МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

Лекция 4

Принцип суперпозиций.
Замкнутые классы логических функций

Суперпозицией булевых функций f_0 и $f_1,\ldots,f_n$ называется функция

$$f(x_1,\ldots,x_m) = f_0(g_1(x_1,\ldots,x_m),\ldots,g_k(x_1,\ldots,x_m)),$$

где каждая из функций $g_i(x_1, \ldots,x_m)$ либо совпадает с одной из переменных (тождественная функция),
либо – с одной из функций $f_1,\ldots,f_n$.

Например:

- Функция $f(x,y) = \neg(x \wedge y)$ является суперпозицией функций $\neg$ и $\wedge$;

Замыкание класса

A - множество логических функций, обладающих некоторым свойством.

Пусть $G(Y_1,Y_2,\ldots,Y_k)\in A$ и $F_i(X_1,X_2,\ldots,X_n)\in A$, $i=1,2,\ldots,k$.

Суперпозиция функций G и F:

$$G[F_1(X_1,\ldots,X_n),\ldots,F_k(X_1,\ldots,X_n)] = H(X_1,\ldots,X_n)$$

Если $H(X_1,\ldots,X_n)\in A$, то A называется *замкнутым классом логических функций* по отношению к рассматриваемому свойству.

Замыкание класса

То есть, множество *A* логических функций называют *замкнутым классом*, если любая суперпозиция функций из *A* снова принадлежит *A*.

«Замечательные» свойства

1. Свойство сохранять 0

Функция $F(X_1,\ldots,X_n)$ называется сохраняющей 0, если $F(0,\ldots,0)=0$.

Функции X_1X_2, $X_1 \vee X_2$, $X_1 \oplus X_2$ сохраняют 0, а $X_1 \rightarrow X_2$, $X_1 \sim X_2$, $X_1 | X_2$ не сохраняют.

$C_0=\{F(X_1,\ldots,X_n) \mid F(0,\ldots,0)=0\}$.

Доказательство замкнутости класса функций, *сохраняющих* 0

Пусть $G(0,...,0)=0$ и $F_i(0,...,0)=0$.

Произведем суперпозицию функций G и F_i:

$G[F_1(X_1,...,X_n),...,F_k(X_1,...,X_n)]$

Определим значение функции на нулевом наборе: $G[F_1(0,...,0),...,F_k(0,...,0)]=G(0,...,0)=0$, т.е. $H(0,...,0)=0$.

1. Свойство сохранять 1

Функция $F(X_1,\ldots,X_n)$ называется *сохраняющей единицу*, если $F(1,\ldots,1)=1$.

Функции X_1X_2, X_1+X_2, $X_1\rightarrow X_2$ сохраняют единицу, а $X_1\oplus X_2$, $X_1|X_2$ не сохраняют.

$C_1=\{F(X_1,\ldots,X_n) \mid F(1,\ldots,1)=1\}$.

Класс C_1 является замкнутым.

3. Самодвойственность

Самодвойственной функцией называется такая функция, для которой справедливо равенство

$$F(X_1,X_2,\dots,X_n)= F^*(X_1,X_2,\dots,X_n),$$

где F^*– двойственная функция по отношению к функции F.

Двойственная функция определяется следующим образом:

$$F^*(X_1,X_2,\dots,X_n)=\overline{F}(\overline{X_1},\overline{X_2},\dots,\overline{X_n})$$

Пример

$F = X_1X_2 + X_1X_3 + X_2X_3$

$$F^* = \overline{\overline{X}_1\overline{X}_2 + \overline{X}_1\overline{X}_3 + \overline{X}_2\overline{X}_3} = \overline{\overline{X}_1\overline{X}_2} \cdot \overline{\overline{X}_1\overline{X}_3} \cdot \overline{\overline{X}_2\overline{X}_3} =$$

$$= (X_1 + X_2)(X_1 + X_3)(X_2 + X_3) = X_1X_2 + X_1X_3 + X_2X_3 = F$$

Класс всех самодвойственных функций: $C_c = \{F(X_1,\ldots,X_n) \mid F(X_1,X_2,\ldots,X_n) = F^*(X_1,X_2,\ldots,X_n)\}$.

X	Y	$F=X\wedge Y$	$\neg X\wedge\neg Y$	$\neg(\neg X\wedge\neg Y)$
0	0	0	1	0
0	1	0	0	1
1	0	0	0	1
1	1	1	0	1

$x \oplus y$ и $x \leftrightarrow y$ – двойственные функции
// (0,1,1,0) и (1,0,0,1)

$F_2=X\vee Y$	F_2^*	$F_3=X\oplus Y$	F_3^*	$F_4=X\equiv Y$	F_4^*
0	0	0	1	1	0
1	0	1	0	0	1
1	0	1	0	0	1
1	1	0	1	1	0

Доказательство замкнутости класса самодвойственных функций

Пусть $G(Y_1,\ldots,Y_n)$ и $F_i(X_1,\ldots,X_n)$ – самодвойственные функции.

Произведем суперпозицию функций G и F_i:

$$G[F_1(X_1,\ldots X_n),\ldots F_n(X_1,\ldots,X_n)]$$

и определим двойственную функцию к ней:

$$\overline{G[F_1(\overline{X}_1,\ldots\overline{X}_n),\ldots F_n(\overline{X}_1,\ldots,\overline{X}_n)]} = \overline{G[\overline{F_1(X_1,\ldots X_n)},\ldots\overline{F_n(X_1,\ldots,X_n)}]} =$$

$$= G[F_1(X_1,\ldots X_n),\ldots F_n(X_1,\ldots,X_n)]$$

$\Rightarrow C_\text{C}$ – замкнутый класс.

4. Монотонность

Критерий сравнения двух наборов аргументов:

- Если значение каждого аргумента одного набора больше или равно значению того же аргумента второго набора, то говорят, что первый набор не меньше второго.

При этом предполагается, что $0 \geq 0$; $1 \geq 0$; $1 \geq 1$.

Например, $(1,1,0,1) \geq (0,1,0,1)$.

Наборы: $(0,1)$ и $(1,0)$

$(0,1,0,1)$ и $(1,0,1,0)$ несравнимы

Логическая функция называется *монотонной*, если при любом возрастании набора значение этой функции не убывает.

(рассматриваются только сравнимые наборы)

Функция $f(x_1, \ldots, x_n)$ *монотонна*, если для любых двоичных наборов δ и τ длины n, при условии $\delta \le \tau$, выполняется условие $f(\delta) \le f(\tau)$.

C_M - класс всех монотонных функций

Например, монотонные функции: $X \& Y$, $X \vee Y$

немонотонные функции: $X \leftrightarrow Y$, $X \rightarrow Y$, $X \oplus Y$

Доказательство замкнутости $C_м$:

Пусть $G(Y_1,\ldots, Y_n)$ и $F_i(X_1,\ldots, X_n)$ - монотонные.

Произведем суперпозицию функций G и F :

$$G[F_1(X_1,\ldots, X_n),\ldots, F_k(X_1,\ldots, X_n)] = H(X_1,\ldots, X_n)$$

Найдем значения функций F_i и G на некотором наборе $X_1,\ldots, X_n$, а затем увеличим этот набор.

Так как функции F_i монотонные, то их значения либо увеличатся, либо останутся без изменения.

Так как функция G монотонная, то ее значение либо увеличится, либо останется без изменения.

$\Rightarrow$значение функции H при увеличении набора либо увеличится, либо останется без изменения,

т.е. функция H тоже является монотонной.

5. Линейность

Логическая функция называется *линейной*, если она может быть представлена полиномом первой степени, т.е. записана в виде $F(X_1,X_2,\ldots,X_n)=A_0\oplus A_1X_1\oplus A_2X_2\oplus\ldots\oplus A_nX_n$,

где A_0, $A_1,\ldots,$ A_n – коэффициенты, равные нулю или единице.

C_L – класс всех линейных функций.

Например, линейные функции:

$$\mathrm{X} \oplus \mathrm{Y}, \quad \mathrm{X} \leftrightarrow \mathrm{Y} = 1 \oplus \mathrm{X} \oplus \mathrm{Y}.$$

Доказательство замкнутости C_L

Пусть функции $G(Y_1,\ldots, Y_k)$ и $F_i(X_1,\ldots, X_n)$ – линейные. Представим их в виде линейных полиномов:

$$G = A_0 \oplus A_1Y_1 \oplus A_2Y_2 \oplus \ldots \oplus A_kY_k,$$

$$F_i = B_{0i} \oplus B_{1i}\, X_1 \oplus B_{2i}\, X_2 \oplus \ldots \oplus B_{ni}X_n.$$

Подставив функции F_i вместо аргументов Y_i в функцию G получим выражение, в котором постоянные коэффициенты A_i умножаются на линейные функции.

При этом получатся снова линейные функции.

Приведя подобные члены, получим функцию $H(X_1,\ldots, X_n)$ в виде линейного полинома.

$\Rightarrow$, что по свойству линейности функции образуют замкнутый класс.

Полином Жегалкина

Полиномом Жегалкина от переменных $x_1, x_2, \ldots x_n$ называется булева функция вида

$$\sum_{i_1, i_2, \ldots i_m}^{\mathrm{mod}2} a_{i_1, i_2, \ldots i_m} x_{i_1} \ldots x_{i_m}$$

Теорема Жегалкина

Теорема: Всякая логическая функция может быть представима единственным полиномом по *mod 2.*

Док-во: Число различных полиномов по mod 2 от переменных $x_1, x_2, \ldots x_n$ - это число выражений вида

$$\sum_{i_1, i_2, \ldots i_m}^{\mathrm{mod}\ 2} a_{i_1, i_2, \ldots i_m} x_{i_1} \ldots x_{i_m}$$

Число членов $x_{i_1} \ldots x_{i_m}$ равно числу множества всех подмножеств – 2^n.

Число полиномов которые можно образовать из них 2^{2^n}.

Число различных логических функций *n*-переменных 2^{2^n}.

Т.об. Каждой логической функции соответствует единственный полином Жегалкина и наоборот.

Свойства функций системы Жегалкина:

1. Ассоциативность:

а) $x(yz) = (xy)z;$

б) $x \oplus (y \oplus z) = (x \oplus y) \oplus z.$

2. Коммутативность:

а) $xy = yx;$

б) $x \oplus y = y \oplus x.$

3. Дистрибутивность: $x(y \oplus z) = xy \oplus xz.$

4. Попарное сокращение: $x \oplus x = 0.$

5. Свойство констант: $x \oplus 0 = x.$

Функция, у которой полином Жегалкина имеет вид

$$\Sigma \alpha_i x_i \oplus \gamma, \text{ где}$$

α_i, γ равны 0 или 1, называется *линейной*.

Связь функций системы Жегалкина с булевыми функциями

1. Выражение отрицания через функции системы Жегалкина:

$$\overline{x} = x \oplus 1.$$

2. Выражение дизъюнкции через функции системы Жегалкина:

$$x \vee y = xy \oplus x \oplus y.$$

Общий вид полинома Жегалкина от двух переменных:

$$P(x, y) = \alpha x \oplus \beta y \oplus \gamma$$

, где $\alpha, \beta, \gamma \in \{0;1\}$.

Функции, получаемые при всех восьми возможных комбинациях значений α, β, γ.

α	β	γ	**Вид полинома Жегалкина**	**Эквивалентные булевы формулы**
0	0	0	xy	$xy = \overline{x \vee y}$
0	0	1	$xy \oplus 1$	$\overline{xy} = \bar{x} \vee \bar{y}$
0	1	0	$xy \oplus y$	$\bar{x}y = \overline{x \vee \bar{y}}$
0	1	1	$xy \oplus y \oplus 1$	$\overline{\bar{x}y} = x \vee \bar{y}$
1	0	0	$xy \oplus x$	$x\bar{y} = \overline{\bar{x} \vee y}$
1	0	1	$xy \oplus x \oplus 1$	$\overline{x\bar{y}} = \bar{x} \vee y$
1	1	0	$xy \oplus x \oplus y$	$x \vee y = \overline{\bar{x}\bar{y}}$
1	1	1	$xy \oplus x \oplus y \oplus 1$	$\overline{x \vee y} = \bar{x}\bar{y}$

Функционально полные системы элементарных булевых функций

Лемма 1. (о немонотонных функциях)

Если функция $f(x_1, x_2, \dots x_n)$ немонотонна, то подстановкой констант из нее можно получить отрицание.

Следствие: Т.е. существует такая подстановка n-1 константы, что функция оставшейся одной переменной является отрицанием.

Док-во: Пусть f немонотонна. $\exists$ наборы σ и τ: $\sigma<\tau$ и $f(\sigma)=1$, $f(\tau)=0$.

Предположим, σ и τ отличаются по k компонентам, в σ - 0, а в τ - 1.

Построим цепочку наборов $\sigma<\omega^1<\omega^2<\ldots<\omega^{k-1}<\tau$, в которой соседние наборы отличаются в одной компоненте.

На каких-то двух соседних наборах происходит переключение значения f: $f(\omega^j)=1$, $f(\omega^{j+1})=0$.

Пусть эти наборы отличаются в i-ой компоненте:

$$\omega^j_i=0,\ \omega^{j+1}_i=1.$$

Обозначим $g(x)=f(\omega^j_1, \ldots, \omega^j_{i-1}, x_i, \omega^j_{i+1}, \ldots \omega^j_n)$.

$g(0)=g(\omega^j_i)=f(\omega^j)=1$,

$g(1)=g(\omega^{j+1}_i)=f(\omega^{j+1})=0$, $\Rightarrow g(x_i)=\overline{x_i}$. Ч.т.д.

<u>*Пример*</u>: необходимо выяснить, можно ли получить функцию $\bar{x}$ из функции $f(x_1, x_2, x_3) = x_1 \oplus x_2 \cdot x_3$ путем соответствующей замены переменных.

Решение: Функция *f* немонотонна, т.к. $f(100)=1$, $f(111)=0 \Rightarrow$ из этой функции можно получить $\bar{x}$.

Подставим вместо x_1 константу 1, а вместо x_2, x_3 – x, тогда $f(1,1,x) = 1 \oplus 1 \cdot x = \bar{x}$.

Чтобы воспользоваться следствием леммы, выберем пару соседних наборов, на которых нарушено условие монотонности. Имеем, $f(110)=1$, $f(111)=0$.

$\Rightarrow f(1,1,x) = 1 \oplus 1 \cdot x = \bar{x}$

Лемма 2. (о нелинейных функциях)

Если функция $f(x_1, \ldots x_n)$ - нелинейна, то с помощью подстановки констант и использования отрицания из нее можно получить $\wedge$ и $\vee$. Т.е. $\exists$ представление $\wedge$ и $\vee$ в виде суперпозиции констант, отрицаний и функции f.

Док-во: Пусть f – нелинейна. Тогда ее полином Жегалкина содержит $\wedge$ переменных.

Выберем самую короткую из них $K = x_{i1}x_{i2}\ldots x_{ik}$.

Положим $x_{i3}=\ldots=x_{ik}=1$,

а для всех x_j, не входящих в K, $x_j=0$.

Подстановка этих констант в полином обратит K в $x_{i1}x_{i2}$, а остальные конъюнкции в 0, f примет вид

$$x_{i1}x_{i2} \oplus \alpha\, x_{i1} \oplus \beta\, x_{i2} \oplus \gamma,\ \alpha,\beta,\gamma \in \{0,1\}$$

Функционально полные системы

Система элементарных булевых функций называется ***функционально полной***, если произвольную булеву функцию можно представить суперпозицией функций этой системы.

Полная система функций образует ***базис***.

Минимальным базисом называется такой, в котором при удалении хотя бы одной функции, образующей этот базис, нарушается его полнота.

I признак функциональной полноты

Если все функции функционально полной системы Σ можно выразить через функции системы Σ^* (является суперпозицией функций этой системы), то Σ^* – является также ***функционально полной системой***.

Примеры:

1. $\Sigma_1 = \{\wedge, \neg\}$ функционально полная система

   Полнота следует из возможности выразить дизъюнкцию через функции этой системы.

   Действительно, $x_1 \vee x_2 = \neg(\overline{x_1} \wedge \overline{x_2})$

2. $\Sigma_2 = \{\vee, \neg\}$ функционально полная система

   Полнота следует из возможности выразить конъюнкцию через функции этой системы,

   $x_1 \wedge x_2 = \neg(\overline{x_1} \vee \overline{x_2})$.

3. $\Sigma_3 = \{|\}$

   Штрих Шеффера представляет функционально полную систему, так как $\overline{x} = x \mid x$, $x_1 \wedge x_2 = \overline{x_1 \mid x_2} = (x_1 \mid x_2) \mid (x_1 \mid x_2)$ и Σ_1 функционально полна.

4. $\Sigma_4 = \{\downarrow\}$ функционально полная система

Так как $\bar{x} = x \mid x$, $\quad x_1 \vee x_2 = \overline{x_1 \downarrow x_2} = (x_1 \downarrow x_2) \downarrow (x_1 \downarrow x_2)$ и Σ_2 функционально полна.

5. $\Sigma_5 = \{\wedge, \oplus, 1\}$

Система функционально полна, так как $\bar{x} = x \oplus 1$, и Σ_1 функционально полна.

II признак функциональной полноты

Для того, чтобы система булевых функций была функционально полной, необходимо и достаточно, чтобы эта система включала:

- хотя бы одну функцию, не сохраняющую 0;
- хотя бы одну функцию, не сохраняющую 1;
- хотя бы одну несамодвойственную функцию;
- хотя бы одну немонотонную функцию;
- хотя бы одну нелинейную функцию.

Рассмотрим некоторые функционально полные системы.

1. **$F=X/Y$**.

   Эта функция не обладает
   ни одним из “замечательных” свойств,
   $\Rightarrow$, она одна образует минимальный базис.

2. **$F=X\downarrow Y$**.

   Так же как и “штрих Шеффера” эта функция
   образует минимальный базис.

3. **$F_1=X\rightarrow Y$ и $F_2=0$**, или **$F_1=Y\rightarrow X$ и $F_2=0$**.

4. **$F_1=X\oplus Y$, $F_2=X\cdot Y$, $F_3=1$**.

   Функции этого базиса входят в полином Жегалкина.

Система функций Σ называется *функционально полной в слабом смысле*, если любая логическая функция может быть представлена формулой над системой $\Sigma\cup\{0,1\}$, т.е. является суперпозицией констант и функций из Σ.

Теорема

(о функциональной полноте в слабом смысле)

Для того чтобы система функций Σ была ФП в слабом смысле, необходимо и достаточно, чтобы она содержала хотя бы одну немонотонную и хотя бы одну нелинейную функцию.

- *Необходимость*. Классы монотонных и линейных функций замкнуты и содержат 0 и 1 $\Rightarrow$ если Σ не содержит немонотонных или нелинейных функций, то их нельзя получить с помощью суперпозиций из Σ и констант.

- *Достаточность*. Пусть Σ содержит немонотонную и нелинейную функции. Тогда по лемме 1 подстановкой констант из монотонной функции получаем отрицание, по лемме 2 из нелинейной с помощью отрицаний - $\wedge$ и $\vee$.

Примеры:

1. $\Sigma = \{\wedge, \oplus, \}$ функциональна полна в слабом смысле, т.к. $\wedge$ – нелинейна, а $\oplus$ – немонотонна.

2. $\Sigma_3 = \{|\}$ функциональна полна в слабом смысле, т.к. Штрих Шеффера – нелинейная и немонотонная функция.