Лемма о несамодвойственной функции

Лемма 1 (о несамодвойственной функции)

Пусть $f \notin \mathbf{S}$. Тогда функции 0 и 1 можно задать формулами над множеством $\{f, \bar{}\}$.

Доказательство:

- пусть f — k-местная несамодвойственная функция

$\Rightarrow$ существует $\vec{b} = (b_1, \ldots, b_k) \in \{0,1\}^k$ такой, что $f(b_1, \ldots, b_k) = f(\bar{b}_1, \ldots, \bar{b}_k)$

- рассмотрим унарную функцию $\phi(x) = f(x^{b_1}, \ldots, x^{b_k})$

$\star$ $\phi(0) = f(0^{b_1}, \ldots, 0^{b_k}) = f(\bar{b}_1, \ldots, \bar{b}_k) = f(b_1, \ldots, b_k) = f(1^{b_1}, \ldots, 1^{b_k}) = \phi(1)$

$\Rightarrow$ $\phi(x)$ — константа

$\star$ вторую константу можно записать формулой $\overline{\phi(x)}$

$\star$ набор функций $x^{b_1}, \ldots, x^{b_k}$, подставляемых в f, содержит только x (при $b_i = 1$) и $\bar{x}$ (при $b_i = 0$)

$\Rightarrow$ $\phi(x)$ и $\overline{\phi(x)}$ задаются формулами над $\{f, \bar{}\}$ $\square$

Лемма 2 (о немонотонной функции)

Пусть $f \notin \mathbf{M}$. Тогда отрицание можно задать формулой над множеством $\{f, 0, 1\}$.

Доказательство:

- пусть f — k-местная немонотонная функция

$\Rightarrow$ существуют $\vec{a} = (a_1, \ldots, a_k), \vec{b} = (b_1, \ldots, b_k) \in \{0,1\}^k$: $\vec{a} \leqslant \vec{b}$, $f(\vec{a}) > f(\vec{b})$

  - т.е. $f(\vec{a}) = 1$, $f(\vec{b}) = 0$

- рассмотрим любой $(\vec{a}, \vec{b})$-путь в ориентированном k-мерном кубе
  - т.е. в диаграмме Хассе ЧУМа $(\{0,1\}^k, \leqslant)$
  - $\star$ так как $\vec{a} \leqslant \vec{b}$, каждая вершина $(\vec{a}, \vec{b})$-пути покрывает предыдущую
- в вершине $\vec{a}$ функция f принимает значение 1, а в вершине $\vec{b}$ – значение 0

$\Rightarrow$ путь содержит пару вершин $(\vec{\alpha}, \vec{\beta})$ такую, что $\vec{\beta}$ покрывает $\vec{\alpha}$, $f(\vec{\alpha}) = 1$, $f(\vec{\beta}) = 0$

$\star$ $\vec{\beta}$ покрывает $\vec{\alpha} \Rightarrow \vec{\alpha} = (c_1, \ldots, c_{i-1}, 0, c_{i+1}, \ldots, c_k)$, $\vec{\beta} = (c_1, \ldots, c_{i-1}, 1, c_{i+1}, \ldots, c_k)$

  - для некоторых битов $c_1, \ldots, c_k$

- рассмотрим унарную функцию $\phi(x) = f(c_1, \ldots, c_{i-1}, x, c_{i+1}, \ldots, c_k)$

$\star$ $\phi(0) = f(\vec{\alpha}) = 1$, $\phi(1) = f(\vec{\beta}) = 0 \Rightarrow \phi(x) = \bar{x}$

$\star$ $c_1, \ldots, c_k \in \{0,1\} \Rightarrow \phi(x)$ задана формулой над $\{f, 0, 1\}$ $\square$

Лемма 3 (о нелинейной функции)

Пусть $f \notin \mathbf{L}$. Тогда конъюнкцию можно задать формулой над множеством $\{f, 0, 1, \bar{}\}$.

Доказательство:

- пусть f — k-местная нелинейная функция, $h(x_1, \ldots, x_k)$ — ее полином Жегалкина

$\Rightarrow$ h содержит нелинейный одночлен

- без ограничения общности считаем, что этот одночлен содержит x_1 и x_2

- если $k = 2$, положим $\psi(x_1, x_2) = h(x_1, x_2)$; пусть $k > 2$
- существуют полиномы $f_1(x_3, \ldots, x_k), f_2(x_3, \ldots, x_k), f_3(x_3, \ldots, x_k), f_4(x_3, \ldots, x_k)$ такие, что

$\star$ $h(x_1, \ldots, x_k) = x_1 x_2 f_1(x_3, \ldots, x_k) + x_1 f_2(x_3, \ldots, x_k) + x_2 f_3(x_3, \ldots, x_k) + f_4(x_3, \ldots, x_k)$

- $f_1(x_3, \ldots, x_k)$ не равен константе 0

$\Rightarrow$ выберем вектор $(c_3, \ldots, c_k)$ так, что $f_1(c_3, \ldots, c_k) = 1$

- положим $\psi(x_1, x_2) = f(x_1, x_2, c_3, \ldots, c_k)$
- пусть $\alpha = f_2(c_3, \ldots, c_k)$, $\beta = f_3(c_3, \ldots, c_k)$, $\gamma = f_4(c_3, \ldots, c_k)$

$\Rightarrow$ $\psi(x_1, x_2) = x_1 x_2 + \alpha x_1 + \beta x_2 + \gamma$

- при $k = 2$ функция $\psi(x_1, x_2)$ имеет такой же вид

- положим $\phi(x_1, x_2) = \psi(x_1 + \beta, x_2 + \alpha) + \alpha\beta + \gamma$

$\Rightarrow$ $\phi(x_1, x_2) = (x_1 + \beta)(x_2 + \alpha) + \alpha(x_1 + \beta) + \beta(x_2 + \alpha) + \gamma + \alpha\beta + \gamma = x_1 x_2$

$\star$ для получения ψ в f подставляются константы

$\star$ для получения ϕ в ψ подставляются сами переменные или их отрицания ($x + 1 = \bar{x}$), и, возможно, берется отрицание итоговой формулы (при $\alpha\beta + \gamma = 1$)

$\Rightarrow$ $\phi(x)$ задана формулой над $\{f, 0, 1, \bar{}\}$ $\square$

Теорема Поста

Критерий полноты множества булевых функций дает следующая

Теорема Поста

Множество B булевых функций является полной системой $\Leftrightarrow$ B не содержится ни в одном из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T_0}, \mathbf{T_1}$.

Доказательство необходимости:

- ни один из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T_0}, \mathbf{T_1}$ не совпадает со множеством всех булевых функций
- если $B \subseteq C$, где $C \in \{\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T_0}, \mathbf{T_1}\}$ — замкнутый класс, то $\langle B \rangle \subseteq C$

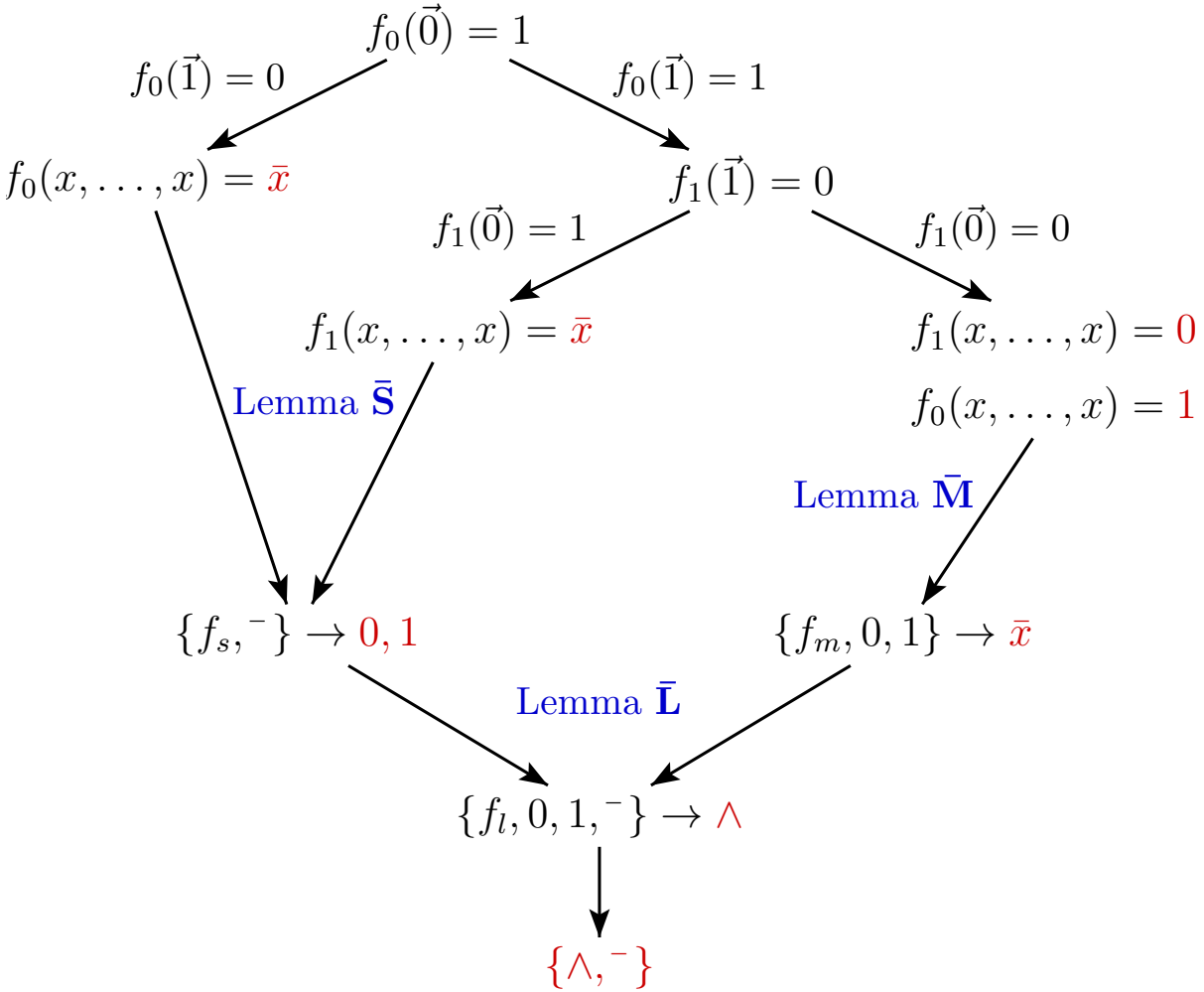
$\Rightarrow$ B не является полной системой $\square$

Доказательство достаточности:

- будем доказывать, что формулами над B можно задать отрицание и конъюнкцию
- так как $\{\wedge, \bar{}\}$ — полная система, отсюда будет следовать полнота B
- доказательство опирается на леммы из предыдущего фрагмента $\Longrightarrow$

Теорема Поста — доказательство достаточности

- Выберем в B функции $f_0 \notin \mathbf{T_0}$, $f_1 \notin \mathbf{T_1}$, $f_s \notin \mathbf{S}$, $f_m \notin \mathbf{M}$, $f_l \notin \mathbf{L}$
  - некоторые из выбранных функций могут совпадать
- Зададим конъюнкцию и отрицание формулой над $\{f_0, f_1, f_s, f_m, f_l\}$:



Алгоритмичность теоремы Поста

- ⋆ Чтобы проверить произвольную систему булевых функций на полноту, надо уметь проверять функцию на принадлежность к каждому из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T_0}, \mathbf{T_1}$
  - пусть функция $f(x_1, \ldots, x_n)$ задана таблицей значений, т.е. битовым вектором $F[0..2^n-1]$
- Принадлежность f ко всем классам может быть проверена за время $O(n \cdot 2^n)$:
  - ⋆ $\mathbf{T_0}$, $\mathbf{T_1}$: проверить один бит в F
  - ⋆ $\mathbf{S}$: сравнить биты $F[i]$ и $F[2^n-i-1]$ для всех i
  - ⋆ $\mathbf{L}$: записать равенство $f(x_1, \ldots, x_n) = a_0 + a_1 x_1 + \cdots a_n x_n$
  - подставить каждое значение вектора $\vec{x}$ и соответствующее значение $f(\vec{x})$
    - получится система 2^n уравнений с $n+1$ неизвестными $a_0, \ldots, a_n$ над $\mathbb{F}_2$
  - проверить совместность системы
  - ! придумайте, как сделать это за время $O(n \cdot 2^n)$
  - ⋆ $\mathbf{M}$: для каждого из $O(n \cdot 2^n)$ ребер n-мерного куба проверить, что значение f на верхнем конце не меньше значения на нижнем

Базисы булевых функций

- Полная система б.ф. называется базисом, если никакое ее собственное подмножество не является полной системой
  - ⋆ в теории булевых схем используется другая терминология: базисом называют любое фиксированное множество б.ф., элементы которого используются в качестве вентилей при составлении схем

Следствие о базисах

Любой базис содержит не более четырех булевых функций.

Доказательство:

- из любой полной системы можно выделить подмножество вида $\{f_0, f_1, f_s, f_m, f_l\}$, тоже являющееся полной системой
- если $f_0(\vec{1}) = 0$, то f_0 немонотонна, а если $f_0(\vec{1}) = 1$, то то f_0 несамодвойственна

$\Rightarrow$ f_m или f_s можно заменить на f_0

$\Rightarrow$ полную систему можно «сократить» до 4-элементного подмножества с сохранением полноты

□

! постройте базис из четырех функций

Замкнутые классы

- Пусть B — некоторое множество булевых функций
- ⋆ $\langle B \rangle$ — множество функций, которые можно записать формулами над B
- ⋆ $\langle \cdot \rangle$ — оператор замыкания:
  - $B \subseteq \langle B \rangle$ (экстенсивность)
  - $A \subseteq B \Rightarrow \langle A \rangle \subseteq \langle B \rangle$ (монотонность)
  - $\langle \langle B \rangle \rangle = \langle B \rangle$ (идемпотентность)
- B называется замкнутым классом (булевых функций), если $B = \langle B \rangle$
- ⋆ B — полная система $\Leftrightarrow \langle B \rangle$ содержит все булевы функции

- Б.ф. f сохраняет 0, если $f(\vec{0}) = 0$, и сохраняет 1, если $f(\vec{1}) = 1$
  - множество всех б.ф., сохраняющих 0 (сохраняющих 1) обозначается $\mathbf{T}_0$ ($\mathbf{T}_1$)
    примеры: $0, \vee, \wedge, + \in \mathbf{T}_0$; $1, \bar{}, \sim, \downarrow \notin \mathbf{T}_0$; $1, \vee, \wedge, \sim \in \mathbf{T}_1$; $0, \bar{}, +, ' \notin \mathbf{T}_1$

Лемма

$\mathbf{T}_0$ и $\mathbf{T}_1$ — замкнутые классы.

Доказательство: рассмотрим формулу над $\mathbf{T}_0$, построим по ней схему
- если любому элементу схемы подать 0 на все входы, то на выходе у него будет 0
- подадим 0 на все входы схемы

$\Rightarrow$ на выходе схемы будет 0
$\Rightarrow$ функция, задаваемая схемой, принадлежит $\mathbf{T}_0$

- для $\mathbf{T}_1$ доказательство аналогично

Линейные функции

- Функция $f(x_1, \ldots, x_k)$ линейна, если ее полином Жегалкина — линейный
  - т.е. $f(x_1, \ldots, x_k) = a_0 + a_1 x_1 + a_2 x_2 + \cdots a_k x_k$ для некоторых $a_0, \ldots, a_k \in \{0, 1\}$
  - ⋆ f обладает свойствами самой обычной линейной функции из курса алгебры
  - множество всех линейных б.ф. обозначается **L**

    примеры: $0, \bar{}, +, \sim \in \mathbf{L}$; $\quad \wedge, \vee, \to, \downarrow \notin \mathbf{L}$

Лемма

L — замкнутый класс.

Доказательство: рассмотрим формулу над **L**, построим по ней схему

- каждый элемент схемы вычисляет линейную функцию своих входов
- линейная функция от линейных функций переменных является линейной функцией этих переменных

$\Rightarrow$ вся схема вычисляет линейную функцию $\square$

Самодвойственные функции

- Функция $f(x_1, \ldots, x_k)$ самодвойственна, если $f(\bar{x}_1, \ldots, \bar{x}_k) = \overline{f(x_1, \ldots, x_k)}$
  - на противоположных наборах аргументов f принимает разные значения
  - множество всех самодвойственных б.ф. обозначается **S**
    примеры: $^-, x + y + z, T_2(x, y, z) \in \mathbf{S}$; $0, \vee, \to, \downarrow \notin \mathbf{S}$

Лемма

S — замкнутый класс.

Доказательство: рассмотрим формулу над **S**, построим по ней схему

- подадим на входы произвольный битовый вектор
- ⋆ на выходе каждого элемента схемы будет некоторый бит
- поменяем биты на всех входах
- ⋆ докажем, что бит на выходе каждого элемента поменялся
  индукцией по максимальной длине n пути от входа до элемента
- база индукции: $n = 1$
- входы элемента являются входами схемы, элемент задает функцию из **S**

⇒ выходной бит изменился, так как поменялись все входы

- шаг индукции:
- входами элемента являются либо входы схемы (поменялись по условию), либо выходы элементов с меньшей длиной пути (поменялись по предположению индукции)

⇒ выход элемента, задающего самодвойственную функцию, поменялся

⇒ в частности, поменялся выходной бит всей схемы

⇒ так как рассуждение верно для любого вектора на входе схемы, схема вычисляет самодвойственную функцию

Монотонные функции

- Введем на битовых векторах равной длины покомпонентный порядок:
  - $(x_1, \ldots, x_k) \leqslant (y_1, \ldots, y_k) \Leftrightarrow x_1 \leqslant y_1, \ldots, x_k \leqslant y_k$
  - диаграмма Хассе ЧУМа $(\{0,1\}^k, \leqslant)$ — k-мерный куб
- Функция $f(\vec{x})$ монотонна, если $f(\vec{x}) \leqslant f(\vec{y})$ для любых $\vec{x} \leqslant \vec{y}$
  - если значения каких-то аргументов f увеличить (подняться вверх по кубу), то значение f не уменьшится
  - множество всех монотонных б.ф. обозначается $\mathbf{M}$
    примеры: $0, \vee, \wedge, T_i \in \mathbf{M}$; $\quad +, \bar{}, \to, ' \notin \mathbf{M}$

Лемма

$\mathbf{M}$ — замкнутый класс.

Доказательство: рассмотрим формулу над $\mathbf{M}$, построим по ней схему

- подадим на входы произвольный битовый вектор, не равный $\vec{1}$
- ⋆ на выходе каждого элемента схемы будет некоторый бит
- поменяем биты на некоторых входах с 0 на 1
- ⋆ докажем, что ни у какого элемента выходной бит не поменялся с 1 на 0 индукцией по максимальной длине n пути от входа до элемента
- ! восстановите детали по аналогии с предыдущей леммой

⇒ выходной бит всей схемы не уменьшился

⇒ так как рассуждение верно для любого вектора на входе схемы, схема вычисляет монотонную функцию

□

Решетка замкнутых классов

- ★ ЧУМ замкнутых классов с отношением включения является решеткой
  - $C_1 \wedge C_2 = C_1 \cap C_2$
  - $C_1 \vee C_2 = \langle C_1 \cup C_2 \rangle$
  - ★ вообще, система замкнутых множеств всегда образует решетку
- Решетку замкнутых классов б.ф. иногда обозначают $\mathcal{P}_2$ в честь Поста
  - $\mathcal{P}_k$ — это решетка замкнутых классов функций на k-элементном множестве
- Единицей решетки $\mathcal{P}_2$ является класс $\mathbf{B}$ всех булевых функций
- Нулем решетки $\mathcal{P}_2$ является класс $\mathbf{Pr} = \{PROJ_i\}$ всех проекций
  - это функции, которые можно задать формулами без операторов (или схемами без вентилей)
- Элемент решетки — атом, если он покрывает 0, и коатом, если его покрывает 1

Следствие о замкнутых классах

Коатомами решетки $\mathcal{P}_2$ являются в точности классы $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1$.

Доказательство:

- классы $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1$ несравнимы по включению
  - см. примеры принадлежности функций классам
- по теореме Поста замкнутый класс, не содержащийся ни в одном из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1$, совпадает с $\mathbf{B}$

$\Rightarrow$ каждый из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1$ — коатом, и других коатомов нет $\square$

Диаграмма Хассе решетки $\mathcal{P}_2$