1 Булевы функции

Обозначим через B двухэлементное множество $\{0,1\}$. Тогда $B^n = \underbrace{B \times B \times \ldots \times B}_{n}$ — это множество всех *двоичных последовательностей (наборов, векторов)* длины n. *Булевой функцией от n переменных* называется любая функция $f(x_1, \ldots, x_n) : B^n \to B$. Каждый из ее аргументов $x_i,\ 1 \le i \le n,$ может принимать одно из двух значений 0 или 1 и значением функции на любом наборе из B^n также может быть 0 или 1. Обозначим через $\mathcal{P}_n$ множество всех булевых функций от n переменных. Нетрудно подсчитать их число.

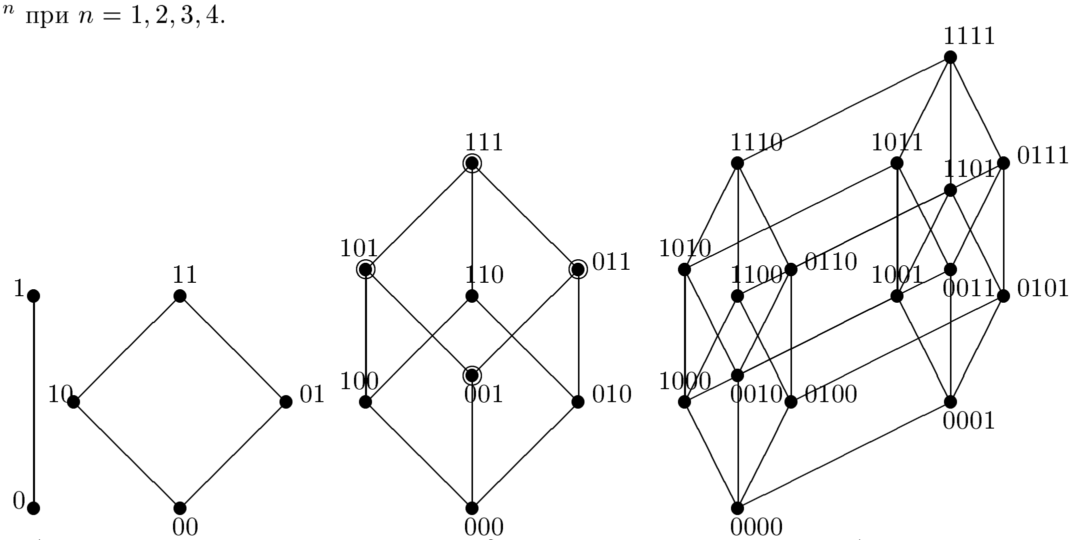
Теорема 1. $|\mathcal{P}_n| = 2^{2^n}$.

*Доказательство.*Действительно, по теореме 1 из Введения число функций из k-элементного множества A в m-элементное множество B равно m^k. В нашем случае $B = \{0,1\}$, а $A = B^n$. Тогда $m = 2$ и $k = |B^n| = 2^n$. Отсюда следует утверждение теоремы.
□

Имеется несколько различных представлений и интерпретаций булевых функций.

1.1 Геометрическое представление

B^n можно рассматривать как *единичный n-мерный куб* . Каждый набор из нулей и единиц длины n задает *вершину* этого куба. На следующем рисунке представлены единичные кубы B^n при $n = 1, 2, 3, 4$.



$\mathbf{B}^1$ $\mathbf{B}^2$ $\mathbf{B}^3$ $\mathbf{B}^4$

При этом существует естественное взимнооднозначное соответствие между подмножествами вершин n-мерных единичных кубов и булевыми функциями от n переменных: подмножеству $A \subseteq B^n$ соответствует его *характеристическая* функция

$$f_A(x_1, \ldots, x_n) = \begin{cases} 1 & \text{при } (x_1, \ldots, x_n) \in A \\ 0 & \text{в противном случае.} \end{cases}$$

Например, верхней грани куба B^3 (ее вершины выделены на рисунке) соответствует функция f: $f(0,0,1) = f(0,1,1) = f(1,0,1) = f(1,1,1) = 1$ и $f(0,0,0) = f(0,1,0) = f(1,0,0) = f(1,1,0) = 0$. Очевидно, что указанное соответствие действительно взаимнооднозначное: каждая булевая функция f от n переменных задает подмножество $A_f = \{(x_1, \ldots, x_n) \mid f(x_1, \ldots, x_n) = 1\}$ вершин B^n. Например, функция, тождественно равная 0, задает пустое множество $\emptyset \subset B^n$, а функция, тождественно равная 1, задает множество всех вершин B^n.

Задача 1. *Какие подмножества вершин B^4 соответствуют следующим булевым функциям:*
а) $f_1(x_1, x_2, x_3, x_4) = 1 \Leftrightarrow\ x_1 = 0$;
б) $f_1(x_1, x_2, x_3, x_4) = 1 \Leftrightarrow\ x_4 = 1$;
в) $f_1(x_1, x_2, x_3, x_4) = 1 \Leftrightarrow\ x_1 + x_2 \ge x_3 + x_4$;
г) $f_1(x_1, x_2, x_3, x_4) = 1 \Leftrightarrow\ x_1x_2x_3x_4 = 0$ *или* $x_1x_2x_3x_4 = 1$.

1.2 Табличное представление

Булевы функции от небольшого числа аргументов удобно представлять с помощью таблиц. Таблица для функции $f(x_1, \ldots, x_n)$ имеет $n+1$ столбец. В первых n столбцах указываются значения аргументов $x_1, \ldots, x_n$, а в $(n+1)$-ом столбце значение функции на этих аргументах — $f(x_1, \ldots x_{n-1}, x_n)$.

Таблица 1: Табличное представление функции $f(x_1, \ldots, x_n)$

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

Наборы аргументов в строках обычно располагаются в *лексикографическом* порядке:
$(\alpha_1, \ldots, \alpha_n) \prec (\beta_1, \ldots, \beta_n) \Leftrightarrow$ существует такое $i \in [1, n]$, что при $j < i$ $\alpha_j = \beta_j$, а $a_i < \beta_i$.
Если эти наборы рассматривать как записи чисел в двоичной системе счисления, то 1-ая строка представляет число 0, 2-ая — 1, 3-я — 2, ... , а последняя — $2^n - 1$.

При больших n табличное представление становится громоздким, например, для функции от 10 переменных потребуется таблица с 1024 строками. Но для малых n оно достаточно наглядно. Представим в виде таблицы все булевы функции от 1-ой переменной.

Таблица 2: Булевы функции от 1-ой переменной

x_1	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0

В этой таблице представлены следующие функции:

1. $f_1(x_1) = 0$ — константа 0;
2. $f_2(x_1) = 1$ — константа 1;
3. $f_3(x_1) = x_1$ — тождественная функция;
4. $f_4(x_1) = \neg x_1$ — отрицание x_1 (используется также обозначение $\overline{x}_1$, а в языках программирования эта функция часто обозначается как NOT).

Таблица 3: Булевы функции от 2-х переменной

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	1	0	1	0	1	0	0	1	0	1	1	1	0	0	1
0	1	0	1	0	1	1	0	0	1	1	1	0	1	0	1	0	0
1	0	0	1	1	0	0	1	0	1	0	1	0	1	0	0	1	1
1	1	0	1	1	0	1	0	1	1	1	0	1	0	0	0	0	1

Многие из этих функций часто используются в качестве "элементарных"и имеют собственные обозначения.

1. $f_1(x_1, x_2) = 0$ — константа 0;
2. $f_2(x_1, x_2) = 1$ — константа 1;

3. $f_3(x_1, x_2) = x_1$ — функция, равная 1-му аргументу ;

4. $f_4(x_1, x_2) = \neg x_1$ — отрицание x_1;

5. $f_5(x_1, x_2) = x_2$ — функция, равная 2-му аргументу ;

6. $f_6(x_1, x_2) = \neg x_2$ — отрицание x_2;

7. $f_7(x_1, x_2) = (x_1 \wedge x_2)$ — *конъюнкция*, читается "x_1 и x_2"(используются также обозначения: $(x_1 \& x_2)$, $(x_1 x_2)$, $\min(x_1, x_2)$, $(x_1 \text{ AND } x_2)$);

8. $f_8(x_1, x_2) = (x_1 \vee x_2)$ — *дизъюнкция*, читается "x_1 или x_2"(используются также обозначения: $(x_1 + x_2)$, $\max(x_1 x_2)$, $(x_1 \text{ OR } x_2)$);

9. $f_9(x_1, x_2) = (x_1 \rightarrow x_2)$ — *импликация*, читается "x_1 влечет x_2"или "из x_1 следует x_2"(используются также обозначения: $(x_1 \supset x_2)$, (IF x_1 THEN x_2));

10. $f_{10}(x_1, x_2) = (x_1 + x_2)$ — *сложение по модулю 2*, читается "x_1 плюс x_2"(используется также обозначение: $(x_1 \oplus x_2)$);

11. $f_{11}(x_1, x_2) = (x_1 \sim x_2)$ — *эквивалентность*, читается "x_1 эквивалентно (равносильно) x_2" (используется также обозначение: $(x_1 \equiv x_2)$);

12. $f_{12}(x_1, x_2) = (x_1 | x_2)$ — *штрих Шеффера* (антиконъюнкция), иногда читается как "не x_1 и x_2";

13. $f_{13}(x_1, x_2) = (x_1 \downarrow x_2)$ — *стрелка Пирса* (антидизъюнкция), иногда читается как "не x_1 или x_2".

В качестве элементарных функций будем также рассматривать 0-местные функции-константы 0 и 1.

Отметим, что функции $f_1(x_1, x_2)$ и $f_2(x_1, x_2)$ фактически не зависят от значений обоих аргументов, функции $f_3(x_1, x_2)$ и $f_4(x_1, x_2)$ не зависят от значений аргумента x_2, а функции $f_5(x_1, x_2)$ и $f_6(x_1, x_2)$ не зависят от значений аргумента x_1. Скажем, что функция $f(x_1, \ldots, x_i, \ldots, x_n)$ *не зависит от аргумента* x_i, если для любого набора значений $\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n$ остальных аргументов f имеет место равенство $f(\sigma_1, \ldots, \sigma_{i-1}, 0, \sigma_{i+1}, \ldots, \sigma_n) = f(\sigma_1, \ldots, \sigma_{i-1}, 1, \sigma_{i+1}, \ldots, \sigma_n)$. Такие аргументы называются *фиктивными*. Аргументы, не являющиеся фиктивными, называются *существенными*.

Определение 1. *Функции $f_1(x_1, \ldots, x_n)$ и $f_2(x_1, \ldots, x_m)$ называются равными, если функцию f_2 можно получить из функции f_1 путем добавления и удаления фиктивных аргументов.*

Например, равными являются одноместная функция $f_3(x_1)$ и двухместная функция $f_3(x_1, x_2)$, так как вторая получается из первой добавлением фиктивного аргумента x_2. Мы не будем различать равные функции и, как правило, будем использовать для обозначения равных функций одно и то же имя функции. В частности, это позволяет считать, что во всяком конечном множестве функций все функции зависят от одного и того же множества переменных.

1.3 Формулы

Как мы видели, геометрическое и табличное представления булевых функций подходят лишь для функций с небольшим числом аргументов. Формулы позволяют, удобно представлять многие функции от большего числа аргументов и оперировать различными представлениями одной и той же функции.

Пусть $\mathcal{B}$ — некоторое (конечное или бесконечное) множество булевых функций. Зафиксируем некоторое счетное множество переменных $V = \{X_1, X_2, \ldots\}$. Определим по индукции множество формул над $\mathcal{B}$ с переменными из V. Одновременно будем определять числовую характеристику $dep(\Phi)$ формулы Φ, называемую ее *глубиной* и множество ее *подформул*.

Определение 2.
а) Базис индукции. *Каждая переменная $X_i \in V$ и каждая константа $c \in \mathcal{B}$ является формулой глубины 0, т.е. $dep(X_i) = dep(c) = 0$. Множество ее подформул состоит из нее самой.*
б) Шаг индукции. *Пусть $f(x_1, \ldots, x_m) \in \mathcal{B}$ и $A_1, \ldots, A_m$ — формулы, и $\max\{dep(A_i) \mid i = 1, \ldots, m\} = k$. Тогда выражение $\Phi = f(A_1, \ldots, A_m)$ является формулой, ее глубина $dep(\Phi)$ равна $k + 1$, а множество подформул Φ включает саму формулу Φ и все подформулы формул $A_1, \ldots, A_m$.*

Каждой формуле $\Phi(X_1, \dots, X_n)$ сопоставим некоторую булеву функцию, которую эта формула задает, используя индукцию по глубине формулы.
Базис индукции. Пусть $dep(\Phi) = 0$ 0. Тогда $\Phi = X_i \in V$ или $\Phi = c \in \mathcal{B}$ В первом случае Φ задает функцию $f_\Phi(X_i) = X_i$, во втором —- функцию, тождественно равную c.
Шаг индукции. Пусть $dep(\Phi) = k + 1$. Тогда $\Phi(X_1, \dots, X_n) = f_i(A_1, \dots, A_m)$, где $f_i \in \mathcal{B}$ и $A_1, \dots, A_m$ — формулы, для которых $\max\{dep(A_i) \mid i = 1, \dots, m\} = k$. Предположим (по индукции), что этим формулам уже сопоставлены функции $g_1(X_1, \dots, X_n), \dots, g_m(X_1, \dots, X_n)$. Тогда формула Φ задает функцию $f_\Phi(X_1, \dots, X_n) = f_i(g_1(X_1, \dots, X_n), \dots, g_m(X_1, \dots, X_n))$.

Далее мы будем рассматривать формулы над множеством элементарных функций $\mathcal{B}_e = \{0, 1, \neg, \wedge, \vee, \to, +, \sim, \ |, \downarrow\}$. Все эти функции, кроме констант, называются *логическими связками или логическими операциями.* При этом для 2-местных функций из этого списка будем использовать *инфиксную запись*, в которой имя логической связки помещается между 1-ым и 2-ым аргументами. Тогда определение формулы имеет следующий вид.

Определение 3.
а) Базис индукции. *0, 1 и каждая переменная $X_i \in V$ являются формулами глубины 0.*
б) Шаг индукции. *Пусть Φ_1 и Φ_2 — формулы, $\circ \in \{\wedge, \vee, \to, +, \sim, \ |, \downarrow\}$. Тогда выражения $\neg\Phi_1$ и $(\Phi_1 \circ \Phi_2)$ являются формулами. При этом $dep(\neg\Phi_1) = (1 + dep(\Phi_1)$, а $dep((\Phi_1 \circ \Phi_2)) = 1 + \max\{dep(\Phi_1), dep(\Phi_2)\}$.*

В соответствии с этим определением выражения $\Phi_1(X_1, X_2) = \neg(X_1 \wedge \neg X_2)$ и $\Phi_2(X_1, X_2, X_3) = ((X_1 \vee \neg\neg X_2) \to (X_3 \sim (X_1 \ \downarrow \ \neg X_2)))$ являются формулами. Глубина Φ_1 равна 3, а глубина Φ_2 равна 4. Выражения же $\neg X_1 + (\neg X_2 \vee X_3)$, $(X_1 \neg \wedge X_2)$ и $(X_1 + X_2 + X_3)$ формулами не являются (*почему?*).

Для определения функции, задаваемой формулой, удобно использовать таблицу, строки которой сответствуют наборам значений переменных, а в столбце под знаком каждой логической связки стоят значения функции, задаваемой соответствующей подформулой. Например, для формулы Φ_2 функция f_{Φ_2} задается выделенным столбцом $\to$ следующей таблицы.

Таблица 4: Функция f_{Φ_2}

X_1	X_2	X_3	$((X_1$	$\vee$	$\neg$	$\neg$	$X_2)$	$\to$	$(X_3$	$\sim$	$(X_1$	$\downarrow$	$\neg$	$X_2)))$
0	0	0	0	0	0	1	0	1	0	1	0	0	1	0
0	0	1	0	0	0	1	0	1	1	0	0	0	1	0
0	1	0	0	1	1	0	1	0	0	0	0	1	0	1
0	1	1	0	1	1	0	1	1	1	1	0	1	0	1
1	0	0	1	1	0	1	0	1	0	1	1	0	1	0
1	0	1	1	1	0	1	0	0	1	0	1	0	1	0
1	1	0	1	1	1	0	1	1	0	1	1	0	0	1
1	1	1	1	1	1	0	1	0	1	0	1	0	0	1

Задача 2. *Построить таблицы значений для следующих булевых функций:*
а) $f_1(X_1, X_2, X_3) = 1 \ \Leftrightarrow \ X_1 + X_3 \geq X_2$;
б) $f_2(X_1, X_2, X_3) = 1 \ \Leftrightarrow$ *сумма* $(X_1 + X_2 + X_3)$ *четна;*
в) $f_3(X_1, X_2, X_3) = 0 \ \Leftrightarrow$ *значение* X_1 *совпадает со значением* X_2 *или со значением* X_3.

Задача 3. *Построить таблицы для функций, задаваемых следующими формулами:*
а) $\Psi_1 = ((X_1 \to \neg X_3) \vee (X_2 + X_3))$;
б) $\Psi_2 = (\neg(X_1 \mid X_2) \sim (\neg X_1 \wedge X_2))$;
в) $\Psi_3 = ((X_2 + \neg X_3) \wedge ((X_1 \vee X_2) \to (X_1 \sim \neg X_3)))$.

Задача 4. *Назовем два набора $\alpha = (\alpha_1, \dots, \alpha_n) \in B^n$ и $\beta = (\beta_1, \dots, \beta_n) \in B^n$* соседними, *если они находятся в соседних строках таблицы для функции от n переменных, т.е. представляют двоичные записи чисел i_α и i_β, для которых $|i_\alpha - i_\beta| = 1$.*

Найти число функций в $\mathcal{P}_n$, которые на любой паре соседних наборов принимают
а) одинаковые значения;
б) разные значения.

Задача 5. *Назовем два набора $\alpha = (\alpha_1, \dots, \alpha_n) \in B^n$ и $\beta = (\beta_1, \dots, \beta_n) \in B^n$* противоположными, *если для всякого i $\alpha_i = 1 \Leftrightarrow \beta_i = 0$ (и, следовательно, $\alpha_i = 0 \Leftrightarrow \beta_i = 1$).*

Найти число функций в $\mathcal{P}_n$, которые на любой паре противоположных наборов принимают разные значения.

Задача 6. *Пусть* $n = 2k$. *Назовем набор* $\alpha = (\alpha_1, \ldots, \alpha_n) \in B^n$ парным, *если для любого* $i = 1, \ldots, k$ $\alpha_i = \alpha_{2i}$, *т.е.* $\alpha = \alpha'\alpha'$ *для некоторого набора* α' *размера* k.

Найти число функций в $\mathcal{P}_n$, *которые на всех парных наборах принимают одинаковое значение.*

1.4 Булевы функции и логика высказываний

Булевы функции названы в честь английского математика XIX века Дж. Буля, который впервые применил алгебраические методы для решения логических задач. Часто их называют *функциями алгебры логики.* Каждую переменную можно рассматривать как некоторое элементарное высказывание, принимающее одно из двух значений: 1 (истина) и 0 (ложь). Сложным высказываниям сооответствуют формулы, построенные из элементарных высказываний с помощью логических связок. Вычисляя значения задаваемых ими функций, можно устанавливать зависимости истинностных значений сложных высказываний от значений входящих в них элементарных высказываний. Рассмотрим следующий пример.

Пример 1. *Пусть известно, что в дорожном проишествии участвовали три автомобиля с водителями:* A, B *и* C. *Свидетели проишествия дали следующие показания:*
1-ый свидетель: если A *виновен, то из остальных* B *и* C *хоть один не виновен;*
2-ой свидетель: если C *не виновен, то виновен кто-то один из пары* A, B *но не оба вместе;*
3-ий свидетель: в столкновении виновны не менее двух водителей.
Можно ли на основании этих показаний сделать вывод, что C *является виновником проишествия? Можно ли однозначно определить второго виновника?*

Для ответа на эти вопросы введем три переменных, соответствующих следующим высказываниям: X_1: “ виновен A ", X_2: “ виновен B "и X_3: “ виновен C ". Тогда показания 1-го свидетеля описываются формулой $\Phi_1 = (X_1 \to (\neg X_2 \vee \neg X_3))$, 2-го свидетеля — $\Phi_2 = (\neg X_3 \to ((X_1 \vee X_2) \wedge \neg(X_1 \wedge X_2)))$, 3-го свидетеля — $\Phi_3 = ((X_1 \wedge X_2) \vee ((X_1 \wedge X_3) \vee (X_2 \wedge X_3)))$. Показаниям всех трех свидетелей соответствует конъюнкция этих формул $\Psi = (\Phi_1 \wedge (\Phi_2 \wedge \Phi_3))$. Составим таблицы значений для функций f_{Φ_i} $(i = 1, 2, 3)$, а затем — для f_Ψ.

Таблица 5: Функция f_{Φ_1}

X_1	X_2	X_3	$(X_1$	$\to$	$(\neg$	X_2	$\vee$	$\neg$	$X_3))$
0	0	0	0	**1**	1	0	1	1	0
0	0	1	0	**1**	1	0	1	0	1
0	1	0	0	**1**	0	1	1	1	0
0	1	1	0	**1**	0	1	0	0	1
1	0	0	1	**1**	1	0	1	1	0
1	0	1	1	**1**	1	0	1	0	1
1	1	0	1	**1**	0	1	1	1	0
1	1	1	1	**0**	0	1	0	0	1

Таблица 6: Функция f_{Φ_2}

X_1	X_2	X_3	$(\neg$	X_3	$\to$	$((X_1$	$\vee$	$X_2)$	$\wedge$	$\neg$	$(X_1$	$\wedge$	$X_2)))$
0	0	0	1	0	**0**	0	0	0	0	1	0	0	0
0	0	1	0	1	**1**	0	0	0	0	1	0	0	0
0	1	0	1	0	**1**	0	1	1	1	1	0	0	1
0	1	1	0	1	**1**	0	1	1	1	1	0	0	1
1	0	0	1	0	**1**	1	1	0	1	1	1	0	0
1	0	1	0	1	**1**	1	1	0	1	1	1	0	0
1	1	0	1	0	**0**	1	1	1	0	0	1	1	1
1	1	1	0	1	**1**	1	1	1	0	0	1	1	1

Таблица 7: Функция f_{Φ_3}

X_1	X_2	X_3	$((X_1$	$\wedge$	$X_2)$	$\vee$	$((X_1$	$\wedge$	$X_3)$	$\vee$	$(X_2$	$\wedge$	$X_3)))$
0	0	0	0	0	0	**0**	0	0	0	0	0	0	0
0	0	1	0	0	0	**0**	0	0	1	0	0	0	1
0	1	0	0	0	1	**0**	0	0	0	0	1	0	0
0	1	1	0	0	1	**1**	0	0	1	1	1	1	1
1	0	0	1	0	0	**0**	1	0	0	0	0	0	0
1	0	1	1	0	0	**1**	1	1	1	1	0	0	1
1	1	0	1	1	1	**1**	1	0	0	0	1	0	0
1	1	1	1	1	1	**1**	1	1	1	1	1	1	1

Таблица 8: Функция f_{Ψ}

X_1	X_2	X_3	$(\Phi_1$	$\wedge$	$(\Phi_2$	$\wedge$	$\Phi_3))$
0	0	0	1	**0**	0	0	0
0	0	1	1	**0**	1	0	0
0	1	0	1	**0**	1	0	0
0	1	1	1	**1**	1	1	1
1	0	0	1	**0**	1	0	0
1	0	1	1	**1**	1	1	1
1	1	0	1	**0**	0	0	1
1	1	1	0	**0**	1	1	1

Из этой таблицы следует, что $f_{\Psi}(X_1, X_2, X_3) = 1$ на двух наборах: $(X_1 = 0, X_2 = 1, X_3 = 1)$ и $(X_1 = 1, X_2 = 0, X_3 = 1)$ (строки с этими наборами подчеркнуты). Поскольку в обоих случаях $X_3 = 1$, можно сделать вывод, что C является одним из виновников проишествия. Однозначно определить второго виновника полученная от свидетелей информация не позволяет, так как в одном случае им является A, а в другом — B.

Задача 7. *Администратор базы данных обнаружил, что одна или несколько из трех записей его базы: A, B и C ошибочна. Он установил, что*
а) если запись B корректна, то A ошибочна;
б) хотя бы одна запись из пары B, C корректна и хотя бы одна запись из пары A, C корректна;
в) если A ошибочна, то хотя одна из записей B, C корректна (но не обе вместе).
Опишите знания администратора в виде булевой формулы. Может ли он сделать вывод, что запись B ошибочна? Можно ли достоверно утверждать, что ошибочная запись единственна?

Задача 8. *Комитет состоит из пяти членов. Решения принимаются большинством голосов, однако, если председатель голосует "против", то решение не принимается. Постройте формулу, зависящую от 5 переменных X_1, X_2, X_3, X_4, Y ($X_i = 1 \Leftrightarrow$ i-ый член комитета голосует "за", $Y = 1 \Leftrightarrow$ председатель "за"), значение которой равно 1 тогда и только тогда, когда в результате голосования решение принимается.*