УНИВЕРСИТЕТ ИТМО

Лекция 4. Нормальные формы. СКНФ, СДНФ, Полином Жегалкина. Классы Поста, теорема Поста

Разложение булевых функций по переменным

- Пусть $x^y \overset{\text{def}}{=} x \wedge y \vee \bar{x} \wedge \bar{y}$. Очевидно, что

$$x^y = \begin{cases} \bar{x}, \text{если } y = 0, \\ x, \text{если } y = 1, \end{cases} \quad x^y = \begin{cases} 1, \text{если } x = y, \\ 0, \text{если } x \neq y, \end{cases} \quad x^y = x \leftrightarrow y.$$

- Теорема (О разложении булевой функции по переменным)

$$f(x_1, \dots, x_m, x_{m+1}, \dots, x_n) =$$

$$= \bigvee_{(\sigma_1, \dots, \sigma_m)} x_1^{\sigma_1} \wedge \dots \wedge x_m^{\sigma_m} \wedge f(\sigma_1, \dots, \sigma_m, x_{m+1}, \dots, x_n),$$

где дизъюнкция берётся по всем возможным наборам значений $(\sigma_1, \dots, \sigma_m)$.

Минимальные термы

- Выражение вида $x_1^{\sigma_1} \wedge \ \dots \ \wedge x_n^{\sigma_n}$ называется минимальным термом, или совершенным одночленом, или конституентой единицы, или минтермом.
- Минтерм является реализацией некоторой булевой функции *n* переменных, которая имеет значение 1 ровно на одном наборе значений переменных, а именно на наборе $(\sigma_1, \dots, \sigma_n)$.
- Следствие (к теореме о разложении булевой функции к переменным).

Любую булеву функцию, кроме 0, можно представить как дизъюнкцию некоторых минтермов.

ДНФ и КНФ

- Дизъюктивной формой называется формула вида

$$\bigvee_{i=1}^{k} K_i, \text{ где } K_i = \bigwedge_{p=1}^{m_i} x_{j_p}^{\sigma_p},$$

т.е. $K_1 \vee \cdots \vee K_k = x_{j_1}^{\sigma_1} \wedge \ldots \wedge x_{j_{m_1}}^{\sigma_{m_1}} \vee \ldots \vee x_{j_1}^{\sigma_1} \wedge \ldots \wedge x_{j_{m_k}}^{\sigma_{m_k}}$

- Формула K_i называется элементарной конъюнкцией, переменные в элементарную конъюнкцию входят в установленном порядке (хотя и не обязательно все n).
- Количество переменных в конъюнкции называется её рангом ($|K_i|$).

ДНФ и КНФ

- Теорема. Число различных дизъюнктивных форм n переменных равно 2^{3^n}.

Булева функция может быть задана бесконечным числом различных, но равносильных формул. Возникает естественная задача: для данной булевой функции найти реализующую формулу, обладающую теми или иными свойствами.

Совершенные нормальные формы

- Реализаций булевой функции $f(x_1, \dots, x_n)$ в виде формулы

$$\bigvee_{\{(\sigma_1, \dots, \sigma_n) \mid f(\sigma_1, \dots, \sigma_n) = 1\}} x_1^{\sigma_1} \wedge \dots \wedge x_n^{\sigma_n}$$

называется <u>совершенной дизъюнктивной нормальной формой</u> (СДНФ).

СДНФ формулы алгебры высказываний называется ее ДНФ, обладающая следующими свойствами:

1) ДНФ не содержит двух одинаковых конъюнкций;
2) Ни одна конъюнкция не содержит одновременно двух одинаковых переменных.

Совершенные нормальные формы

3) Ни одна конъюнкция не содержит одновременно некоторую переменную и ее отрицание.

4) Каждая конъюнкция содержит либо переменную x_i, либо ее отрицание $\overline{x_i}$ для всех переменных, входящих в формулу.

- Реализаций булевой функции $f(x_1, \ldots, x_n)$ в виде формулы

$$f(x_1, \ldots, x_n) = \bigwedge_{\{(\sigma_1,\ldots,\sigma_n) | f^*(\sigma_1,\ldots,\sigma_n)=1\}} x_1^{\sigma_1} \vee \ \ldots \vee x_n^{\sigma_n}$$

называется <u>совершенной конъюнктивной нормальной формой</u> (СКНФ).

Совершенные нормальные формы

<u>Совершенной конъюнктивной нормальной формой</u> (СКНФ) данной алгебры высказываний называется такая ее КНФ, которая удовлетворяет следующим свойствам:

1) КНФ не содержит двух одинаковых дизъюнкций;
2) Ни одна из дизъюнкций не содержит одновременно двух одинаковых переменных;
3) Ни одна из дизъюнкций не содержит одновременно некоторую переменную и ее отрицание;
4) Каждая дизъюнкция СКНФ содержит либо переменную x_i, либо ее отрицание x_i для всех переменных, входящих в формулу.

Совершенные нормальные формы

- Теорема 1

Всякая булева функция имеет единственную СДНФ.

- Теорема 2

Всякая булева функция имеет единственную совершенную конъюнктивную нормальную форму (СКНФ).

Совершенные нормальные формы

- Следствие

Всякая булева функция может быть выражена через дизъюнкцию, конъюнкцию и отрицание.

- Замечание
- Принято считать, что пустая дизъюнкция имеет значение 0, а пустая конъюнкция – значение 1.
- Замечание

Если $f = 0$, то $\{(\sigma_1, \dots, \sigma_n) | f(\sigma_1, \dots, \sigma_n) = 1\} = \emptyset$. В соответствии с соглашением предыдущего замечания пустая формула считается СДНФ нуля.

Построение СДНФ и СКНФ

I. С помощью таблицы истинности

Исходя из таблицы истинности булевой функции, можно построить СДНФ функции: для каждого набора $\tau = (\tau_1, \tau_2, \dots, \tau_n)$, такого, что $f(\tau) = 1$, составляется конъюнкция $x_1^{\tau_1} \wedge x_2^{\tau_2} \wedge \dots \wedge x_n^{\tau_n}$, а затем все эти конъюнкции соединяются знаком дизъюнкции.

Для построения СКНФ функции выписываем наборы $\bar{\tau} = (\overline{\tau_1}, \overline{\tau_2}, \dots, \overline{\tau_n})$ такие, что $f(\bar{\tau}) = 0$. Для такого набора составляется дизъюнкция

$$x_1^{\overline{\tau_1}} \vee x_2^{\overline{\tau_2}} \vee \dots \vee x_n^{\overline{\tau_n}},$$

а затем все такие дизъюнкции соединяют знаком конъюнкции.

Построение СДНФ и СКНФ

II. С помощью эквивалентных преобразований.

1) Элиминация операций.

Любая булева функция реализуется формулой над базисом $\{\wedge, \vee, \neg\}$ (например, в виде СДНФ). Таким образом, присутствующая в формуле подформула с главной операцией, отличной от дизъюнкции, конъюнкции и отрицания, может быть заменена подформулой, содержащей только три базисные операции.

Например, элиминация импликации выполняется с помощью равносильности $x_1 \to x_2 = \neg x_1 \vee x_2$. В результате первого шага в формуле остаются только базисные операции.

Построение СДНФ и СКНФ

2) Протаскивание отрицаний.

С помощью инволютивности отрицания и правил де Моргана ($\bar{\bar{x}} = x$, $\overline{x \vee y} = \bar{x} \wedge \bar{y}$, $\overline{x \wedge y} = \bar{x} \vee \bar{y}$) операция отрицания «протаскивается» к переменным. В результате второго шага отрицания могут присутствовать в формуле только непосредственно перед переменными.

3) Раскрытие скобок.

По дистрибутивности конъюнкции относительно дизъюнкции раскрываются все скобки, являющиеся операндами конъюнкции. В результате третьего шага формула приобретает вид <u>дизъюнктивной формы</u>: $\vee\left(A_i \wedge \ \ldots \wedge A_j\right)$, где A_k - это либо переменная, либо отрицание переменной,

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

Построение СДНФ и СКНФ

4) Удаление нулей.

Если в слагаемое дизъюнктивной формы входят переменная и ее отрицание $(x \land \neg x = 0)$, то такое слагаемое удаляется. Если при это формула оказывается пустой, то процесс прерывается и считается завершённым (исходная формула реализует 0).

5) Приведение подобных.

С помощью идемпотентности конъюнкции удаляются повторные вхождения переменных в каждую конъюнкцию $(x \land x = x)$, а затем с помощью идемпотентности дизъюнкции $(x \lor x = x)$ удаляются повторные вхождения одинаковых конъюнкций в дизъюнкцию. В результате формула не содержит «лишних» переменных и «лишних» конъюнктивных слагаемых.

Построение СДНФ и СКНФ

6) Расщепление переменных.

По правилу расщепления в каждую конъюнкцию, которая содержит не все переменные, добавляются недостающие таким образом: $x = x \vee 0 = x \vee (y \wedge \bar{y}), x = x \wedge 1 = x \wedge (y \vee \bar{y})$

В результате шестого шага формула становится «совершенной», то есть в каждой конъюнкции содержатся все переменные.

7) Сортировка.

С помощью коммутативности переменные в каждой конъюнкции, а затем конъюнкции в дизъюнкции сортируются в установленном порядке.

В результате седьмого шага формула приобретает вид

Многочлены Жегалкина

- Многочлен Жегалкина – многочлен, являющийся суммой константы и различных одночленов, в которые каждая из переменных входит не выше, чем в первой степени.
- Многочлен Жегалкина константы равен самой же константе.
- Многочлен Жегалкина булевой функции *одной переменной*

$$f(x) = a_0 \oplus a_1 x.$$

- Многочлен Жегалкина булевой функции *двух переменных*

$$f(x_1, x_2) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 (x_1 \wedge x_2).$$

- Многочлен Жегалкина булевой функции *трех переменных*

$$f(x_1, x_2, x_3) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_3 \oplus a_4 (x_1 \wedge x_2) \oplus$$
$$\oplus a_5 (x_1 \wedge x_3) \oplus a_6 (x_2 \wedge x_3) \oplus a_7 (x_1 \wedge x_2 \wedge x_3)$$

Коэффициенты $a_i, i = 1, .. 2^n$ и свободный член a_0 принимают значения 0 или 1, а число слагаемых в формуле равно 2^n

Многочлены Жегалкина

- Теорема (Жегалкина)

Каждая булева функция $f(x_1, x_2, \dots, x_n)$ может быть представлена в виде многочлена Жегалкина и притом единственным образом, с точностью до порядка слагаемых.

Многочлены Жегалкина

- Первый алгоритм построения:

1) Находим множество тех двоичных наборов, на которые функция принимает значение 1;

2) Составляем СДНФ;

3) В СДНФ каждый знак дизъюнкции меняем на суммы Жегалкина;

4) Упрощаем, если можно, полученное выражение, используя тождество $\overline{x_i} \oplus x_i = 1$;

5) В полученной формуле каждое отрицание $\overline{x_i}$ заменяем на $x_i \oplus 1$;

6) Раскрываем скобки в полученной формуле, содержащей только функции $\wedge$ и $\oplus$ и константу 1;

7) Приводим подобные члены, используя тождество $x_i \oplus x_i = 0$

Многочлены Жегалкина

- Второй алгоритм построения:

Составляем систему линейных уравнений относительно 2^n неизвестных коэффициентов, содержащую 2^n уравнений, решением которой являются коэффициенты $a_0, a_1, \dots, a_{2^n-1}$ многочлена Жегалкина.

- Многочлен Жегалкина называется <u>нелинейным</u>, если он содержит конъюнкции переменных, а если он не содержит конъюнкции переменных, то он называется <u>линейным</u>.
- Функция $f(x_1, x_2, \dots, x_n)$ называется <u>линейной</u>, если ее многочлен Жегалкина имеет вид $a_0 \oplus a_1 x_1 \oplus \ \dots \ \oplus a_n x_n$, и <u>нелинейной</u> в противном случае.

Многочлены Жегалкина

- Для линейной булевой функции коэффициенты при переменных $x_1, x_2, \dots, x_n$ и свободный член вычисляются по формулам:

$$a_0 = f(0, \dots, 0),$$
$$a_1 = f(0, \dots, 0) \oplus f(1, \dots, 0),$$
$$a_2 = f(0, \dots, 0) \oplus f(0, 1, \dots, 0),$$
$$\dots$$
$$a_n = f(0, \dots, 0) \oplus f(0, \dots, 1).$$

Многочлены Жегалкина

- Алгоритм определения линейности булевой функции

1) По таблицам истинности булевой функции $f(x_1, x_2, \dots, x_n)$ находим коэффициенты: $(a_0, a_1, \dots, a_n)$.

2) Выписываем многочлен $\Phi(x_1, \dots, x_n) = = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n$ и проверяем, задает ли он эту функцию.

Для этого строим таблицу истинности многочлена $\Phi(x_1, x_2, \dots, x_n)$ и сравниваем ее с таблицей истинности функции $f(x_1, x_2, \dots, x_n)$.

Если таблицы истинности совпадают, то функция $f(x_1, x_2, \dots, x_n)$ <u>линейная</u> и $\Phi(x_1, x_2, \dots, x_n)$ - ее многочлен Жегалкина. В противном случае функция <u>нелинейная</u>.

Полные системы булевых функций

- Пусть даны булевы функции $f(x_1, x_2, \dots, x_n)$, $g_1(x_1, x_2, \dots, x_n)$, $g_2(x_1, x_2, \dots, x_n)$, …, $g_m(x_1, x_2, \dots, x_n)$.
- Подставим функции g_i в функцию f.
- Получим новую булеву функцию: $f(g_1(x_1, x_2, \dots, x_n), g_2(x_1, x_2, \dots, x_n), \dots, g_m(x_1, x_2, \dots, x_n))$, которую называют <u>суперпозицией функций</u> $f, g_2, \dots, g_m$.
- Метод получения произвольных булевых функций через базисные называют <u>операцией суперпозиции булевых функций</u>.

Полные системы булевых функций

- Набор булевых функций $M = \{f_1, \dots, f_m\}$ называется полной системой булевых функций, или базисом, если любая булева функция выражается через них при помощи операции суперпозиции в конечном числе раз.
- Набор булевых функций $M = \{\vee,\ \wedge,\ \neg\}$ является полной системой булевых функций, так как любая булева функция может быть аналитически представлена в форме СДНФ или СКНФ. Эту полную систему называют стандартным базисом.

Полные системы булевых функций

- Теорема о двух системах.
- Пусть имеется булевых функций $M = \{f_1, \dots, f_m\}$.
- Тогда для полноты некоторой другой системы булевых функций N= $\{g_1, \dots, g_n\}$ необходимо и достаточно, чтобы любая функция $f_i \in M$ выражалась через функции системы N при помощи операции суперпозиции.
- Примеры других полных систем:

1) $N = \{\oplus, \cdot, 1\}$ – является полной, так как любая функция из стандартного базиса выражается через функции из N:

$$x_1 \wedge x_2 = x_1 \cdot x_2,$$

$$\bar{x} = x \oplus 1,$$

Полные системы булевых функций

$$x_1 \vee x_2 = \overline{\overline{x_1} \cdot \overline{x_2}} = \overline{x_1} \oplus \overline{x_2} \oplus 1 = (x_1 \oplus 1) \cdot (x_2 \oplus 1) = x_1 \cdot$$
$$\cdot\, x_2 \oplus x_1 \oplus x_2 \oplus 1.$$

- Эта полная система называется базисом Жегалкина. Любая булева функция может быть представлена в этом базисе в форме многочлена Жегалкина по степеням неизвестных, например:

$$\overline{x_1} \cdot \overline{x_2} = (x_1 \oplus 1) \cdot (x_2 \oplus 1) = x_1 \cdot x_2 \oplus x_1 \oplus x_2 \oplus 1.$$

2) Полной является система, состоящая из одной функции Шеффера: $N = \{|\}$. Через нее выражаются функции стандартного базиса:

$$\bar{x} = x|x,$$

$$x_1 \wedge x_2 = (x_1|x_2)|(x_1|x_2),$$

Полные системы булевых функций

- Класс булевых функций K называется замкнутым, если всякая суперпозиция функций этого класса будет функцией из этого класса.
- Важные замкнутые классы Поста:

- класс T_0 - множество булевых функций, равных 0 на нулевых значениях всех переменных;

- класс T_1 - множество булевых функций, равных 1 на единичных значениях всех переменных;

- класс S - множество самодвойственных функций, которые обладают свойством:

$$f(x_1, \dots, x_n) = \overline{f(\overline{x_1}, \dots, \overline{x_n})};$$

Полные системы булевых функций

- класс L – множество линейных функций, которые в базисе Жегалкина представляются многочленом не выше первой степени;

- класс M – множество монотонных функций, которые обладают свойством:

$$f(x_1, \dots, x_n) \le f(y_1, \dots, y_n), \text{ если все } x_i \le y_i \,.$$

Полные системы булевых функций

Теорема Поста-Яблонского

- Для того, чтобы множество N булевых функций было полной системой, необходимо и достаточно найти для каждого из пяти замкнутых классов Поста T_0, T_i, S, L, M функцию из N, которая ему не принадлежит.

Полные системы булевых функций

- Рассмотрим множество из одной функции Шеффера $N = \{|\}$. Известно, что это полная система. Проверим это вторым алгоритмом определения полноты системы булевых функций.
- Согласно теореме Поста такая единственная функция не должна принадлежать ни одному из классов Поста.

  Так как $x_1|x_2 = \overline{x_1 \vee x_2} = \overline{x_1} \wedge \overline{x_2}$, то имеем $0|0 = 1$. Следовательно штрих Шеффера *не принадлежит классу* T_0.
- Теперь покажем, что он *не самодвойственная функция*:

$$\overline{\overline{x_1}|\overline{x_2}} = \overline{x_1} \cdot \overline{x_2} \neq x_1|x_2.$$

- Штрих Шеффера *не является линейной функцией*, так как

$$x_1|x_2 = x_1 \cdot x_2 \oplus 1.$$

Полные системы булевых функций

- Штрих Шеффера *не принадлежит классу монотонных функций*, так как

$$0|0 = 1, \qquad 1|1 = 0.$$

УНИВЕРСИТЕТ ИТМО

Спасибо за внимание!

Санкт-Петербург, 2022