Нижние оценки схемной сложности булевых функций

Эдуард Гирш

Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН

(совм. с: А.Г.Головнёв, А.А.Кноп, А.С.Куликов, М.Г.Финд)

Нижние оценки схемной сложности булевых функций

Эдуард Гирш

Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН

(совм. с: А.Г.Головнёв, А.А.Кноп, А.С.Куликов, М.Г.Финд)

- Схемная сложность, введение.
- Линейные оценки на сложность явных функций.
- Ограничения на метод устранения гейтов.

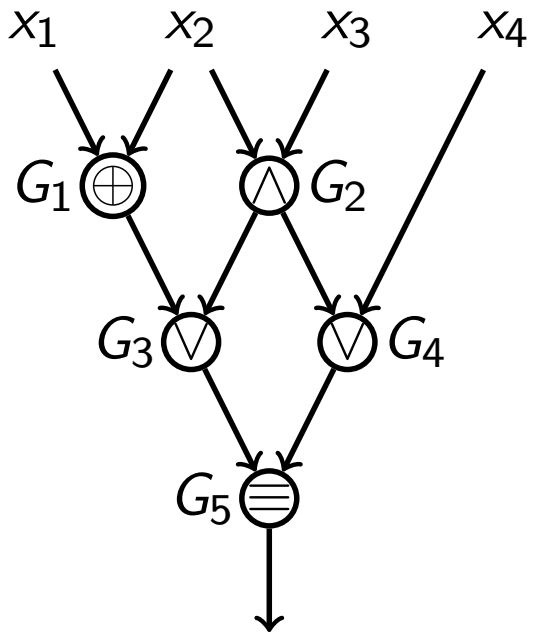
Булевы схемы как модель вычислений

- Булевы функции $f : \{0,1\}^n \to \{0,1\}$.
- Вычисляем при помощи бинарных операций:

Входы:
$x_1, \ldots, x_n$

Операции (гейты, элементы):
бинарные

$$
\begin{aligned}
G_1 &= x_1 \oplus x_2 \\
G_2 &= x_2 \wedge x_3 \\
G_3 &= G_1 \vee G_2 \\
G_4 &= G_2 \vee x_4 \\
G_5 &= G_3 \equiv G_4
\end{aligned}
$$



Оценки схемной сложности

Произвольные функции:

Нижняя:	$\Omega(2^n/n)$	[Шеннон 1949].
Верхняя:	$(1+o(1))2^n/n$	[Лупанов 1958].

Оценки схемной сложности

Произвольные функции:

Нижняя:	$\Omega(2^n/n)$	[Шеннон 1949].
Верхняя:	$(1+o(1))2^n/n$	[Лупанов 1958].

Явные функции (нижние оценки с точностью до $-o(n)$):

$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	[Клосс, Малышев 1965]
$2n$	$f(x) = [\sum x_i \equiv 0 \pmod 3]$	[Шнорр 1974]
$2.5n$	$f(x,a,b) = x_a \oplus x_b$	[Пол 1977]
$3n$	$f(x,a,b,c,\delta) = x_a^\delta \wedge (x_b \oplus x_c)$	[Н.Блюм 1984]

$x \in \{0,1\}^n$, $\quad a,b,c \in \{0,1\}^{\log_2 n}$, $\quad \delta \in \{0,1\}$

Оценки схемной сложности

Произвольные функции:

Нижняя:	$\Omega(2^n/n)$	[Шеннон 1949].
Верхняя:	$(1+o(1))2^n/n$	[Лупанов 1958].

Явные функции (нижние оценки с точностью до $-o(n)$):

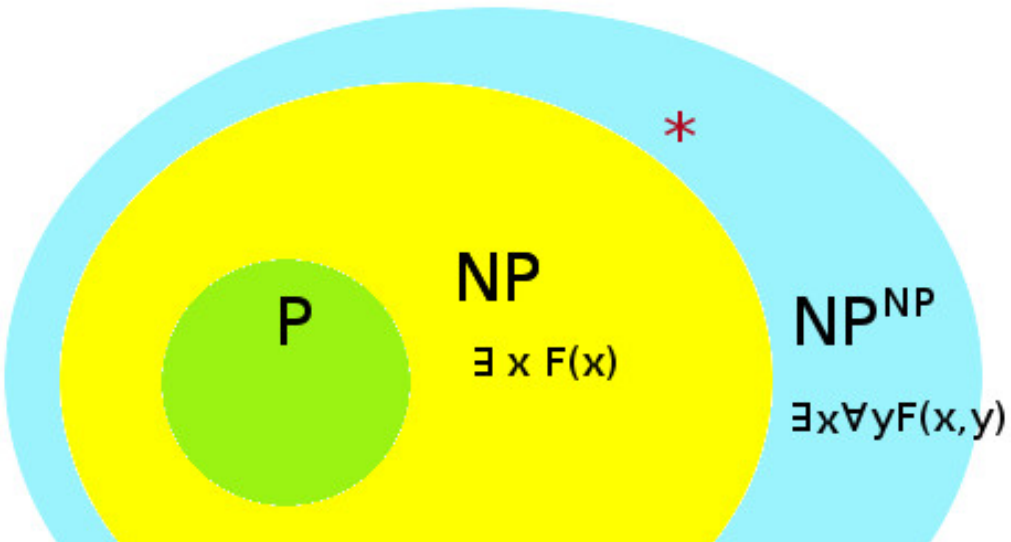
$2n$	$f(x) = \bigoplus_{i<j} x_i x_j$	[Клосс, Малышев 1965]
$2n$	$f(x) = [\sum x_i \equiv 0 \pmod 3]$	[Шнорр 1974]
$2.5n$	$f(x,a,b) = x_a \oplus x_b$	[Пол 1977]
$3n$	$f(x,a,b,c,\delta) = x_a^\delta \wedge (x_b \oplus x_c)$	[Н.Блюм 1984]

$x \in \{0,1\}^n, \quad a,b,c \in \{0,1\}^{\log_2 n}, \quad \delta \in \{0,1\}$

Экспоненциальные нижние оценки для ограниченных моделей вычислений [Разборов], [Хостад] и др.

Что известно ещё о размере схем?

- Полиномиальные верхние оценки на размер схем для NP влекут коллапс полиномиальной иерархии до NP^{NP} [Карп-Липтон 1980], но нелинейных нижних не доказано.
- Полиномиальные нижние оценки для функций из классов большей сложности [Каннан 1982]

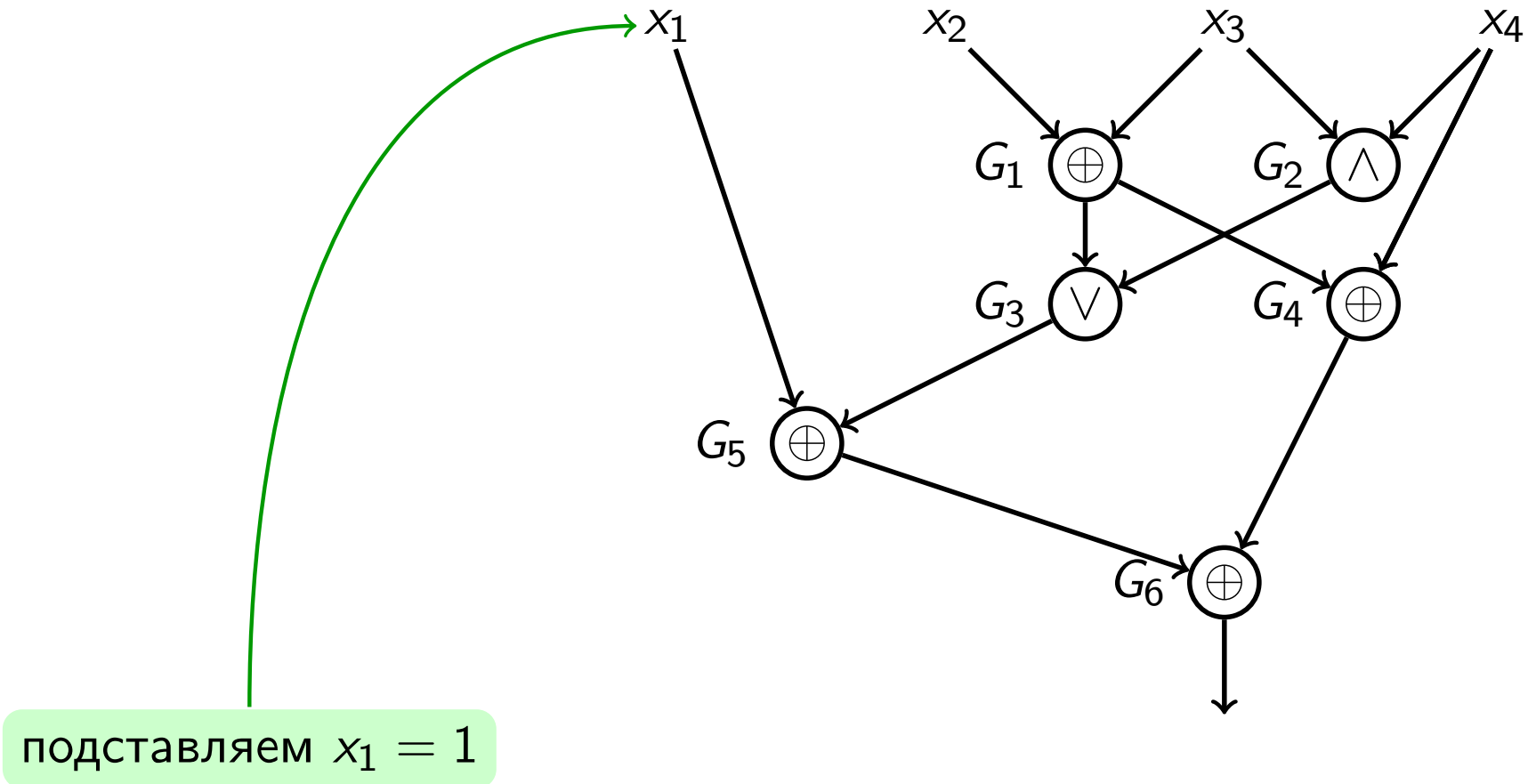


Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.

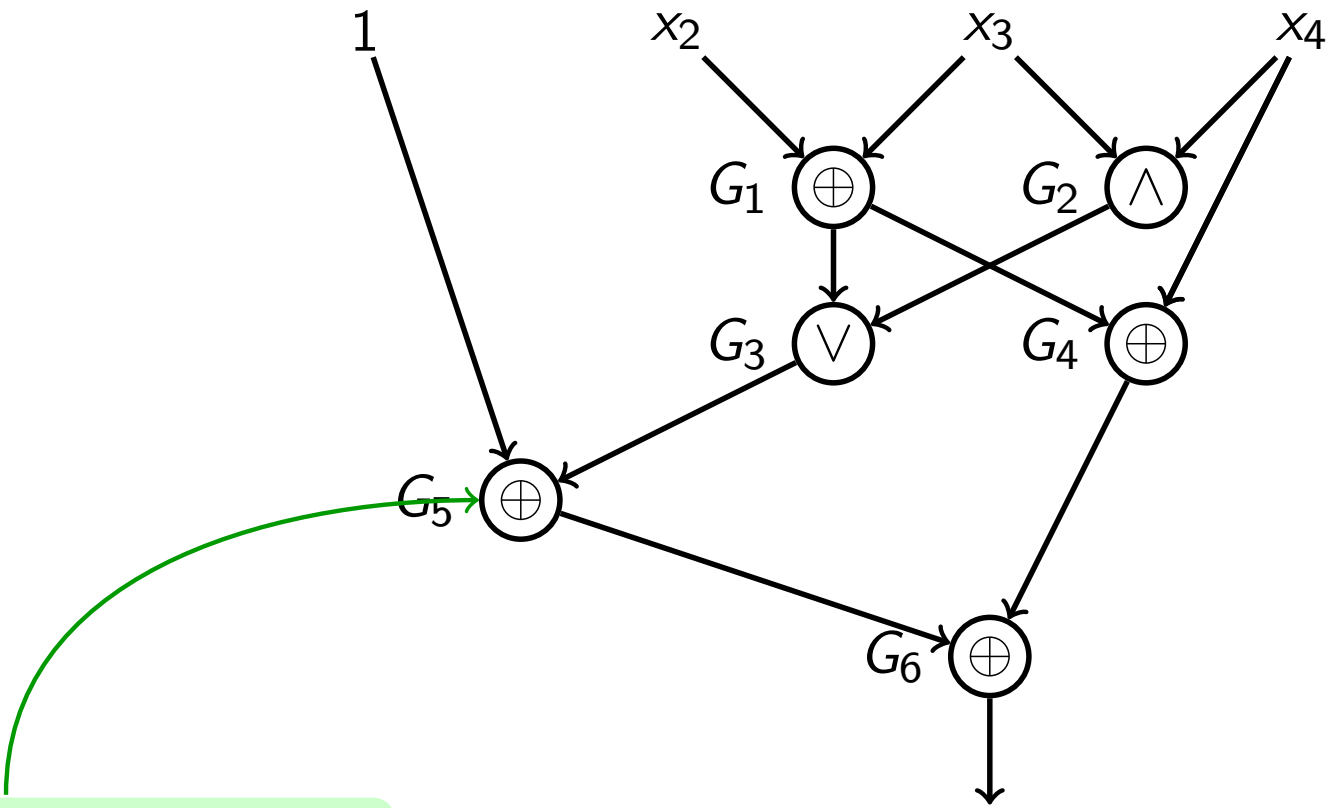
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



Новая линейная нижняя оценка для явной функции

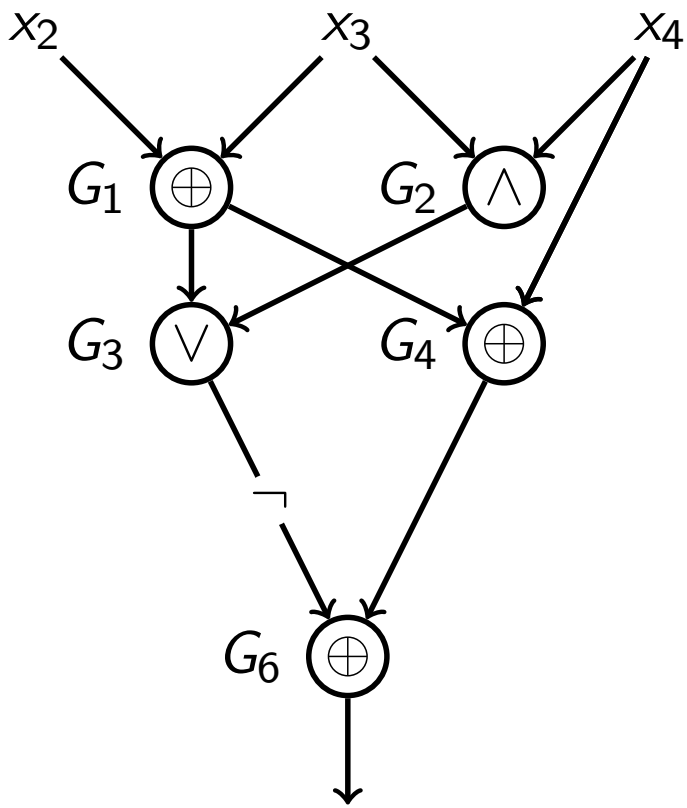
- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



G_5 вычисляет $G_3 \oplus 1 = \neg G_3$

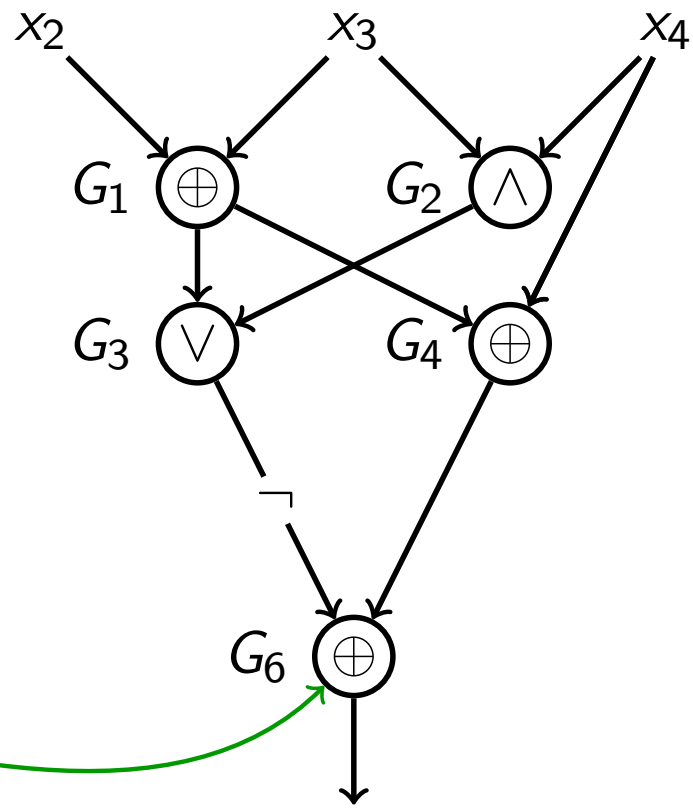
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



Новая линейная нижняя оценка для явной функции

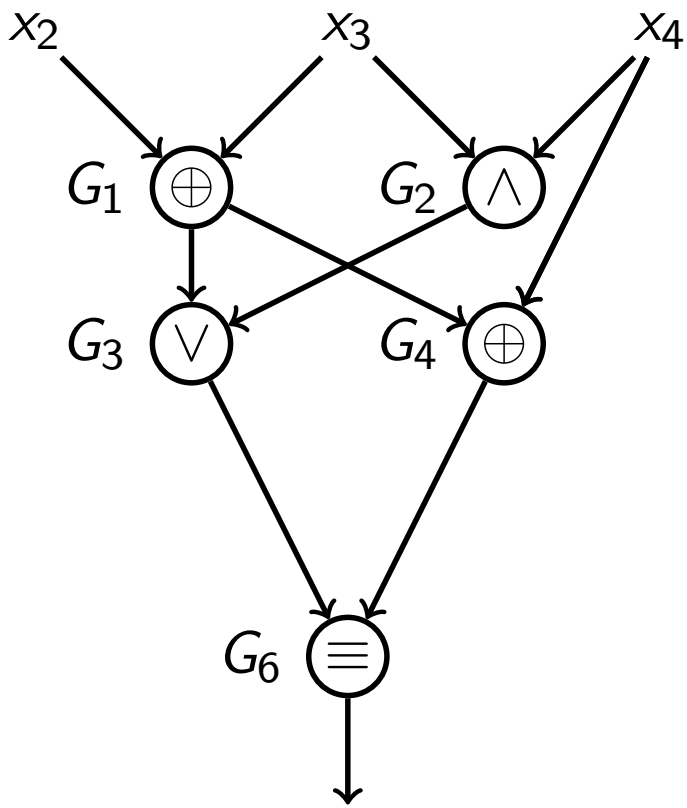
- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



вносим отрицание в G_6

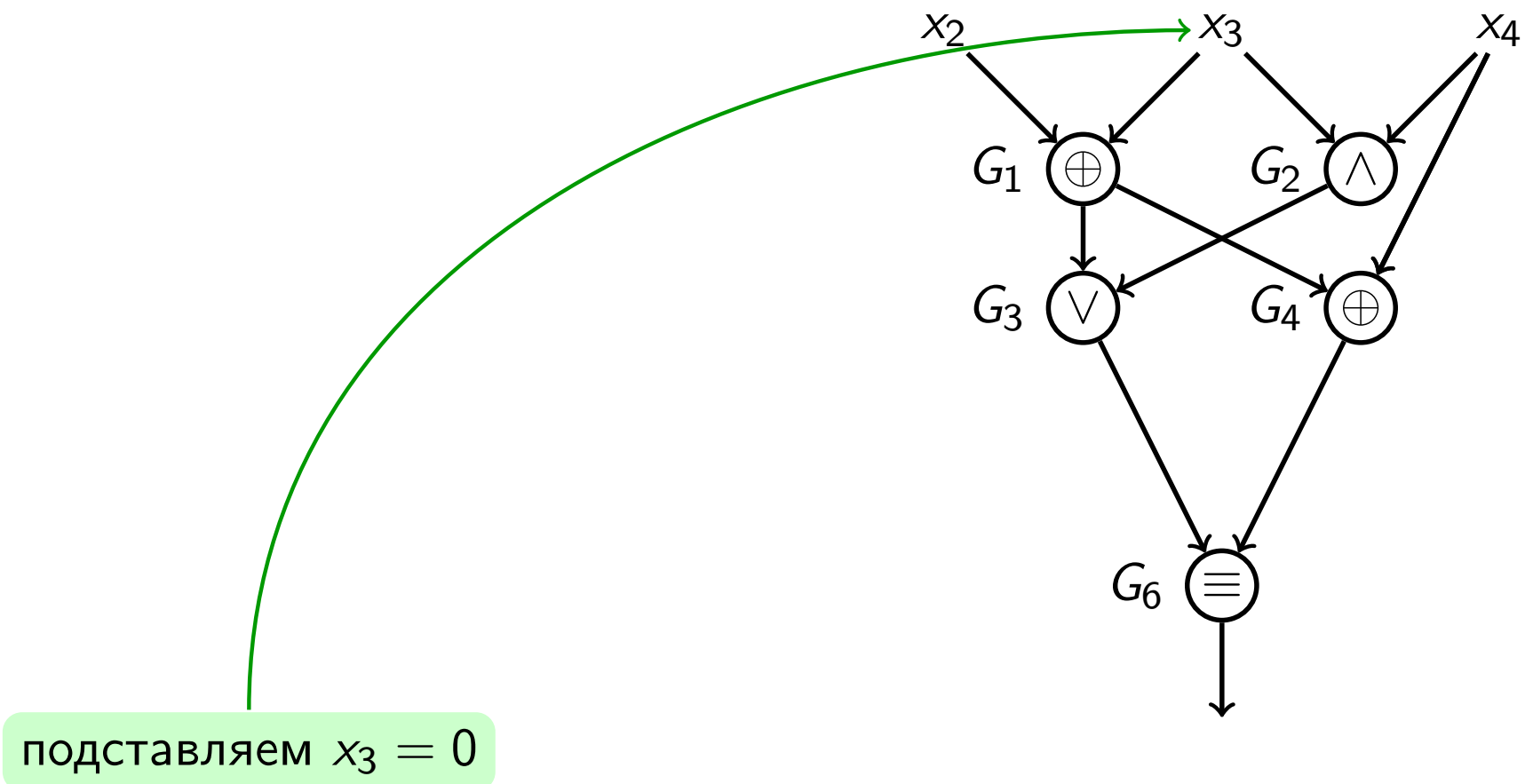
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



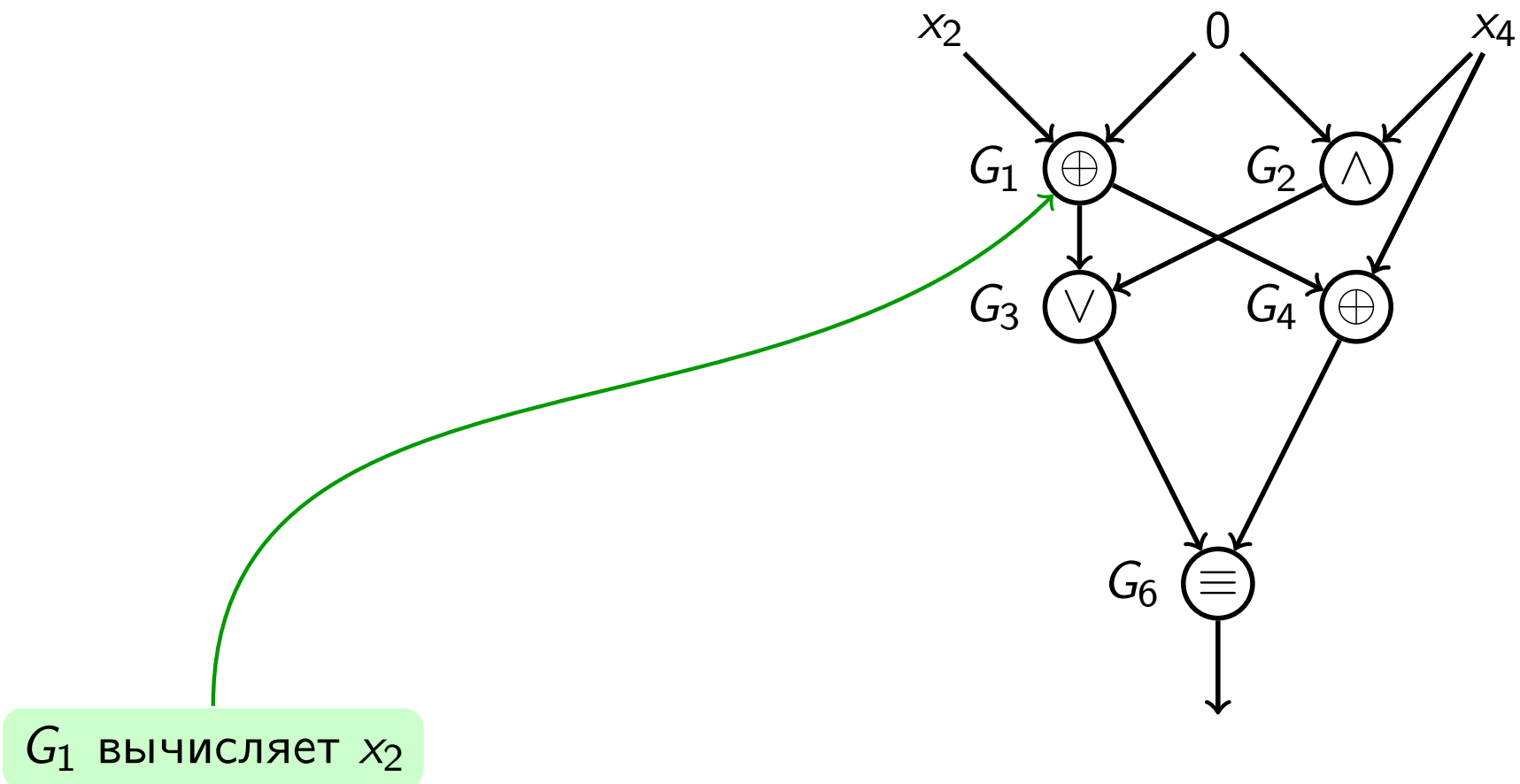
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



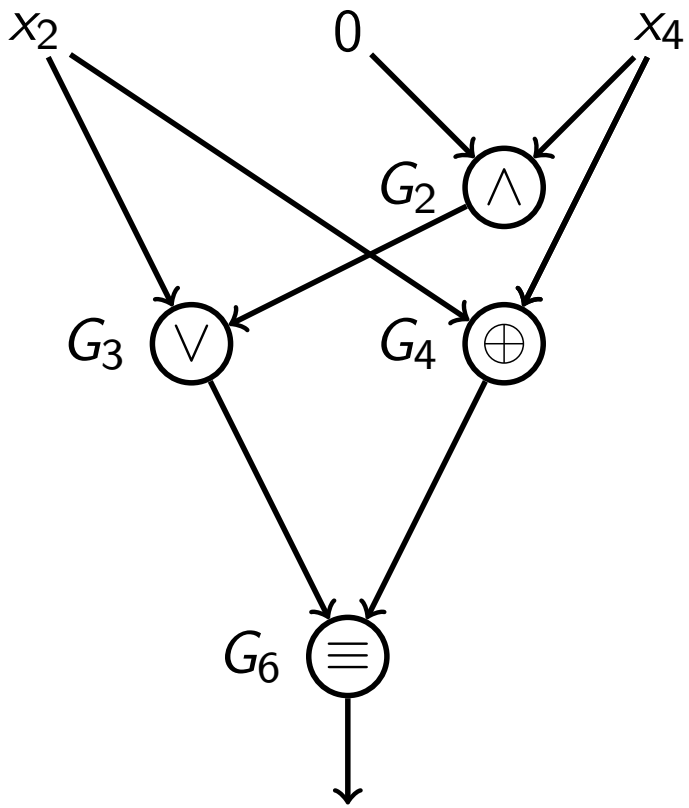
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



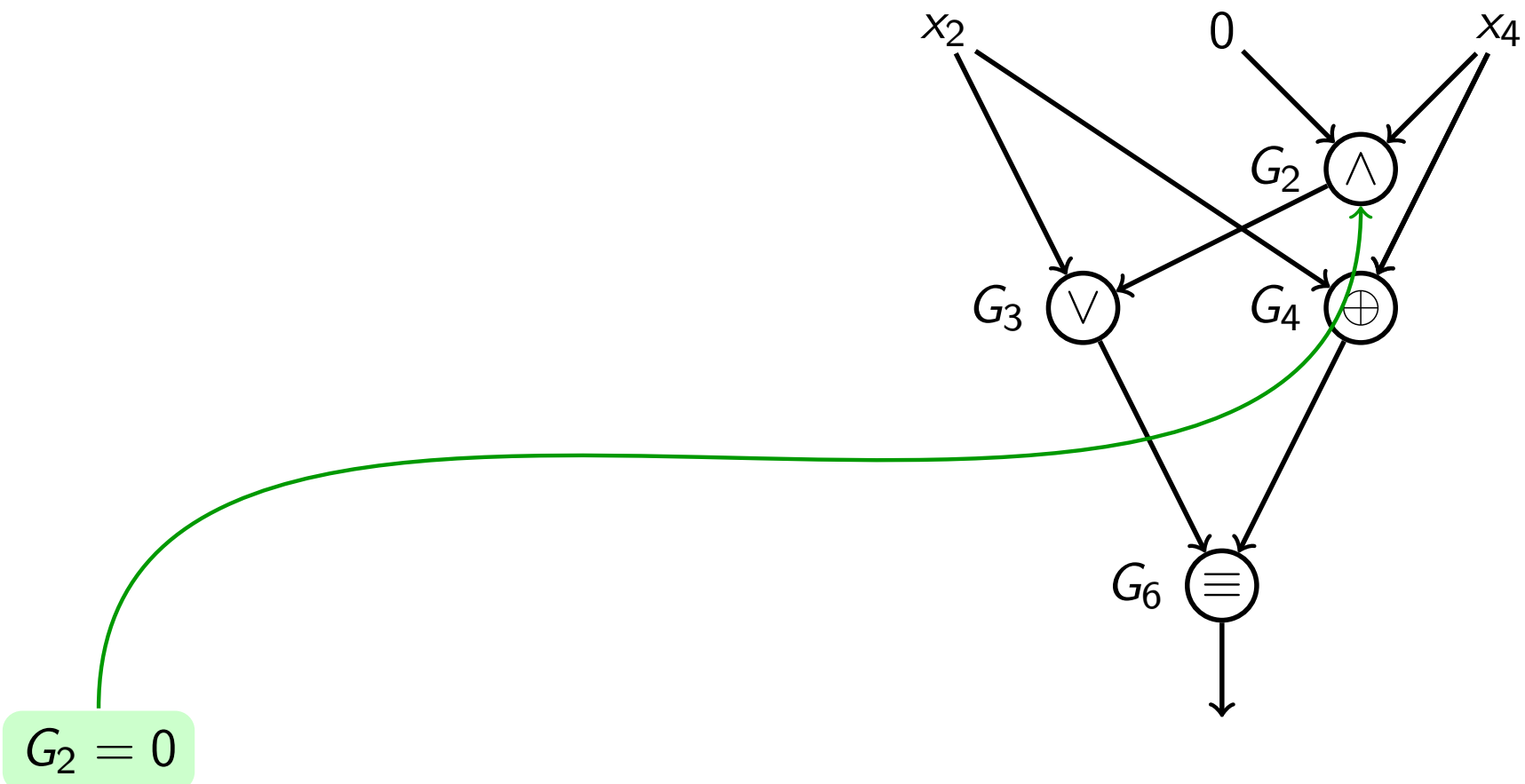
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



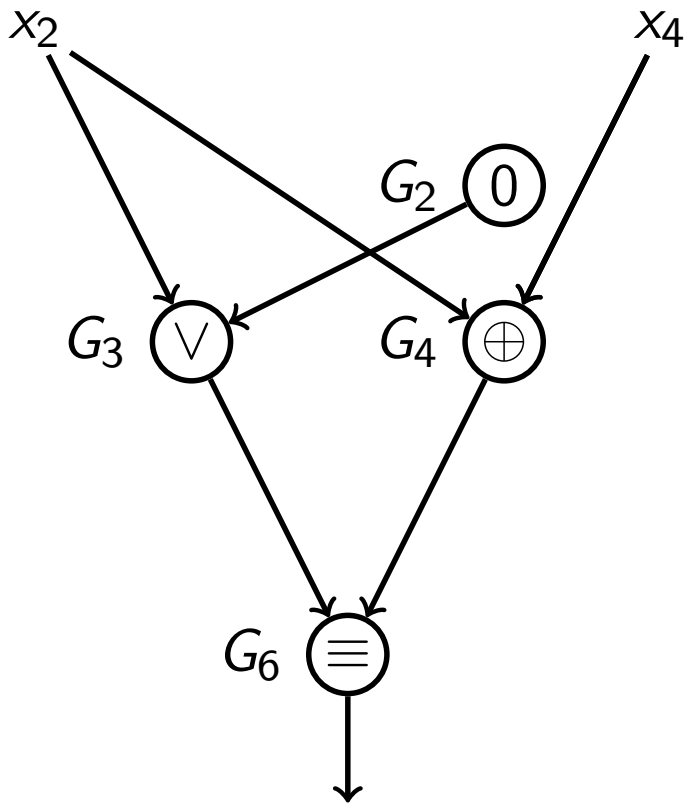
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



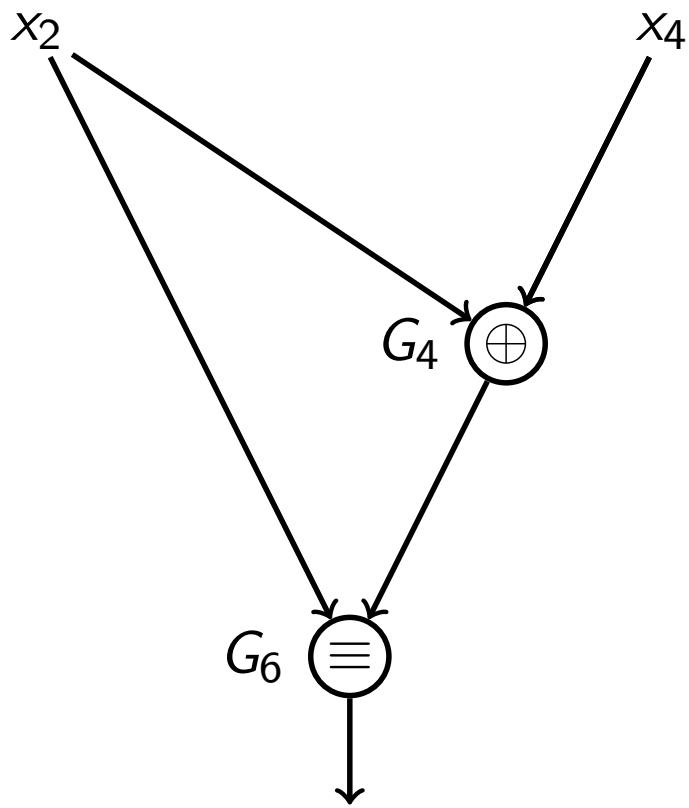
Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.



Новая линейная нижняя оценка для явной функции

- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.

- Новая оценка: $(3 + \frac{1}{86})n - o(n)$.
- Функция: аффинный дисперсер размерности $d(n) = o(n)$: на любом аффинном подпространстве $\mathbb{F}_2^n$ размерности $d(n)$ не константа.

Новая линейная нижняя оценка для явной функции

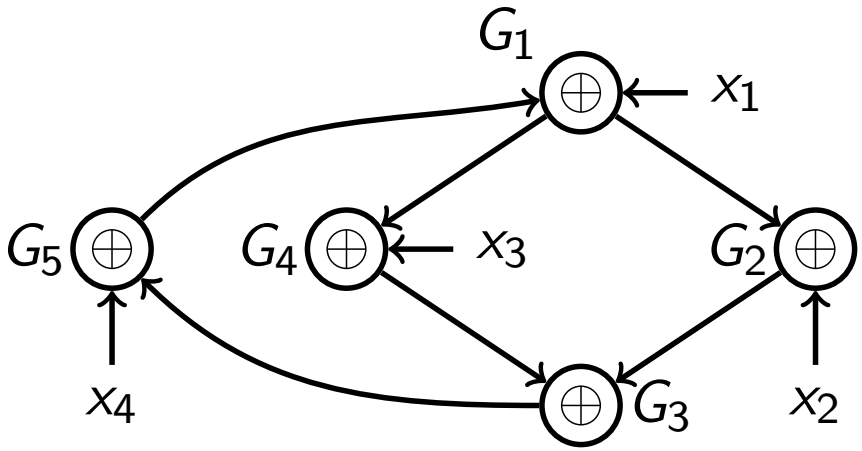
- Лучшая предыдущая оценка: $3n - o(n)$ [Н.Блюм 1984].
- Доказывается по индукции: подставляем значения переменным, сложность падает на 3 гейта.

- Новая оценка: $(3 + \frac{1}{86})n - o(n)$.
- Функция: аффинный дисперсер размерности $d(n) = o(n)$: на любом аффинном подпространстве $\mathbb{F}_2^n$ размерности $d(n)$ не константа.
- Можно подставлять линейные функции, не заботясь о нетривиальности результата — даёт ту же оценку $3n - o(n)$ [Деменков, Куликов 2012].
- Явная конструкция: [Бен-Сассон, Коппарти 2012]

Идеи доказательства $3\frac{1}{86}n - o(n)$

Циклические схемы

Обобщение булевых схем: циклические схемы.



Идеи доказательства $3\frac{1}{86}n - o(n)$

Квадратичные подстановки

- Разрешаем подстановки $z = x \wedge y$.

Идеи доказательства $3\frac{1}{86}n - o(n)$

Квадратичные подстановки

- Разрешаем подстановки $z = x \wedge y$.

- Квадратичные подстановки требуют квадратичных дисперсеров.
- Явные конструкции квадратичных дисперсеров неизвестны.

Идеи доказательства $3\frac{1}{86}n - o(n)$

Квадратичные подстановки

- Разрешаем подстановки $z = x \wedge y$.

- Квадратичные подстановки требуют квадратичных дисперсеров.
- Явные конструкции квадратичных дисперсеров неизвестны.

- Необходимо найти аффинное пространство внутри многообразия.
- Композиции подстановок вида $z = \sum x_i x_j \oplus \sum x_k$,
  в произведениях каждая x_i участвует единожды.

Идеи доказательства $3\frac{1}{86}n - o(n)$

Сложностная мера

- Учитываем:
  - число гейтов g,
  - число переменных v,
  - число квадратичных подстановок q,
  - число специальных ситуаций s.
- Мера $\mu = g + 6\frac{2}{43}v + 1\frac{22}{43}q + \frac{1}{43}s$.
- На каждом шаге уменьшаем на $9\frac{3}{43}$.
- Итого не менее $3\frac{1}{86}n - o(n)$ гейтов.

Теорема

Схемная сложность аффинного дисперсера размерности $o(n)$ составляет не менее $3\frac{1}{86}n - o(n)$ гейтов.

Алгебраический вопрос

- Явная конструкция квадратичного дисперсера размерности $o(n)$?
- Упрощает и усиливает оценку [Головнёв, Куликов 2015].
- Известны конструкции для линейной размерности [Двир 2012, Коэн-Тал 2015, Шалтиел 2011].

Ограничения на метод

Формулировки метода

- Теоремы об ограничениях на методы — обычное дело в теории сложности:
  - релятивизация [Бейкер, Гилл, Соловей 1975],
  - “естественные” доказательства [Разборов, Рудич 1997],
  - “алгебраизация” [Ааронсон, Вигдерсон 2009].

Ограничения на метод

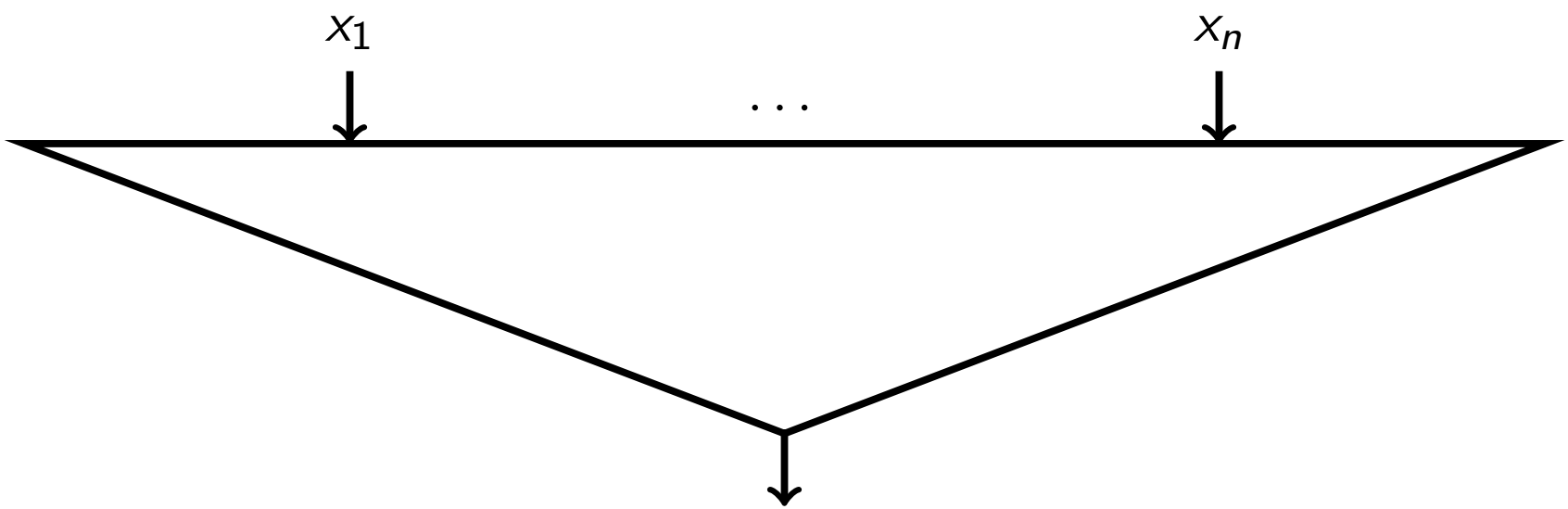
Формулировки метода

- Теоремы об ограничениях на методы — обычное дело в теории сложности:
  - релятивизация [Бейкер, Гилл, Соловей 1975],
  - “естественные” доказательства [Разборов, Рудич 1997],
  - “алгебраизация” [Ааронсон, Вигдерсон 2009].
- Можно ли доказать нелинейную оценку методом элиминации гейтов?
- Варианты метода:
  - одна подстановка или несколько,
  - мера сложности: гейты, гейты с переменными, произвольная субаддитивная, ..?
  - класс функций?
- Есть ли функции, устойчивые относительно подстановок:

$$\forall \pi \; C(f|_\pi) \geq C(f) - \mathrm{const}$$

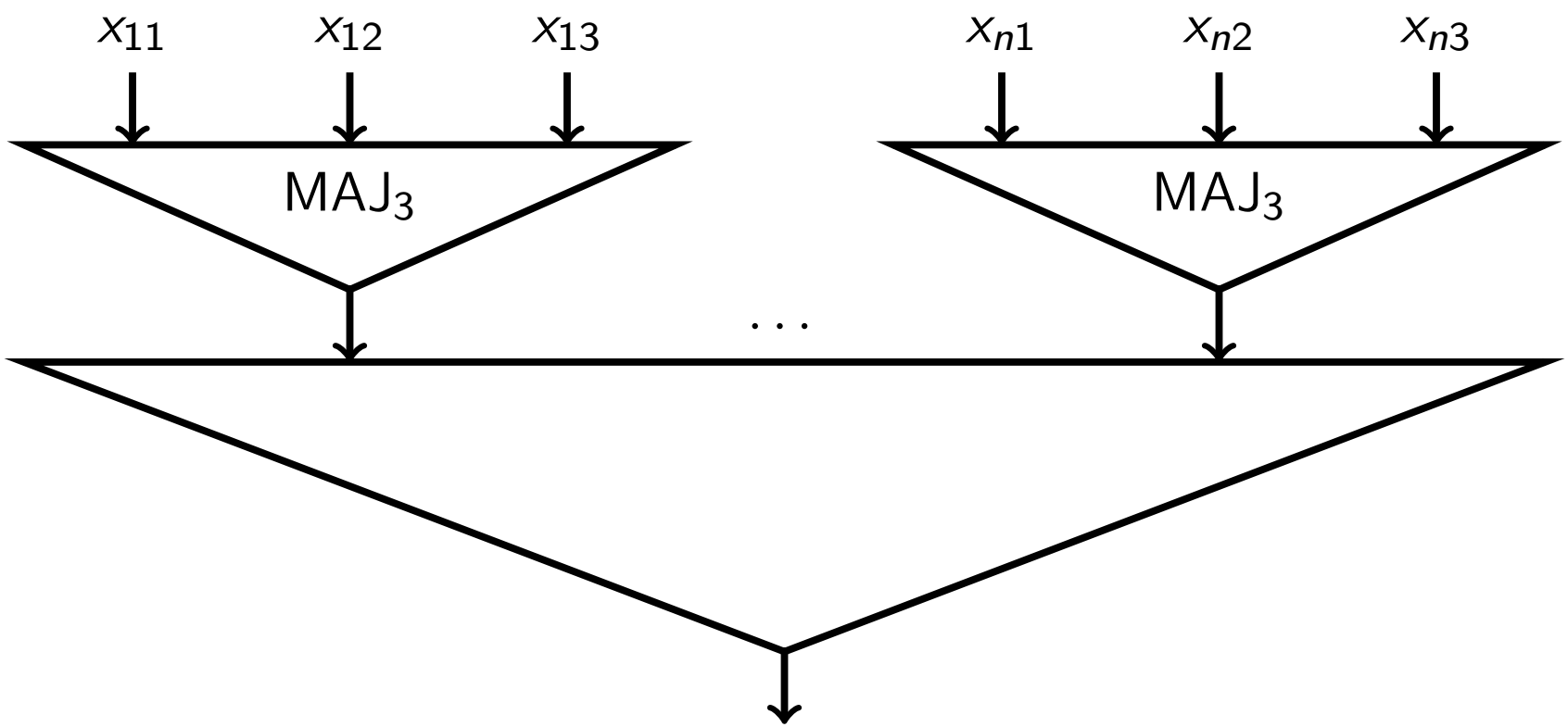
Ограничения на метод

Конструкция устойчивой функции



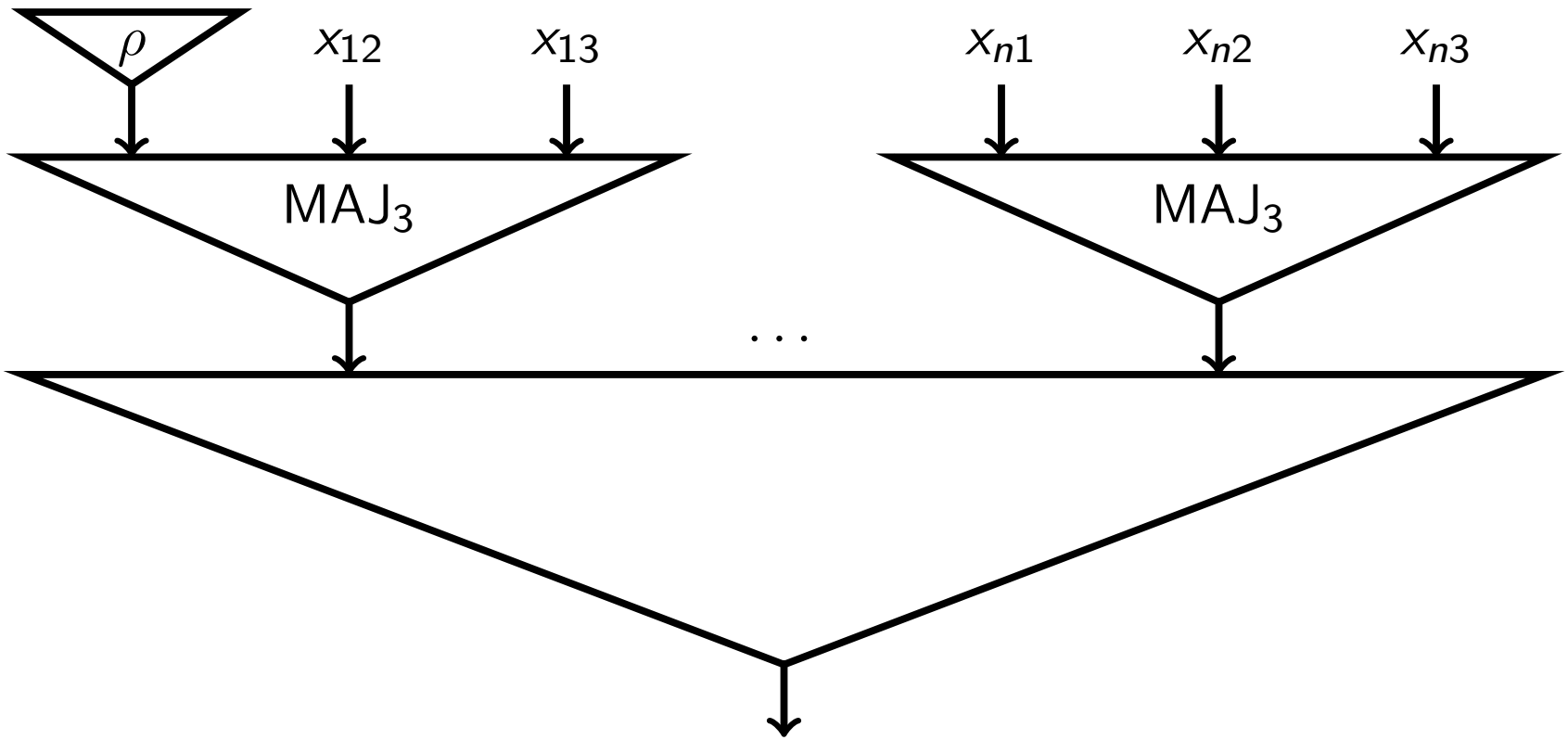
Ограничения на метод

Конструкция устойчивой функции



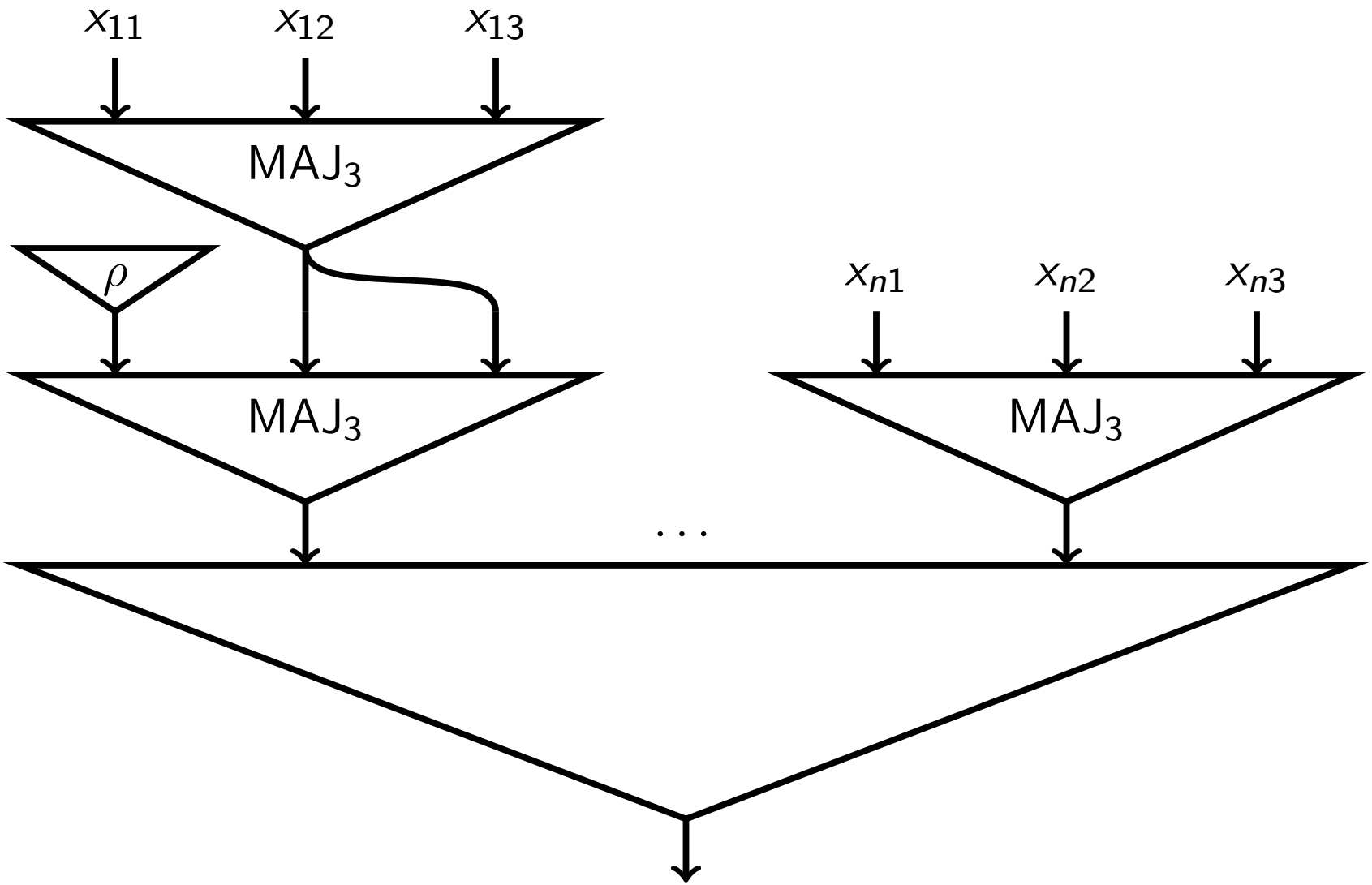
Ограничения на метод

Конструкция устойчивой функции



Ограничения на метод

Конструкция устойчивой функции



Ограничения на метод

Линейные комбинации числа гейтов и переменных

Определение (m-стабильная функция)

- $g\colon \{0,1\}^k \to \{0,1\}$
- S — *множество подставляемых переменных,* $|S|{=}m$,
- σ — *вектор значений для* S,
- x_i — *главная переменная* ($\notin S$),
- R — *все остальные переменные* ($k-m-1$ *шт.*),
- ρ — *вектор значений для* R.

$\forall S\ \forall i\ \exists \rho\ \forall \sigma\ g|_{\rho,\sigma} = x_i$ *или* $x_i \oplus 1$.

Конструкция (1-стабильная):

- $E\colon \{1,\ldots,7\} \to \{0,1\}^8$ код с расстоянием 4,
- $g(x) = 0$ на кодовых словах $x = E(i)$,
  - в т.ч. с изменённым битом i;
- $g(x) = 1$ на кодовых словах $E(i)$ с измененным битом $j \neq i$
  - в т.ч. с изменённым битом i.

Нелинейные оценки нельзя получить, рассматривая $O(1)$ подстановок:

- Субаддитивная мера сложности.
- Последовательность мер, линейная комбинация числа гейтов и переменных.
  - Рассматривая одну подстановку, нельзя доказать оценку лучше $11n$.
  - Рассматривая m подстановок и только число гейтов, нельзя доказать оценку лучше $4.5(2m + 1)n$.

Ограничения на метод

Вопросы

1. Можно ли найти устойчивую функцию, являющуюся одновременно аффинным дисперсером?

2. Существуют ли
   - $f : \{0,1\}^n \to \{0,1\}$ суперлинейной сложности и
   - $\varphi(n) = o(n)$,

   такие что
   - $\forall \pi$ — подстановки $n - \varphi(n)$ переменным функций от $\varphi(n)$ переменных

     $$C(f|_\pi) \geq C(f) - \mathrm{const} \cdot n$$

     ?