Методы дискретного анализа в организационных системах. Алгоритмический подход.

Институт проблем управления РАН,
Физический факультет МГУ
http://www.ipu.ru/
http://www.phys.msu.ru/rus/about/structure/div/div-experimental/chair-upravleniya/
http://www.orsot.ru/
Лазарев Александр Алексеевич
2009-2010 учебный год

План

- Функции алгебры логики
- Элементы комбинаторики
- Элементы теории графов
- Три контрольные работы (в редакторе TeX, http://miktex.org/2.8/setup)

Рекомендуемая литература

- **1. Журавлёв Ю.И., Флёров Ю.А. Дискретный анализ. Часть I: Учебное пособие. – М.: МФТИ, 1999.**
- 2. Стэнли Р. Перечислительная комбинаторика. -М.: Мир, 1990.
- 3. Липский В. Комбинаторика для программистов. - М.: Мир, 1988.
- 4. Рыбников К.А. Введение в комбинаторный анализ. - М.: МГУ,1985.
- 5. Гаврилов Г.И., Сапоженко А.А. Задачи и упражнения по курсу дискретной математики. -М.: Наука, 1992.
- 6. Риордан Дж. Введение в комбинаторный анализ. - М.: ИЛ, 1963.
- **7. Холл М. Комбинаторика. - М.: Мир, 1970.**
- **8. Мендельсон Э. Введение в математическую логику.- М.: Наука, 1976.**
- 9. Дискретная математика и математические вопросы кибернетики/
- Под ред. С.В.Яблонского, О.В.Лупанова, Т.1, -М.; Наука, 1974.
- **10. Яблонский С.В. Введение в дискретную математику. -М.: Наука, 1986.**
- **11. Оре О. Теория графов. - М.: Наука, 1968.**
- 12. Кристофидис Н. Теория графов. Алгоритмический подход. -М.: Мир, 1987.
- 13. Емеличев В.А., Мельников О.И. и др. Лекции по теории графов. М.: Наука, 1990.
- 14. Уилсон Р.Дж. Введение в теорию графов. - М.: Мир, 1977.
- 15. Харари Ф. Теория графов. - М.: Мир,1973.
- **16. Журавлёв Ю.И., Флёров А.А., Федько О.С., Дадашев Т.М. Сборник задач по дискретному анализу. – М.: МФТИ, 2000.**
- 17. Гжегорчик А. Популярная логика.- М.: Наука, 1979.
- 18. Леонтьев В.К. Избранные задачи комбинаторного анализа. – М. Изд-во МГТУ им. Н.Э. Баумана, 2001.
- 19. Лазарев А.А. Теория расписаний. Оценки абсолютной погрешности и схема приближённого решения задач теории расписаний: Учебное пособие. – М.: МФТИ, 2008.
- **20. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. – М.: Мир. – 1982.**
- **21. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. – М. – 2005. 1293 с.**

Функции алгебры логики

- Джордж Буль (1815-1864)

“Математический анализ логики, являющийся очерком, касающимся исчисления дедуктивных рассуждений”, (1847 г.),

“Исследования законов мысли. на которых основываются математические теории логики и вероятностей”, (1854 г.).

- Аугустус (Огастес, Август) де Морган (1806-1871)

“Формальная логика или исчисление выводов, необходимых и возможных” (1847 г.).

БУЛЬ, ДЖОРДЖ (Boole, George) (1815-1864), английский математик. Родился 2 ноября 1815 в Линкольне. В возрасте 16 лет стал помощником учителя частной школы в Донкастере, в 1835 открыл собственную школу в Линкольне. В свободное время читал математические журналы, работы И.Ньютона, П.Лапласа и Ж.-Л.Лагранжа, начал вести самостоятельные алгебраические исследования. В 1839 написал первую научную работу ***Исследования по теории аналитических преобразований*** (***Researches on the Theory of Analytical Transformations***), которая была опубликована "Кембриджским математическим журналом" ("Cambridge Mathematical Journal"). В 1844 появилась его первая работа, где высказывалась идея объединения алгебры и логики, а в 1847 вышла в свет статья ***Математический анализ логики*** (***The Mathematical Analysis of Logic***), которая положила начало созданию "алгебры высказываний", получившей впоследствии название булевой алгебры. Благодаря этой публикации Буль в 1849 был назначен профессором математики Куинз-колледжа (Корк, Ирландия), где преподавал до конца жизни. В 1857 был избран членом Лондонского королевского общества. Основные идеи Буля суммированы в его работе ***Исследование законов мышления, на которых основаны математические теории логики и вероятностей*** (***An Investigation of the Laws of Thought, on Which Are Founded the Mathematical Theories of Logic and Probabilities***, 1854). Здесь впервые определено в явном виде исчисление классов (или множеств), введено обозначение для их пересечения, объединения и т. д., показано, что исчисление классов можно интерпретировать как исчисление высказываний. Булевы алгебры — особые алгебраические системы, для которых определены две операции, — нашли широкое применение в различных разделах математики: в теории вероятностей, топологии, функциональном анализе, а также в создании вычислительных машин. Умер Буль в Баллинтемпле (графство Корк, Ирландия) 8 декабря 1864.

- **Огастес (Август) де Морган** (англ. *Augustus de Morgan*, 27 июня 1806), Мадура, Индия — 8 марта 1871, Лондон) — шотландский математик и логик; профессор математики университетского колледжа в Лондоне (1828—1831, 1836—1866); первый президент (1866) Лондонского математического общества.
- Основные труды: по математической логике и теории рядов; к своим идеям в алгебре логики пришёл независимо от Дж. Буля; изложил (1847) элементы логики высказываний и логики классов, дал первую развитую систему алгебры отношений; с его именем связаны известные теоретико-множественные соотношения (законы де Моргана).

Функции алгебры логики. Табличное задание функций. Элементарные функции, их свойства, таблица операций, коммутативность, ассоциативность, дистрибутивность элементарных функций.

Формулы и функции алгебры логики. Теоремы о разложении функций по одной и нескольким переменным. Совершенная дизъюнктивная нормальная форма. Задача о ВЫПОЛНИМОСТИ. Определение понятия NP-трудности задач.

Функциональная полнота систем функций алгебры логики. Замкнутые классы. Пять предполных замкнутых классов T_0, T_1, L, S, M. Пересечение данных классов. Теорема о функции двойственной к суперпозиции. Критерий функциональной полноты систем функций алгебры логики (теорема Поста). Примеры полных систем функций алгебры логики. Основная лемма. Лемма о несамодвойственной функции. Лемма о немонотонной функции. Лемма о нелинейной функции. Следствия из критерия полноты.

Функции алгебры логики.

- Область определения логических или булевых переменных 0 и 1
- Область значений функций также 0 и 1
- Функция от одной переменной f(x)

x	f(x)			
0	0	0	1	1
1	0	1	0	1
	0	x	⌉x	1

$\overline{x}$

$x \in \{\text{истина},\ \text{ложь}\} = \{1, 0\};$

$\text{истина} = 1;$

$\text{ложь} = 0.$

Операции над двумя переменными (двухместные, бинарные операции)

x	y	$x \wedge y$	$x \vee y$	$x \to y$	$x \equiv y$	$x + y$	$x \mid y$	$x \downarrow y$
0	0	0	0	1	1	0	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	0	0	1	1	0
1	1	1	1	1	1	0	0	0

2^n ***конъюнкция*** $\wedge$ **&** И ***min(x,y)*** ***дизъюнкция*** $\vee$ ***max (x,y)*** ***импликация*** $\to$ $\supset$

эквивалентность $\equiv$ $\sim$ $\leftrightarrow$ ***сумма по модулю 2*** $+$ $\oplus$

штрих **(Шеффера)** $\mid$ **“не x или не y”** ***стрелка*** **(Пирса)** $\downarrow$ **“не x и не y”.**

Индуктивное определение формулы:

- Пусть U - множество переменных. Тогда множество формул алгебры логики над U определяется следующим образом:
- 1. Всякая переменная - формула.
- 2. Константы 0 и 1 - формулы.
- 3. Если A - формула, то $\rceil$A (или в другой записи $\overline{A}$) - формула.
- 4. Если A и B - формулы, то (A$\wedge$B), (A$\vee$B), (A$\rightarrow$B), (A+B), (A≡B), (A|B), (A↓B) - формулы.
- 5. Формулами являются те и только те выражения, которые могут быть получены из констант, переменных и логических связок за конечное число шагов 1- 4.

Определение. Функция от n переменных

$$F(x_1, x_2, x_3, \ldots, x_n),$$

определенная на множестве

$$B^n = \{\|(x_1, \ldots, x_n), x_i \in \{0,1\}\}$$

и принимающая значения из множества {0, 1}, называется функцией алгебры логики или булевой функцией.

«Табличное» задание функции

x_1	x_2	…	x_{n-1}	x_n	$f(x_1, x_2, \ldots x_{n-1}, x_n)$
0	0	…	0	0	$f(0, 0, \ldots, 0, 0)$
0	0	…	0	1	$f(0, 0, \ldots, 0, 1)$
0	0	…	1	0	$f(0, 0, \ldots, 1, 0)$
…………………					
1	1	…	1	1	$f(1, 1, \ldots, 1, 1)$

$\mathbf{2^n}$

Алгебраические свойства элементарных операций

- **1. Коммутативность** (или перестановочность) операции * означает, что $x*y = y*x$. Логическая операция * коммутативна, если связка * принадлежит следующему множеству связок (существенно только, чтобы символ * в равенстве всюду имел один и тот же смысл):
- $$* \in \left\{ \vee , \wedge , + , \equiv , | , \downarrow \right\}$$

- **2. Ассоциативность** операции * означает, что $x * (y * z) = (x * y) * z$.Свойство ассоциативности позволяет записывать формулы, содержащие одинаковые ассоциативные связки, без скобок, например, $x \vee y \vee z, x \wedge y \wedge z$.
- Логическая операция * ассоциативна, если связка * принадлежит следующему множеству связок (существенно только, чтобы символ * в равенстве всюду имел один и тот же смысл):
- .

$$* \in \{ \wedge , \vee , + , \equiv \}$$

- **3. Дистрибутивность** (распределительный закон) операции * относительно операции · означает, что $x*(y\bullet z)=(x*y)\bullet(x*z)$.

Дистрибутивность конъюнкции:

- $x\wedge(y\vee z)=(x\wedge y)\vee(x\wedge z)$ - дистрибутивность конъюнкции относительно дизъюнкции;
- $x\wedge(y+z)=(x\wedge y)+(x\wedge z)$ - дистрибутивность конъюнкции относительно суммы по модулю 2.

Дистрибутивность дизъюнкции:

- $x\vee(y\wedge z)=(x\vee y)\wedge(x\vee z)$ - дистрибутивность дизъюнкции относительно конъюнкции;
- $x\vee(y\to z)=(x\vee y)\to(x\vee z)$ - дистрибутивность дизъюнкции относительно импликации;
- $x\vee(y\equiv z)=(x\vee y)\equiv(x\vee z)$ - дистрибутивность дизъюнкции относительно эквивалентности.

Дистрибутивность импликации:

- $x \to (y \wedge z) = (x \to y) \wedge (x \to z)$ - дистрибутивность импликации относительно конъюнкции;
- $x \to (y \vee z) = (x \to y) \vee (x \to z)$ - дистрибутивность импликации относительно дизъюнкции;
- $x \to (y \to z) = (x \to y) \to (x \to z)$ - дистрибутивность импликации относительно импликации.

- **4.** Имеет место следующее соотношение для двойного отрицания:

$$\overline{\overline{x}} = x$$

- **5.** Имеют место следующие соотношения между отрицанием, конъюнкцией и дизъюнкцией:
- $$\left.\begin{aligned}\overline{x \wedge y} &= \bar{x} \vee \bar{y}\\ \overline{x \vee y} &= \bar{x} \wedge \bar{y}\end{aligned}\right\}$$

закон (правила) де Моргана.

Указанные соотношения отражают отношение двойственности между дизъюнкцией и конъюнкцией.

- **6.** Имеют место следующие соотношения, связанные с “навешиванием отрицания” на элементарные логические функции:

$$\overline{x \mid y} = x \wedge y;$$

$$\overline{x \downarrow y} = x \vee y;$$

$$\overline{x + y} = x \equiv y$$

$$\overline{x \equiv y} = x + y$$

$$\overline{x \to y} = \overline{\bar{x} \vee y} = x\bar{y}$$

- **7.** Константы могут быть выражены следующим образом:

$$0 = x \wedge \bar{x} = x \wedge 0 = x + x$$

$$1 = x \vee \bar{x} = x \vee 1 = x \equiv x$$

- **8.** Правила поглощения:

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

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

- **9.** Выполняются следующие свойства конъюнкции и дизъюнкции:
-

$$x \wedge x = x, \qquad x \vee x = x,$$

$$x \wedge \overline{x} = 0, \qquad x \vee \overline{x} = 1,$$

$$x \wedge 0 = 0, \qquad x \vee 0 = x,$$

$$x \wedge 1 = x, \qquad x \vee 1 = 1$$

- Все указанные тождества могут быть проверены путем сопоставления функций, реализуемых правой и левой частями формул, сопоставление таблиц значений функций.

- Все элементарные функции могут быть выражены через одну-единственную: штрих Шеффера или стрелку Пирса.

Определение. Через $P_2(n)$ будем обозначать множество всех разных булевых функций размерности n.

- **Теорема.** Число $p_2(n)$ всех функций из $P_2(n)$, зависящих от переменных x_1, x_2, ... , x_n , равно 2^{2^n} .

- Переменная x_i ($1 \le i \le n$) функции $f(x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n)$ из $P_2(n)$называется ***существенной***, если можно указать такие наборы $$\tilde{\alpha} = (\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n)$$

и

$$\tilde{\beta} = (\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n)$$

значений переменных, что $$f(\tilde{\alpha}) \neq f(\tilde{\beta})$$

В противном случае переменную x_i называют ***несущественной*** или ***фиктивной*** переменной функции f.

- Две функции $f(x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n)$ и $g(x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n)$ называются ***равными***, если множества их существенных переменных совпадают и на любых двух наборах

$$(x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) \text{ и}$$
$$(y_1, y_2, \dots, y_{i-1}, y_i, y_{i+1}, \dots, y_n),$$

различающихся быть может только значениями несущественных переменных, значения функций одинаковы: $f(x)=g(y)$.

Если $f(x)$ и $g(y)$ - равные функции, то одну из них можно получить из другой путем добавления и/или изъятия несущественных переменных.

- **8.** Правила поглощения:

$$x \vee \left(x \wedge y\right) = x$$

$$x \wedge \left(x \vee y\right) = x$$

Разложение функций алгебры логики по переменным

- Чтобы иметь возможность единообразно записывать переменные с отрицанием и без отрицания введем следующее обозначение:

$$x^{\sigma} = \begin{cases} x, если \ \ \sigma = 1 \\ \bar{x}, если \ \ \sigma = 0. \end{cases}$$

- Легко видеть, что $x^{\sigma} = 1$ тогда и только тогда, когда $x = \sigma$, то есть значение “основания” равно значению “показателя”.

- **Лемма.** (О разложении функции по одной переменной). Пусть $f(x_1, \dots, x_n)$ - произвольная функция алгебры логики, тогда справедливо следующее представление f в форме разложения по переменной x_1 :

$$f(x_1, \dots, x_n) = \\ = x_1 \cdot f(1, x_2, \dots, x_n) \vee \bar{x}_1 \cdot f(0, x_2, \dots, x_n) \quad (2.1)$$

- *Доказательство*. Отметим прежде всего, что представление (2.1), естественно, справедливо для произвольной переменной x_i из множества переменных функции f. Для доказательства рассмотрим произвольный набор значений переменных $(\alpha_1, \dots, \alpha_n)$ и покажем, что левая и правая части соотношения (2.1) принимают на нем одно и то же значение.
- Рассмотрим набор значений переменных $(1, \alpha_2, \dots, \alpha_n)$. Левая часть (2.1) принимает на этом наборе значение $f(1, \alpha_2, \dots, \alpha_n)$, а правая часть - значение

$$1 \cdot f(1, \alpha_2, \dots, \alpha_n) \vee 0 \cdot f(0, \alpha_2, \dots, \alpha_n) = f(1, \alpha_2, \dots, \alpha_n).$$

Таким образом, на наборах $(1, \alpha_2, \dots, \alpha_n)$ левая и правая части (2.1) принимают одинаковые значения.
- Рассмотрим набор значений переменных $(0, \alpha_2, \dots, \alpha_n)$. Левая часть (2.1) принимает на этом наборе значение $f(0, \alpha_2, \dots, \alpha_n)$, а правая часть - значение

$$0 \cdot f(1, \alpha_2, \dots, \alpha_n) \vee 1 \cdot f(0, \alpha_2, \dots, \alpha_n) = f(0, \alpha_2, \dots, \alpha_n).$$

Таким образом, на наборах $(0, \alpha_2, \dots, \alpha_n)$ левая и правая части (2.1) принимают одинаковые значения.
- Тем самым мы доказали, что левая и правая части соотношения (2.1) принимают одинаковые значения на всех наборах $(\alpha_1, \dots, \alpha_n)$. **€**

- **Лемма 2.3.** Конъюнкция (произведение) $x_1^{\sigma_1} K \ x_n^{\sigma_n} = 1$ тогда и только тогда, когда

$$(x_1, K \ , x_n) = (\sigma_1, K \ , \sigma_n).$$

- *Доказательство*. Произведение (конъюнкция) равно 1 тогда и только тогда, когда каждый сомножитель равен 1, но $x^\sigma = 1$ тогда и только тогда, когда $x = \sigma$. €

- В дальнейшем будем употреблять следующие обозначения:

$$\bigwedge_{i=1}^{k} x_i = x_1 \wedge x_2 \wedge \ldots \wedge x_k = x_1 x_2 \ldots x_k, \quad \bigvee_{i=1}^{k} x_i = x_1 \vee x_2 \vee \ldots \vee x_k.$$

- **Теорема 2.4.** (О разложении функции по нескольким переменным). Пусть $f(x_1, \ldots, x_n)$ - произвольная функция алгебры логики. Тогда ее можно представить в следующей форме:

$$
\begin{aligned}
& f(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) = \\
& = \bigvee_{(\sigma_1, \ldots, \sigma_k)} x_1^{\sigma_1} \ldots x_k^{\sigma_k} \cdot f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n).
\end{aligned}
\tag{2.2}
$$

- *Доказательство*. Рассмотрим произвольный набор значений переменных (α_1, ... , α_n) и покажем, что левая и правая части соотношения (2.2) принимают на нем одно и то же значение. Левая часть дает

$f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$.

Правая часть дает

$$\bigvee_{(\sigma_1,\ldots,\sigma_k)} x_1^{\sigma_1} \ldots x_k^{\sigma_k} \cdot f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n) =$$

$$= \alpha_1^{\sigma_1} \ldots \alpha_k^{\sigma_k} \cdot f(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n).$$

- Представление (2.2) называется дизъюнктивным разложением функции по k переменным.
- **Пример.** Для k = 2 разложение в дизъюнктивную форму имеет вид:

$$
\begin{aligned}
& f(x_1,\dots,x_n) = \\
& = \bar{x}_1\bar{x}_2 \cdot f(0,0,x_3,\dots x_n) \vee \\
& \vee \bar{x}_1 x_2 \cdot f(0,1,x_3,\dots x_n) \vee \\
& \vee x_1\bar{x}_2 \cdot f(1,0,x_3,\dots x_n) \vee \\
& \vee x_1 x_2 \cdot f(1,1,x_3,\dots x_n).
\end{aligned}
$$

- Выпишем такое разложение для конкретной функции трех переменных по переменным x_2 и x_3:

$$
\begin{aligned}
(x_1 \to x_2) \equiv (x_2 \to x_3) = \bar{x}_2\bar{x}_3 \cdot ((x_1 \to 0) \equiv (0 \to 0)) \vee \\
\vee\, \bar{x}_2 x_3 \cdot ((x_1 \to 0) \equiv (0 \to 1)) \vee \\
\vee\, x_2\bar{x}_3 \cdot ((x_1 \to 1) \equiv (1 \to 0)) \vee \\
\vee\, x_2 x_3 \cdot ((x_1 \to 1) \equiv (1 \to 1)).
\end{aligned}
$$

- Если k = n , то получаем разложение

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

Оно может быть преобразовано при $f(x_1, \dots , x_n) \neq 0$ следующим образом:

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

- Итак, в этом случае разложение имеет вид:

$$f(x_1,\ldots,x_n) = \bigvee_{\substack{(\sigma_1,\ldots,\sigma_n)\\ f(\sigma_1,\ldots,\sigma_n)=1}} x_1^{\sigma_1}\ldots x_n^{\sigma_n}.$$

- Это разложение называется совершенной дизъюнктивной нормальной формой (совершенная ДНФ.). Оно определено для любой функции f, не равной константе 0.

- **Теорема 2.5.** Произвольную функцию алгебры логики можно выразить формулой при помощи операций $\wedge$, $\vee$, $\rceil$, причем операция $\rceil$ применяется только к переменным

- *Доказательство*.
- 1. Пусть $f(x_1, \ldots , x_n) = 0$. Тогда, очевидно,

$f(x1, \ldots , xn) = x_1 \land \rceil x_1$.
- 2. Пусть $f(x_1, \ldots , x_n) \neq 0$. Представим ее в форме совершенной ДНФ:

$$f(x_1, \ldots, x_n) = \bigvee_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \ldots x_n^{\sigma_n}.$$

- Таким образом, в обоих случаях функция f выражается в виде формулы через конъюнкцию, дизъюнкцию и отрицание, причем отрицание применяется только к символам переменных. **€**

- Любую булеву функцию можно выразить формулой над множеством операций $\{\wedge, \vee, \rceil\}$, состоящим из трех функций: отрицания, конъюнкции и дизъюнкции. Данная теорема носит конструктивный характер, так как она позволяет для каждой функции построить реализующую ее формулу (совершенную ДНФ). А именно, берем таблицу для функции $f(x_1, \dots, x_n)$ $(f \neq 0)$ и отмечаем в ней все строки $(\sigma_1, \dots, \sigma_n)$, в которых $f(\sigma_1, \dots, \sigma_n) = 1$, для каждой такой строки образуем логическое произведение

$$x_1^{\sigma_1} \wedge \dots \wedge x_n^{\sigma_n}$$

а затем соединяем все полученные конъюнкции знаком дизъюнкции.

- **Пример**. Построить совершенную ДНФ для функции, заданной таблицей:

x_1 x_2 x_3	$f(x_1, x_2, x_3)$	x_1 x_2 x_3	$f(x_1, x_2, x_3)$
0 0 0	1	1 0 0	0
0 0 1	1	1 0 1	1
0 1 0	0	1 1 0	0
0 1 1	0	1 1 1	1

Имеем: $$f(x_1, x_2, x_3) = \bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2 x_3 \vee x_1\bar{x}_2 x_3 \vee x_1 x_2 x_3$$

- **Задача выполнимости булевых формул (SAT или ВЫП)** — задача распознавания, важная для теории вычислительной сложности.
- Экземпляром задачи **SAT** является булева формула, состоящая только из имен переменных, скобок и операций (*И*), (*ИЛИ*) и (*НЕ*). Задача заключается в следующем: можно ли назначить всем переменным, встречающимся в формуле, значения *ЛОЖЬ* и *ИСТИНА* так, чтобы формула стала истинной.
- Согласно теореме Кука, доказанной Стивеном Куком в 1971-м году, задача SAT NP-полна.

- Чтобы четко сформулировать задачу распознавания, необходимо условиться об алфавите, с помощью которого задаются экземпляры языка. Этот алфавит должен быть фиксирован и конечен. Обычно используют следующий алфавит:

{ ∨, ∧, ⌉, (,), *x*, 0, 1}.

- При использовании такого алфавита скобки и операторы записываются естественным образом, а переменные получают следующие имена: x1, x10, x11, x100 и т. д., согласно их номерам, записанным в двоичной системе счисления.
- Пусть некоторая булева формула, записанная в обычной математической нотации, имела длину *N* символов. В ней каждое вхождение каждой переменной было описано хотя бы одним символом, следовательно, всего в данной формуле не более *N* переменных. Значит, в предложенной выше нотации каждая переменная будет записана с помощью символов. В таком случае, вся формула в новой нотации будет иметь длину $O(\log N)$мволов, то есть длина строки возрастет в полиномиальное число раз. $O(N \log N)$
- Например, формула

$$a \wedge \neg(b \vee c)$$

примет вид $$x1 \wedge \neg(x10 \vee x11)$$

- **Вычислительная сложность**
- В 1971-м году в статье Стивена Кука был впервые введен термин «NP-полная задача», и задача SAT была первой задачей, для которой доказывалось это свойство.
- В доказательстве теоремы Кука каждая задача из класса NP в явном виде сводится к SAT. После появления результатов Кука была доказана NP-полнота для множества других задач. При этом чаще всего для доказательства NP-полноты некоторой задачи приводится полиномиальное сведение задачи SAT к данной задаче, возможно в несколько шагов, то есть с использованием нескольких промежуточных задач.

Две задачи

Пример 4. *Сложение n-разрядных двоичных чисел.* Мы исходим из обычного алгоритма сложения «столбиком»

$$\begin{array}{r} x_n \ldots x_2 x_1 \\ + \\ y_n \ldots y_2 y_1 \\ \hline z_{n+1} z_n \ldots z_2 z_1 . \end{array}$$

Требуется выразить значения разрядов суммы через значения разрядов слагаемых. Для решения этого вопроса рассматривают вспомогательные величины $w_n, w_{n-1}, \ldots$ $\ldots, w_1$, где w_i обозначает результат переноса из i-го разряда в $(i+1)$-й разряд. Эти параметры появляются в упомянутом алгоритме.

Ясно, что тогда

$$z_i = ((x_i + y_i) + w_{i-1})$$

$$(w_0 = 0, \quad x_{n+1} = y_{n+1} = 0, \quad i = 1, \ldots, n+1).$$

Величина w_i определяется условием переноса из i-го разряда в $(i+1)$-й разряд: «перенос в $(i+1)$-й разряд имеет место тогда и только тогда, когда по крайней мере две из трех величин x_i, y_i, w_{i-1} равны 1». Это высказывание более подробно можно сформулировать так: «x_i и y_i» или «x_i и w_{i-1}» или «y_i и w_{i-1}».

Если теперь заменить союзы «и» и «или» символами & и $\vee$, то получим следующую формулу для w_i:

$$w_i = \{[(x_i \,\&\, y_i) \vee (x_i \,\&\, w_{i-1})] \vee (y_i \,\&\, w_{i-1})\},$$

$$(i = 1, \ldots, n).$$

Пример 5. *Задача о вызове свободного лифта.* Пусть в подъезде имеется три лифта, обслуживающих n этажей. На каждом этаже имеется устройство, которое позволяет при нажатии кнопки вызывать ближайший свободный лифт. Спрашивается, как можно на логическом языке записать условие вызова i-го лифта ($i = 1, 2, 3$)? Мы рассмотрим эту задачу для случая вызова лифта на первом этаже.

Для описания исходной информации введем $3n$ аргументов

$$x_1, y_1, z_1, x_2, y_2, z_2, \ldots, x_n, y_n, z_n,$$

где $x_i = 1$ тогда и только тогда, когда 1-й лифт находится на i-м этаже и свободен; $y_i = 1$ тогда и только тогда, когда 2-й лифт находится на i-м этаже и свободен; $z_i = 1$ тогда и только тогда, когда 3-й лифт находится на i-м этаже и свободен.

Обозначим через

$$f_1(x_1, y_1, z_1, \ldots, x_n, y_n, z_n), \ldots, f_{III}(x_1, y_1, z_1, \ldots, x_n, y_n, z_n)$$

функции, равные 1 тогда и только тогда, когда вызывается лифт с номером соответственно 1, 2, 3. Условие вызова 1-го лифта, или функция f_I, характеризуется тем, что «1-й лифт свободен и нет свободных лифтов, расположенных на более низком этаже, чем 1-й лифт». Это высказывание можно выразить подробнее следующим образом: «1-й лифт вызывается тогда и только тогда, когда 1-й лифт находится на 1-м этаже и свободен или на 1-м этаже нет свободных лифтов с номерами 2 и 3, и в этом случае 1-й лифт находится на 2-м этаже и свободен, или на 2-м этаже нет свободных лифтов с номерами 2 и 3 и здесь, в свою очередь...» Запишем это высказывание через высказывания $x_1, y_1, z_1, \ldots$ $\ldots, x_n, y_n, z_n$: «1-й лифт вызывается тогда и только тогда, когда x_1, или когда «не y_1 и не z_1», и в этом случае x_2 или «не y_2 и не z_2» и здесь, в свою очередь...». Теперь нетрудно получить формулу для f_{I}, если заменить союзы «и» и «или» на & и $\vee$, частицу «не» на $^{-}$ и расставить скобки в соответствии с соединительными словами:

$$f_{\mathrm{I}}(x_1, y_1, z_1, \ldots, x_n, y_n, z_n) =$$
$$= \{x_1 \vee \{(\bar{y}_1 \mathbin{\&} \bar{z}_1) \mathbin{\&} [x_2 \vee [(\bar{y}_2 \mathbin{\&} \bar{z}_2) \mathbin{\&} (\ldots)]]\}\}.$$

Аналогичные формулы получаются для функций f_{II} и f_{III}:

$$f_{\mathrm{II}}(x_1, y_1, z_1, \ldots, x_n, y_n, z_n) =$$
$$= \{y_1 \vee \{(\bar{x}_1 \mathbin{\&} \bar{z}_1) \mathbin{\&} [y_2 \vee [(\bar{x}_2 \mathbin{\&} \bar{z}_2) \mathbin{\&} (\ldots)]]\}\},$$

$$f_{\mathrm{III}}(x_1, y_1, z_1, \ldots, x_n, y_n, z_n) =$$
$$= \{z_1 \vee \{(\bar{x}_1 \mathbin{\&} \bar{y}_1) \mathbin{\&} [z_2 \vee [(\bar{x}_2 \mathbin{\&} \bar{y}_2) \mathbin{\&} (\ldots)]]\}\}.$$

Функциональная полнота систем функций алгебры логики

- Выше мы видели, что всякая функция алгебры логики может быть выражена в виде формулы через элементарные функции $\bar{x}$, $x \wedge y$, $x \vee y$. В связи с этим возникает вопрос, какими свойствами должна обладать система функций, чтобы через функции этой системы можно было выразить произвольную функцию алгебры логики?
- Новые функции получаются из имеющихся в заданной системе функций с помощью операций замены переменных и суперпозиции. Опишем эти две операции.

1. Замена переменных.

- Пусть $f(x_1, x_2, \dots, x_n)$ - заданная функция алгебры логики. Будем говорить, что функция $\phi(y_1, y_2, \dots, y_n)$ получена операцией замены переменных из функции $f(x_1, x_2, \dots, x_n)$, если осуществлена подстановка переменных

$$s = \begin{pmatrix} x_1 \dots x_n \\ y_1 \dots y_n \end{pmatrix}$$

Пример. Пусть имеется функция $f(x_1, x_2) = x_1 | x_2$

Тогда при замене переменных $\begin{pmatrix} x_1 & x_2 \\ y & y \end{pmatrix}$

из функции $f(x_1, x_2)$

можно получить функцию $\varphi(y) = f(y, y) = y | y = \bar{y}$

.

2. Суперпозиция функций алгебры логики.

- Пусть имеется функция $f(x_1, x_2, \dots, x_n)$ и функции

$$f_i(x_{i_1}, \dots, x_{i_{m_i}}),\ i = 1, \dots, n\ ,$$

- тогда функцию

$$\varphi = f(f_1(x_{1_1}, \dots, x_{1_{m_1}}), \dots, f_n(x_{n_1}, \dots, x_{n_{m_n}}))$$

будем называть *суперпозицией функции* $f(x_1, x_2, \dots, x_n)$ *и функций* $f_i(x_{i_1}, \dots, x_{i_{m_i}}),\ i = 1, \dots, n$.

- Другими словами: пусть $F = \{ f_j \}$ - набор функций алгебры логики, не обязательно конечный. Функция f называется суперпозицией функций из множества F или функцией над F, если она получена из функции

$$f_j \in F$$

путем замены одной или нескольких ее переменных функциями из множества F.

- **Пример**.
- Пусть задано множество функций $F = \{f_1(x_1), f_2(x_1, x_2, x_3), f_3(x_1, x_2)\}$.
- Тогда суперпозициями функций из F будут, например, функции:
- $\varphi_1(x_2, x_3) = f_3(f_1(x_2), f_1(x_3))$;
- $\varphi_2(x_1, x_2) = f_2(x_1, f_1(x_1), f_3(x_1, x_2))$.
- Совершенная ДНФ - суперпозиция функций из множества

$$\{x_1 \vee x_2, \quad x_1 \wedge x_2, \bar{x}\}$$

. €

- Система функций называется ***полной***, если при помощи операций суперпозиции и замены переменных из функций этой системы может быть получена любая функция алгебры логики. **€**

- Мы уже имеем некоторый набор полных систем:

$$\{x \vee y, xy, \overline{x}\}$$

$$\{xy, \overline{x}\} \qquad x \vee y = \overline{\overline{x} \wedge \overline{y}}$$

$$\{x \vee y, \overline{x}\} \qquad xy = \overline{\overline{x} \vee \overline{y}}$$

{x+y, xy, 1}.

Как определить условия, при которых система полна?

Замкнутые классы.

- Множество (класс) K функций алгебры логики называется ***замкнутым классом***, если оно содержит все функции, получающиеся из K операциями суперпозиции и замены переменных, и не содержит никаких других функций.
- Пусть K - некоторое подмножество функций из $P_2(n)$. Замыканием K называется множество всех булевых функций, представимых с помощью операций суперпозиции и замены переменных функций из множества K. Замыкание множества K обозначается через [K].
- В терминах замыкания можно дать другие определения замкнутости и полноты (эквивалентные исходным):
- K- замкнутый класс, если K = [K];
- K - полная система, если [K] = $P_2(n)$.

- **Примеры.**
- {0}, {1} - замкнутые классы.
- Множество функции одной переменной - замкнутый класс.
- $\{x, \overline{x}\}$ - замкнутый класс.
- Класс {1, x+y} не является замкнутым классом.

Замкнутые классы.

- **1. T_0** - класс функций, сохраняющих 0.

Обозначим через T_0 класс всех функций алгебры логики $f(x_1, x_2, \dots, x_n)$, сохраняющих константу 0, то есть функций, для которых $f(0, \dots, 0) = 0$.

$$T_0 = \{f(x_1,\ x_2,\ \dots\ ,\ x_n) \mid f(0,\dots,0) = 0\}$$

$0,\ x,\ xy,\ x \vee y,\ x+y \in T_0$;

$1, \bar{x} \notin T_0$. Из того, что $\bar{x} \notin T_0$ следует, например, что $\bar{x}$ нельзя выразить через дизъюнкцию и конъюнкцию.

- Поскольку таблица для функции f из класса T_0 в первой строке содержит фиксированное значение 0, то для функций из T_0 можно задавать произвольные значения только на $2^n - 1$ наборе значений переменных, то есть

$$\left|T_0^{(n)}\right| = 2^{2^n - 1} = \frac{1}{2}\left|P_2\right| ,$$

где $T_0^{(n)}$ - множество функций, сохраняющих 0 и зависящих от n переменных.

- Покажем, что T_0 - замкнутый класс. Так как $x \in T_0$, то для обоснования замкнутости достаточно показать замкнутость относительно операции суперпозиции, поскольку операция замены переменных есть частный случай суперпозиции с функцией x.

$$f(\widetilde{x}_m), f_1(\widetilde{x}_{k_1}),\dots, f_m(\widetilde{x}_{k_m}) \in T_0$$

$$\varphi = f(f_1,\dots,f_m) \in T_0$$

$$\varphi(0,\dots,0) = f(f_1(0,\dots0),\dots,f_m(0,\dots,0)) = f(0,\dots,0) = 0$$

2. T_1 - класс функций, сохраняющих 1.

- $f(1, \ldots, 1) = 1$

$$T_1 = \{f(x_1,\ x_2,\ \ldots\ ,\ x_n) \mid f(1,\ldots,1) = 1\}$$

$1, x, xy, x \vee y, x \equiv y \in T_1$;

$0, \quad \overline{x} \quad, x+y \notin T_1$

Из того, что $x + y \notin T_1$ следует, например, что $x + y$ нельзя выразить через дизъюнкцию и конъюнкцию.

- T_1 - замкнутый класс

$$\left|T_1^{(n)}\right| = 2^{2^n - 1} = \frac{1}{2}\left|P_2\right|$$

3. L - класс линейных функций.

$$L = \left\{ f(x_1, x_2, \dots, x_n) \;\middle|\; \begin{array}{l} f(x_1, x_2, \dots, x_n) = \\ = \alpha_0 + \alpha_1 x_1 + \dots + \alpha_n x_n;\ \alpha_i \in \{0,1\},\ i = 1, \dots, n \end{array} \right\}$$

$0,\ 1,\ x,\ x+y,\ x_1 \equiv x_2 = 1 + x_1 + x_2,$ $= x+1 \in L;$

$xy,\ x \vee y \notin L$.

- Докажем, что $x \vee y \notin L$.
- Предположим противное. Будем искать выражение для $x \vee y$ в виде линейной функции с неопределенными коэффициентами:

$$x \vee y = \alpha + \beta x + \gamma y$$

При $x = y = 0$ имеем $\alpha=0$,
при $x = 1$, $y = 0$ имеем $\beta = 1$,
при $x = 0$, $y = 1$ имеем $\gamma = 1$,
но тогда при $x = 1$, $y = 1$ имеем $1 \vee 1 \neq 1 + 1$, что доказывает нелинейность функции дизъюнкция $x \vee y$.
Доказательство замкнутости класса линейных функций очевидно.

- Поскольку линейная функция однозначно определяется заданием значений n+1 коэффициента α_0, ... , α_n , число линейных функций в классе L(n) функций, зависящих от n переменных равно 2n+1.

$$\left|L^{(n)}\right| = 2^{n+1}$$

4. **S** - класс самодвойственных функций.

- Функция $f^*(\widetilde{x}_n)$, определяемая равенством

$$f^*(\widetilde{x}_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n)$$

называется ***двойственной*** *к функции*

$f(\widetilde{x}_n)$

Таблица для двойственной функции (при стандартной упорядоченности наборов значений переменных) получается из таблицы для исходной функции инвертированием (то есть заменой 0 на 1 и 1 на 0) столбца значений функции и его переворачиванием.

$0^* = 1,$

$1^* = 0,$

$x^* = x,$

$\overline{x}^* = \overline{x}$

$(x_1 \vee x_2)^* = x_1 \wedge x_2,$
$(x_1 \wedge x_2)^* = x_1 \vee x_2.$

$\mathbf{(f^*)^* = f}$

функция f является двойственной к f*.

Теорема. Если функция ϕ получена как суперпозиция функций f, f_1, f_2, ... , f_m, то функция, двойственная к суперпозиции, есть суперпозиция двойственных функций.

$$\varphi(x_1,\ldots,x_n) = f(f_1(x_{11},\ldots,x_{1p_1}),\ldots,f_m(x_{m1},\ldots,x_{mp_m}))$$

$$\varphi^*(x_1,\ldots,x_n) = f^*(f_1^*(x_{11},\ldots,x_{1p_1}),\ldots,f_m^*(x_{m1},\ldots,x_{mp_m}))$$

- *Доказательство*.

$\varphi^*(x_1 ,..., x_n) = \square\ f(\square x_1 ,...,\square\ x_n) =$

$$\varphi^*(x_1,\ldots,x_n) = \overline{\varphi}(\bar{x}_1,\ldots,\bar{x}_n) =$$

$$= \bar{f}(f_1(\bar{x}_{11},\ldots,\bar{x}_{1p_1}),\ldots,f_m(\bar{x}_{m1},\ldots,\bar{x}_{mp_m})) =$$

$$= \bar{f}(\bar{\bar{f}}_1(\bar{x}_{11},\ldots,\bar{x}_{1p_1}),\ldots,\bar{\bar{f}}_m(\bar{x}_{m1},\ldots,\bar{x}_{mp_m})) =$$

$$= \bar{f}(\bar{f}_1^*(x_{11},\ldots,x_{1p_1}),\ldots,\bar{f}_m^*(x_{m1},\ldots,x_{mp_m})) =$$

$$= f^*(f_1^*(x_{11},\ldots,x_{1p_1}),\ldots,f_m^*(x_{m1},\ldots,x_{mp_m})).$$

- Обозначим через S класс всех самодвойственных функций из P_2:

$S = \{f \mid f^* = f\}$

$x, \quad \bar{x} \in S;$

$0,\ 1,\ xy,\ x \vee y \notin S.$

Для самодвойственной функции имеет место тождество

$$f(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n)$$

- На наборах $(\alpha_1,\ldots,\alpha_n)$ и $(\overline{\alpha}_1,\ldots,\overline{\alpha}_n)$, которые мы будем называть противоположными, самодвойственная функция принимает противоположные значения. Отсюда следует, что самодвойственная функция полностью определяется своими значениями на первой половине строк стандартной таблицы. Поэтому число самодвойственных функций в классе S(n) функций, зависящих от n переменных, равно:

$$\left|S^{(n)}\right| = 2^{2^{n-1}}$$

- Докажем теперь, что класс S замкнут. Так как $x \in S$, то для обоснования замкнутости достаточно показать замкнутость относительно операции суперпозиции, поскольку операция замены переменных есть частный случай суперпозиции с функцией x.

- Пусть $f(\widetilde{x}_m), f_1(x_{k_1}), \ldots, f_m(\widetilde{x}_{k_m}) \in S$. Тогда достаточно показать, что

$$\varphi = f(f_1, \ldots, f_m) \in S$$

Последнее устанавливается непосредственно:

$$\varphi^* = f^*(f_1^*, \ldots, f_m^*) = f(f_1, \ldots, f_m)$$

5. M - класс монотонных функций.

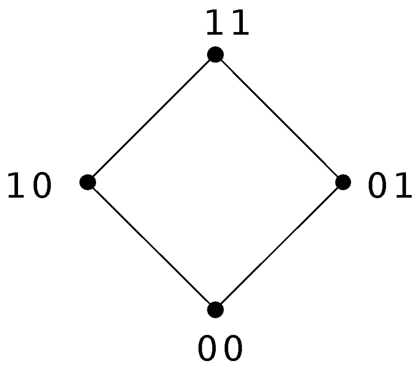
Набор $\widetilde{\alpha} = \widetilde{\alpha}_n = (\alpha_1, ..., \alpha_n)$ предшествует набору,

$\widetilde{\beta} = \widetilde{\beta}_n = (\beta_1, ..., \beta_n)$

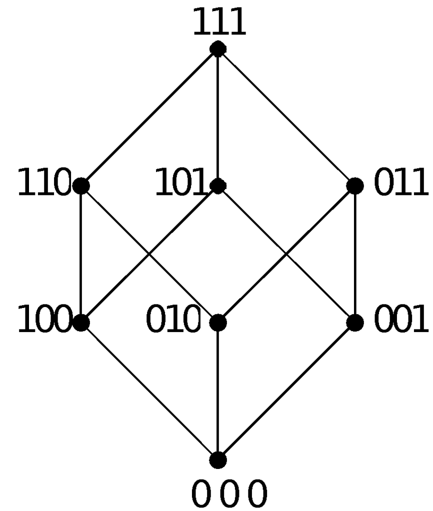
$$\widetilde{\alpha} \le \widetilde{\beta}$$

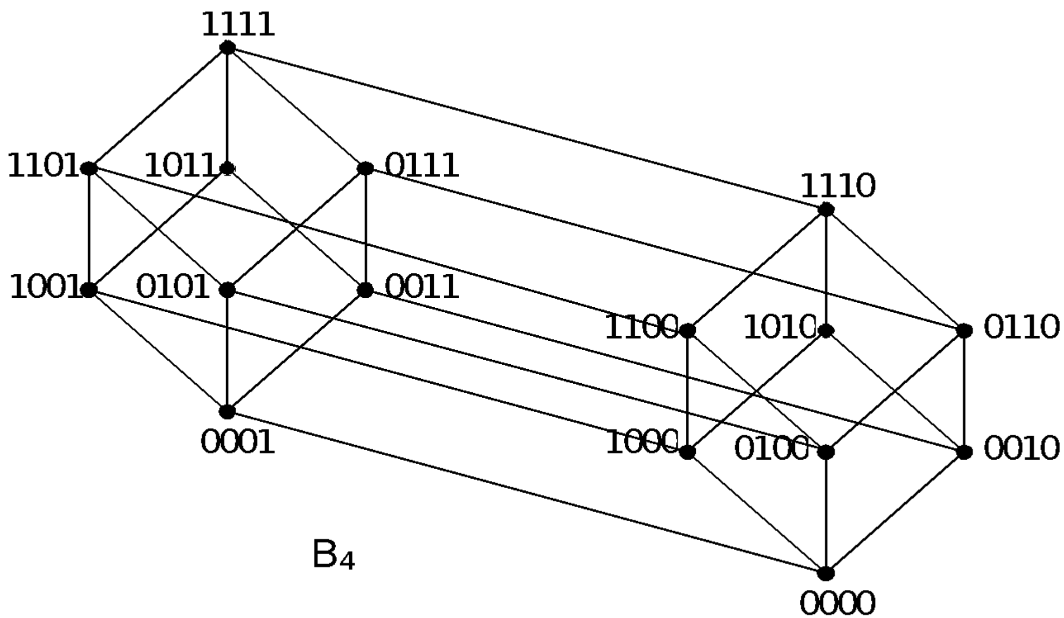
если $\alpha_i \le \beta_i$ для всех $i = 1, ..., n$.

Наборы α и β называются сравнимыми, если либо α≤β либо β≤α.В случае, когда ни одно из этих оотношений не выполняется, то наборы называются несравнимыми.


11
10
01
00

B_2


111
110
101
011
100
010
001
000


1111
1101
1011
0111
1110
1001
0101
0011
1100
1010
0110
1000
0100
0010
0001
0000

B_4

- Функция алгебры логики называется ***монотонной***, если для любых двух наборов $\tilde{\alpha}_n$ и $\tilde{\beta}_n$, таких, что , имеет место неравенство $f(\tilde{\alpha}_n) \leq f(\tilde{\beta}_n)$. Множество всех монотонных функций алгебры логики обозначается через M, а множество всех монотонных функций, зависящих от n переменных - через M(n).

- 0, 1, x, xy, $x \vee y \in M$;
- $x+y$, $x \rightarrow y$, $x \equiv y \notin M$.
- Покажем, что класс монотонных функций M - замкнутый класс. Так как $x \in M$, то для обоснования замкнутости достаточно показать замкнутость относительно операции суперпозиции, поскольку операция замены переменных есть частный случай суперпозиции с функцией x.

$$f(\widetilde{x}_m), f_1(\widetilde{x}_{k_1}), \dots, f_m(\widetilde{x}_{k_m}) \in M$$

$$\varphi = f(f_1, \dots, f_m) \in M$$

$$\widetilde{x} = \widetilde{x}_n = (x_1, \dots, x_n), \widetilde{x}_{k_1} = (x_{11}, \dots, x_{1k_1}), \dots, \widetilde{x}_{k_m} = (x_{m1}, \dots, x_{mk_m})$$

наборы переменных, соответственно, функций ϕ, f_1, ... , f_m , причем множество переменных функции ϕ состоит из тех и только тех переменных, которые встречаются у функций f_1, ... , f_m .