Занятие 15

ФКН ВШЭ, курс «Дискретная математика», основной поток

2015/16 уч. год

Определения. *Булева функция* — это всюду определённая функция $\{0,1\}^n \to \{0,1\}$. *Базис* — любое множество булевых функций (быть может, бесконечное). *Стандартный базис* состоит из трёх функций $\{\neg, \wedge, \vee\}$.

Суперпозицией булевых функций (или *подстановкой* функций $g_i(x_1, \ldots, x_n)$, $1 \leqslant i \leqslant m$, в функцию $f(x_1, \ldots, x_m)$) называется функция

$$f(g_1(x_1, \ldots, x_n), g_2(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).$$

Булева схема в базисе B от переменных $x_1, \ldots, x_n$ — это последовательность булевых функций $g_1, \ldots, g_s$, в которой всякая g_i или равна одной из переменных, т.е. $g_i = x_j$, $1 \leqslant j \leqslant n$, или получается из предыдущих функций последовательности подстановкой в одну из базисных функций. Более точно второе условие формулируется так: существуют базисная функция $f(y_1, \ldots, y_r) \in B$ и такая последовательность индексов $1 \leqslant j_1, \ldots, j_r < i$, что

$$g_i(x_1, \ldots, x_n) = f(g_{j_1}(x_1, \ldots, x_n), g_{j_2}(x_1, \ldots, x_n), \ldots, g_{j_r}(x_1, \ldots, x_n))$$

для всех наборов значений переменных $x_1, \ldots, x_n$.
Неформально полезно представлять написанное выше равенство как определение функции g_i. Такого рода определения обычно называются *присваиваниями* и записываются «несимметричным равенством» $:=$ (присваивание определяет левую часть равенства через значение правой части).

Булева схема $g_1, \ldots, g_s$ *вычисляет функцию* f, если $f = g_s$. Число s называется *размером схемы*.

Базис B называется *полным*, если любая булева функция вычисляется схемой в базисе B.

Формулой называется такая схема $g_1, \ldots, g_s$, в которой все g_i кроме переменных входят в правые части присваиваний

$$g_i(x_1, \ldots, x_n) := f(g_1(x_1, \ldots, x_n), g_2(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

не более одного раза (переменные могут входить сколько угодно раз).

Примечание. Обычно формулами называются выражения, составленные из скобок, запятых, имён функций и имён переменных. По такому выражению определена

последовательность вычисления значений входящих в него функций, т.е. схема в соответствии с данным выше определением. Например, функция $x_1 \oplus x_2$ сложения по модулю 2 тождественно равна ДНФ

$$(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2).$$

Чтобы вычислить значение этой формулы при заданных значениях переменных, нужно вычислить $x_1 \wedge \neg x_2$, затем $(\neg x_1 \wedge x_2)$, после чего взять конъюнкцию полученных значений.

Схемы, которые получаются из формул в обычном смысле, не произвольны. Если в формуле нужно использовать дважды значение конъюнкции $x_1 \wedge \neg x_2$, то придётся написать это выражение дважды. Поэтому схема, которая задаёт последовательность вычислений по формуле, удовлетворяет указанному выше ограничению.

Основные факты.

1. Стандартный базис полный.

2. Если любая функция f из полного базиса B_1 вычисляется схемой в базисе B_2, то базис B_2 полный.

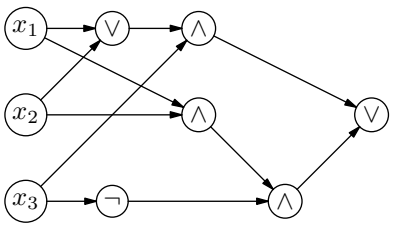
3. Пусть P — такое собственное множество булевых функций (т.е. не совпадающее с множеством всех булевых функций), которое содержит все функции вида

   $$\pi_{i,n}(x_1, \ldots, x_n) = x_i$$

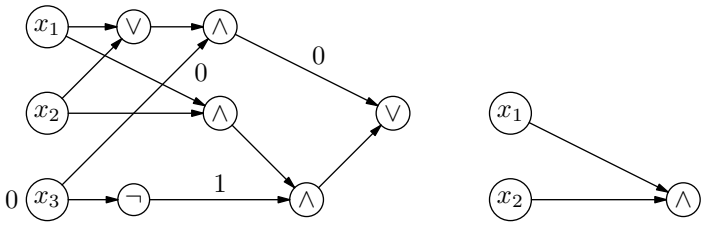
   (*проекции*) и замкнуто относительно суперпозиции базисных функций и функций из P (подстановка функций из множества P в функцию из базиса B принадлежит множеству P). Тогда базис B неполный.

   (По индукции легко доказать, что все функции, вычислимые схемами в базисе B, принадлежат множеству P, которое не совпадает с множеством всех булевых функций по сделанному выше предположению.)

Задача 15.1. Найдите функцию, которую вычисляет схема в стандартном базисе, представленная графически как

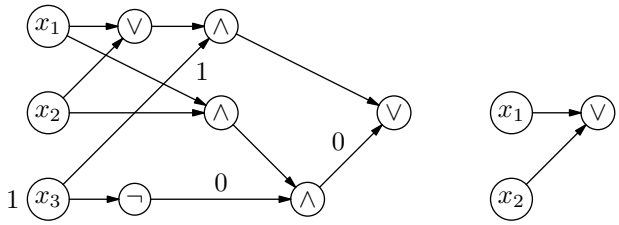


Решение. Пусть $x_3 = 0$. Так как $\neg 0 = 1$, $x \wedge 0 = 0$, $x \wedge 1 = x$, $0 \vee x = x$, то схема упрощается, как показано на рисунках



В этом случае значение функции, вычисляемой схемой, равно 1 тогда и только тогда, когда $x_1 = x_2 = 1$.

Пусть $x_3 = 1$. Так как $\neg 1 = 0$, $x \wedge 0 = 0$, $x \wedge 1 = x$, $0 \vee x = x$, то схема упрощается, как показано на рисунках



В этом случае значение функции, вычисляемой схемой, равно 1 тогда и только тогда, когда $x_1 = 1$ или $x_2 = 1$.

Во всех случаях значение функции, которую вычисляет схема, равно 1 тогда и только тогда, когда хотя бы две переменные равны 1.

Ответ: это функция $\mathrm{MAJ}(x_1, x_2, x_3)$, которая равна 1 тогда и только тогда, когда больше половины аргументов равны 1. □

Задача 15.2. Существует ли такая булева функция f от двух переменных, что схема в базисе $\{\wedge, f\}$

$$x_1,\ x_2,\ s_1 := f(x_1, x_2);\ s_2 := f(x_2, x_1);\ s_3 := s_1 \wedge s_2$$

вычисляет **а)** функцию x_1? **б)** функцию $x_1 \oplus x_2$?

Решение. **а)** Ответ: нет. Схема из условия задачи вычисляет функцию, которая не изменяется при перестановке переменных (симметрическая функция), так как

$$f(x_1, x_2) \wedge f(x_2, x_1) = f(x_2, x_1) \wedge f(x_1, x_2).$$

А функция x_1 не симметрическая: при перестановке переменных $x_1 \leftrightarrow x_2$ она переходит в функцию x_2.

б) Ответ: да. Поскольку $x \wedge x = x$, в качестве $f(x_1, x_2)$ нужно взять $x_1 \oplus x_2$. □

Задача 15.3. Являются ли полными базисы

а) $\{\neg; \equiv\}$, где $x \equiv y$ равна $(x \to y) \wedge (y \to x)$?

б) $\{\neg, \to\}$, где $\to$ — импликация?

в) $\{\wedge, \vee, \setminus\}$, где $x \setminus y$ равна $x \wedge \neg y$?

Решение. **а)** Ответ: нет. Функции $\neg x = 1 \oplus x$ и $(x \equiv y) = 1 \oplus x_1 \oplus x_2$ являются линейными. Подстановка линейных функций в функции из этого базиса также является линейной функцией:

$$1 \oplus \left(a_0 \oplus \bigoplus_i a_i \wedge x_i \right) = (1 \oplus a_0) \oplus \bigoplus_i a_i \wedge x_i,$$
$$1 \oplus \left(a_0 \oplus \bigoplus_i a_i \wedge x_i \right) \oplus \left(b_0 \oplus \bigoplus_i b_i \wedge x_i \right) = (1 \oplus a_0 \oplus b_0) \oplus \bigoplus_i (a_i \oplus b_i) \wedge x_i.$$

Эти равенства справедливы в силу свойств коммутативности, ассоциативности и дистрибутивности арифметических операций по модулю 2.

Таким образом, схемы в данном базисе вычисляют только линейные функции. Количество линейных функций от n переменных равно 2^{n+1} (выбор одного из двух возможных значений для каждого из $1 + n$ коэффициентов), а количество всех булевых функций равно 2^{2^n} (выбор одного из двух возможных значений для каждого набора значений переменных, то есть элемента множества $\{0,1\}^n$). При достаточно большом n выполняется строгое неравенство $2^{n+1} < 2^{2^n}$, поэтому не все функции вычисляются в данном базисе.

б) Ответ: да. Тождества

$$x_1 \vee x_2 = (\neg x_1) \to x_2,$$
$$x_1 \wedge x_2 = \neg(x_1 \to (\neg x_2))$$

дают формулы, которые вычисляют функции из стандартного базиса в базисе $\{\neg, \to\}$.

в) Все функции из данного базиса сохраняют 0:

$$0 \wedge 0 = 0, \quad 0 \vee 0 = 0, \quad 0 \setminus 0 = 0.$$

В общем случае мы говорим, что функция $f(x_1, \ldots, x_n)$ *сохраняет* 0, если

$$f(0, 0, \ldots, 0) = 0.$$

Подстановка функций, сохраняющих 0, в функцию, сохраняющую 0, даёт функцию, сохраняющую 0:

$$f(g_1(0, \ldots, 0), g_2(0, \ldots, 0), \ldots, g_m(0, \ldots, 0)) = f(0, 0, \ldots, 0) = 0.$$

Значит, схемы в данном базисе вычисляют только функции, сохраняющие 0.

Примером функции, не сохраняющей 0 (т.е. не вычислимой в данном базисе), является $\neg x$. □

Задача 15.4. Назовём *функцией большинства* $\mathrm{MAJ}(x_1, x_2, \ldots, x_n)$ булеву функцию, значение которой совпадает с тем значением, которое принимает большинство переменных (если мнения разделились поровну, MAJ = 0). Схемы в базисе $\{\vee, \wedge\}$ называются *монотонными*. Вычисляется ли MAJ монотонной схемой?

Решение. Для каждого подмножества $S \subseteq \{1, 2, \ldots, n\}$ размера больше $n/2$ существует монотонная схема, вычисляющая конъюнкцию переменных x_i, $i \in S$. Если $S = \{i_1, \ldots, i_r\}$, то эта схема имеет вид

$$x_1,\ \ldots,\ x_n,\ g_{n+1} := x_{i_1} \wedge x_{i_2},\ g_{n+2} := g_{n+1} \wedge x_{i_3},\ \ldots, g_{n+r-1} := g_{n+r-2} \wedge x_{i_r}.$$

Последней функции в этой схеме для удобства дадим ещё одно имя g_S.

Объединим вычисление всех этих конъюнкций в одну схему. Возьмём схему, которая аналогичным образом вычисляет дизъюнкцию всех g_S. Добавим её к построенной ранее схеме, вычисляющей все конъюнкции g_S.

Докажем, что полученная в результате схема вычисляет $\mathrm{MAJ}(x_1, x_2, \ldots, x_n)$. Функция, которую вычисляет схема, равна 1 тогда и только тогда, когда хотя бы один из членов дизъюнкции равен 1. Это равносильно тому, что для какого-то множества S размера больше $n/2$ конъюнкция g_S равна 1, т.е. все переменные, входящие в эту конъюнкцию, равны 1. Поэтому $\mathrm{MAJ}(x_1, \ldots, x_n) = 1$.

В обратную сторону: если $\mathrm{MAJ}(x_1, \ldots, x_n) = 1$, то множество $S = \{i : x_i = 1\}$ имеет размер больше $n/2$. Конъюнкция g_S равна 1. Значит, и дизъюнкция всех g_S равна 1.

Итак, функция, вычисляемая построенной схемой, равна 1 тогда и только тогда, когда $\mathrm{MAJ}(x_1, \ldots, x_n) = 1$, что и требовалось доказать. □

Задача 15.5. Булева функция $f(x_1, \ldots, x_n)$ называется *самодвойственной* (или нечётной), если для всех $x_1, \ldots, x_n$ выполняется равенство

$$f(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n).$$

а) Являются ли самодвойственными функции $x_1 \vee x_2$, $x_1 \wedge x_2$?

б) Докажите, что схема в базисе, состоящем из самодвойственных функций, вычисляет самодвойственную функцию.

Решение. **а)** Ответы: нет, нет.

Назовём функцию $g(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n)$ *двойственной функцией* к функции f.

Из правил де Моргана и тождества $\neg\neg x = x$ получаем

$$\neg(\neg x_1 \vee \neg x_2) = x_1 \wedge x_2, \quad \neg(\neg x_1 \wedge \neg x_2) = x_1 \vee x_2.$$

То есть конъюнкция и дизъюнкция двойственны друг другу и не являются самодвойственными функциями.

б) Функции x_i самодвойственные: $\neg(\neg x) = x$. Осталось проверить, что подстановка самодвойственных функций в самодвойственную функцию даёт самодвойственную функцию:

$$\begin{aligned}\neg f(g_1(\neg x_1, \ldots, \neg x_n), g_2(\neg x_1, \ldots, \neg x_n), \ldots, g_m(\neg x_1, \ldots, \neg x_n)) = \\ = \neg f(\neg g_1(x_1, \ldots, x_n), \neg g_2(x_1, \ldots, x_n), \ldots, \neg g_m(x_1, \ldots, x_n)) = \\ = f(g_1(x_1, \ldots, x_n), g_2(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).\end{aligned}$$

В первом равенстве использована самодвойственность функций g_i, в втором — самодвойственность функции f. □

Задача 15.6. Пусть $f(x_1, \ldots, x_n)$ — несамодвойственная функция. Докажите, что константы 0, 1 вычисляются в базисе $\{\neg, f\}$.

Решение. Если f не является самодвойственной, то для некоторого набора значений переменных $a = (a_1, \ldots, a_n)$ выполняется равенство

$$f(a_1, \ldots, a_n) = f(\neg a_1, \ldots, \neg a_n). \tag{1}$$

Будем использовать «экспоненциальную запись» литералов: $x^1 := x$, $x^0 := \neg x$.

Рассмотрим схему в базисе $\{\neg, f\}$, которая вычисляет значение выражения

$$f(x_1^{a_1}, x_1^{a_2}, \ldots, x_1^{a_n}) \tag{2}$$

(сначала вычисляем все отрицания переменных, а потом применяем f к набору литералов $x_1^{a_i}$). При $x_1 = 1$ получаем $x_1^{a_i} = a_i$. При $x_1 = 0$ получаем $x_1^{a_i} = \neg a_i$. В силу равенства (1) схема (2) в обоих случаях даёт одно и то же значение, то есть вычисляет одну из констант 0 или 1. Вторая константа получается применением отрицания, которое есть в базисе. □

Задача 15.7. Многочленом Жегалкина называется формула вида

$$\bigoplus_{S \subseteq \{1,\ldots,n\}} a_S \bigwedge_{i \in S} x_i, \qquad a_S \in \{0, 1\},$$

булевы значения a_S называются коэффициентами многочлена Жегалкина. Докажите, что каждая булева функция однозначно представляется в виде многочлена Жегалкина.

Решение. Заметим, что *базис Жегалкина* $\{1, \wedge, \oplus\}$ полный, так как функции из стандартного базиса в нём выражаются:

$$\neg x = 1 \oplus x,$$
$$x \vee y = x \oplus y \oplus (x \wedge y),$$

а конъюнкция (произведение по модулю 2) сама входит в базис Жегалкина.

Многочлен Жегалкина — это особая формула в базисе Жегалкина. В правых частях присваиваний такой формулы сначала встречаются только произведения, а потом — только суммы.

Для преобразования любой схемы в схему такого вида воспользуемся тем, что для арифметических операций по модулю 2 выполняются свойства ассоциативности, коммутативности и дистрибутивности. Поэтому можно «раскрывать скобки»

$$(x \oplus y) \wedge z = (x \wedge z) \oplus (y \wedge z),$$

т.е. менять порядок вычисления сумм и произведений. Пока какое-то произведение применяется к сумме, можно преобразовать схему в схему, вычисляющую ту же функцию, но с изменённым порядком суммы и произведения.

Закончатся такие преобразования в тот момент, когда в схеме все произведения применяются только к переменным или другим произведениям. Это ещё не многочлен Жегалкина — одно и то же произведение может встретиться в схеме много раз. Теперь мы «приведём подобные», т.е. будем преобразовывать схему, используя равенство

$$x \oplus x = 0.$$

Сокращая пары одинаковых произведений, мы получаем схему, которая вычисляет ту же функцию.

После всех сокращений и получится многочлен Жегалкина.

Чтобы доказать единственность представления функции многочленом Жегалкина, заметим, что по определению многочлен Жегалкина задаётся набором коэффициентов a_S, $S \subseteq \{1, \ldots, n\}$. Количество различных наборов коэффициентов равно 2^{2^n} (выбор одного из двух возможных значений для каждого подмножества $\{1, \ldots, n\}$, всего подмножеств 2^n). Столько же булевых функций от n переменных (выбор одного из двух возможных значений для каждого набора значений переменных, то есть элемента множества $\{0, 1\}^n$).

Рассмотрим отображение из наборов коэффициентов $(a_S : S \subseteq \{1, \ldots, n\})$ в булевы функции, задаваемое формулой для многочлена Жегалкина. Как было показано выше, это отображение является сюръективным (для каждой функции есть многочлен Жегалкина).

Как уже не раз говорилось, сюръективное отображение конечного множества в множество с тем же количеством элементов является также инъективным (и потому биективным). Значит, для каждой функции есть ровно один многочлен Жегалкина (инъективность). □