Лекция Л6. Полные системы булевых функций

Система булевых функций $\{f_1,..., f_m\}$ называется *полной*, если любая булева функция может быть выражена через функции $f_1,..., f_m$ с помощью *суперпозиций* (т.е. составления сложных функций). Приведем определение суперпозиции функций (см. [1, стр. 50]). Пусть

$$K^0 = \{f_1(X_1,..., X_{k_1}), f_2(X_1,..., X_{k_2}),..., f_m(X_1,..., X_{k_m})\}$$

- конечная система булевых функций. Функция f называется суперпозицией ранга 1 (или элементарной суперпозицией) функций $f_1,..., f_m$, если f может быть получена одним из следующих способов: (а) переименованием некоторой переменной X_j какой-нибудь функции f_i, т.е. $f = f_i(X_1,..., X_{j-1}, Y, X_{j+1},..., X_{k_i}),$ где Y может совпасть с любой переменной; (б) подстановкой некоторой функции f_l $(1 \le l \le m)$ вместо какой-нибудь переменной X_j любой из функций $f_i \in K^0$, т.е. $f = f_i(X_1,..., X_{j-1}, f_l(X_1,..., X_{k_l}), X_{j+1},..., X_{k_i}).$

Суперпозиции ранга 1 образуют класс функций K^1. Класс функций, получающийся из функций класса K^{r-1} (множества суперпозиций ранга $r-1$, где $r \ge 2$) с помощью элементарных суперпозиций, обозначается K^r - класс суперпозиций ранга r. *Суперпозициями* функций из K^0 называются функции, входящие в какой-либо из классов K^r, где $r \in \{0,1,...\}$.

Пример 1.23. Покажем, что булева функция $X_1X_2X_3 \vee X_1\overline{X}_2\overline{X}_3$ является суперпозицией системы булевых функций $\{\overline{X}_1, X_1X_2, X_1 \vee X_2\}$.

Решение. Переход от одной или двух формул к новой формуле с помощью одной из элементарных суперпозиций будем обозначать ограниченной стрелкой $\mapsto$. Используя элементарные суперпозиции переименования одной из переменных, получаем:

$$X_1X_2 \mapsto X_1X_3 \mapsto X_2X_3,\ X_1 \vee X_2 \mapsto X_1 \vee X_4.$$

Подстановкой функции X_2X_3 вместо переменной X_2 в формуле X_1X_2 получаем:

$$X_1X_2 \mapsto X_1X_2X_3.$$

Подстановкой функции $X_1X_2X_3$ вместо переменной X_1 в функции $X_1 \vee X_4$ получаем:

$$X_1 \vee X_4 \mapsto X_1X_2X_3 \vee X_4.$$

Используя элементарное преобразование переименования одной из переменных, имеем:

$$\overline{X}_1 \mapsto \overline{X}_2,\ \overline{X}_1 \mapsto \overline{X}_3,$$

откуда, используя элементарные подстановки полученных функций вместо одной из переменных, получаем:

$$X_1X_2X_3 \mapsto X_1\overline{X}_2X_3 \mapsto X_1\overline{X}_2\overline{X}_3.$$

Но тогда

$$X_1X_2X_3 \vee X_4,\ X_1\overline{X}_2\overline{X}_3 \mapsto X_1X_2X_3 \vee X_1\overline{X}_2\overline{X}_3.$$

Из рассмотрения примера 1.23 с очевидностью заключаем, что любая булева функция $f(X_1,..., X_n)$, выраженная формулой, находящейся в СДНФ (или СКНФ) относительно списка переменных $\langle X_1,..., X_n \rangle$, является суперпозицией системы булевых функций

$\{\overline{X}_1, X_1X_2, X_1 \vee X_2\}$ (или более кратко, системы $\{\neg,\cdot,\vee\}$, поскольку при построении суперпозиций мы можем произвольным образом переименовывать переменные в исходных булевых функциях системы). Таким образом, справедливо

Утверждение 6.1. Система булевых функций $\{\neg, \cdot, \vee\}$ (или $\{\neg,\ \&, \vee\}$) является полной.

Можно показать, что справедливо

Утверждение 6.2. Пусть система булевых функций $\{f_1,..., f_m\}$ является полной, и любая из функций этой системы может быть выражена с помощью суперпозиций через булевы функции $g_1,..., g_k$. Тогда система функций $\{g_1,..., g_k\}$ также является полной.

Пример 1.24. Используя утверждение 6.2, докажем полноту следующих систем булевых функций: (а) $\{\neg, \vee\}$; (б) $\{\neg, \cdot\}$; (в) $\{\neg, \supset\}$; (г) $\{|\}$ (где $X \mid Y = \neg(X \vee Y)$); (д) $\{\circ\}$ (где $X \circ Y = \neg(XY)$).

Решение. Воспользуемся полнотой системы $\{\neg, \cdot, \vee\}$. Тогда в силу утверждения 6.2 для доказательства полноты системы (а) выразим $\cdot$ через $\neg, \vee$ по формуле: $XY = \neg(\overline{X} \vee \overline{Y})$; (б) $X \vee Y = \neg\overline{X}\overline{Y}$; (в) $XY = \neg(X \supset \overline{Y})$, $X \vee Y = \neg X \supset Y$. Для доказательства полноты системы (г) воспользуемся полнотой системы (а) и выразим: $\overline{X} = \neg(X \vee X) = X \mid X$, $X \vee Y = \neg\neg(X \vee Y) = \neg(X \mid Y) = (X \mid Y) \mid (X \mid Y)$. Для доказательства полноты системы (д) воспользуемся полнотой системы (б) и выразим: $\overline{X} = \neg(XX) = X \circ X$, $XY = \neg\neg(XY) = \neg(X \circ Y) = (X \circ Y) \circ (X \circ Y)$.

Многочлен Жегалкина. Рассмотрим систему булевых функций $\{+, \cdot, 1\}$. Эта система является полной, что следует из утверждения 6/2, полноты системы $\{\neg, \cdot\}$ (см. пример 1.24 (б)), и равенству функций $\neg X = X + 1$ (см. таблицы их значений).

Приведем некоторые свойства булевых функций системы $\{+, \cdot, 1\}$ (легко проверяются таблично):

1. $XY = YX$;	1′. $X + Y = Y + X$;
2. $X(YZ) = (XY)Z$;	2′. $X + (Y + Z) = (X + Y) + Z$;
3. $XX = X$;	3′. $X + X = 0$;
4. $X \cdot 1 = X$;	4′. $X + 1 = \neg X$;
5. $X \cdot 0 = 0$;	5′. $X + 0 = X$.

6. $X(Y + Z) = XY + XZ$

(будем считать операцию $\cdot$ более «сильной», чем $+$, т.е. выполняемой в первую очередь).

Многочленом Жегалкина от переменных $X_1,..., X_n$ называется выражение вида (используя приведенные свойства функций системы $\{+, \cdot, 1\}$, получаем, что значения этого выражения можно рассматривать как булеву функцию от этих переменных и значение этой функции на каждой оценке списка переменных $\langle X_1,..., X_n\rangle$ однозначно определено)

$$\sum_{1 \le i_1 \le ... \le i_k \le n} X_{i_1} \cdots X_{i_k} + \alpha, \text{ где } \alpha \in \{0, 1\}, \tag{1}$$

и члены в (1) являются попарно различными.

Степенью одночлена $X_{i_1} \cdots X_{i_k}$ в (1) является число k. Степенью многочлена (1) является максимальная степень его одночленов.

Пример 1.25. Многочленами Жегалкина от переменных X, Y, Z являются: $XYZ + XY + XZ + X + Y + 1,\ XY + XZ + Y,\ X + Y + 1,\ X + 1,\ Y,\ 1,\ 0.$ Первый из этих многочленов имеет степень 3, а многочлены $1,\ 0$ имеют степень 0.

Упражнение 6.1. Показать, что количество многочленов Жегалкина от переменных $X_1,..., X_n$ равно 2^{2^n}, т.е. равно числу булевых функций от этих переменных (см. упражнение 1.1).

Решение. Можно составить $2^n - 1$ попарно различных одночленов в выражении (1), содержащих хотя бы одну переменную (каждая из n переменных $X_1,..., X_n$ независимо от других либо войдет в этот одночлен, либо нет, т.е. имеем 2^n вариантов составления одночлена; исключив одночлен без букв, получаем указанное число). Каждый из этих одночленов может войти или не войти (независимо от других) в выражение (1), т.е. буквенная часть выражения (1) может быть составлена $2^{(2^n - 1)}$ способами. Умножая это число на 2 (количество вариантов выбора числа α), получаем 2^{2^n}.

Используя приведенные свойства системы $\{+, \cdot, 1\}$, а также упражнение 6.1, нетрудно доказать, что справедливо

Утверждение 6.3 Любая булева функция $f(X_1,..., X_n)$ может быть выражена многочленом Жегалкина от переменных $X_1,..., X_n$, причем единственным образом (с точностью до перестановки одночленов).

В зависимости от того, каким образом задана булева функция $f(X_1,..., X_n)$ (формулой логики высказываний или таблицей своих значений) приведем соответствующие алгоритмы выражения булевой функции многочленом Жегалкина.

Алгоритм 6.1 (случай, когда булева функция $f(X_1,..., X_n)$ задана формулой логики высказываний F со списком переменных $\langle X_1,..., X_n \rangle$)

1-й этап. Избавляемся в F от операций $\supset, \sim$ (т.е. выражаем эти логические операции через $\neg,\ \&, \vee,$ аналогично алгоритмам нахождения ДНФ и КНФ).

2-й этап. Избавляемся в полученной на 1-м этапе формуле от $\vee,$ используя равносильность $A \vee B \equiv \neg(\overline{A}\ \&\ \overline{B}).$

3-й этап. Избавляемся в полученной на 2-м этапе формуле от $\&, \neg$ по формулам: $A\ \&\ B = AB,\ \neg A = \overline{A} = A + 1.$

4-й этап. Используя приведенные свойства 1-6 системы $\{+, \cdot, 1\}$, раскрываем в полученной на 3-м этапе формуле скобки и приводим подобные члены.

Упражнение 6.2. Выразить многочленами Жегалкина булевы функции $X \supset Y, X \vee Y, X \sim Y, X \circ Y, X \mid Y$.

Решение. Используя алгоритм 6.1, основные равносильности логики высказываний, а также приведенные ранее свойства 1-6 системы $\{+, \cdot, 1\}$, получаем:

$$X \supset Y = \overline{X} \vee Y = \neg(X\ \& \overline{Y}) = X(Y + 1) + 1 = XY + X + 1,$$

$$X \vee Y = \neg(\overline{X}\ \& \overline{Y}) = (X + 1)(Y + 1) + 1 = XY + X + Y + 1 + 1 = XY + X + Y,$$

$$X \sim Y = \neg(X + Y) = X + Y + 1,\ \ X \circ Y = \neg(X \,\&\, Y) = XY + 1,$$
$$X \mid Y = \neg(X \vee Y) = XY + X + Y + 1.$$

Пример 1.26. Используя алгоритм 1.7, выразим многочленом Жегалкина булеву функцию f_F, соответствующую формуле $F = \neg(Y \,\&\, \neg Z) \sim \neg(\neg Y \supset \neg X)$ из примера 1.5. Будем при этом использовать, полученные в упражнении 6.2 формулы.

$$f_F = \neg(Y \,\&\, \neg Z) \sim \neg(\neg Y \supset \neg X) = \neg(Y \,\&\, \neg Z) \sim \neg(Y \vee \neg X) =$$
$$= \neg(Y \,\&\, \neg Z) \sim (\overline{Y} \,\&\, X) = \neg(Y \,\&\, \neg Z) + (\overline{Y} \,\&\, X) + 1 = Y(Z+1) + 1 + (Y+1)X + 1 =$$
$$= YZ + Y + 1 + YX + X + 1 = XY + YZ + X + Y.$$

Следствием утверждения 4.1 является

Утверждение 6.4. Пусть $f(X_1,..., X_n)$ - булева функция, не равная тождественно 0. Тогда справедливо представление

$$f(X_1,..., X_n) = \sum_{f(\varepsilon_1,...,\varepsilon_n)=1} (X_1^{\varepsilon_1} \cdots X_n^{\varepsilon_n}), \qquad (2)$$

где сложение (по модулю 2) берется по всем оценкам $\langle \varepsilon_1,..., \varepsilon_n \rangle$, для которых $f(\varepsilon_1,..., \varepsilon_n) = 1$.

Опишем теперь

Алгоритм 6.2 (случай, когда булева функция $f(X_1,..., X_n)$ задана таблично)

1-й этап. Пусть имеет место нетривиальный случай, когда функция f не равна тождественно 0 (в противном случае многочленом Жегалкина, выражающим f, является 0). Воспользуемся представлением (2).

2-й этап. Избавляемся в правой части равенства (2) от отрицаний по формуле $\overline{A} = A + 1$.

3-й этап. Используя приведенные свойства 1-6 системы $\{+, \cdot, 1\}$, раскрываем в полученной на 2-м этапе формуле скобки и приводим подобные члены.

Пример 1.27. Используя алгоритм 6.2, выразим многочленом Жегалкина булеву функцию f_F, соответствующую формуле $F = \neg(Y \,\&\, \neg Z) \sim \neg(\neg Y \supset \neg X)$ из примера 1.5. Будем при этом использовать приведенную в примере 1.15 табл. 1.4 со значениями булевой функции f_F. Согласно формуле (2) получим равенство (сравни с примером 1.26)

$$f_F = XY\overline{Z} + X\overline{Y}Z + X\ \overline{Y}\ \overline{Z} + \overline{X}Y\overline{Z} =$$
$$= XY(Z+1) + X(Y+1)Z + X\ (Y+1)\ (Z+1) + (X+1)Y(Z+1) =$$
$$= X(Z+1)(Y+Y+1) + XYZ + XZ + XYZ + XY + YZ + Y =$$
$$= X(Z+1) + XYZ + XZ + XYZ + XY + YZ + Y =$$
$$= XZ + X + XZ + XY + YZ + Y = XY + YZ + X + Y\ .$$