Здравствуйте!
Алгоритм действия такой:
1. Ознакомьтесь с содержанием лекции.
2. Сделайте краткий конспект.

Многочлены Жегалкина

Многочлены Жегалкина являются еще одним интересным *подклассом* формул, позволяющим однозначно представлять *булевы функции*.

Определение . *Многочленами Жегалкина* названются формулы над множеством функций F_J={ 0, 1, *, +} (здесь * - это другое обозначение конъюнкции).

Таким образом, каждый *многочлен Жегалкина* (возможно, после раскрытия скобок и "приведения" подобных членов) представляет сумму (по модулю 2) *положительных (монотонных) элементарных конъюнкций* (т.е. *элементарных конъюнкций* без отрицаний). Поскольку для + и * справедливы *законы ассоциативности*, мы будем при записи *многочлена Жегалкина* опускать скобки, считая, что * связывает аргументы сильнее, чем +

Нетрудно проверить, что справедливы следующие эквивалентности:

$$
\begin{array}{lrcl}
(J1) & \neg X & \equiv & (X+1), \\
(J2) & (X_1 \wedge X_2) & \equiv & (X_1 * X_2), \\
(J3) & (X_1 \vee X_2) & \equiv & (X_1 * X_2 + X_1 + X_2), \\
(J4) & (X_1 + X_2) * (X_3 + X_4) & \equiv & (X_1 * X_2 + X_1 * X_3 + X_2 * X_3 + X_2 *
\end{array}
$$

Из этих эквивалентностей и теоремы 4.1 легко получить первую часть следующего утверждения.

Теорема . Для любой *булевой функции* существует задающий ее *многочлен Жегалкина*. Он единственен с точностью до перестановок слагаемых и порядка переменных в конъюнкциях.

Доказательство Существование такого многочлена следует из того, что для любой *ДНФ* или *КНФ* можно с помощью указанных эквивалентностей найти эквивалентный *многочлен Жегалкина*: (J1)-(J3) позволяют заменять все вхождения $\neg, \wedge$ и $\vee$ на + и *, а (J4) - перемножать получившиеся после такой замены многочлены.

Для доказательства единственности представления подсчитаем число различных *многочленов Жегалкина* от n переменных. Каждая положительная *элементарная конъюнкция* имеет вид $X_{i1} * ... * X_{ik}$, где $1 <= i_1 < ... < i_k <= n$. Таких конъюнкций столько же, сколько подмножеств *множества* $\mathbf{X} = \{X_1, \ldots, X_n\}$, т.е. 2_n . (*Конъюнкция,*

соответствующая пустому подмножеству переменных равна 1). Упорядочим их произвольным образом (например, лексикографически): $K_1, K_2, \ldots, K_{2^n}$. Тогда каждый *многочлен Жегалкина* единственным образом можно представить как сумму

$$\alpha_1 * K_1 + \alpha_2 * K_2 + \ldots + \alpha_{2^n} * K_{2^n},$$

где каждый из коэффициентов α_i равен 0 или 1. Следовательно, число *многочленов Жегалкина* равно 2^{2^n}, т.е. числу всех булевых функций от n переменных. Поэтому каждая *функция* задается в точности одним *многочленом Жегалкина*.

Пример

Пусть *функция* $f(X_1,X_2,X_3)$ задается *ДНФ* $\Phi = (X_1 \wedge \neg X_2) \vee (\neg X_1 \wedge X_2 \wedge \neg X_3)$. Найдем *полином Жегалкина*, который также задает эту функцию.

Сначала заменяем $\wedge$ на *, а затем,применяя *эквивалентность* (J1), устраняем отрицания и получаем:

$$\Phi \equiv X_1 * (X_2 + 1) \vee (X_1 + 1) * X_2 * (X_3 + 1).$$

Перемножив по правилам (J4), получим:

$$\Phi \equiv (X_1*X_2+X_1)\vee(X_1*X_2*X_3+X_1*X_2+X_2*X_3+X_2)$$

Эквивалентность (J3) позволяет устранить $\vee$:

$$\Phi \equiv (X_1 * X_2 + X_1) * (X_1 * X_2 * X_3 + X_1 * X_2 + \\ + X_2 * X_3 + X_2) + (X_1 * X_2 + X_1) + \\ + (X_1 * X_2 * X_3 + X_1 * X_2 + X_2 * X_3 + X_2).$$

Снова, используя (J4), перемножим первые две скобки и устраним повторения переменных в конъюнкциях:

$$\Phi \equiv (X_1 * X_2 * X_3 + X_1 * X_2 + X_1 * X_2 * X_3 + \\ +X_1*X_2*X_3+X_1*X_2+X_1*X_2*X_3+X_1*X_2+X_1*X_2)+ \\ +(X_1*X_2+X_1)+(X_1*X_2*X_3+X_1*X_2+X_2*X_3+X_2).$$

Упростим эту сумму, используя эквивалентности: $X + X \equiv 0$ и $X + 0 \equiv X$. В результате получим *многочлен Жегалкина*

$$P(X_1, X_2, X_3) = X_1 + X_2 + X_2 * X_3 + X_1 * X_2 * X_3$$

эквивалентный исходной *ДНФ* Φ.

Если *функция* $f(X_1, ..., X_n)$ задана таблично, то для построения реализующего ее *многочлена Жегалкина* можно применить метод неопределенных коэфициентов.

Сопоставим i -ому набору значений переменных $\sigma_i = (\sigma_i^1, \ldots, \sigma_i^n)$ в таблице

положительную конъюнкцию $K_i = \bigwedge_{\sigma_i^j=1} X_j$ переменных, равных 1 в этом наборе. В частности, K_1 - пустая *конъюнкция*, $K_2 = X_n$, $K_3 = X_{n-1}$, $K_4 = (X_n * X_{n-1})$. и т.д. Тогда для получения нужного *многочлена Жегалкина* достаточно определить все *коэффициенты* $\alpha_i,\ i = 1, \ldots, 2^n$, в выражении

$$f(X_1, \ldots, X_n) = \alpha_1 * K_1 + \alpha_2 * K_2 + \ldots + \alpha_{2^n} * K_{2^n},$$

Подставляя в это *равенство* значения переменных из набора $\sigma_i,\ i = 1, \ldots, 2^n$, мы получим 2^n *линейных уравнений* относительно 2^n неизвестных коэффициентов α_i. Решив эту систему, получим требуемый *многочлен Жегалкина*. Эта система треугольная и легко решается "сверху-вниз": каждое α_i определяется по значениям $\alpha_1, \ldots, \alpha_{i-1}$ из уравнения, соответствующего набору σ_i.

Пример Рассмотрим в качестве примера функцию $f(X_1, ..., X_n)$, заданную следующей таблицей.

Таблица 4.1. Функция $f(X_1, X_2, X_3)$

X_1	**X_2**	**X_3**	**$f(X_1, X_2, X_3)$**
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1.	1	1

Многочлен Жегалкина для нее (как и для любой функции от 3-х переменных) представляется в виде

$$p(X_1, X_2, X_3) = \alpha_0 + \alpha_1 * X_1 + \alpha_2 * X_2 + \alpha_3 * X_3 + \alpha_{12} * X_1 * X_2 + \\ + \alpha_{13} * X_1 * X_3 + \alpha_{23} * X_2 * X_3 + \alpha_{123} * X_1 * X_2 * X_3$$

В этом представлении в индексах у коэффициентов α перечислены переменные, входящие в соответствующие конъюнкции.

Последовательно подставляя значения переменных и f из таблицы, получаем:

$$p(0,0,0) = \alpha_0 = 1;$$
$$p(0,0,1) = \alpha_0 + \alpha_3 = 0 \Rightarrow \alpha_3 = 1;$$
$$p(0,1,0) = \alpha_0 + \alpha_2 = 0 \Rightarrow \alpha_2 = 1;$$
$$p(0,1,1) = \alpha_0 + \alpha_2 + \alpha_3 + \alpha_{23} = 0 \Rightarrow \alpha_{23} = 1;$$
$$p(1,0,0) = \alpha_0 + \alpha_1 = 1 \Rightarrow \alpha_1 = 0;$$
$$p(1,0,1) = \alpha_0 + \alpha_1 + \alpha_3 + \alpha_{13} = 0 \Rightarrow \alpha_{13} = 0;$$
$$p(1,1,0) = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_{12} = 0 \Rightarrow \alpha_{12} = 0;$$
$$p(1,1,1) = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_{12} + \alpha_{13} + \alpha_{23} + \alpha_{123} = 1 \Rightarrow \alpha_{123} = 1$$

Следовательно, *функция* f(X_1, X_2, X_3) представляется *многочленом Жегалкина*

$$p_f(X_1, X_2, X_3) = 1 + X_3 + X_2 + X_2 * X_3 + X_1 * X_2 * X_3.$$

Задачи

Задача 1. Проверьте все приведенные в "лекции 4" эквивалентности (1) - (8), непосредственно вычисляя функции, представляемые их левыми и правыми частями.

Задача 2. Назовем **логическим произведением** формулу вида $\Phi_1 \wedge \Phi_2 \wedge \ldots \wedge \Phi_n$ (в этом выражении использованы соглашения о сокращении записи!). Ее *подформулы* $\Phi_i, 1 \leq i \leq n$, , будем называть **сомножителями**. Аналогично, **логической суммой** назовем формулу вида $\Phi_1 \vee \Phi_2 \vee \ldots \vee \Phi_n$. Ее *подформулы* $\Phi_i, 1 \leq i \leq n$,, будем называть **слагаемыми**.

Покажите, что из *основных тождеств* можно вывести следующие правила преобразования логических произведений и сумм.

1. Если в логическом произведении один из сомножителей равен 0, то и все произведение равно 0.
2. Если в логической сумме одно из слагаемых равно 1, то и вся сумма равна 1.
3. Если в логическом произведении n >= 2 и есть сомножитель, равный 1, то его можно вычеркнуть.
4. Если в логической сумме n >= 2 и есть слагаемое, равное 0, то его можно вычеркнуть.