Лекция 5. Покрытие множества и покрытие матрицы. Градиентное покрытие. Лемма о градиентном покрытии. Оценки мощности затеняющего множества булева куба. Оценки длины полиномиальных нормальных форм булевых функций.

Лектор - доцент Селезнева Светлана Николаевна

Лекции по “Избранным вопросам дискретной математики”.
3-й курс, группа 318,
факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mathcyb.cs.msu.su

Покрытие множества

Покрытием множества A называется такое семейство непустых его подмножеств $A_1, \ldots, A_k$, что

$$\bigcup_{i=1}^{k} A_i = A.$$

Другими словами, если $A_1, \ldots, A_k$ – покрытие множества A, то **любой** элемент $a \in A$ лежит **хотя бы в одном** из множеств $A_1, \ldots, A_k$.

В отличие от разбиения в покрытии **не требуется**, чтобы множества $A_1, \ldots, A_k$ не пересекались.

Покрытие матрицы

Мы будем рассматривать матрицы из нулей единиц, не содержащие нулевых столбцов.

Покрытием матрицы M размера $m \times n$ называется такое такое подмножество ее строк $i_1, \ldots, i_k$, что для каждого j, $j = 1, \ldots, n$, найдется такой номер $s = s(j)$, $1 \leq s(j) \leq k$, что $m_{s(j),j} = 1$.

Другими словами, подмножество строк $i_1, \ldots, i_k$ матрицы M является ее **покрытием**, если в подматрице, образованной этими строками **нет нулевых столбцов**.

Покрытие матрицы также называется *покрытием столбцов матрицы ее строками*.

Пример покрытия матрицы

Пример 1. Пусть

$$M = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Тогда 1-я и 2-я строки не покрывают матрицу M:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix};$$

а 1-я и 3-я строки – являются покрытием матрицы M:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Кратчайшее покрытие матрицы

Число строк в покрытии матрицы называется его **мощностью**.

Понятно, что для матрицы M (без нулевых столбцов) размера $m \times n$ всегда надется покрытие мощности m (почему?).

Кратчайшим покрытием матрицы M называется ее покрытие минимальной мощности.

Градиентное покрытие матрицы

Градиентным покрытием матрицы M называется ее покрытие $i_1, \ldots, i_k$, полученное при помощи следующей пошаговой процедуры:

Шаг 1. В матрице M выбирается строка i_1, содержащая **максимальное** число единиц; из матрицы M вычеркивается эта строка и все столбцы, на пересечении которых со строкой i_1 стоят единицы; получается матрица M_1.

Шаг $(s+1)$. Пусть уже проделано s шагов, и получена матрица M_s. В матрице M_s выбирается строка i_{s+1}, содержащая **максимальное** число единиц; из матрицы M_s вычеркивается эта строка и все столбцы, на пересечении которых со строкой i_{s+1} стоят единицы; получается матрица M_{s+1}.

Процедура заканчивается, если матрица M_s не содержит единиц.

Пример градиентного покрытия матрицы

Пример 2. Рассмотрим матрицу (слева указаны номера строк):

$$M = \left(\begin{array}{c|cccc} 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 & 1 \\ 3 & 1 & 0 & 0 & 1 \\ 4 & 1 & 1 & 0 & 0 \end{array}\right).$$

На первом шаге выберем строку 1, получим матрицу M_1:

$$M_1 = \left(\begin{array}{c|cc} 2 & 0 & 1 \\ 3 & 1 & 1 \\ 4 & 1 & 0 \end{array}\right);$$

а на втором шаге выберем строку 3, получим матрицу $M_2 = \emptyset$.

Градиентное покрытие – 1-я и 3-я строки.

Пример градиентного покрытия матрицы

Пример 2 (продолжение). Для этой же матрицы M мы могли по-другому строить градиентное покрытие:

$$M = \left(\begin{array}{c|cccc} 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 & 1 \\ 3 & 1 & 0 & 0 & 1 \\ 4 & 1 & 1 & 0 & 0 \end{array}\right).$$

На первом шаге выберем строку 2, получим матрицу M'_1:

$$M'_1 = \left(\begin{array}{c|cc} 1 & 0 & 1 \\ 3 & 1 & 0 \\ 4 & 1 & 1 \end{array}\right);$$

тогда на втором шаге надо выбрать строку 4, получим матрицу $M'_2 = \emptyset$.

Градиентное покрытие – 2-я и 4-я строки.

Неоднозначность градиентного покрытия матрицы

Пример 2 показывает, что градиентное покрытие матрицы, вообще говоря, **не является однозначно определенным**.

Это происходит потому, что на каждом шаге градиентной процедуры выбор строки с максимальным числом единиц может быть неоднозначным.

Соотношение между градиентным и кратчайшим покрытиями матрицы

Для матрицы из примера 2 градиентная процедура всегда строит ее кратчайшее покрытие (проверьте, что это действительно так!).

Однако в общем случае градиентное покрытие **не является кратчайшим**.

Градиентное покрытие матрицы не обязательно кратчайшее

Пример 3. Рассмотрим матрицу (слева указаны номера строк):

$$M = \left(\begin{array}{c|cccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right).$$

Тогда на первом шаге мы обязаны выбрать строку 1, получим матрицу M_1:

$$M_1 = \left(\begin{array}{c|ccc} 2 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{array}\right);$$

из которой мы последовательно обязаны выбрать строки 2, 3, и 4, и получить градиентное покрытие из всех строк матрицы M.

А кратчайшее покрытие матрицы M – 2-я, 3-я и 4-я строки.

Мощность градиентного покрытия матрицы

Мощностью градиентного покрытия матрицы M будем называть **максимальную** мощность ее покрытия, полученного при помощи градиентной процедуры.

В следующей лемме доказывается верхняя оценка мощности градиентного покрытия.

Лемма о градиентном покрытии

Лемма 1 (о градиентном покрытии). *Пусть M – матрица из нулей и единиц (без нулевых столбцов) размера $p \times q$, причем в каждом ее столбце находится не менее t единиц. Тогда для любого градиентного покрытия Γ этой матрицы верна оценка:*

$$|\Gamma| \leq 1 + \frac{p}{t} \ln \left(e \cdot \frac{qt}{p} \right),$$

где $e = 2,71\ldots$ – основание натурального логарифма.

Доказательство. Пусть δ_s – доля столбцов матрицы M, не покрытых после шага s. По определению $\delta_0 = 1$.

Лемма о градиентном покрытии

Доказательство (продолжение). Посмотрим как меняется значение δ_{s+1} по сравнению со значением δ_s.

В матрице M_s всего $\delta_s \cdot q$ столбцов, в каждом из которых не менее t единиц.

Поэтому в матрице M_s есть не менее $\delta_s \cdot q \cdot t$ единиц.

В матрице M_s всего $(p - s)$ строк.

Следовательно, в ней найдется строка, в которой не менее $\frac{\delta_s \cdot q \cdot t}{p-s}$ единиц.

Значит, в матрице M_{s+1} будет не более $\delta_s \cdot q - \frac{\delta_s \cdot q \cdot t}{p-s}$ столбцов.

Откуда в матрице M_{s+1} не более $\delta_s \cdot q \left(1 - \frac{t}{p}\right)$ столбцов.

Получаем:

$$\delta_{s+1} \leq \delta_s \cdot \left(1 - \frac{t}{p}\right).$$

Лемма о градиентном покрытии

Доказательство (продолжение). Из неравенства $\delta_{s+1} \leq \delta_s \cdot \left(1 - \frac{t}{p}\right)$ с учетом $\delta_0 = 1$ получаем:

$$\delta_s \leq \left(1 - \frac{t}{p}\right)^s.$$

Т.к. после шага s остается матрица с $\delta_s \cdot q$ столбцами, для любого градиентного покрытия Γ верна оценка:

$$|\Gamma| \leq s + \delta_s \cdot q.$$

Воспользовавшись неравенством $(1-\alpha)^s \leq e^{-\alpha s}$ при $|\alpha| < 1$ и полагая

$$s = \lceil \frac{p}{t} \ln\left(\frac{qt}{p}\right) \rceil,$$

получаем оценку из утверждения леммы.

Лемма о градиентном покрытии

Доказательство (продолжение). Действительно,

$$|\Gamma| \leq s + q \cdot e^{-\frac{t}{p}s} \leq \left\lceil \frac{p}{t} \ln\left(\frac{qt}{p}\right) \right\rceil + qe^{-\frac{t}{p}\left\lceil \frac{p}{t} \ln\left(\frac{qt}{p}\right) \right\rceil} \leq$$

$$\leq 1 + \frac{p}{t} \ln\left(\frac{qt}{p}\right) + qe^{-\ln\left(\frac{qt}{p}\right)} \leq 1 + \frac{p}{t} \ln\left(e \cdot \frac{qt}{p}\right).$$

□

Применение леммы о градиентном покрытии

При помощи леммы о градиентном покрытии мы можем получать оценки мощности покрытий множеств.

Мы рассмотрим применение этой леммы к решению двух задач: о покрытии куба B^n тенями и о длине полиномиальных нормальных форм булевых функций.

Тень набора

Тенью набора $\alpha \in B^n$ называется множество

$$S(\alpha) = \{\beta \in B^n \mid |\beta| = |\alpha| - 1, \beta < \alpha\}.$$

Т.е. тень набора, это множество наборов **непосредственно предшествующих** этому набору.

Например, $S(0,1,0,1) = \{(0,0,0,1),(0,1,0,0)\}$.

Заметим, что если $\alpha \in B_k^n$, то $S(\alpha) \subseteq B_{k-1}^n$.

Отметим, что в тени набора веса k лежит **ровно** k наборов.

Затеняющее множество булева куба

Тенью множества наборов $A \subseteq B^n$ называется множество

$$S(A) = \bigcup_{\alpha \in A} S(\alpha).$$

Множество наборов T, $T \subseteq B^n$ называется **затеняющим** множеством (куба B^n), если

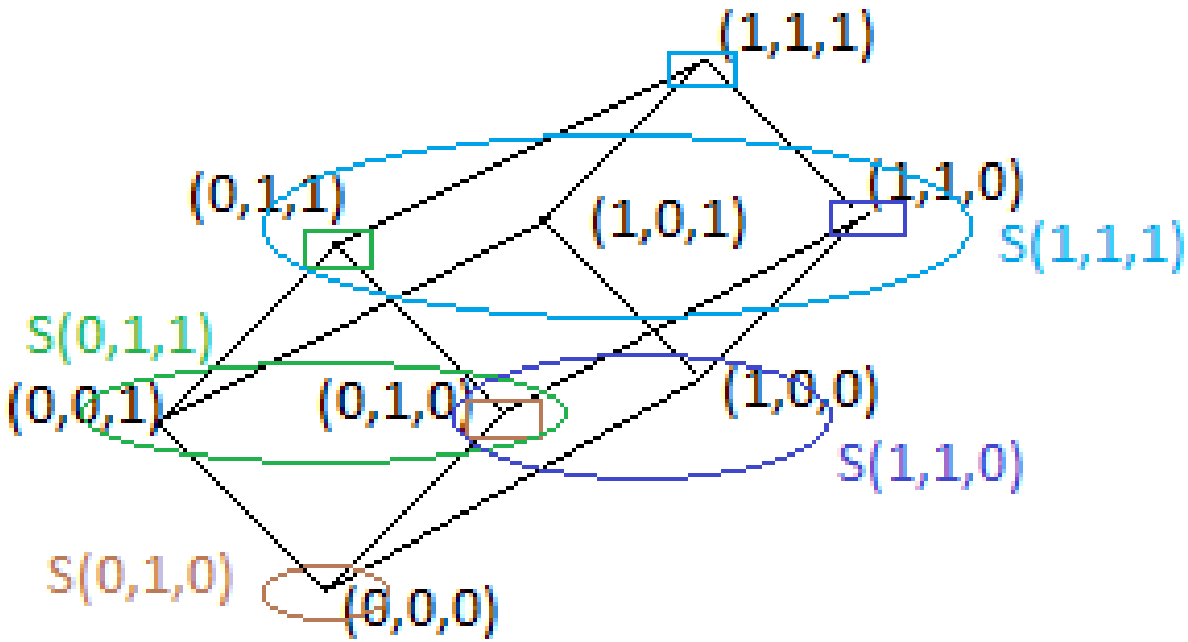
$$S(T) = B^n \setminus \{(1, \ldots, 1)\}.$$

Т.е. затеняющее множество **покрывает тенями** все наборы куба B^n, кроме единичного набора.

(Понятно, что единичный набор не лежит в тени никакого набора.)

Затеняющее множество куба B^3

Затеняющее множество $T = \{(1,1,1),(1,1,0),(0,1,1),(0,1,0)\}$.



Минимальное затеняющее множество куба B^n

Понятно, что сам куб B^n является затеняющим множеством куба B^n.

Кратчайшим затеняющим множеством куба B^n называется его затеняющее множество с минимальной мощностью.

Мы оценим мощность кратчайшего затеняющего множества куба B^n.

Лемма о мощности затеняющего множества слоя куба

Лемма 2 (о мощности затеняющего множества слоя куба). *Пусть $n \geq 1$, $0 \leq k \leq n-1$. Можно построить такое множество T_k^n, $T_k^n \subseteq B_{k+1}^n$, $S(T_k^n) = B_k^n$, для мощности которого верно двойное неравенство:*

$$\frac{C_n^k}{k+1} \leq |T_k^n| \leq 1 + \frac{C_n^{k+1}}{n-k} \ln(en),$$

где $e = 2,71\ldots$ – основание натурального логарифма.

Доказательство. 1. Нижняя оценка. Заметим, что один набор $\alpha \in B_{k+1}^n$ затеняет ровно $(k+1)$ наборов из слоя B_k^n.

Поэтому, если число наборов в множестве T_k^n будет меньше указанной в лемме нижней оценки, то их просто не хватит, чтобы затенить все наборы слоя B_k^n, которых ровно C_n^k.

Лемма о мощности затеняющего множества слоя куба

Доказательство (продолжение). 2. Верхняя оценка. Построим матрицу $M_{n,k}$ из нулей и единиц размера $C_n^{k+1} \times C_n^k$.

В этой матрице строки помечены наборами из слоя B_{k+1}^n, а столбцы помечены наборами из слоя B_k^n.

На пересечении строки, помеченной набором α, и столбца, помеченного набором β, находится единица, в том и только в том случае, когда $\beta \in S(\alpha)$.

Заметим, что по построению матрицы $M_{n,k}$ если множество строк T является ее покрытием, то оно затеняет слой B_k^n, т.е. $S(T) = B_k^n$.

Иллюстрация покрытия матрицы $M_{n,k}$

В качестве примера рассмотрим матрицу $M_{4,2}$:

	0	0	0	1	1	1
	0	1	1	0	0	1
	1	0	1	0	1	0
	1	1	0	1	0	0
$0,1,1,1$	1	1	1	0	0	0
$1,0,1,1$	1	0	0	1	1	0
$1,1,0,1$	0	1	0	1	0	1
$1,1,1,0$	0	0	1	0	1	1

Покрытие $T = \{(0,1,1,1),(1,0,1,1),(1,1,0,1)\}$ матрицы $M_{4,2}$ затеняет слой B_2^4.

Лемма о мощности затеняющего множества слоя куба

Доказательство (продолжение). Для матрицы $M_{n,k}$ построим градиентное покрытие T_k^n.

Мощность этого покрытия можно оценить по лемме о градиентном покрытии.

В нашем случае: число строк $p = C_n^{k+1}$; число столбцов $q = C_n^k$; в любом столбце ровно $(n-k)$ единиц.
Поэтому

$$|T_k^n| \leq 1 + \frac{C_n^{k+1}}{n-k} \ln\left(e \cdot \frac{C_n^k(n-k)}{C_n^{k+1}}\right).$$

Заметим, что

$$\frac{C_n^k(n-k)}{C_n^{k+1}} = \frac{n!(n-k)(k+1)!(n-k-1)!}{k!(n-k)!n!} = k+1 \leq n.$$

Откуда $|T_k^n| \leq 1 + \frac{C_n^{k+1}}{n-k} \ln(en)$. $\square$

Теорема о кратчайшем затеняющем множестве куба B^n

Теорема 3 (о кратчайшем затеняющем множестве). *Пусть $n \geq 1$. Для мощности кратчайшего затеняющего множества T куба B^n верно двойное неравенство:*

$$\frac{2^{n+1}}{n+1} - 1 \leq |T_k^n| \leq n + \frac{2^{n+1}}{n+1} \ln(en),$$

где $e = 2,71\ldots$ – основание натурального логарифма.

Доказательство. Пусть T – кратчайшее затеняющее множество куба B^n.

Разобьем множество T на затеняющие множества T_k^n слоев B_k^n, $k = 0, \ldots, (n-1)$.

По лемме 2 верно

$$\frac{C_n^k}{k+1} \leq |T_k^n| \leq 1 + \frac{C_n^{k+1}}{n-k} \ln(e \cdot n).$$

Теорема о кратчайшем затеняющем множестве куба B^n

Доказательство (продолжение). 1. Нижняя оценка.

$$|T| = \sum_{k=0}^{n-1} |T_k^n| \geq \sum_{k=0}^{n-1} \frac{C_n^k}{k+1} = \sum_{k=0}^{n-1} \frac{n!}{k!(n-k)!(k+1)} =$$

$$= \sum_{k=0}^{n-1} \frac{n!(n+1)}{(k+1)!(n-k)!(n+1)} = \frac{1}{n+1} \sum_{k=0}^{n-1} C_{n+1}^{k+1} =$$

$$= \frac{1}{n+1} \sum_{l=1}^{n} C_{n+1}^{l} = \frac{2^{n+1}-2}{n+1} \geq \frac{2^{n+1}}{n+1} - 1.$$

Теорема о кратчайшем затеняющем множестве куба B^n

Доказательство (продолжение). 2. Верхняя оценка.

$$|T| = \sum_{k=0}^{n-1} |T_k^n| \le \sum_{k=0}^{n-1} \left(1 + \frac{C_n^{k+1}}{n-k} \ln(en)\right) \le$$

$$\le n + \ln(en) \sum_{k=0}^{n-1} \frac{n!}{(k+1)!(n-k-1)!(n-k)} =$$

$$= n + \ln(en) \sum_{k=0}^{n-1} \frac{n!(n+1)}{(k+1)!(n-k)!(n+1)} =$$

$$= n + \frac{\ln(en)}{n+1} \sum_{k=0}^{n-1} C_{n+1}^{k+1} = n + \frac{\ln(en)}{n+1} \sum_{l=1}^{n} C_{n+1}^{l} \le n + \frac{2^{n+1}}{n+1} \ln(en).$$

□

Применения затеняющих множеств

Зачем мы искали затеняющие множества и оценивали их мощности?

Одно из применений – мы можем оценить **длину** полиномиальных нормальных форм булевых функций.

Дизъюнктивные нормальные и полиномиальные нормальные формы

Вспомним, что выражение вида $x_{i_1}^{\sigma_1} \cdot \dots \cdot x_{i_r}^{\sigma_r}$, в котором переменные x_{i_j} попарно различны, а $x^\sigma = \begin{cases} x, & \sigma = 1; \\ \bar{x}, & \sigma = 0; \end{cases}$, называется **элементарной конъюнкцией ранга** r.

Выражение вида $K_1 \vee \dots \vee K_l$, в котором K_i – попарно различные элементарные конъюнкции, называется **дизъюнктивной нормальной формой** (ДНФ) **длины** l.

Выражение вида $K_1 \oplus \dots \oplus K_l$, в котором K_i – попарно различные элементарные конъюнкции, называется **полиномиальной нормальной формой** (ПНФ) **длины** l.

Теоремы о совершенной ДНФ и совершенной ПНФ

Теорема 4 (о совершенной ДНФ) *Каждая булева функция* $f(x_1, \ldots, x_n)$, *не равная тождественно нулю, может быть задана совершенной ДНФ:*

$$f(x_1, \ldots, x_n) = \bigvee_{\substack{(\sigma_1, \ldots, \sigma_n) \in B^n : \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Теорема 5 (о совершенной ПНФ) *Каждая булева функция* $f(x_1, \ldots, x_n)$, *не равная тождественно нулю, может быть задана совершенной ПНФ:*

$$f(x_1, \ldots, x_n) = \bigoplus_{\substack{(\sigma_1, \ldots, \sigma_n) \in B^n : \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Доказывается теорема 5 аналогично теореме о СДНФ.

Свойства ДНФ и ПНФ

СДНФ и СПНФ имеют много хороших свойств, но обладают существенным недостатком: как правило, их длина достаточно велика. Но почти всегда для булевой функции можно найти ДНФ и ПНФ с меньшей длиной.

Например, для функции $f(x_1, x_2) = x_1 \vee x_2$ верно

$$f(x_1, x_2) = \bar{x}_1 x_2 \vee x_1 \bar{x}_2 \vee x_1 x_2 = x_1 \vee x_2;$$
$$f(x_1, x_2) = \bar{x}_1 x_2 \oplus x_1 \bar{x}_2 \oplus x_1 x_2 = \bar{x}_1 x_2 \oplus x_1.$$

А **насколько** можно уменьшить длину ДНФ или ПНФ?

Вопрос об упрощении ДНФ рассматривается в курсе “Основы кибернетики”.

Упрощение же ПНФ можно проводить при помощи затеняющих множеств булева куба.

Полином Жегалкина

Напомним, что элементарная конъюнкция без отрицаний переменных называется **монотонной**. По определению полагают, что константа 1 является монотонной элементарной конъюнкцией.

Выражение вида $K_1 \oplus \cdots \oplus K_l$, где K_i – попарно различные монотонные элементарные конъюнкции, $l \geq 0$, называется **полиномом Жегалкина**. Верна теорема Жегалкина.

Теорема 6 (Жегалкина) *Каждая булева функция $f(x_1, \ldots, x_n)$ может быть задана полиномом Жегалкина, причем однозначно.*

Полином Жегалкина – частный случай ПНФ. Однако и в полиноме Жегалкина может быть достаточно много слагаемых. В худшем случае, – 2^n для функции, зависящей от n переменных.

Соответствие между монотонными элементарными конъюнкциями и наборами булева куба

Напомним взаимно однозначное соответствие между монотонными элементарными конъюнкциями от переменных $x_1, \ldots, x_n$ и наборами куба B^n.

Если $\alpha = (a_1, \ldots, a_n) \in B^n$, то положим $K_\alpha = \prod\limits_{a_i=1} x_i$.

Например, пусть $n = 3$. Тогда

$$K_{(1,1,0)} = x_1 x_2; \quad K_{(0,1,0)} = x_2.$$

По определению $K_{(0,\ldots,0)} = 1$.

Упрощение ПНФ при помощи затеняющего множества

Выше мы построили затеняющее множество куба B^3:
$T = \{(1,1,1),(1,1,0),(0,1,1),(0,1,0)\}$.

Посмотрим, как при помощи этого затеняющего множества упрощать ПНФ функций, зависящих от трех переменных.

Пусть нам дана булева функция в виде полинома Жегалкина:

$$f(x_1,x_2,x_3) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus 1.$$

Длина ее полинома равна 5.

Упрощение ПНФ при помощи затеняющего множества

$$T = \{(1,1,1),(1,1,0),(0,1,1),(0,1,0)\}.$$

Шаг 1. Выберем в ПНФ функции f все монотонные элементарные конъюнкции ранга $n-1=2$:

$$f(x_1,x_2,x_3) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus 1.$$

Т.к. T – затеняющее множество, в нем есть наборы, которые затеняют все соответствующие этим конъюнкциям наборы. В нашем случае – это один набор $(1,1,1) \in T$:
$\{(1,1,0),(1,0,1)\} \subseteq S((1,1,1))$.
Рассмотрим $K_{(1,1,1)} = x_1x_2x_3$. Заметим, что

$$x_1\bar{x}_2\bar{x}_3 = x_1(x_2 \oplus 1)(x_3 \oplus 1) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1.$$

Поэтому перепишем функцию $f(x_1,x_2,x_3)$ в виде

$$f(x_1,x_2,x_3) = x_1\bar{x}_2\bar{x}_3 \oplus x_1 \oplus x_2 \oplus 1.$$

Упрощение ПНФ при помощи затеняющего множества

$$T = \{(1,1,1),(1,1,0),(0,1,1),(0,1,0)\}.$$

Шаг 2. Выберем в ПНФ функции f, полученной на предыдущем шаге, все монотонные элементарные коъюнкции ранга $n-2=1$:

$$f(x_1,x_2,x_3) = x_1\bar{x}_2\bar{x}_3 \oplus x_1 \oplus x_2 \oplus 1.$$

Множество T – затеняющее, поэтому в нем есть наборы, которые затеняют все соответствующие этим конъюнкциям наборы. В нашем случае – это набор $(1,1,0) \in T$: $\{(1,0,0),(0,1,0)\} \subseteq S((1,1,0))$.
Теперь рассмотрим $K_{(1,1,0)} = x_1x_2$. Заметим, что

$$\bar{x}_1\bar{x}_2 = (x_1 \oplus 1)(x_2 \oplus 1) = x_1x_2 \oplus x_1 \oplus x_2 \oplus 1.$$

Поэтому

$$f(x_1,x_2,x_3) = x_1\bar{x}_2\bar{x}_3 \oplus x_1x_2 \oplus \bar{x}_1\bar{x}_2.$$

Упрощение ПНФ при помощи затеняющего множества

В итоге мы нашли ПНФ для функции $f(x_1, x_2, x_3)$:

$$f(x_1, x_2, x_3) = x_1\bar{x}_2\bar{x}_3 \oplus x_1x_2 \oplus \bar{x}_1\bar{x}_2.$$

Ее длина равна 3. Т.е. исходную ПНФ (полином Жегалкина) мы упростили.

В общем случае, длина получающейся по этому алгоритму ПНФ функции, зависящей от n переменных, не будет превосходить величину $2 \cdot |T|$, где T – затеняющее множество куба B^n (почему?).

Оценки длины ПНФ

Теорема 7 (Кириченко). *Каждая булева функция $f(x_1, \ldots, x_n)$ может быть задана ПНФ с длиной, не превосходящей величину $|T| + 1$, где T – мощность кратчайшего затеняющего множества куба B^n.*

Следствие 7.1. *Каждая булева функция $f(x_1, \ldots, x_n)$ может быть задана ПНФ длины $l(n)$, где*

$$l(n) \leq n + \frac{2^{n+1}}{n+1} \ln(en),$$

где $e = 2,71\ldots$ – основание натурального логарифма.

Программируемые логические матрицы (ПЛМ)

А зачем упрощать ДНФ и ПНФ?

Одно из применений – в БИС/СБИС с программируемой структрой, как например, программируемые логические матрицы (ПЛМ).

Структура ПЛМ такова, что она соотвествует ДНФ или ПНФ булевой функции (или системы булевых функций).

И чем меньше длина ДНФ или ПНФ, тем меньший размер ПЛМ можно применять для реализации этой функции и тем эффективней ПЛМ.

Задачи для самостоятельного решения

1. [2] Гл. IX 1.6-1.7.

2. Применить алгоритм упрощения ПНФ к функциям:
1) $f(x_1, x_2, x_3) = x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3$;
2)
$f(x_1, x_2, x_3, x_4) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4$.

3. Доказать, что по алгоритму упрощения ПНФ для произвольной функции $f(x_1, \ldots, x_n)$ будет построена ПНФ с длиной, не более, чем в два раза превышающей мощность кратчайшего покрытия куба B^n.

Литература к лекции 5

1. Сапоженко А.А. Проблема Дедекинда и метод граничных функционалов. М.: Физматлит, 2009.

2. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004.

Конец лекции 5