Б-2. Полные системы булевых функций

6 декабря 2024 г. 10:38

Замкнутые классы

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 $\square$

Линейные функции

$\bar{x} = x+1$, => $\bar{}$ - линейная ф-ия

$\sim = \bar{+}$, т.е. $++1$

$\wedge = xy$ => не линейна

- Функция $f(x_1, \ldots, x_k)$ линейна, если ее полином Жегалкина — линейный
  - т.е. $f(x_1, \ldots, x_k) = a_0 + a_1x_1 + a_2x_2 + \cdots a_kx_k$ 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 $\mathbf{L}$
    примеры: $0, \bar{}, +, \sim \in \mathbf{L}$; $\wedge, \vee, \rightarrow, \downarrow \notin \mathbf{L}$

Лемма

$\mathbf{L}$ — замкнутый класс.

очев

лин.+лин.=лин.

Доказательство: рассмотрим формулу над $\mathbf{L}$, 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

$\bar{}$ - самодв., т.к. $\bar{\bar{x}} = x$.

$f(x,y,z) = x+y+z$. $f(\bar{x},\bar{y},\bar{z}) = x+1+y+1+z+1 = (x+y+z)+1 = \overline{f(x,y,z)}$

! Самодв. функция должна уметь принимать 2 разных значения,
-> конст. не S

- 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 $\mathbf{S}$
    примеры: $\bar{}, x+y+z, T_2(x,y,z) \in \mathbf{S}$; $0, \vee, \rightarrow, \downarrow \notin \mathbf{S}$
    ↑ функция большинства

Лемма

$\mathbf{S}$ — замкнутый класс.

Доказательство: рассмотрим формулу над $\mathbf{S}$, 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 $\mathbf{S}$
- $\Rightarrow$ 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)
- $\Rightarrow$ выход элемента, задающего самодвойственную функцию, поменялся
- $\Rightarrow$ в частности, поменялся выходной бит всей схемы
- $\Rightarrow$ так как рассуждение верно для любого вектора на входе схемы, схема вычисляет самодвойственную функцию $\square$

Монотонные функции

- Введем на битовых векторах равной длины покомпонентный порядок:
  - $(x_1, \dots, x_k) \leqslant (y_1, \dots, y_k) \Leftrightarrow x_1 \leqslant y_1, \dots, x_k \leqslant y_k$
  - 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 **M**
    примеры: $0, \vee, \wedge, T_i \in \mathbf{M}$; $\quad +, ^{-}, \to, ' \notin \mathbf{M}$
    пороговые ф-ии

Лемма

M — замкнутый класс.

Доказательство: рассмотрим формулу над **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 □

Три леммы о функциях

Лемма о несамодвойственной функции

Лемма 1 (о несамодвойственной функции)

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

Доказательство:
- пусть f — k-местная несамодвойственная функция
- ⇒ существует $\vec{b} = (b_1, \dots, b_k) \in \{0,1\}^k$ такой, что $f(b_1, \dots, b_k) = f(\bar{b}_1, \dots, \bar{b}_k)$
- рассмотрим унарную функцию $\phi(x) = f(x^{b_1}, \dots, x^{b_k})$ $\quad x^{b_1} = x \sim b_1$
- ⋆ $\phi(0) = f(0^{b_1}, \dots, 0^{b_k}) = f(\bar{b}_1, \dots, \bar{b}_k) = f(b_1, \dots, b_k) = f(1^{b_1}, \dots, 1^{b_k}) = \phi(1)$
- ⇒ $\phi(x)$ — константа
- ⋆ вторую константу можно записать формулой $\overline{\phi(x)}$
- ⋆ набор функций $x^{b_1}, \dots, x^{b_k}$, подставляемых в f, содержит только x (при $b_i = 1$) и $\bar{x}$ (при $b_i = 0$)
- ⇒ $\phi(x)$ и $\overline{\phi(x)}$ задаются формулами над $\{f, ^{-}\}$ □

Лемма о немонотонной функции

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
- ⇒ существуют $\vec{a} = (a_1, \dots, a_k), \vec{b} = (b_1, \dots, b_k) \in \{0,1\}^k$: $\vec{a} \leqslant \vec{b}$, $f(\vec{a}) > f(\vec{b})$
  - 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 $(\{0,1\}^k, \leqslant)$
  - ⋆ 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
- ⇒ путь содержит пару вершин $(\vec{\alpha}, \vec{\beta})$ такую, что $\vec{\beta}$ покрывает $\vec{\alpha}$, $f(\vec{\alpha}) = 1$, $f(\vec{\beta}) = 0$
- ⋆ $\vec{\beta}$ покрывает $\vec{\alpha} \Rightarrow \vec{\alpha} = (c_1, \dots, c_{i-1}, 0, c_{i+1}, \dots, c_k)$, $\vec{\beta} = (c_1, \dots, c_{i-1}, 1, c_{i+1}, \dots, c_k)$
  - для некоторых битов $c_1, \dots, c_k$
- рассмотрим унарную функцию $\phi(x) = f(c_1, \dots, c_{i-1}, x, c_{i+1}, \dots, c_k)$
- ⋆ $\phi(0) = f(\vec{\alpha}) = 1$, $\phi(1) = f(\vec{\beta}) = 0 \Rightarrow \phi(x) = \bar{x}$
- ⋆ $c_1, \dots, c_k \in \{0, 1\} \Rightarrow \phi(x)$ задана формулой над $\{f, 0, 1\}$ □

Лемма о нелинейной функции

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, $h(x_1, \dots, x_k)$ — ее полином Жегалкина
- ⇒ 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 $f_1(x_3, \dots, x_k), f_2(x_3, \dots, x_k), f_3(x_3, \dots, x_k), f_4(x_3, \dots, x_k)$ такие, что
- ⋆ $h(x_1, \dots, x_k) = x_1x_2f_1(x_3, \dots, x_k) + x_1f_2(x_3, \dots, x_k) + x_2f_3(x_3, \dots, x_k) + f_4(x_3, \dots, x_k)$
- $f_1(x_3, \dots, x_k)$ не равен константе 0
- ⇒ выберем вектор $(c_3, \dots, c_k)$ так, что $f_1(c_3, \dots, c_k) = 1$
- положим $\psi(x_1, x_2) = f(x_1, x_2, c_3, \dots, c_k)$
- пусть $\alpha = f_2(c_3, \dots, c_k)$, $\beta = f_3(c_3, \dots, c_k)$, $\gamma = f_4(c_3, \dots, c_k)$, $\alpha, \beta, \gamma \in \{0,1\}$
- ⇒ $\psi(x_1, x_2) = x_1x_2 + \alpha x_1 + \beta x_2 + \gamma$
  - при $k = 2$ функция $\psi(x_1, x_2)$ имеет такой же вид
- положим $\phi(x_1, x_2) = \psi(x_1 + \beta, x_2 + \alpha) + \alpha\beta + \gamma$
- ⇒ $\phi(x_1, x_2) = (x_1 + \beta)(x_2 + \alpha) + \alpha(x_1 + \beta) + \beta(x_2 + \alpha) + \gamma + \alpha\beta + \gamma = x_1x_2$
- ⋆ для получения ψ в f подставляются константы
- ⋆ для получения ϕ в ψ подставляются сами переменные или их отрицания $(x + 1 = \bar{x})$, и, возможно, берется отрицание итоговой формулы (при $\alpha\beta + \gamma = 1$)
- ⇒ $\phi(x)$ задана формулой над $\{f, 0, 1, \bar{\ }\}$ □

Теорема Поста о полноте

Теорема Поста

Критерий полноты множества булевых функций дает следующая

Теорема Поста

Множество B булевых функций является полной системой ⇔ B не содержится ни в одном из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1$.

Доказательство необходимости:

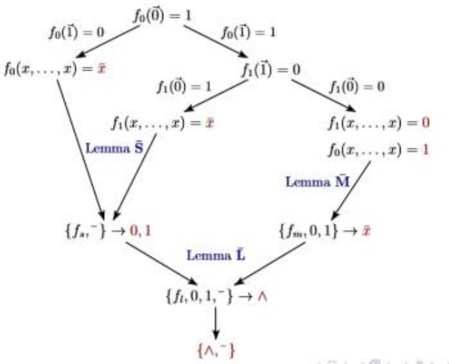
- ⋆ ни один из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1$ не совпадает со множеством всех булевых функций
- если $B \subseteq C$, где $C \in \{\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1\}$ — замкнутый класс, то $\langle B \rangle \subseteq C$
- ⇒ B не является полной системой □

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 ⟹

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

! Возможно, полезно для КП

- ⋆ 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 $f(x_1, \dots, x_n)$ 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 $f(x_1, \dots, x_n) = a_0 + a_1x_1 + \cdots a_nx_n$
  - \- подставить каждое значение вектора $\vec{x}$ и соответствующее значение $f(\vec{x})$
    - получится система 2^n уравнений с $n+1$ неизвестными $a_0, \dots, a_n$ 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

Алгоритмичность теоремы Поста

! Возможно, полезно для КП

- ★ 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 $f(x_1, \ldots, x_n) = a_0 + a_1x_1 + \cdots a_nx_n$
  - \- 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

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:

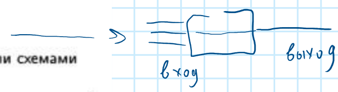
- из любой полной системы можно выделить подмножество вида $\{f_0, f_1, f_s, f_m, f_l\}$, тоже являющееся полной системой
- если $f_0(\vec{1}) = 0$, то f_0 немонотонна, а если $f_0(\vec{1}) = 1$, то то f_0 несамодвойственна
- ⇒ f_m или f_s можно заменить на f_0
- ⇒ полную систему можно «сократить» до 4-элементного подмножества с сохранением полноты □

! постройте базис из четырех функций

Решётка замкнутых классов

Решетка замкнутых классов

- ★ ЧУМ замкнутых классов с отношением включения является **решеткой**
  - $C_1 \wedge C_2 = C_1 \cap C_2$ - inf
  - $C_1 \vee C_2 = \langle C_1 \cup C_2 \rangle$ -sup
  - ★ 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)



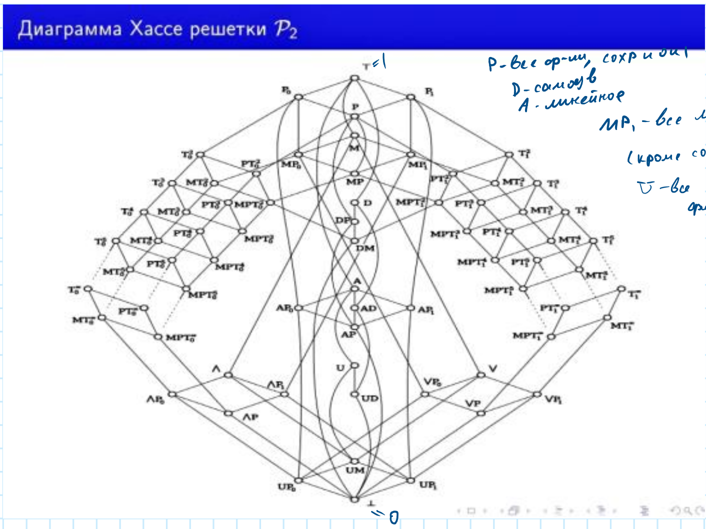
- Элемент решетки — **атом**, если он покрывает 0, и **коатом**, если его покрывает 1

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 $\mathbf{B}$
- ⇒ каждый из классов $\mathbf{L}, \mathbf{S}, \mathbf{M}, \mathbf{T}_0, \mathbf{T}_1$ — коатом, и других коатомов нет □



P - все ф-ии, сохр и 0 и 1
D - самодув
A - линейное

MP_1 - все мон. ф-ии, сохр 1
(кроме const=0)

U - все переменные фиктивны, кроме одной

Эта решётка счётна