Лекция 3. Полином Жегалкина. Способы построения полинома Жегалкина функции. Линейная имплицента функции. Линейная конъюнктивная нормальная форма (ЛКНФ). Линейная соимплицента функции. Поиск всех линейных соимплицент функции.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Монотонная ЭК

ЭК, в которой не встречаются отрицания переменных, назовем **монотонной** ЭК, или **мономом** (или **одночленом**).

Т. е. **монотонная** ЭК — выражение (формула) вида

$$x_{i_1} \cdot \ldots \cdot x_{i_r},$$

где $x_{i_1}, \ldots, x_{i_r}$ — различные переменные, или константа 1.

Например, x_1, $x_1 x_3 x_4$, 1 — монотонные ЭК.

Полином Жегалкина

Полиномом (или **многочленом**) **Жегалкина** длины l, $l \geqslant 1$, называется сумма по модую два различных монотонных ЭК.

Полиномом Жегалкина длины 0 назовем константу 0.

Т. е. **полином Жегалкина** — выражение (формула) вида

$$K_1 \oplus \ldots \oplus K_l,$$

где $K_1, \ldots, K_l$ — различные монотонные ЭК, или константа 0.

Считаем, что два полинома Жегалкина совпадают, если они отличаются только порядком входящих в него ЭК.

Приведение к полиному Жегалкина

Отметим, что любую сумму по модулю два монотонных ЭК с коэффициентами из E_2 при помощи тождеств алгебры логики можно привести к какому-то полиному Жегалкина.

Примем, что любая сумма по модулю два монотонных ЭК с коэффициентами из E_2 всегда приведена к соответствующему полиному Жегалкина.

Представление функций полиномами Жегалкина

Каждый полином Жегалкина определяет какую-то функцию $f \in P_2$.

Каждая функция $f \in P_2$ может быть представлена **однозначным** полиномом Жегалкина P_f.

Критерий существенности переменной

Утверждение 1. *Переменная* x_i, $1 \leqslant i \leqslant n$, *встречается в полиноме Жегалкина* P_f *функции* $f \in P_2^{(n)}$ *тогда и только тогда, когда* x_i *является существенной переменной функции* f.

Доказательство.

1. Если переменная x_i не встречается в полиноме Жегалкина P_f, то x_i не может быть существенной переменной функции f.

Критерий существенности переменной

2. Пусть переменная x_i встречается в полиноме Жегалкина P_f. Не ограничивая общности рассуждений, пусть $i = 1$. Тогда

$$P_f = x_1 \cdot P_g \oplus P_h$$

для некоторых $g(x_2, \ldots, x_n), h(x_2, \ldots, x_n) \in P_2$, причем $g \neq 0$.

Значит, найдется такой набор $\alpha \in E_2^{n-1}$, что $g(\alpha) = 1$.

Критерий существенности переменной

Итак,

$$P_f = x_1 \cdot P_g \oplus P_h, \quad g(\alpha) = 1, \alpha \in E_2^{n-1}.$$

Рассмотрим следующие наборы $\beta = (0, \alpha) \in E_2^n$ и $\gamma = (1, \alpha) \in E_2^n$, соседние по 1-й переменной:

$$\begin{array}{rcccccc} & & 1 & 2 & \dots & n & \\ \beta & = & (& 0 & \alpha_1 & \dots & \alpha_{n-1} &), \\ \gamma & = & (& 1 & \alpha_1 & \dots & \alpha_{n-1} &). \end{array}$$

Тогда

$$\begin{aligned} f(\beta) &= h(\alpha), \\ f(\gamma) &= g(\alpha) \oplus h(\alpha) = 1 \oplus h(\alpha). \end{aligned}$$

Т. е. $f(\beta) \neq f(\gamma)$, что доказывает существенность переменной x_1 для функции f.

□

Мономы над $x_1, \ldots, x_n$

Если $f \in P_2^{(n)}$, то ее полином Жегалкина P_f однозначно определяется своими коэффициентами при всех возможных монотонных ЭК над переменными $x_1, \ldots, x_n$.

Мономы над $x_1, \ldots, x_n$

Если $\alpha \in E_2^n$, то положим

$$x^\alpha = \begin{cases} \prod\limits_{\alpha_i=1} x_i, & \alpha \neq (0, \ldots, 0), \\ 1, & \alpha = (0, \ldots, 0). \end{cases}$$

Как правило, мы будем рассматривать мономы над переменными $x_1, \ldots, x_n$.

Иногда будет удобно под x^α, где $\alpha \in E_2^n$, понимать моном над некоторым другим заданным множеством n переменных.

Каждый раз будет ясно над каким множеством переменных рассматриваются мономы.

Мономы над $x_1, \ldots, x_n$

Если α пробегает по всем возможным наборам из E_2^n, то x^α соответствуют всем возможным мономам над $x_1, \ldots, x_n$.

Например, если $n = 2$, $\alpha \in E_2^2$ и рассматриваем переменные x_1, x_2, то

$$x^\alpha = \begin{cases} 1, & \alpha = (0,0), \\ x_2, & \alpha = (0,1), \\ x_1, & \alpha = (1,0), \\ x_1 x_2, & \alpha = (1,1). \end{cases}$$

Коэффициенты полинома Жегалкина

Пусть $c_f(\alpha)$, $\alpha \in E_2^n$, обозначает **коэффициент** при мономе x^α в полиноме Жегалкина P_f функции $f \in P_2^{(n)}$.

Если $f(x_1, \ldots, x_n) \in P_2$, то

$$P_f = \bigoplus_{\alpha \in E_2^n} c_f(\alpha) \cdot x^\alpha.$$

Поэтому для построения полинома Жегалкина P_f функции f достаточно найти все коэффициенты $c_f(\alpha)$, $\alpha \in E_2^n$.

Функции одной переменной

Если $f(x) \in P_2^{(1)}$, то

$$\begin{aligned} f(x) &= \bar{x} \cdot f(0) \oplus x \cdot f(1) = (x \oplus 1) \cdot f(0) \oplus x \cdot f(1) = \\ &= x \cdot (f(0) \oplus f(1)) \oplus f(0). \end{aligned}$$

Поэтому

$$\begin{aligned} c_f(0) &= f(0), \\ c_f(1) &= f(0) \oplus f(1). \end{aligned}$$

Подфункции

Если $f(x_1, \ldots, x_n) \in P_2^{(n)}$ и $\sigma \in E_2^k$, $0 \leqslant k \leqslant n$, то положим

$$f_\sigma(x_{k+1}, \ldots, x_n) = \begin{cases} f(x_1, \ldots, x_n), & k = 0, \\ f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n), & 1 \leqslant k \leqslant n. \end{cases}$$

Функция f_σ, $\sigma \in E_2^k$, называется σ-**подфункцией** функции f по k первым переменным.

При этом функции f_0 и f_1 соответственно называются 0-**подфункцией** и 1-**подфункцией** функции f по первой переменной.

Вычисление коэффициентов

Теорема 1. *Если* $n \geqslant 1$, $f(y, x_1, \ldots, x_n) \in P_2^{(n+1)}$, *то для каждого* $\alpha \in E_2^n$ *верны равенства:*

$$c_f(0, \alpha) = c_{f_0}(\alpha),$$
$$c_f(1, \alpha) = c_{f_0}(\alpha) \oplus c_{f_1}(\alpha).$$

Вычисление коэффициентов

Доказательство. Представим функцию $f(y, x_1, \ldots, x_n) \in P_2^{(n+1)}$ в следующем виде:

$$\begin{aligned} f(y, x_1, \ldots, x_n) &= \bar{y} \cdot f(0, x_1, \ldots, x_n) \oplus y \cdot f(1, x_1, \ldots, x_n) = \\ &= (y \oplus 1) \cdot f_0 \oplus y \cdot f_1 = y \cdot (f_0 \oplus f_1) \oplus f_0. \end{aligned}$$

Значит,

$$P_f = y \cdot P_{f_0 \oplus f_1} \oplus P_{f_0},$$

откуда следуют указанные в теореме равенства.

□

Построение полинома Жегалкина

Из теоремы 1 извлекаем следующий способ построения полинома Жегалкина функции $f \in P_2$ по вектору ее значений.

Построение полинома Жегалкина по вектору значений

Алгоритм 3. *Построение полинома Жегалкина функции $f \in P_2$ по вектору значений.*

Вход: вектор значений α_f функции $f \in P_2^{(n)}$, $n \geqslant 1$.

Выход: полином Жегалкина P_f функции f.

Построение полинома Жегалкина по вектору значений

Алгоритм 3.

1.1. Для каждого $\beta \in E_2^{n-1}$ выполнить

$$c_{f_\beta}(0) := f_\beta(0),$$
$$c_{f_\beta}(1) := f_\beta(0) \oplus f_\beta(1).$$

1.i, $i = 2, \ldots, n$. Для каждого $\beta \in E_2^{n-i}$ и каждого $\alpha \in E_2^{i-1}$ выполнить

$$c_{f_\beta}(0, \alpha) := c_{f_{(0,\beta)}}(\alpha),$$
$$c_{f_\beta}(1, \alpha) := c_{f_{(0,\beta)}}(\alpha) \oplus c_{f_{(1,\beta)}}(\alpha).$$

2. $P_f := \bigoplus_{\alpha \in E_2^n : c_f(\alpha) \neq 0} x^\alpha$.

Построение полинома Жегалкина по вектору значений

Пример. Построим по алгоритму 3 полином Жегалкина P_f функции $f(x_1, x_2, x_3) \in P_2$ по ее вектору значений $\alpha_f = (0110\ 1001)$:

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Построение полинома Жегалкина по вектору значений

1.1.

x_1	x_2	x_3	f	1
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	0	1
1	0	0	1	1
1	0	1	0	1
1	1	0	0	0
1	1	1	1	1

Построение полинома Жегалкина по вектору значений

1.2.

x_1	x_2	x_3	f	1	2
0	0	0	0	0	0
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	0	1	0
1	0	0	1	1	1
1	0	1	0	1	1
1	1	0	0	0	1
1	1	1	1	1	0

Построение полинома Жегалкина по вектору значений

1.3.

x_1	x_2	x_3	f	1	2	3
0	0	0	0	0	0	0
0	0	1	1	1	1	1
0	1	0	1	1	1	1
0	1	1	0	1	0	0
1	0	0	1	1	1	1
1	0	1	0	1	1	0
1	1	0	0	0	1	0
1	1	1	1	1	0	0

2.

$$P_f = x_3 \oplus x_2 \oplus x_1.$$

Линейная форма

Выражение (формула) вида

$$x_{i_1} \oplus \ldots \oplus x_{i_r} \oplus c_0,$$

где $x_{i_1}, \ldots, x_{i_r}$ — различные переменные, $c_0 \in E_2$ — свободный член, называется **линейной формой** (ЛФ) ранга r, $r \geqslant 1$.

Линейными формами ранга 0 назовем константы 0 и 1.

При этом константу 0 будем также называть нулевой ЛФ.

Считаем, что две ЛФ совпадают, если они отличаются только порядком входящих в них переменных.

Приведение к ЛФ

Отметим, что любую сумму по модулю два переменных с коэффициентами из E_2 или констант при помощи тождеств алгебры логики можно привести к некоторой ЛФ.

Примем, что любая сумма по модулю два переменных с коэффициентами из E_2 или констант всегда приведена к соответствующей ЛФ.

ЛКНФ

Линейной конъюнктивной нормальной формой (ЛКНФ) длины l, $l \geqslant 1$, назовем конъюнкцию l различных ЛФ.

Считаем, что в любой ЛКНФ выполнены все поглощения, а именно:

1) если ЛКНФ содержит нулевую ЛФ 0, то никаких других ЛФ она не содержит;

2) если ЛКНФ содержит ЛФ 1 и еще какие-то ЛФ, то ЛФ 1 из нее убираем.

Считаем, что две ЛКНФ совпадают, если они отличаются только порядком входящих в них ЛФ.

Приведение к ЛКНФ

Отметим, что любую конъюнкцию ЛФ или констант при помощи тождеств алгебры логики можно привести к некоторой ЛКНФ.

Представимость ЛКНФ

Каждая ЛКНФ над переменными $x_1, \ldots, x_n$ определяет какую-то функцию $f(x_1, \ldots, x_n) \in P_2^{(n)}$.

Обратное в общем случае неверно. Существуют такие функции алгебры логики, которые не представимы никакой ЛКНФ.

Линейная имплицента функции

Линейной имплицентой функции $f \in P_2$ называется такая ЛФ L, что $N_0(L) \subseteq N_0(f)$.

Отметим, что ЛФ L является линейной имплицентой функции $f \in P_2^{(n)}$, если для любого набора $\alpha \in E_2^n$ из $L(\alpha) = 0$ следует $f(\alpha) = 0$.

Если L — линейная имплицента функции $f \in P_2$, то ЛФ $\bar{L} = L \oplus 1$ называется **линейной соимплицентой** функции f.

Конъюнкция всех линейных имплицент функции

Утверждение 2. *Конъюнкция L_f всех линейных имплицент функции $f \in P_2$ является ЛКНФ, представляющей эту функцию f, тогда и только тогда, когда функция f представима ЛКНФ*.

Конъюнкция всех линейных имплицент функции

Доказательство.
1. Пусть $f \in P_2^{(n)}$ **представима ЛКНФ** и $\alpha \in E_2^n$.

1.1. Если $f(\alpha) = 0$, то, т. к. функция f **представима ЛКНФ**, найдется какая-то линейная имплицента L функции f, что $L(\alpha) = 0$.

Но L_f содержит **все** линейные имплиценты функции f, поэтому L входит в L_f. Значит, $L_f(\alpha) = 0$.

1.2. Если же $f(\alpha) = 1$, то ни одна линейная имплицента функции f не может принимать на наборе α нулевое значение по определению линейной имплиценты функции. Поэтому $L_f(\alpha) = 1$.

Конъюнкция всех линейных имплицент функции

Доказательство.

2. Если $f \in P_2$ **не представима ЛКНФ**, то конъюнкция всех ее линейных имплицент не может представлять эту функцию f, т. к. сразу появляется противоречие.

□

Сокращенная ЛКНФ

Если функция $f \in P_2$ представима ЛКНФ, то конъюнкцию L_f всех линейных имплицент функции f назовем ее **сокращенной** ЛКНФ.

По определению для каждой функции $f \in P_2$, представимой ЛКНФ, ее сокращенная ЛКНФ L_f единственна.

Линейная независимость ЛФ

Линейные формы $L_1, \ldots, L_m$, где $m \geqslant 1$, называются **линейно независимыми**, если из

$$c_1 \cdot L_1 \oplus \ldots \oplus c_m \cdot L_m = 0,$$

где $c_1, \ldots, c_m \in E_2$, следует

$$c_1 = \ldots = c_m = 0.$$

В обратном случае линейные формы $L_1, \ldots, L_m$ называются **линейно зависимыми**.

Линейная соимплицента функции

Линейной соимплицентой функции $f \in P_2$ называется такая ЛФ L, что $N_1(L) \subseteq N_0(f)$.

Отметим, что ЛФ L является линейной соимплицентой функции $f \in P_2^{(n)}$, если для любого набора $\alpha \in E_2^n$ из $L(\alpha) = 1$ следует $f(\alpha) = 0$, или, что то же самое,

$$L \cdot f = 0.$$

Линейное пространство линейных соимплицент

Пусть $f \in P_2$ и $L(f)$ — множество всех **линейных соимплицент** функции f.

Ясно, что $0 \in L(f)$.

Множество $L(f)$ является **линейным пространством** над полем F_2 вычетов по модулю два.

Действительно, если $L_1, L_2 \in L(f)$ и $c_1, c_2 \in E_2$, то

$$(c_1 \cdot L_1 \oplus c_2 \cdot L_2) \cdot f = c_1 \cdot L_1 \cdot f \oplus c_2 \cdot L_2 \cdot f = 0.$$

Поэтому

$$L = c_1 \cdot L_1 \oplus c_2 \cdot L_2 \in L(f).$$

Базис пространства линейных соимплицент

Выделим **базис** $L_1, \ldots, L_k$ линейного пространства $L(f)$, т. е. максимальное (по включению) множество линейно независимых ЛФ из $L(f)$.

Примем, что если $L(f) = \{0\}$, то константа 0 является (вырожденным) базисом этого линейного пространства $L(f)$.

ЛКНФ функции

Утверждение 3. *Пусть $L_1, \ldots, L_k$ — базис линейного пространства $L(f)$ функции $f \in P_2$. Если функция f представима ЛКНФ, то конъюнкция*

$$L_f = (L_1 \oplus 1) \cdot \ldots \cdot (L_k \oplus 1)$$

является ЛКНФ, представляющей эту функцию f.

ЛКНФ функции

Доказательство.
Пусть $f \in P_2^{(n)}$ *представима ЛКНФ* и $\alpha \in E_2^n$.

1. Если $f(\alpha) = 0$, то, т. к. функция f *представима ЛКНФ*, найдется такая линейная имплицента L функции f, что $L(\alpha) = 0$.

Значит, для линейной соимплиценты $L_0 = \bar{L} = L \oplus 1$ функции f верно $L_0(\alpha) = 1$.

Кроме того, для некоторых $c_1, \ldots, c_k \in E_2$ верно:

$$L_0 = c_1 L_1 \oplus \ldots \oplus c_k L_k.$$

Предположим, что $L_f(\alpha) = 1$, т. е. $L_1(\alpha) = \ldots = L_k(\alpha) = 0$.

Но тогда $L_0(\alpha) = c_1 L_1(\alpha) \oplus \ldots \oplus c_k L_k(\alpha) = 0$ — противоречие.

Значит, $L_f(\alpha) = 0$.

ЛКНФ функции

2. Если же $f(\alpha) = 1$, то ни одна линейная имплицента функции f не может принимать на наборе α нулевое значение по определению линейной имплиценты функции.

Поэтому $L_f(\alpha) = 1$.

□

Кратчайшая ЛКНФ

Если функция $f \in P_2$ представима ЛКНФ, то конъюнкцию

$$L_f = (L_1 \oplus 1) \cdot \ldots \cdot (L_k \oplus 1),$$

где $L_1, \ldots, L_k$ — какой-то базис линейного пространства $L(f)$, назовем **кратчайшей** ЛКНФ функции f.

Поиск линейных соимплицент функции

Алгоритм 4. *Поиск всех линейных соимплицент функции $f \in P_2$ по полиному Жегалкина*.

Вход: полином Жегалкина $P_f = K_1 \oplus \ldots \oplus K_l$ функции $f \in P_2^{(n)}$.

Выход: линейные соимплиценты $L_1, \ldots, L_k$ функции f, образующие какой-то базис пространства $L(f)$.

Поиск линейных соимплицент функции

Алгоритм 4.

1. Рассмотреть уравнение:

$$(c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n)(K_1 \oplus \ldots \oplus K_l) = 0,$$

где $c_0, c_1, \ldots, c_n$ — неизвестные.

2. Перемножив скобки слева и приравняв коэффициенты слева и справа при каждом из мономов K_j, $x_i \cdot K_j$, $i = 1, \ldots, n$, $j = 1, \ldots, l$, получить систему из не более $(n+1) \cdot l$ линейных уравнений с $(n+1)$ неизвестными $c_0, c_1, \ldots, c_n$.

3. Решить полученную систему линейных уравнений в поле вычетов по модулю 2.

4. Если $c_0 = a_0$, $c_1 = a_1$, ..., $c_n = a_n$, где $a_0, a_1, \ldots, a_n \in E_2$, — одно из базисных решений системы, то $L = a_1 x_1 \oplus \ldots \oplus a_n x_n \oplus a_0$ — линейная соимплицента функции f.

Сложность алгоритма

Правильность алгоритма 4 следует из следующего свойства: ЛФ L является линейной соимплицентой функции $f \in P_2$ тогда и только тогда, когда $L \cdot f = 0$.

Отметим, что если решать систему линейных уравнений полиномиальным алгоритмом, например, методои исключения неизвестных, то алгоритм 4 имеет **полиномиальную** сложность относительно $N = n \cdot l$, где n — число переменных функции $f \in P_2$, а l — длина полинома Жегалкина P_f.

Поиск линейных соимплицент функции

Пример. Найдем по алгоритму 4 какой-то базис пространства $L(f)$ для функции $f \in P_2$ по ее полиному Жегалкина

$$P_f = x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3.$$

Поиск линейных соимплицент функции

1. Получаем уравнение:

$$(c_0 \oplus c_1 x_1 \oplus c_2 x_2 \oplus c_3 x_3)(x_1 \oplus x_1 x_2 \oplus x_2 x_3 \oplus x_1 x_2 x_3) = 0.$$

2. Находим систему:

$$\begin{array}{lrcl}
x_1: & c_0 \oplus c_1 & = & 0, \\
x_1 x_2: & c_0 \oplus c_1 & = & 0, \\
x_2 x_3: & c_0 \oplus c_2 \oplus c_3 & = & 0, \\
x_1 x_2 x_3: & c_0 \oplus c_2 & = & 0, \\
x_1 x_3: & c_3 & = & 0.
\end{array}$$

Поиск линейных соимплицент функции

3. Решаем систему:

$$\begin{cases} c_0 \oplus c_1 = 0, \\ c_0 \oplus c_2 \oplus c_3 = 0, \\ c_0 \oplus c_2 = 0, \\ c_3 = 0, \end{cases} \quad \begin{cases} c_0 \oplus c_1 = 0, \\ c_0 \oplus c_2 = 0, \\ c_3 = 0. \end{cases}$$

Получаем:

$$\begin{aligned} c_0 &\in E_2, \\ c_1 &= c_0, \\ c_2 &= c_0, \\ c_3 &= 0. \end{aligned}$$

4. Значит, $L_1 = x_1 \oplus x_2 \oplus 1$ образует **базис** пространства $L(f)$.

Поиск линейных соимплицент функции

Итак, для функции $f \in P_2$,

$$P_f = x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3,$$

найдена линейная соимплицента $L_1 = x_1 \oplus x_2 \oplus 1$, образующая базис пространства $L(f)$.

Несложно увидеть, что функция f не задается ЛКНФ $L_f = x_1 \oplus x_2$, поэтому по утверждению 3 функция f не представима ЛКНФ.

Поиск линейных соимплицент функции

Пример. По алгоритму 4 найдем какой-то базис пространства $L(f)$ для функции $f \in P_2$, где

$$P_f = x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3.$$

Поиск линейных соимплицент функции

Применим алгоритм 4 к функции f.

1. Получаем уравнение:

$$(c_0 \oplus c_1x_1 \oplus c_2x_2 \oplus c_3x_3)(x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3) = 0.$$

2. Находим систему:

$$\begin{array}{lrcl}
x_1: & c_0 \oplus c_1 & = & 0,\\
x_1x_2: & c_0 \oplus c_1 & = & 0,\\
x_1x_3: & c_0 \oplus c_1 & = & 0,\\
x_2x_3: & c_0 \oplus c_2 \oplus c_3 & = & 0,\\
x_1x_2x_3: & c_1 \oplus c_2 \oplus c_3 & = & 0.
\end{array}$$

Поиск линейных соимплицент функции

3. Решаем систему:

$$\begin{cases} c_0 \oplus c_1 = 0, \\ c_0 \oplus c_2 \oplus c_3 = 0, \\ c_1 \oplus c_2 \oplus c_3 = 0, \end{cases} \quad \begin{cases} c_1 = c_0, \\ c_2 = c_0 \oplus c_3. \end{cases}$$

Получаем:

$$\begin{aligned} c_0 &\in E_2, \\ c_1 &= c_0, \\ c_2 &= c_0 \oplus c_3, \\ c_3 &\in E_2. \end{aligned}$$

Поиск линейных соимплицент функции

Итак,

$$\begin{aligned} c_0 &\in E_2, \\ c_1 &= c_0, \\ c_2 &= c_0 \oplus c_3, \\ c_3 &\in E_2. \end{aligned}$$

4.

c_0	c_1	c_2	c_3
0	0	1	1
1	1	1	0

Значит, ЛФ $L_1 = x_1 \oplus x_2 \oplus 1$, $L_2 = x_2 \oplus x_3$ образуют какой-то **базис** пространства $L(f)$.

Поиск линейных соимплицент функции

Итак, для функции $f \in P_2$,

$$P_f = x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3,$$

найдены линейные соимплиценты $L_1 = x_1 \oplus x_2 \oplus 1$, $L_2 = x_2 \oplus x_3$, образующие *базис* пространства $L(f)$.

Можно проверить, что функция f задается ЛКНФ

$$L_f = (L_1 \oplus 1)(L_2 \oplus 1) = (x_1 \oplus x_2)(x_2 \oplus x_3 \oplus 1),$$

поэтому функция f представима ЛКНФ.

Конец лекции