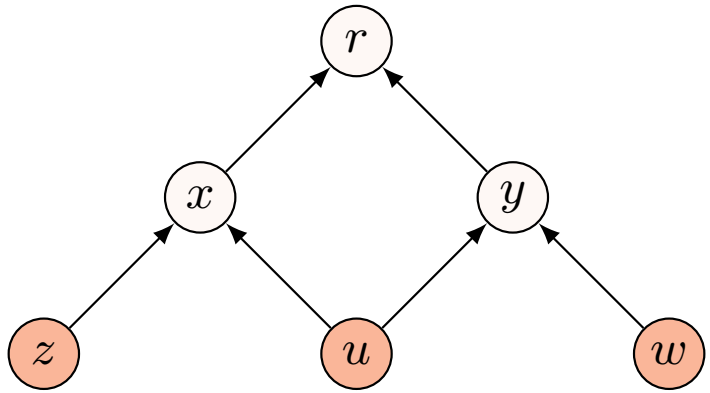


Pebbing



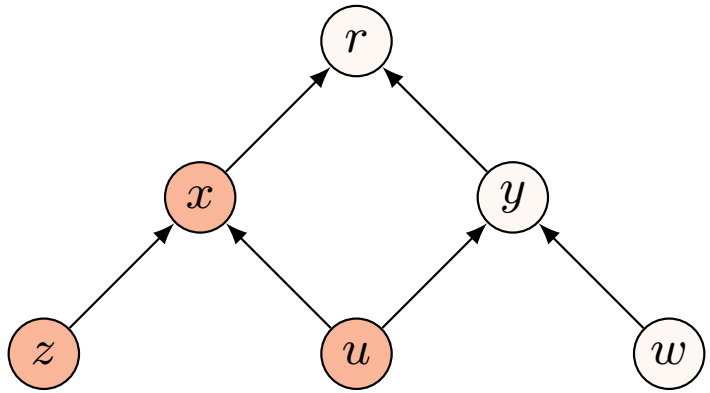
- $(\neg r)$;

Pebbing



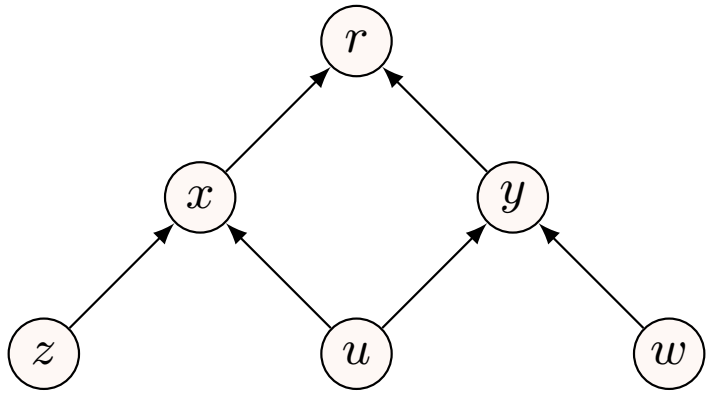
- $(\neg r)$;
- $(z), (u), (w)$;

Pebbing



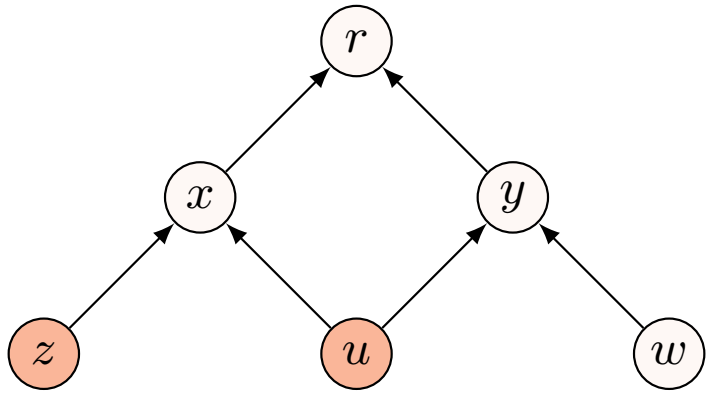
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x)$.

Pebbing



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

Pebbing



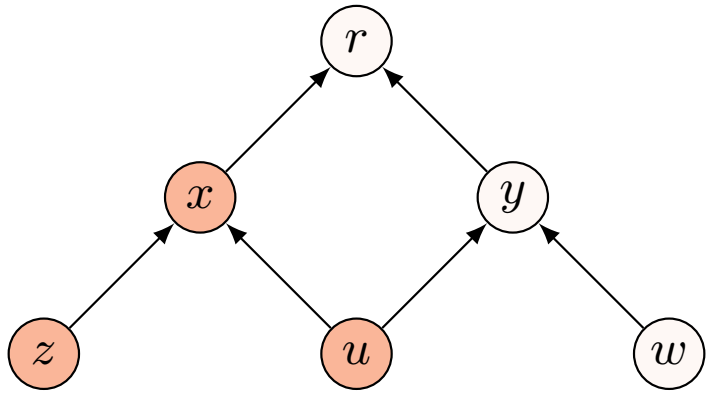
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x)$.

u

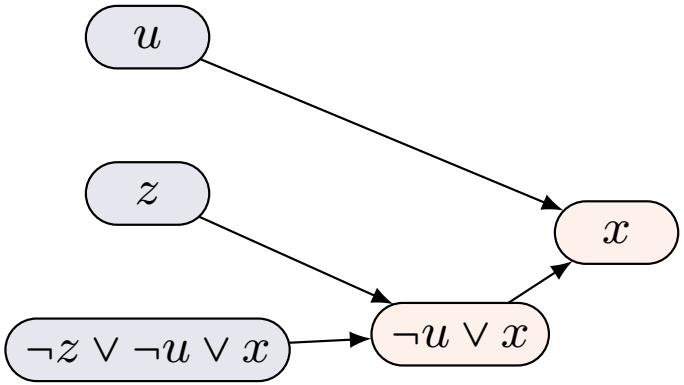
z

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

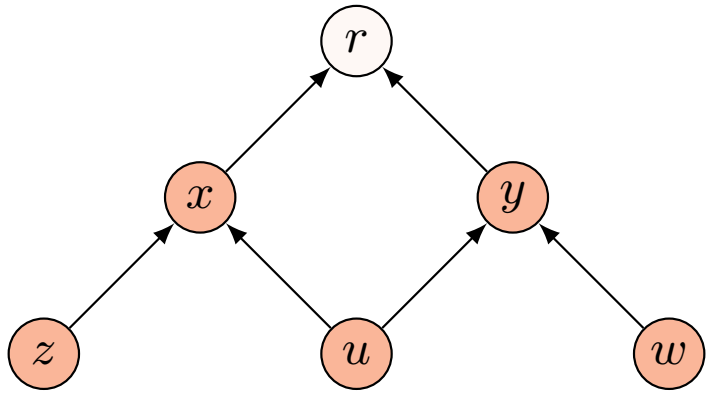
Pebbing



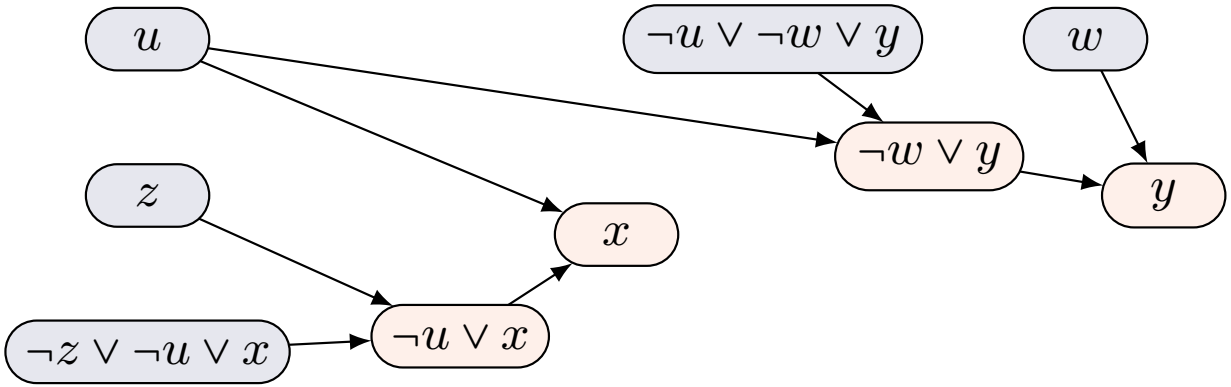
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x)$.



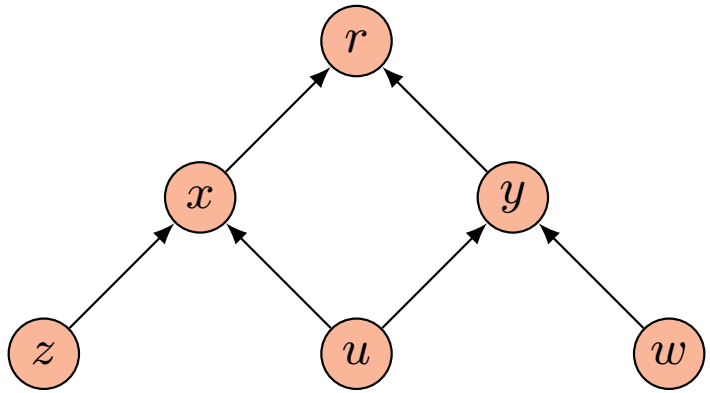
Pebbing



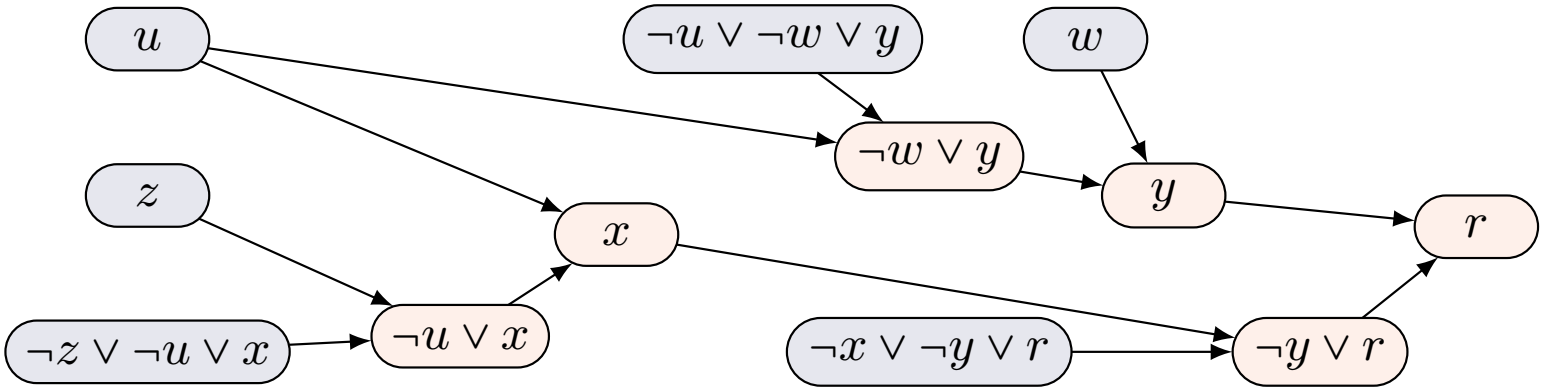
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x)$.



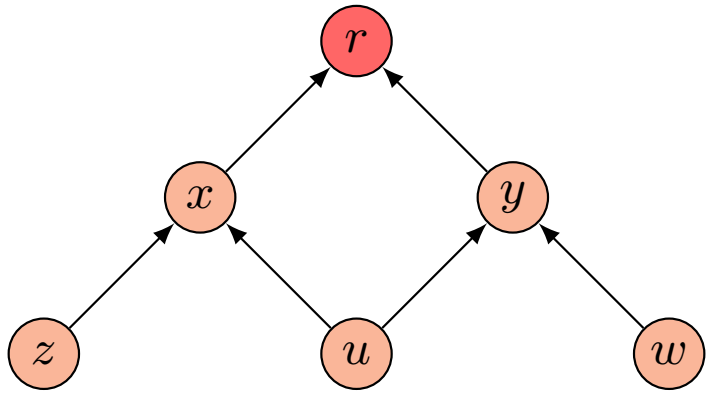
Pebbing



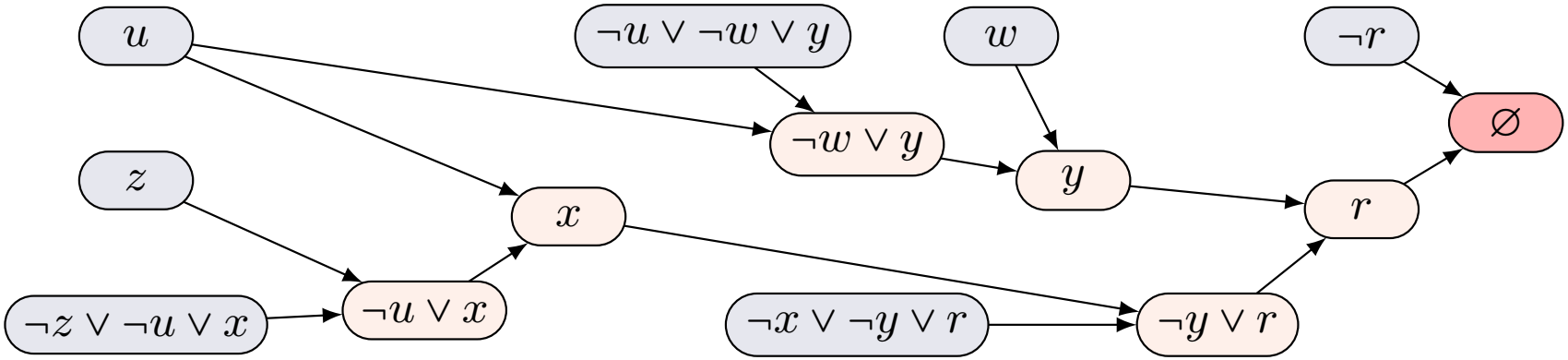
- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x)$.



Pebbing

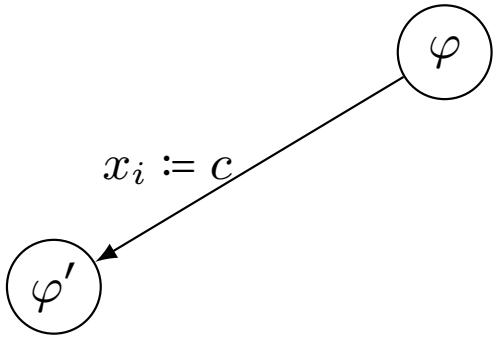


- $(\neg r)$;
- $(z), (u), (w)$;
- $(\neg z \vee \neg u \vee x)$.

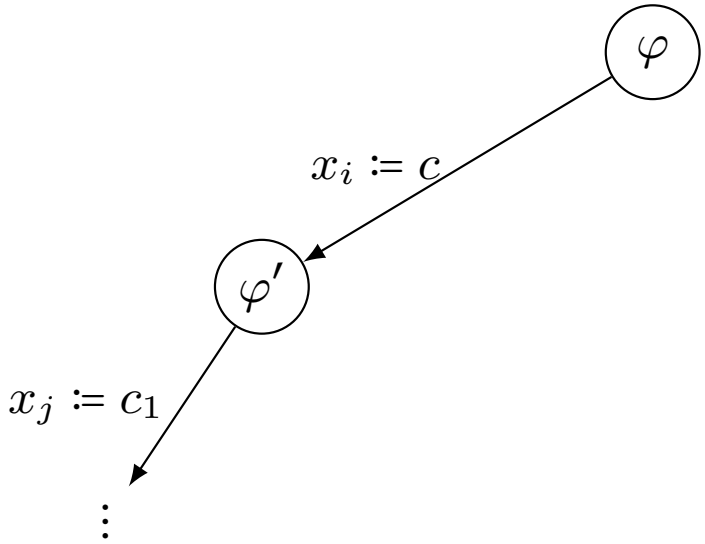


DPLL **алгоритмы**

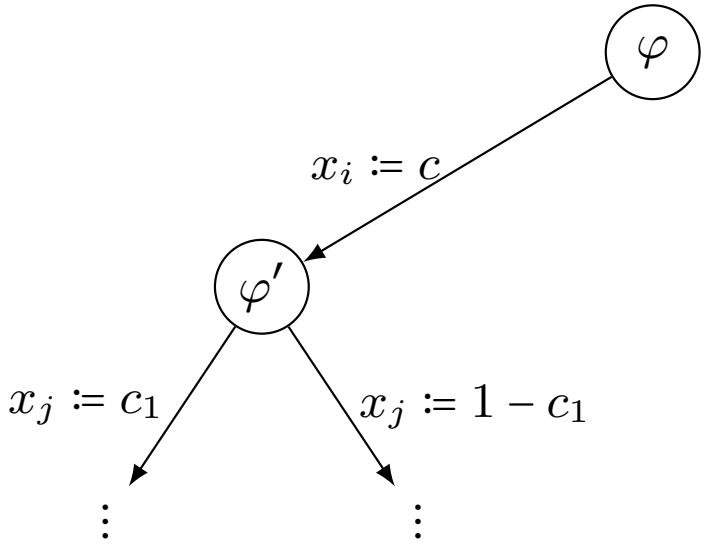
DPLL **алгоритмы**



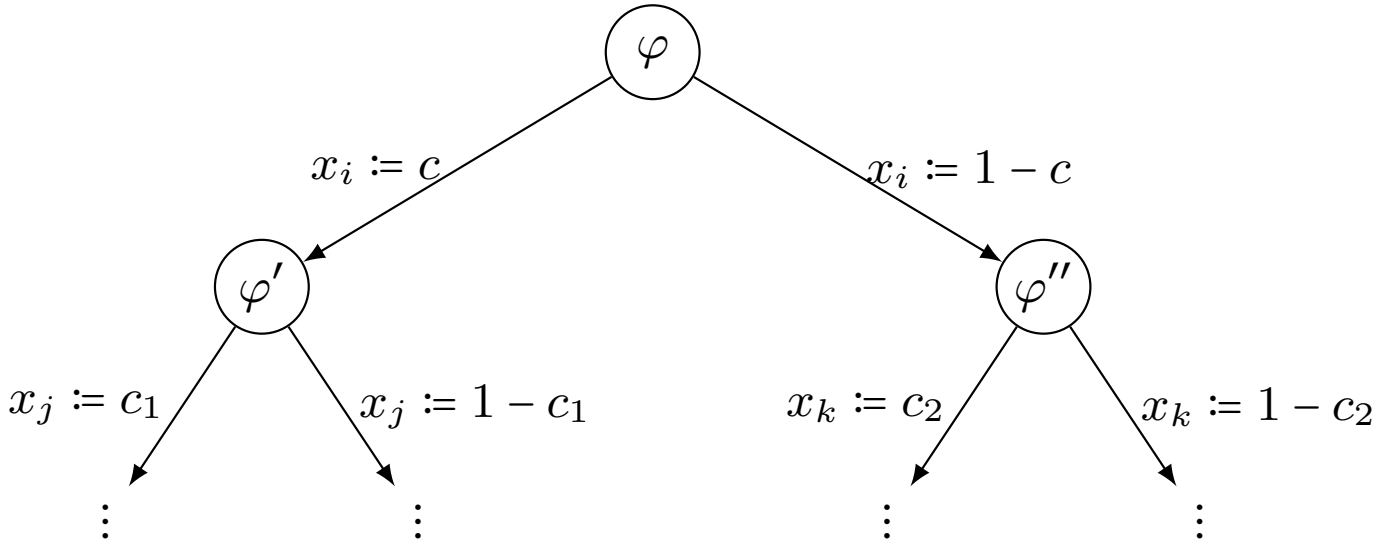
DPLL **алгоритмы**



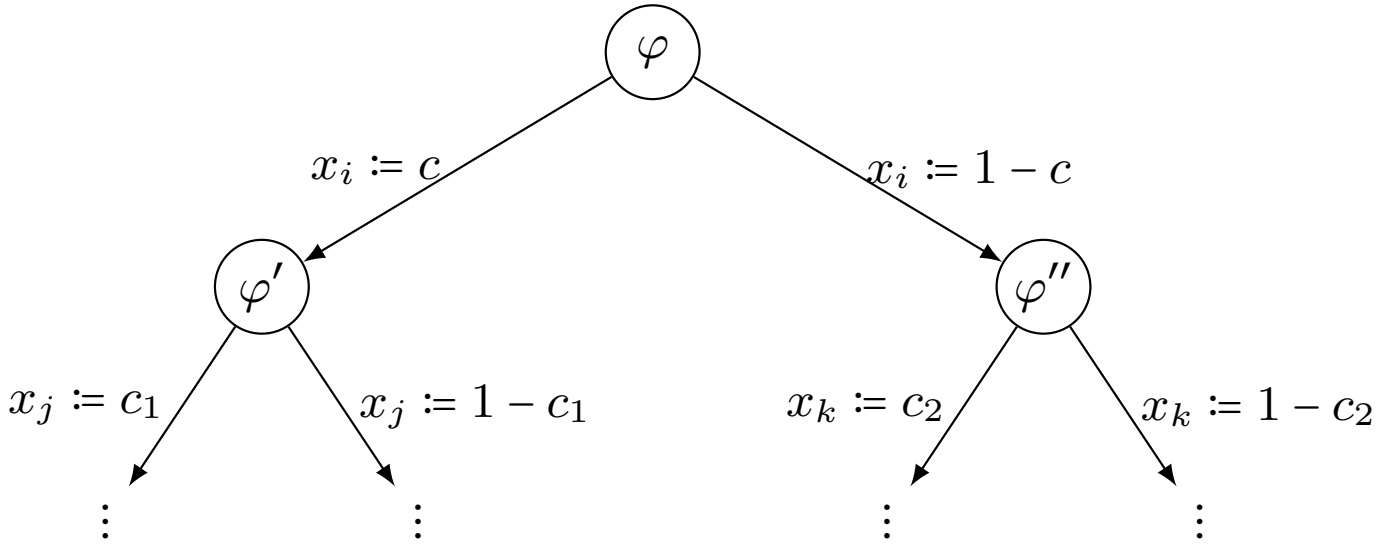
DPLL **алгоритмы**



DPLL **алгоритмы**

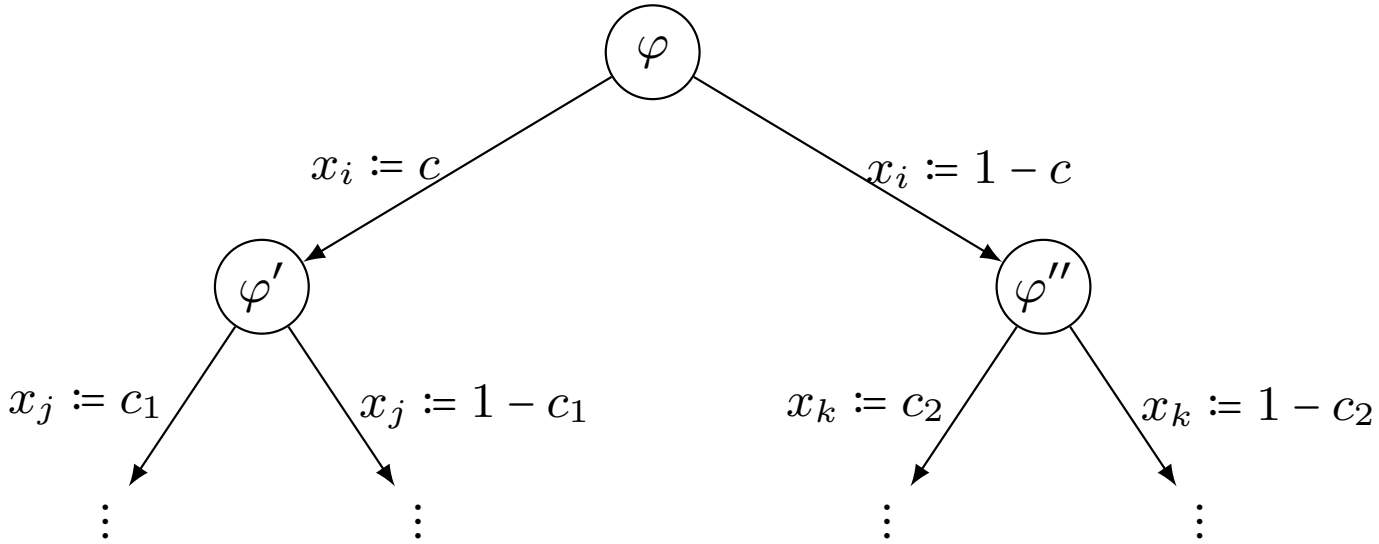


DPLL **алгоритмы**



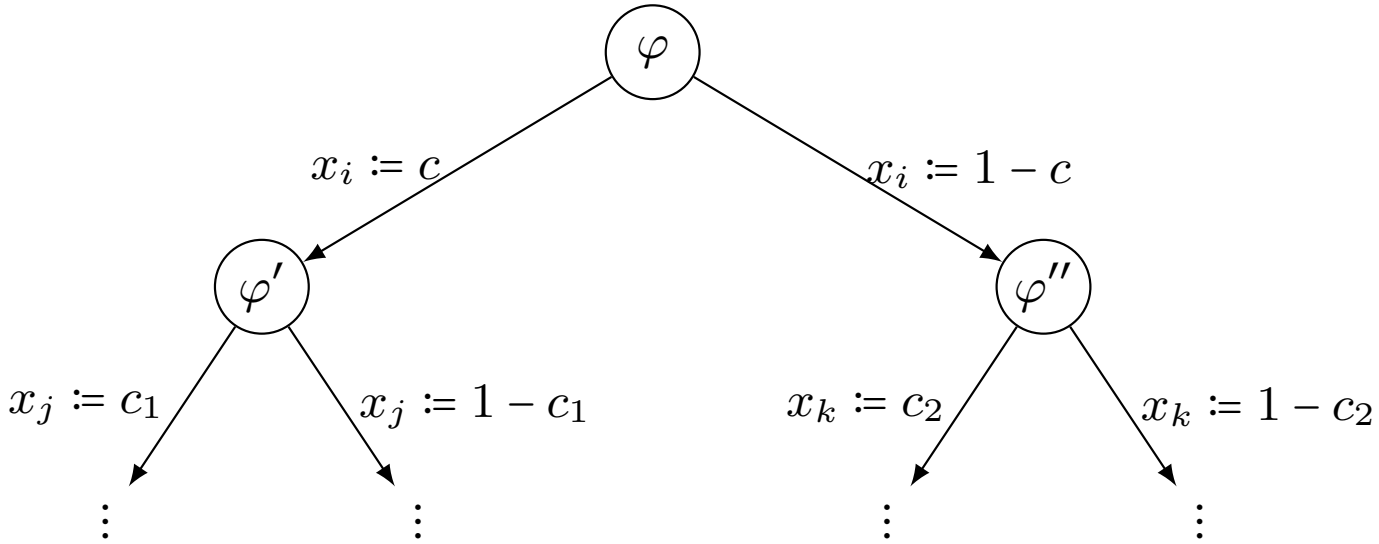
- Эвристика **A** выбирает переменную для расщепления.

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

$$\varphi \coloneqq \bigvee_i C_i$$

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

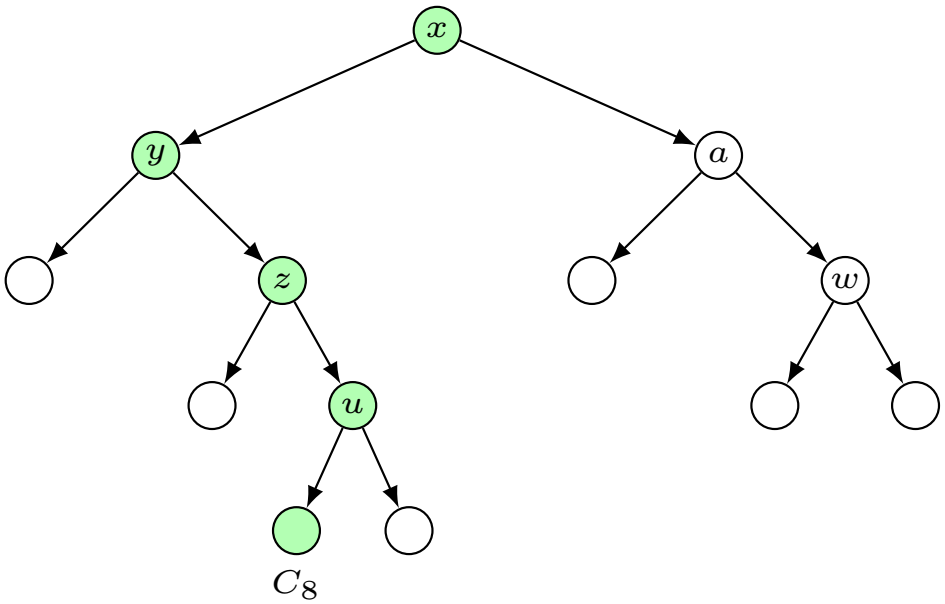
DPLL **и резолюция**

Теорема

DPLL алгоритм делает t расщеплений на невыполнимой формуле

$$\varphi \coloneqq \bigvee_i C_i$$

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



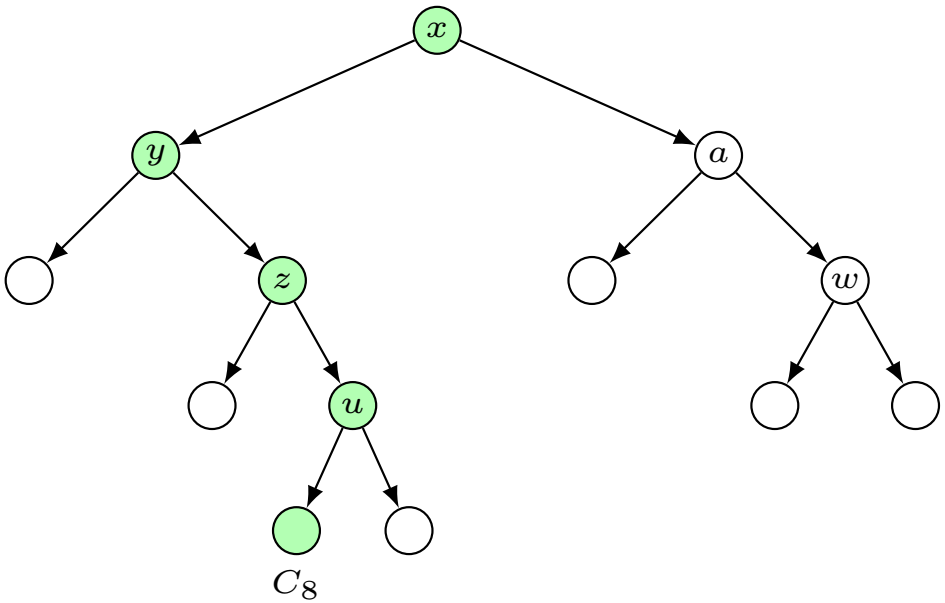
DPLL и резолюция

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 отрицаний запросов.
- $(x \vee \neg y \vee \neg z \vee u)$.

Pigeonhole Principle и DPLL алгоритмы

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

Pigeonhole Principle и DPLL алгоритмы

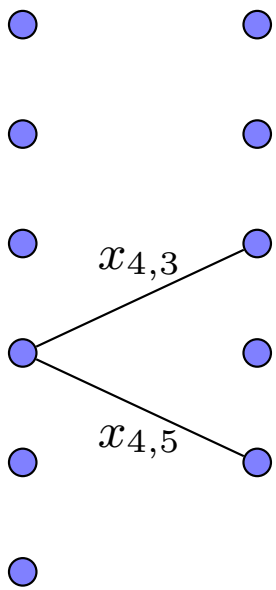
Переменные: $x_{i,j}$, $i \in \{1, 2, \ldots, n+1\}$, $j \in \{1, 2, \ldots, n\}$.

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

Pigeonhole Principle и DPLL алгоритмы

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

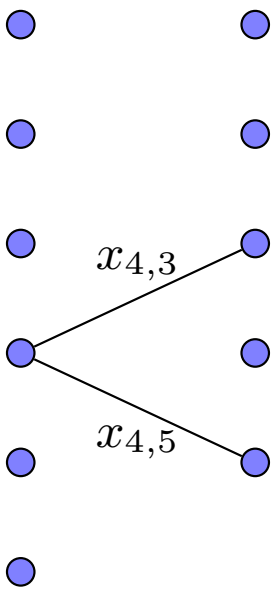
- $\bigvee_{j=1}^{n} x_{i,j}$;
- $\neg x_{i,j} \vee \neg x_{i',j}$.

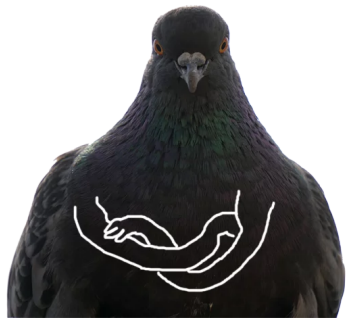


Pigeonhole Principle и DPLL алгоритмы

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

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

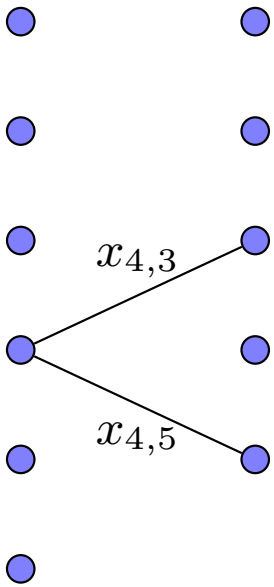


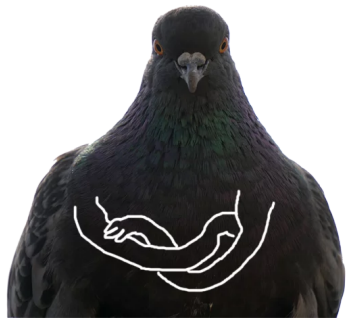


Pigeonhole Principle и DPLL алгоритмы

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

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

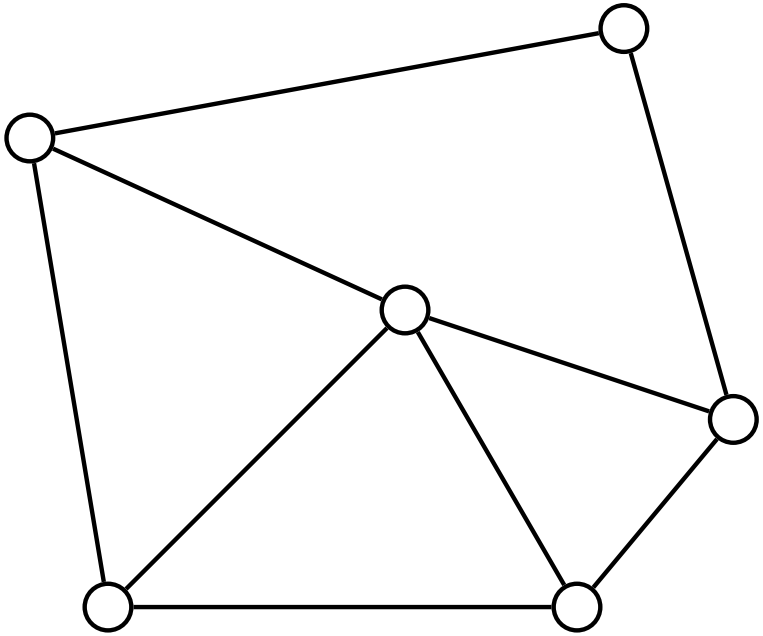


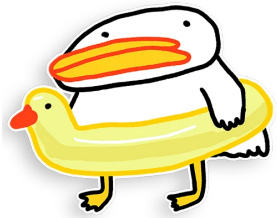


Теорема[Haken 85]

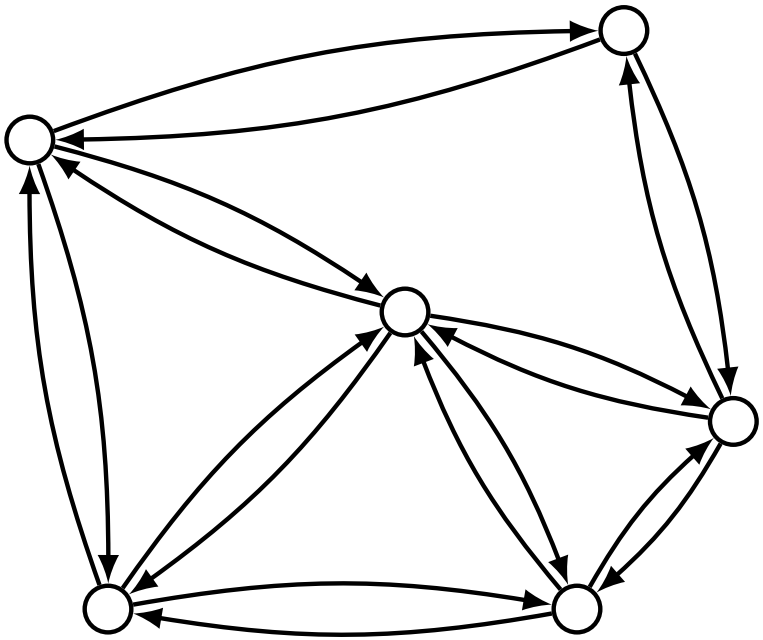
Любое резолюционное доказательство данной формулы имеет размер $2^{\Omega(n)}$.

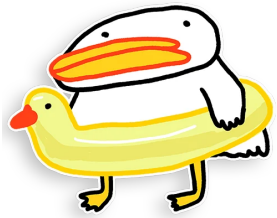
Flow **формулы**



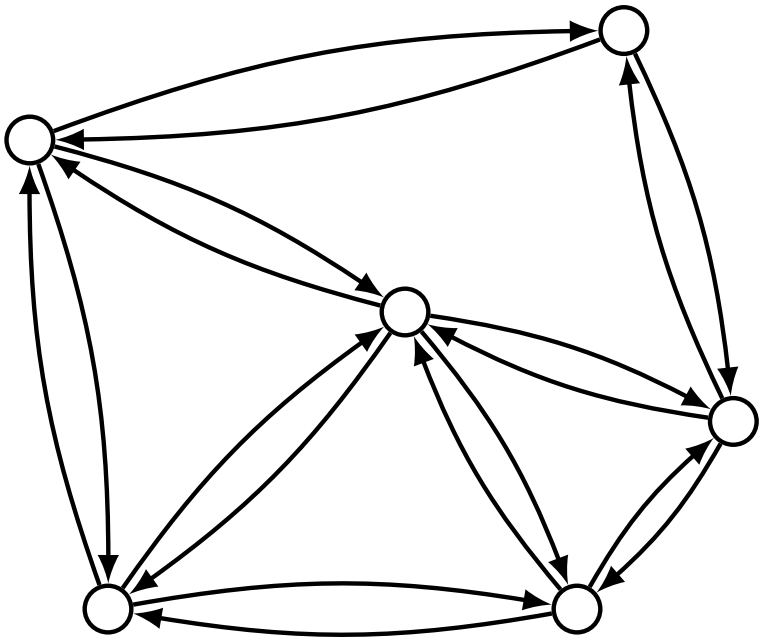


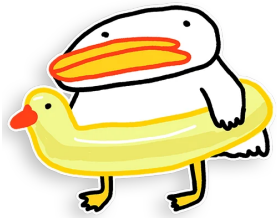
Flow **формулы**





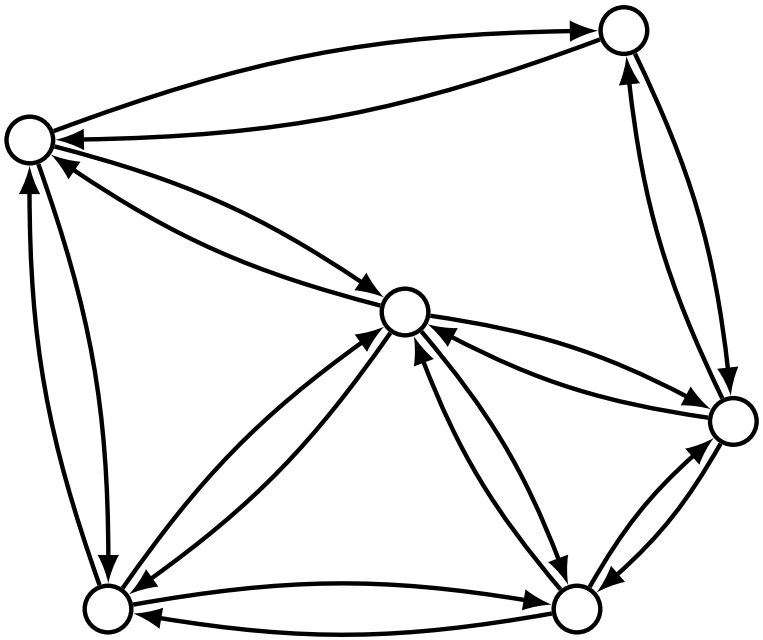
Flow **формулы**

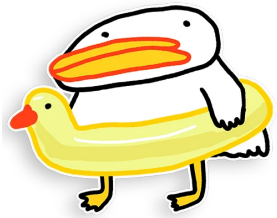




- v: $\sum\limits_{e \in E_v^{\text{in}}} x_e - \sum\limits_{e \in E_v^{\text{out}}} x_e = c(v)$ $(\mathbb{R})$;
- $\sum\limits_v c(v) = 1$ $(\mathbb{R})$;
- степень графа: Δ.

Flow **формулы**

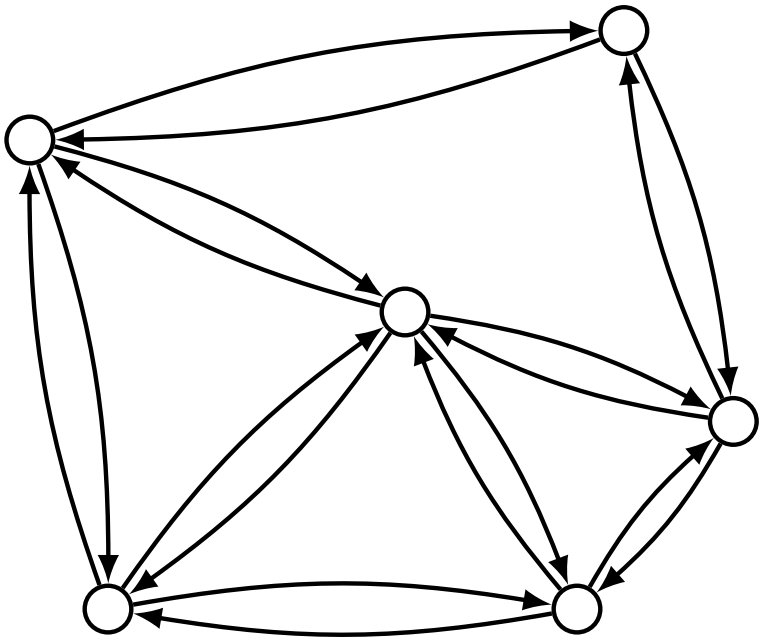


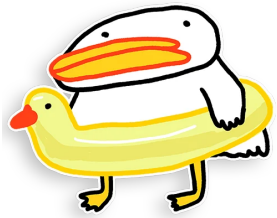


- v: $\sum\limits_{e \in E_v^{\text{in}}} x_e - \sum\limits_{e \in E_v^{\text{out}}} x_e = c(v)$ $(\mathbb{R})$;
- $\sum\limits_v c(v) = 1$ $(\mathbb{R})$;
- степень графа: Δ.

- Существует эффективное Nullstellensatz доказательство Flow.
- [Alekhnovich, Razborov 03] Если G — (n, Δ, α)-экспандер $\Rightarrow$ любое резолюционное доказательство имеет размер $2^{\Omega(n)}$.

Flow **формулы**





- 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: Δ.

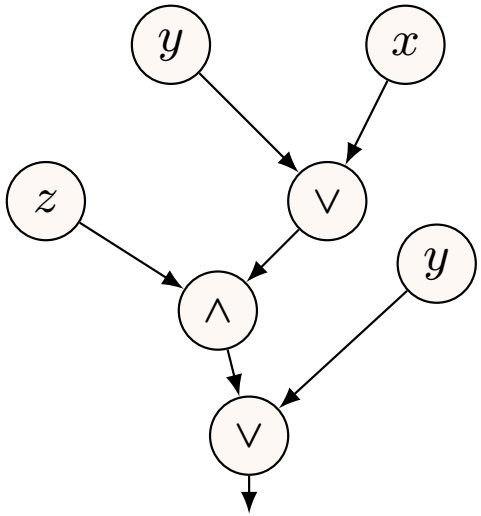
- Существует эффективное Nullstellensatz доказательство Flow.
- [Alekhnovich, Razborov 03] Если G — (n, Δ, α)-экспандер $\Rightarrow$ любое резолюционное доказательство имеет размер $2^{\Omega(n)}$.

Следствие[Göös, Kamath, Robere, S 19]

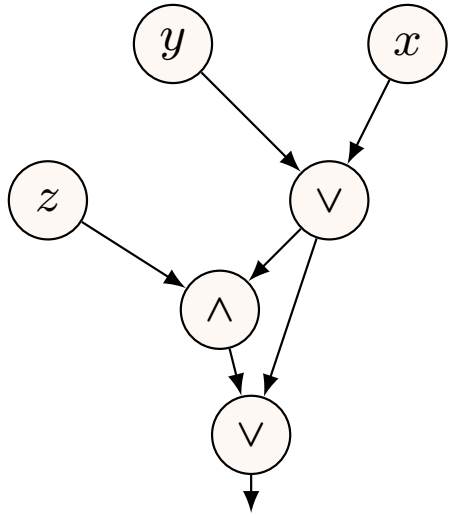
Существует монотонная функция в классе $\mathbf{NC}^2$, которая не может быть вычислена субэкспоненциальной монотонной схемой.

Монотонные вычисления

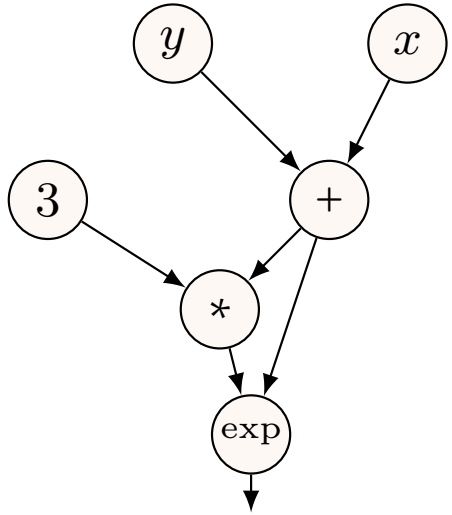
Формулы



Схемы

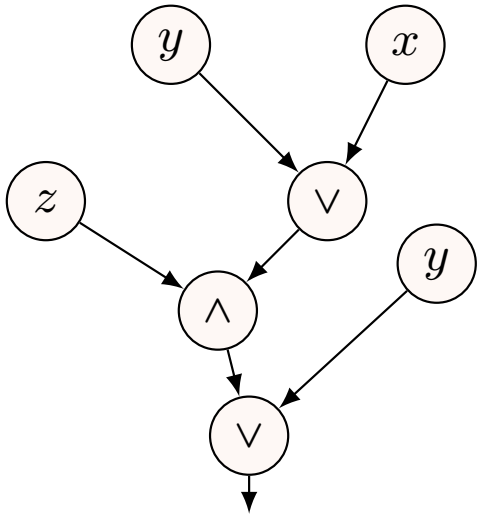


Больше схем

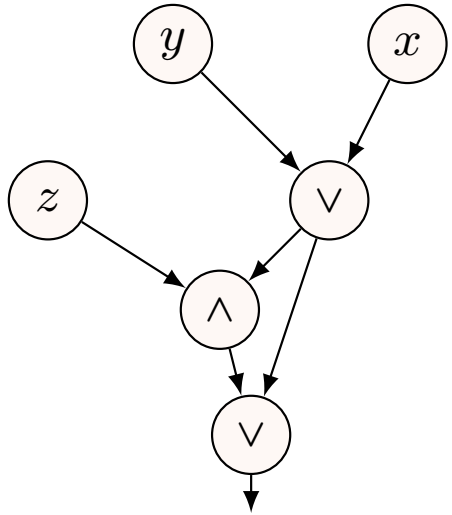


Монотонные вычисления

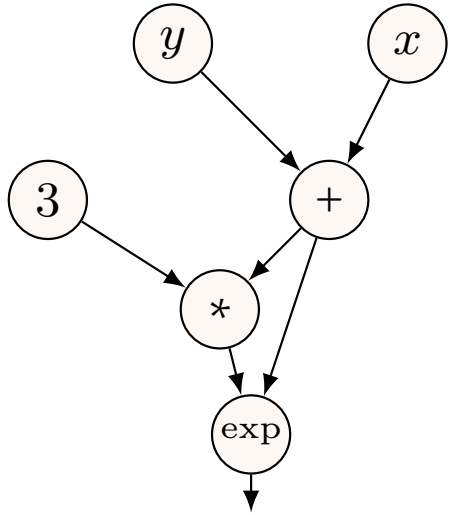
Формулы



Схемы



Больше схем

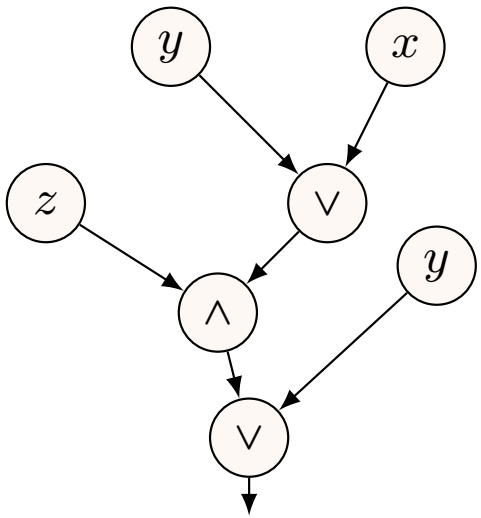


Почему мы беспокоимся о монотонных вычислениях?

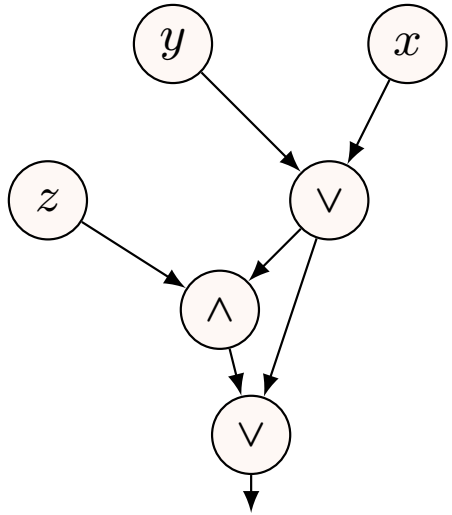
- Можем что-то доказать!

Монотонные вычисления

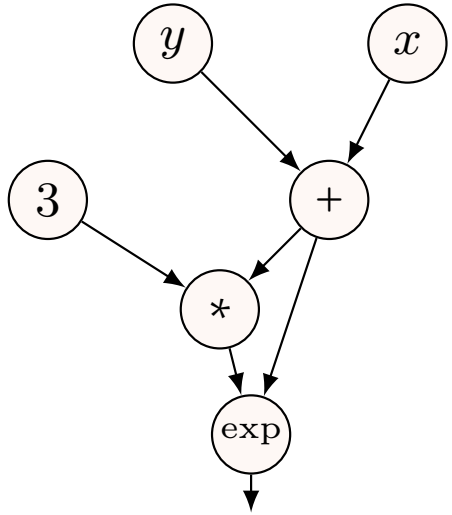
Формулы



Схемы



Больше схем

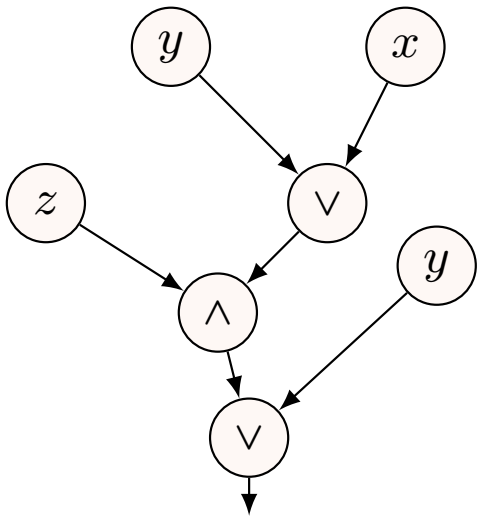


Почему мы беспокоимся о монотонных вычислениях?

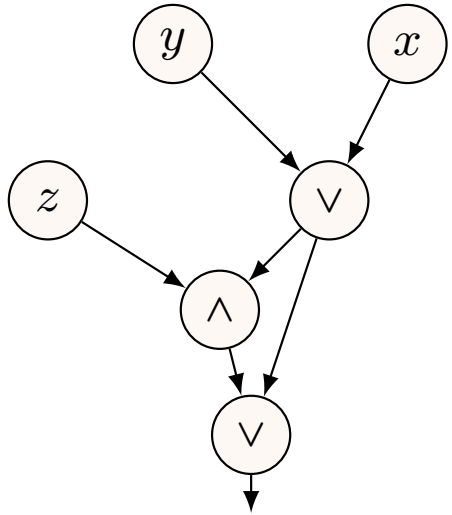
- Можем что-то доказать!
- Контроль относительной погрешности.

Монотонные вычисления

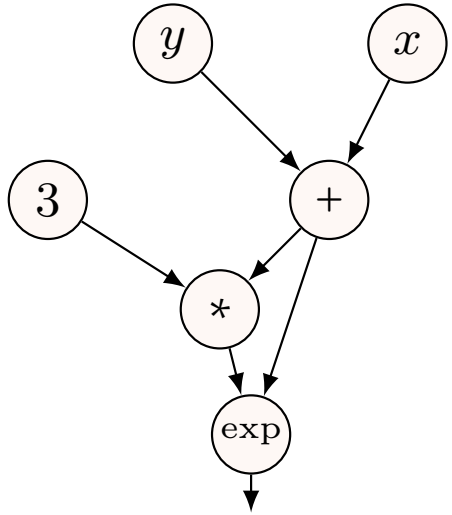
Формулы



Схемы



Больше схем

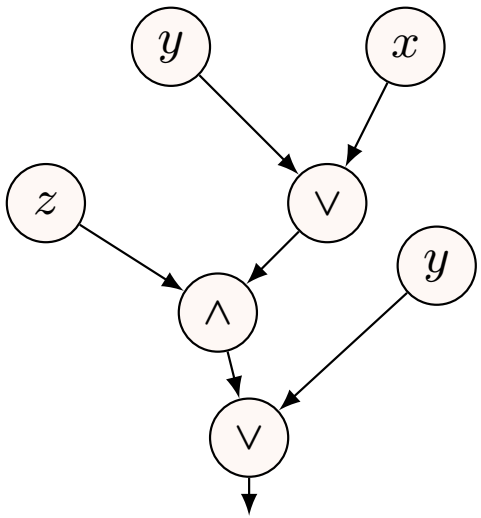


Почему мы беспокоимся о монотонных вычислениях?

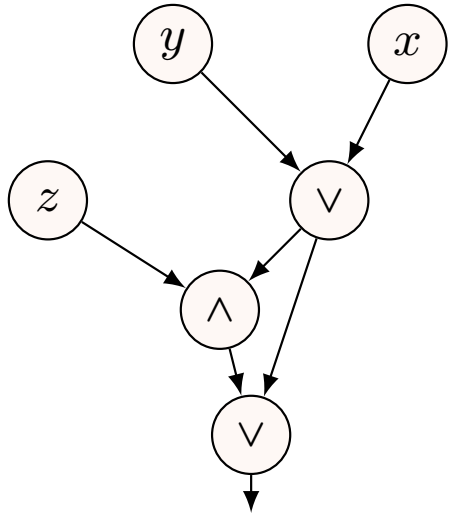
- Можем что-то доказать!
- Контроль относительной погрешности.
- Достаточно сильные оценки на монотонные схемы ⇒ нижние оценки на общие схемы.

Монотонные вычисления

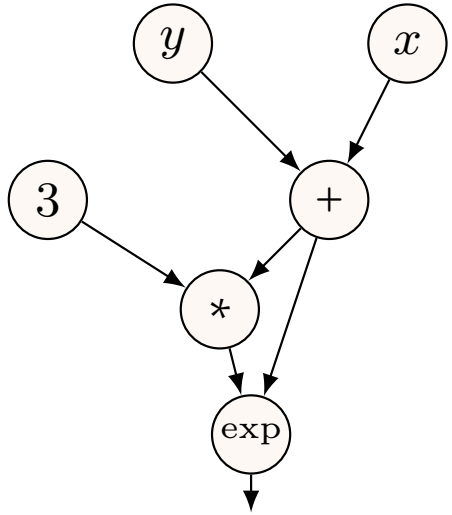
Формулы



Схемы



Больше схем



Почему мы беспокоимся о монотонных вычислениях?

- Можем что-то доказать!
- Контроль относительной погрешности.
- Достаточно сильные оценки на монотонные схемы ⇒ нижние оценки на общие схемы.
- Протоколы разделения секрета/криптография.

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

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

$x \in U$

$y \in V$

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

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

$x \in U$

$$r_1 = a(x)$$

$y \in V$

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

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

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

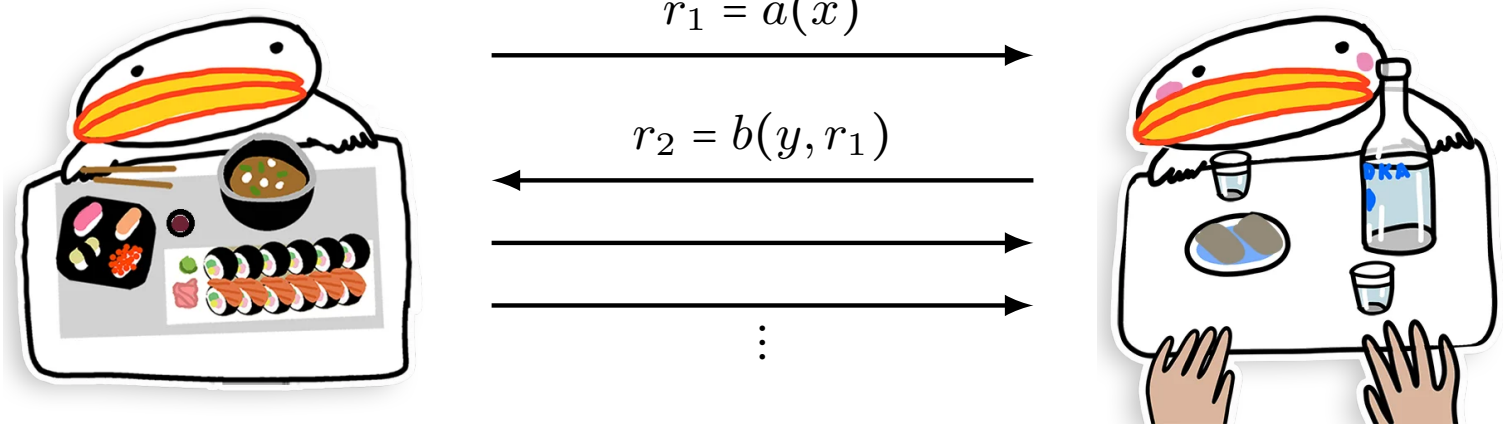
$$r_1 = a(x)$$

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

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

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

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



Задача KW [Karchmer, Wigderson 90]

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

KW:

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

Задача KW [Karchmer, Wigderson 90]

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

KW:

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

Монотонная верия KW^{m}:

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

Задача KW [Karchmer, Wigderson 90]

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

KW:

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

Монотонная верия KW^{m}:

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

Теорема[Karchmer, Wigderson 90]

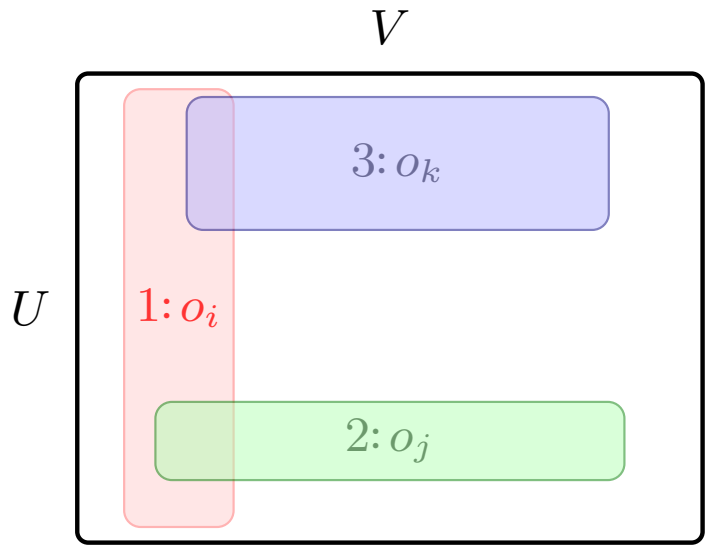
Монотонная формула для функции f размера $S \Leftrightarrow$ коммуникационный протокол для KW^{m} KW размера S, где $U \coloneqq f^{-1}(1), V \coloneqq f^{-1}(0)$.

KW^{m} — «полное отношение»

- $\mathcal{S} \subseteq U \times V \times \mathcal{O}$;
- определим такую функцию $F_{\mathcal{S}}\colon \{0,1\}^m \to \{0,1\}$, что $\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.

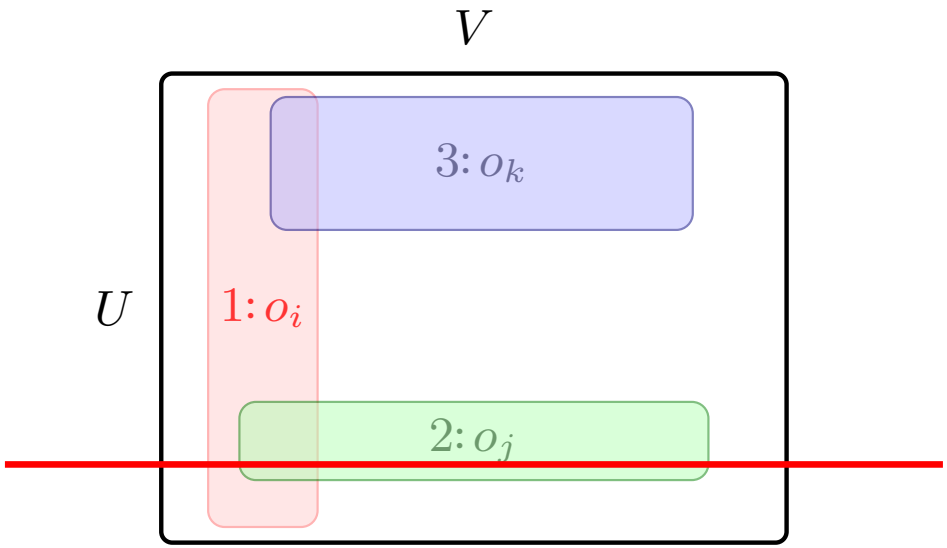
KW^{m} — «полное отношение»

- $\mathcal{S} \subseteq U \times V \times \mathcal{O}$;
- определим такую функцию $F_{\mathcal{S}}\colon \{0,1\}^m \to \{0,1\}$, что $\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.



KW^{m} — «полное отношение»

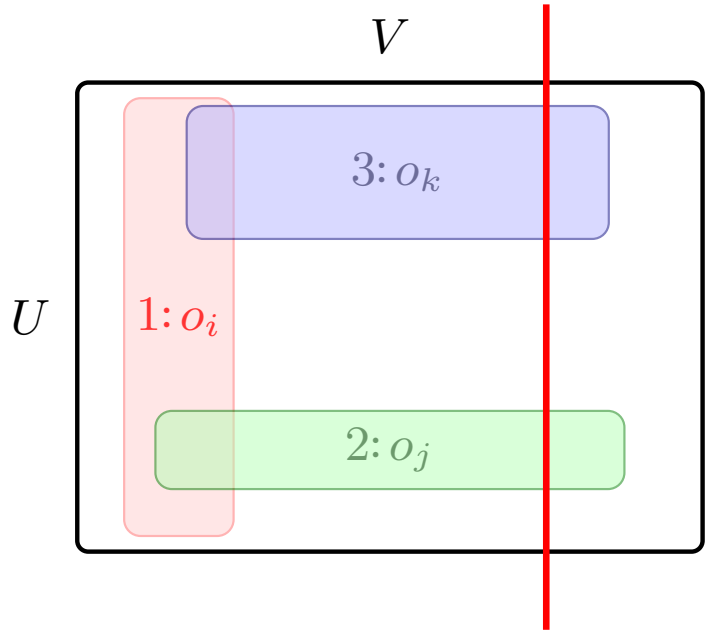
- $\mathcal{S} \subseteq U \times V \times \mathcal{O}$;
- определим такую функцию $F_{\mathcal{S}}\colon \{0,1\}^m \to \{0,1\}$, что $\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.



$F_{\mathcal{S}}(1,1,0,\dots) \coloneqq 1$

KW^{m} — «полное отношение»

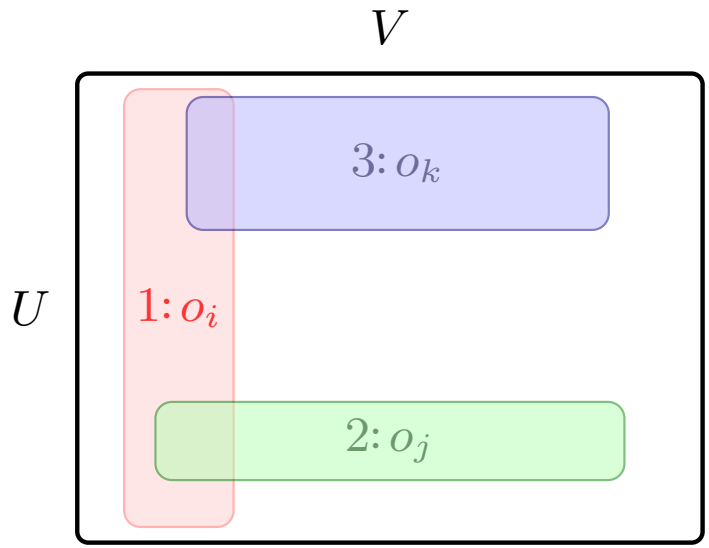
- $\mathcal{S} \subseteq U \times V \times \mathcal{O}$;
- определим такую функцию $F_{\mathcal{S}}\colon \{0,1\}^m \to \{0,1\}$, что $\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.



$F_{\mathcal{S}}(1,1,0,\dots) \coloneqq 1, \quad F_{\mathcal{S}}(1,0,0,\dots) \coloneqq 0$

KW^{m} — «полное отношение»

- $\mathcal{S} \subseteq U \times V \times \mathcal{O}$;
- определим такую функцию $F_{\mathcal{S}}\colon \{0,1\}^m \to \{0,1\}$, что $\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.



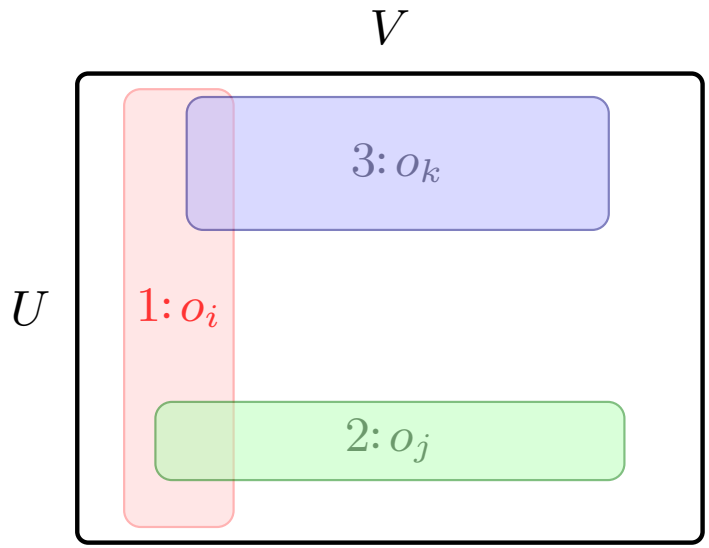
$F_{\mathcal{S}}(1,1,0,\dots) \coloneqq 1, \quad F_{\mathcal{S}}(1,0,0,\dots) \coloneqq 0$

Лемма

$\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.

KW^{m} — «полное отношение»

- $\mathcal{S} \subseteq U \times V \times \mathcal{O}$;
- определим такую функцию $F_{\mathcal{S}}\colon \{0,1\}^m \to \{0,1\}$, что $\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.



$F_{\mathcal{S}}(1,1,0,\dots) \coloneqq 1, \quad F_{\mathcal{S}}(1,0,0,\dots) \coloneqq 0$

Лемма

$\mathrm{D}(\mathsf{KW}^{\mathsf{m}}_{F_{\mathcal{S}}}) = \mathrm{D}(S)$.

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

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

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

$\varphi(z) \coloneqq \bigwedge_{i=1}^{m} C_i$ — 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]

$\varphi(z) \coloneqq \bigwedge_{i=1}^{m} C_i$ — 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:

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

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

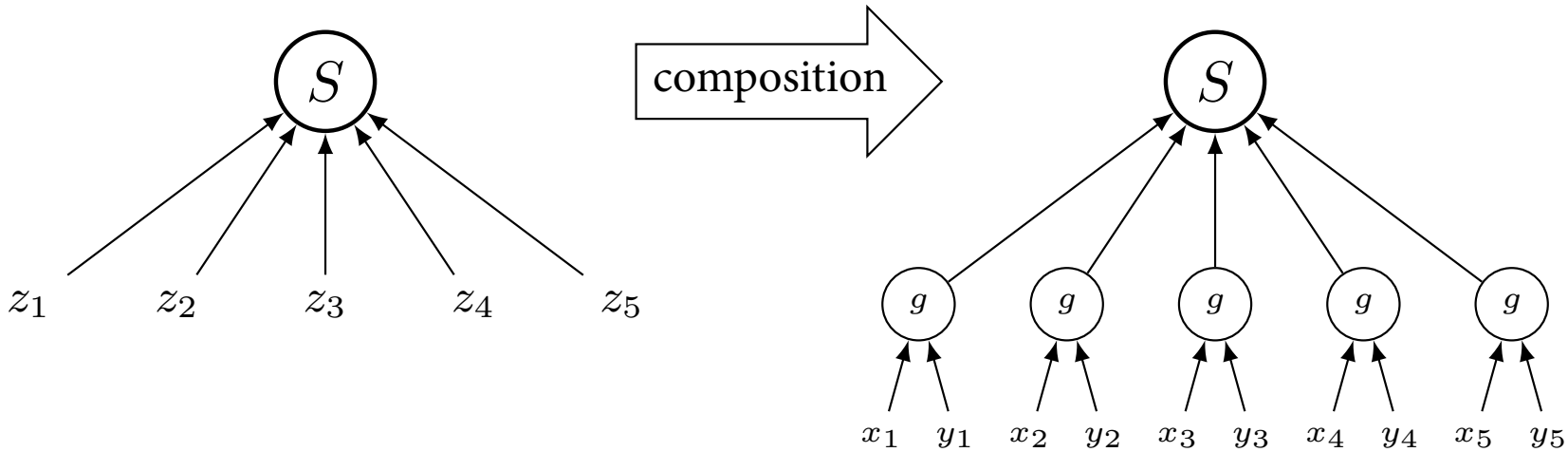
$\varphi(z) \coloneqq \bigwedge_{i=1}^{m} C_i$ — невыполнимая КНФ формула.

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

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

Коммуникационная версия:

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



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

Лифтинг

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

Резолюционная глубина φ не менее $d \Rightarrow \mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \geq n^{\mathcal{O}(d)}$, 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}.

Лифтинг

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

Резолюционная глубина φ не менее $d \Rightarrow \mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \geq n^{\mathcal{O}(d)}$, 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 $\Omega(S)$, где $m \coloneqq \mathsf{poly}(n)$.

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

Лифтинг

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

Резолюционная глубина φ не менее $d \Rightarrow \mathrm{D}(\mathsf{Search}_\varphi \circ \mathsf{Ind}_m) \geq n^{\mathcal{O}(d)}$, 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 $\Omega(S)$, где $m \coloneqq \mathsf{poly}(n)$.

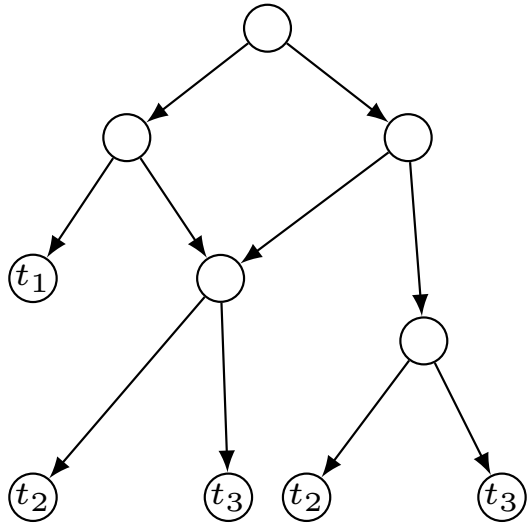
Следствие: нижние оценки на мототонные схемы 2^{n^ε}.

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

Nullstellensatz $\Leftrightarrow$ Алгебраические замощения для $\mathsf{Search}_\varphi \circ g$.

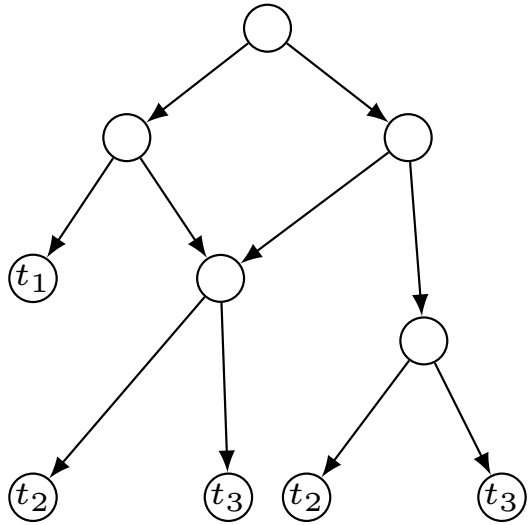
Dag-like протоколы. $f\colon X \times Y \to Z$

- H — граф, выходящая степень 2, $\forall h \in H,\ R_h \coloneqq X_h \times Y_h$;
- $R_{\text{root}} = X \times Y$;
- a, b — дети $h \Rightarrow R_h \subseteq R_a \cup R_b$;
- h — лист $\Rightarrow h$ помечен $z \in Z$ и $f^{-1}(z) \supseteq R_h$.

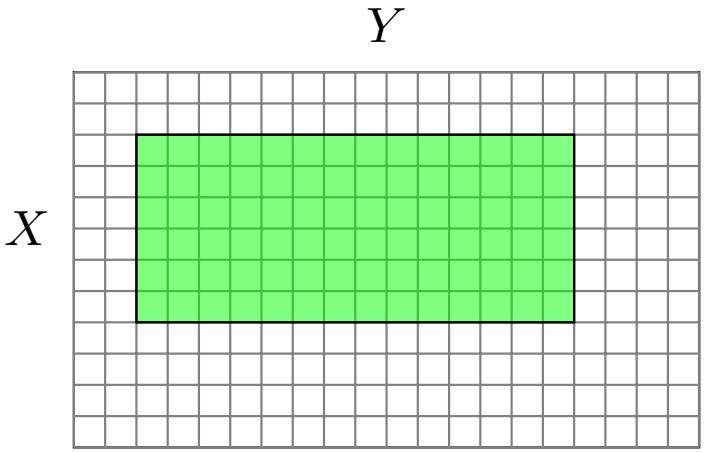


Dag-like протоколы. $f\colon X \times Y \to Z$

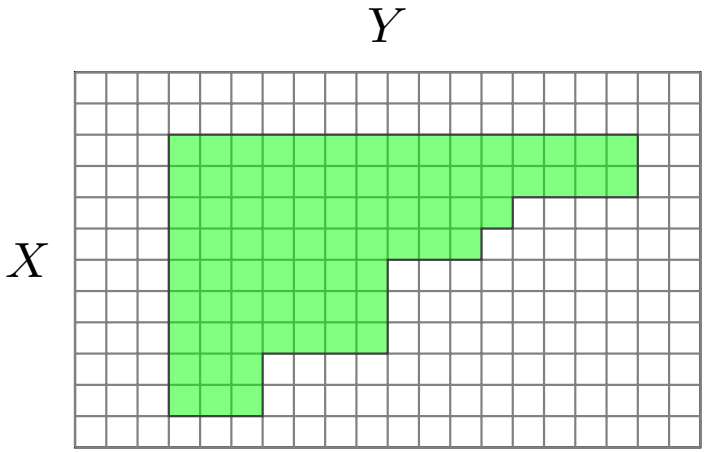
- H — граф, выходящая степень 2, $\forall h \in H,\ R_h \coloneqq X_h \times Y_h$;
- $R_{\text{root}} = X \times Y$;
- a, b — дети $h \Rightarrow R_h \subseteq R_a \cup R_b$;
- h — лист $\Rightarrow h$ помечен $z \in Z$ и $f^{-1}(z) \supseteq R_h$.



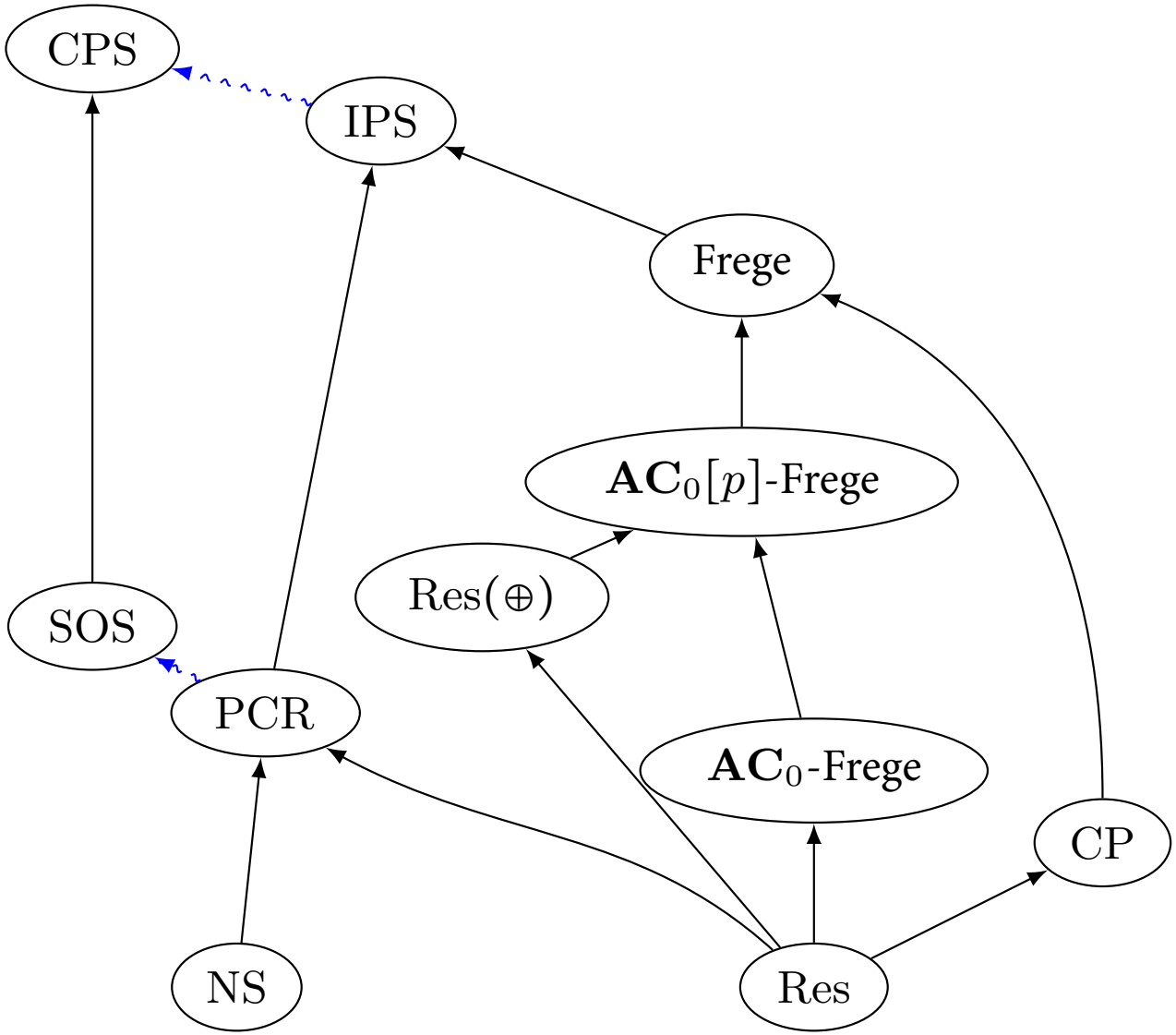
Прямоугольники:



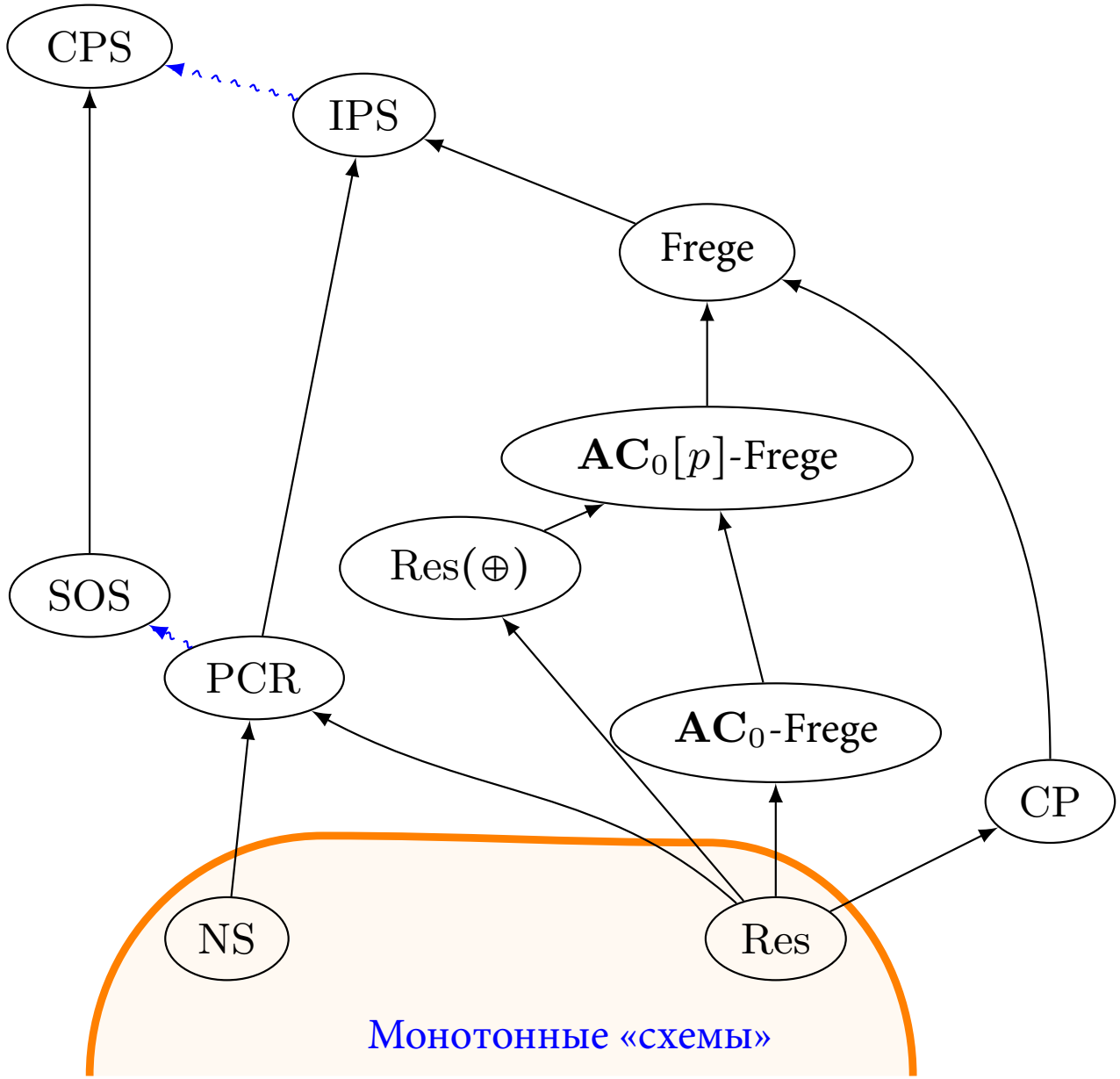
Треугольники:



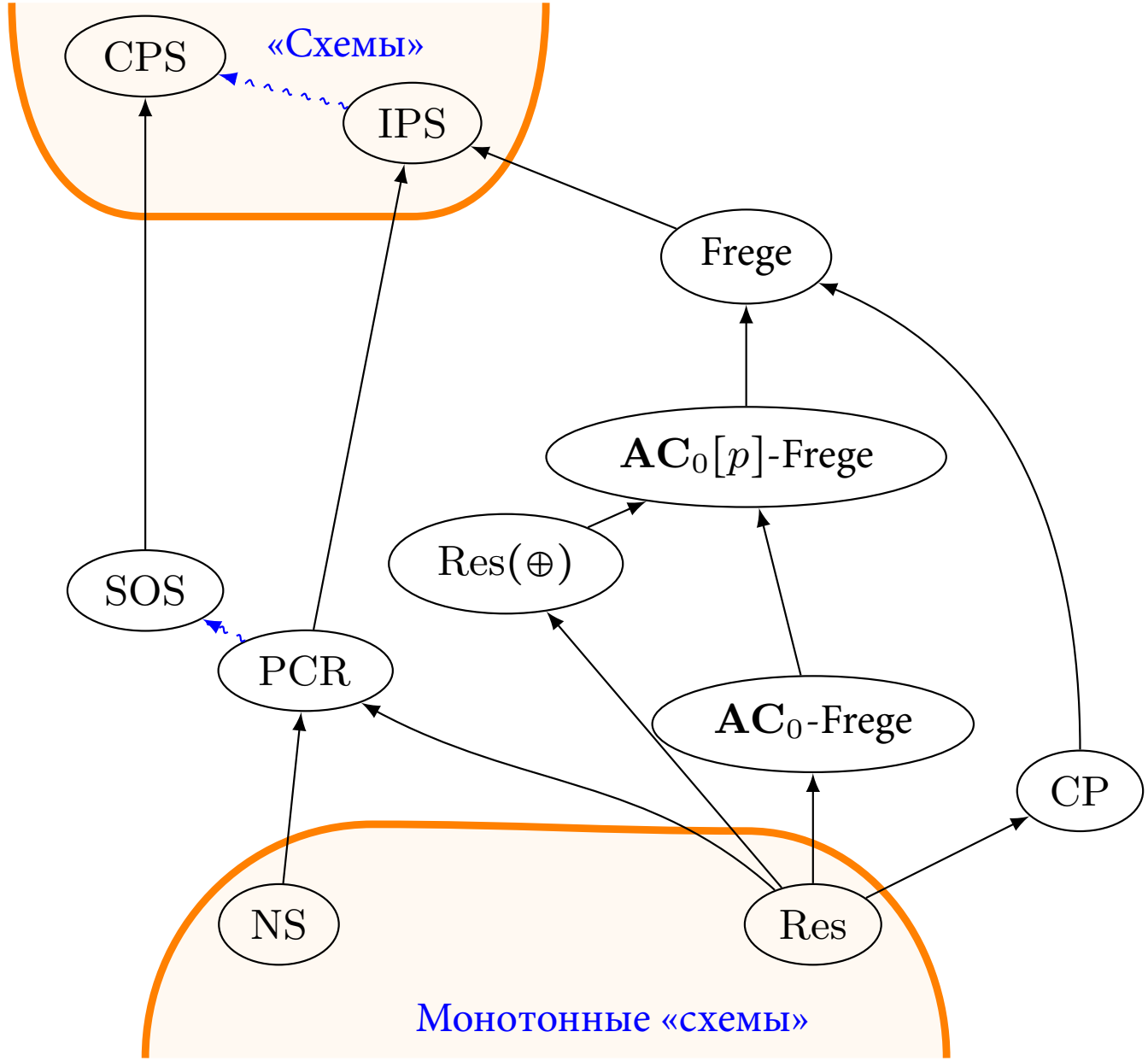
Иерархия


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

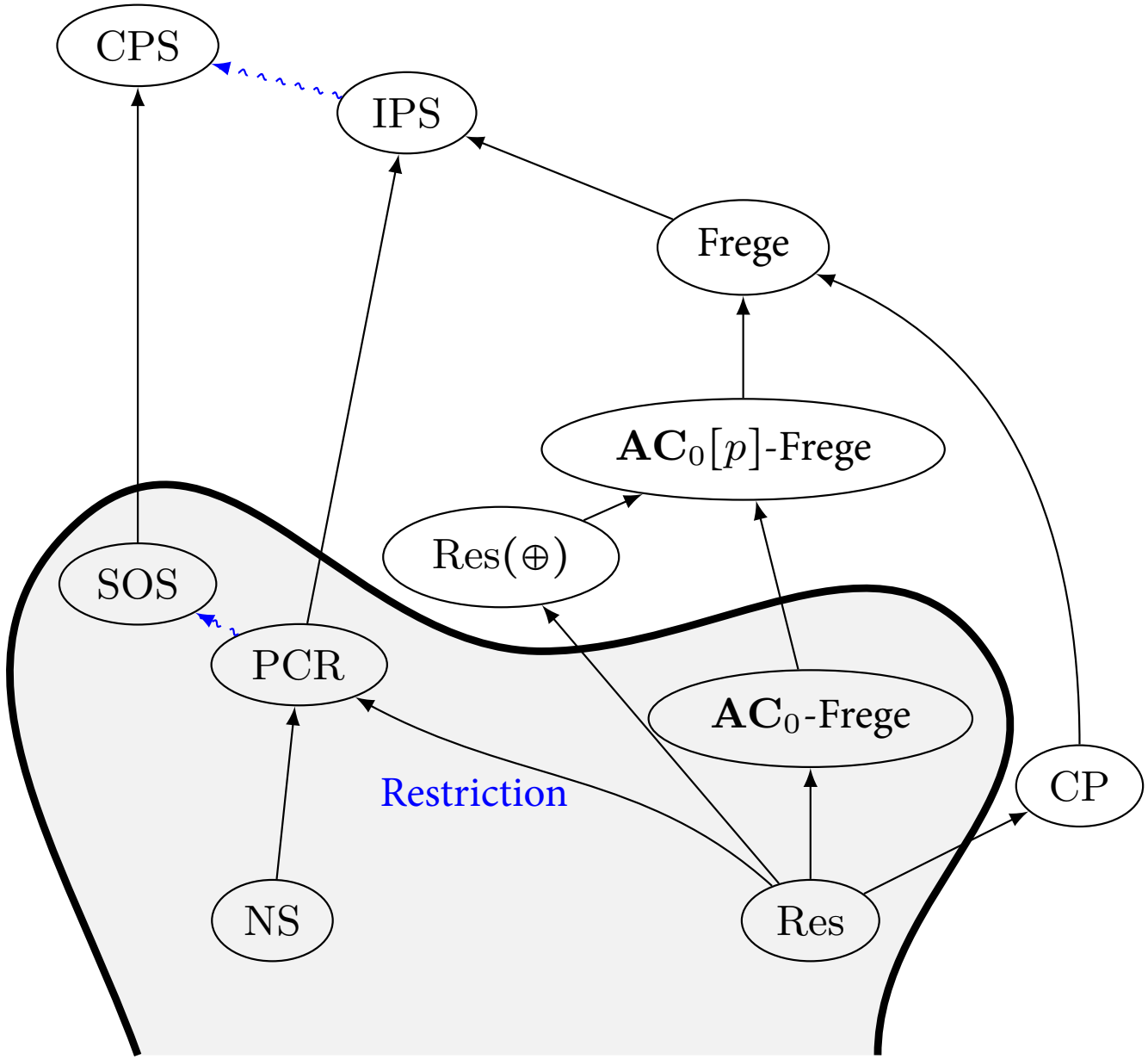
Иерархия


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

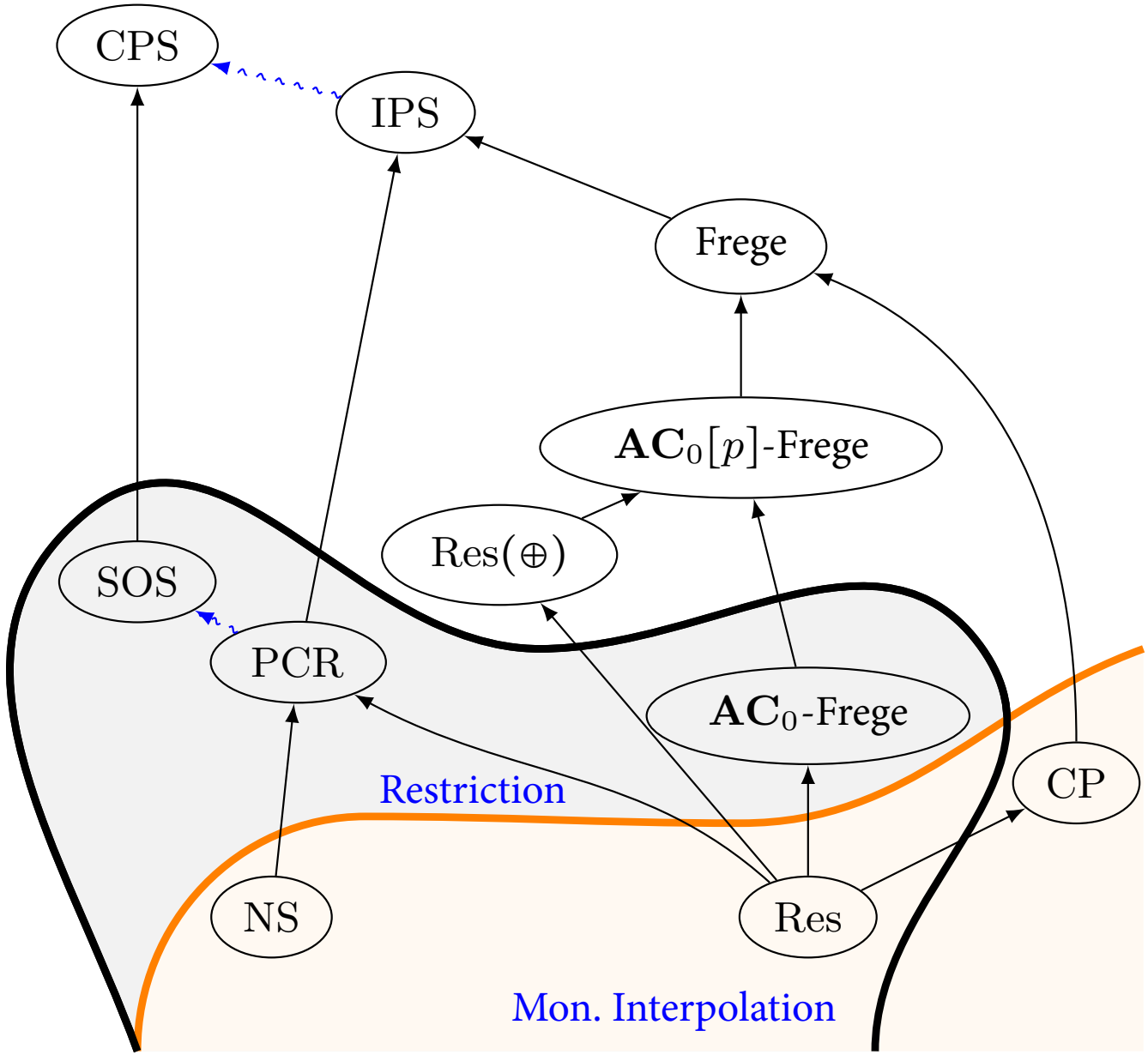
Иерархия


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

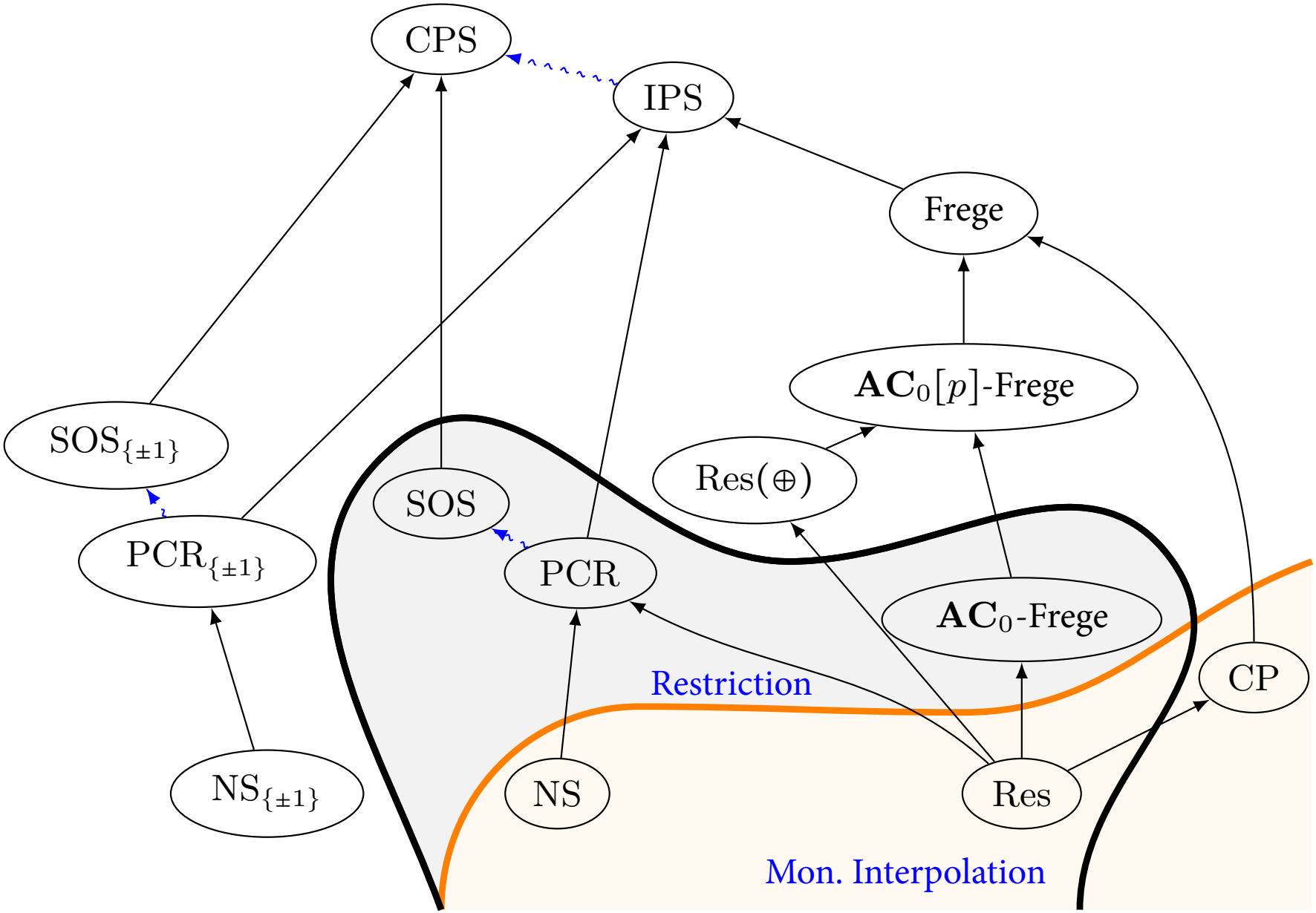
Иерархия


CPS
IPS
Frege
$\mathbf{AC}_0[p]$-Frege
Res($\oplus$)
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
$\mathrm{SOS}_{\{\pm 1\}}$
Res($\oplus$)
SOS
$\mathrm{PCR}_{\{\pm 1\}}$
PCR
$\mathbf{AC}_0$-Frege
CP
Restriction
$\mathrm{NS}_{\{\pm 1\}}$
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

Mod_p