Часть VII

Решение булевых уравнений

Зачем нужно уметь решать булевы уравнения?

- Функциональная диагностика логических устройств
- Логически синтез дискретных устройств
- Логические модели объекта в распознавании и классификации (связь объект-признак-класс)

Разделы

Булева алгебра: определение

Определение

Булевой алгеброй $\mathcal{B}$ называется множество B, содержащее по крайней мере два элемента — o (нуль) и ι (единица), с заданными на нём бинарными операциями $\sqcup$ (объединения), $\sqcap$ (пересечения) и унарной операцией $'$ (дополнения).
При этом для любых $x, y, z \in B$ выполняются следующие законы (аксиомы) булевой алгебры:

$$Com\sqcup: \quad x \sqcup y = y \sqcup x, \qquad Com\sqcap: \quad x \sqcap y = y \sqcap x,$$
$$Dtr1: \quad (x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z),$$
$$Dtr2: \quad (x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z),$$
$$\sqcup o: \quad x \sqcup o = x, \qquad \sqcap \iota: \quad x \sqcap \iota = x,$$
$$Cmp': \quad x \sqcup x' = \iota, \qquad Isl': \quad x \sqcap x' = o,$$
$$Inv': \quad (x')' = x,$$
$$\iota': \quad \iota' = o, \qquad o': \quad o' = \iota,$$

Булева алгебра: определение...

Определение (продолжение)

$$
\begin{array}{rlrl}
DeM1: & (x \sqcup y)' = x' \sqcap y', & DeM2: & (x \sqcap y)' = x' \sqcup y', \\
\sqcup\iota: & x \sqcup \iota = \iota, & \sqcap o: & x \sqcap o = o, \\
Ass\sqcup: & x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z, & & \\
Ass\sqcap: & x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z, & & \\
Id\sqcup: & x \sqcup x = x, & Id\sqcap: & x \sqcap x = x, \\
Abs1: & x \sqcap (x \sqcup y) = x, & Abs2: & x \sqcup (x \sqcap y) = x.
\end{array}
$$

Множество B называется носителем булевой алгебры $\mathcal{B}$, а o и ι — *выделенными элементами* или универсальными гранями.

Введённые операции называют абстрактными, поскольку ни они сами, ни носитель, на котором они определены, никак не конкретизируются.

В приложениях элементы булевой алгебры интерпретируются как подмножества некоторых множеств, события, высказывания, сигналы и др.

Основные соотношения в булевой алгебре

Лемма. (основные свойства элементов булевой алгебры)
Для любых элементов x *и* y *булевой алгебры справедливы следующие утверждения:*

1) $x \sqcup y = o \Leftrightarrow x = y = o$ *и* $x \sqcap y = \iota \Leftrightarrow x = y = \iota$;

2) *следующие четыре соотношения эквивалентны —*
$$x \sqcap y = x\,, \quad x \sqcup y = y\,, \quad x' \sqcup y = \iota\,, \quad x \sqcap y' = o;$$

3) *лемма о единственности дополнения —*
$$\begin{cases} x \sqcap y = o \\ x \sqcup y = \iota \end{cases} \Leftrightarrow y = x'$$

Принцип двойственности для булевой алгебры

Пусть V — выражение или равенство булевой алгебры.

Обозначения для результата одновременной замены всех символов в V:

$V^\sharp$ — $\sqcap \leftrightarrow \sqcup$ и $\iota \leftrightarrow o$;

$V^\flat$ — $x \leftrightarrow x'$, где x — элемент носителя, не являющийся универсальной гранью;

V^* — когда производятся обе указанные замены.

Принцип двойственности

Если V —

— булево равенство, истинное для любых входящих в него элементов, то равенства $V^\sharp$, $V^\flat$ и V^* также истинны.

— выражение булевой алгебры, то $V^* = V'$.

Системы аксиом для булевой алгебры

Приведённая системы из 21-ой аксиомы избыточна.

1. Пары аксиом Com, Dtr, вместе с $\sqcup o$, $\sqcap \iota$, Cmp' и Isl' (первые 8 из приведенных выше законов).
   Данная система не является независимой:
   например, каждый из законов $\sqcup o$ и $\sqcap \iota$ выводим из остальных семи.

2. Пары законов законов Dtr, Abs вместе с Cmp' и Isl'.
   Это единственная кратчайшая (6 аксиом) известная на сегодняшний день безызбыточная самодвойственная система аксиом булевой алгебры.

3. $Com\sqcup$, $Ass\sqcup$ и уравнение Роббинса:
   $$((x \sqcup y)' \sqcup (x \sqcup y')')' = x.$$

Алгебры множеств: определение

- $A \neq \varnothing$ — множество, $\mathcal{P}(A)$ — множество всех подмножеств (булеан) A;
- $\mathcal{S}(A)$ — некоторая совокупность подмножеств A, устойчивая относительно объединения $\cup$, пересечения $\cap$ и дополнения до A $(^{-})$, а также содержащая $\varnothing$ и A.
- Понятно, что $\{\varnothing, A\} \subseteq \mathcal{S}(A) \subseteq \mathcal{P}(A)$.

АС $\langle \mathcal{S}(A), \underbrace{\cup, \cap, {}^{-}, \varnothing, A}_{\text{сигнатура}} \rangle$ — алгебра множеств.

Алгебра множеств с носителем $\mathcal{P}(A)$ — тотальная (над A), а с двухэлементным носителем $\{\varnothing, A\}$ — тривиальная.

Утверждение.
Всякая алгебра множеств $\mathcal{S}(A)$ есть булева алгебра с нулём $\varnothing$ и единицей A.

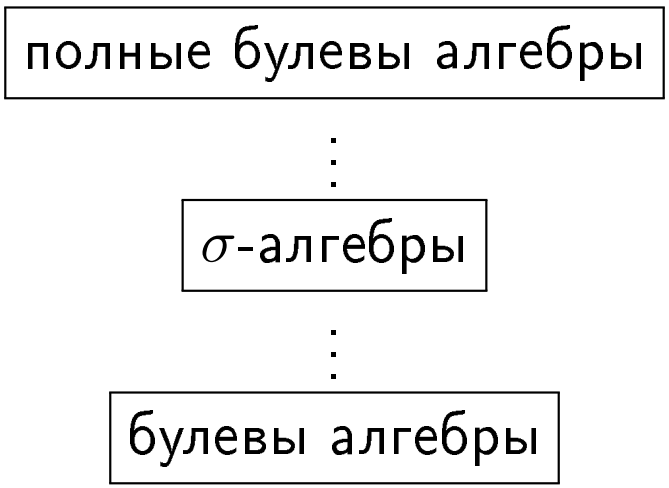
σ- и полные булевы алгебры

Пример (из аксиоматики теории вероятностей)

σ-алгебра подмножеств пространства элементарных событий есть алгебра множеств и, следовательно, булева алгебра.

Булева алгебра, в которой операции $\sqcup$ и $\sqcap$ определены для произвольной совокупности её элементов называется полной.

Любая алгебра множеств — полная



Булева алгебра отображений

Теорема

Пусть $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ *— булева алгебра и* A *— непустое множество. Тогда множество* B^A *всех отображений из* A *в* B *также будет булевой алгеброй относительно «поточечных» операций* $\dot{\sqcup}$, $\dot{\sqcap}$ *и* $\backprime$*:* $\quad (f\backprime)(x) = (f(x))'$

$$(f \mathbin{\dot{\sqcup}} g)(x) = f(x) \sqcup g(x), \quad (f \mathbin{\dot{\sqcap}} g)(x) = f(x) \sqcap g(x),$$

для любых $f, g \in B^A$*. Нулём и единицей* B^A *будут постоянные отображения* $f_0(x) \equiv o$ *и* $f_1(x) \equiv \iota$ *соответственно;* $x \in A$*.*

Доказательство.

Проверка аксиом булевой алгебры.

При $A = B^n$ получим булеву алгебру B^{B^n} всех функций из B^n в B, и если $B = \mathbf{2}$ — булеву алгебру $\mathbf{2}^{\mathbf{2}^n}$ всех булевых функций от n переменных.

Изоморфизм булевых алгебр: определение

Определение

Пусть даны две булевы алгебры B_1 и B_2 и биекция $\varphi\colon B_1 \to B_2$ такая, что равенства

$$\varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y)\,, \quad \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y)\,, \quad \varphi(x') = \varphi(x)'$$

справедливы для всех $x, y \in B_1$.
Тогда говорят, что φ — булев изоморфизм между B_1 и B_2, а данные алгебры булево изоморфны (символически $B_1 \cong_b B_2$).

Замечание

Из указанных равенств следует

$$\varphi(o) = o \text{ и } \varphi(\iota) = \iota :$$

Действительно:
$\varphi(o) = \varphi(x \sqcap x') = \varphi(x) \sqcap \varphi(x') = \varphi(x) \sqcap \varphi(x)' = o$ и аналогично для $\varphi(\iota)$.

Изоморфизм булевых алгебр: примеры

Пример

1. Тривиальная алгебра множеств, очевидно, изоморфна алгебре $\mathbf{2} = \langle \{0,1\}, \vee, \cdot, {}^{-}, 0, 1 \rangle$, которую будем называть алгеброй высказываний или алгеброй Буля (символ $\cdot$ в формулах будем, как правило, опускать, но иногда использовать вместо него символ $\&$).

2. Определим для булевой алгебры $\mathcal{B} = \langle B, \sqcup, \sqcap, {}', o, \iota \rangle$ двойственную к ней $\mathcal{B}^* = \langle B^*, \sqcup^*, \sqcap^*, {}'^*, o^*, \iota^* \rangle$, положив $B^* = B$, $\sqcup^* = \sqcap$, $\sqcap^* = \sqcup$, ${}'^* = {}'$, $o^* = \iota$, $\iota^* = o$. В силу принципа двойственности будем иметь $B^* \cong_b B$.

3. Тотальная алгебра над n-элементным множеством $A = \{a_1, \ldots, a_n\}$ изоморфна булевой алгебре n-мерных двоичных векторов $\mathbf{2}^n$.

Булевы подагебры. Теорема Стоуна о представлении

Если $\mathcal{B}$ — булева алгебра и B_1 такое подмножество её носителя, что все операции на B_1 являются сужениями операций на B, то B_1 — подалгебра B (символически $\mathcal{B}_1 \leqslant \mathcal{B}$).

Теорема (Стоун)
Всякая булева алгебра изоморфна подходящей алгебре множеств: для любой булевой алгебры $\mathcal{B}$ существует такое множество M, что $\mathcal{B} \hookrightarrow \mathcal{P}(M)$.

Теорема Стоуна утверждает, что $\mathcal{B} \cong_b \mathcal{B}_1 \leqslant \mathcal{P}(M)$.

Алгебраические кольца

Кольцом называется АС $\langle R, +, \cdot, 0 \rangle$, где R — множество, содержащее элемент нуль (0), на котором определены две бинарные операции сложение $(+)$ и умножение $(\cdot)$ такие, что для любых $x, y, z \in R$ справедливы соотношения

$$(x + y) + z = x + (y + z), \quad x + y = y + x,$$
$$x + 0 = x, \quad \forall x \, \exists y \colon (x + y = 0)$$

(указанное означает, что редукт $\langle R, +, 0 \rangle$ кольца есть абелева группа по сложению, или модуль) и

$$(x + y) \cdot z = x \cdot z + y \cdot z, \qquad x \cdot (y + z) = x \cdot y + x \cdot z,$$

(дистрибутивность умножения по отношению к сложению).

Алгебраические кольца: напоминание

Нуль кольца единственен.
Элемент y такой, что $x + y = 0$ называют обратным к x, его обозначение $(-x)$ в силу единственности.

Если умножение обладает свойством ассоциативности

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

и/или коммутативности

$$x \cdot y = x \cdot y,$$

то и кольцо называют соответствующе.

Если кольцо содержит единицу 1 — уникальный элемент, для которого

$$x \cdot 1 = 1 \cdot x = x,$$

то говорят о кольце с единицей (унитальном): $\langle R, +, \cdot, 0, 1 \rangle$.

Булевы кольца

Определение

Ассоциативное кольцо, обладающие свойством $x^2 = x$ для любого своего элемента называется булевым кольцом.

Теорема

Булево кольцо $\langle R, +, \cdot, 0 \rangle$ *коммутативно и* $-x = x$.

Теорема

Пусть $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ *— булева алгебра.*
Для любых $x, y \in B$ *положим*

$$x + y = (x \sqcap y') \sqcup (x' \sqcap y), \quad x \cdot y = x \sqcap y.$$

Тогда АС $\mathcal{B}^* = \langle B, +, \cdot, o, \iota \rangle$ *— булево кольцо с единицей* ι.

Основным примером булева кольца и является как раз кольцо $\langle \mathcal{P}(A), \oplus, \cap, \varnothing, A \rangle$.

От булева кольца к булевой алгебре

Теорема

Пусть $\mathcal{R} = \langle R, +, \cdot, 0, 1 \rangle$ *— булево кольцо с единицей.*
Для любых $x, y \in R$ *положим*

$$x \sqcup y = x + y + x \cdot y, \quad x \sqcap y = x \cdot y, \quad x' = x + 1.$$

Тогда АС $\mathcal{R}^* = \langle R, \sqcup, \sqcap, ', 0, 1 \rangle$ *— булева алгебра.*

Определение

АС $\langle B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \rangle$ такая, что $\langle B, \sqcup, \sqcap, ', o, \iota \rangle$ — булева алгебра, а отношение $\sqsubseteq$ задаются по правилу

$$x \sqsubseteq y \stackrel{\text{def}}{=} x \sqcap y = x \ (\text{или } x \sqsubseteq y \stackrel{\text{def}}{=} x \sqcup y = y)$$

называется булевой структурой.

Булева алгебра = дистрибутивная решётка с дополнениями и в ней справедлив модулярный закон

$$Mod: \ x \sqsubseteq y \ \Rightarrow \ x \sqcup (y \sqcap z) = y \sqcap (x \sqcup z)$$

Конусы и грани ч.у. множества

Определение

Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $A \subseteq P$.
Множества $A^{\triangle}$ и $A^{\triangledown}$ определяемые условиями

$$A^{\triangle} = \left\{ x \in P \mid \underset{A}{\forall} a \; (a \sqsubseteq x) \right\} \text{ и } A^{\triangledown} = \left\{ x \in P \mid \underset{A}{\forall} a \; (x \sqsubseteq a) \right\}$$

называются *верхним* и *нижним конусами множества* A,
а их элементы — *верхними* и *нижними гранями множества* A
соответственно.

Для одноэлементного множества $A = \{a\}$ используются обозначения $a^{\triangle}$ и $a^{\triangledown}$.

Понятно, например, что если $a \sqsubseteq b$, то $a^{\triangle} \cap b^{\triangledown} = [a, b]$.

Точные грани ч.у. множества: определение

Определение

Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $A \subseteq P$.
Если в $A^{\triangle}$ существует наименьший элемент, то он называется *точной верхней гранью множества* A и обозначается $\sup A$.
Если в $A^{\triangledown}$ существует наибольший элемент, то он называется *точной нижней гранью множества* A и обозначается $\inf A$.

Если $\sup A$ или $\inf A^{\triangle}$ существует, то $\sup A = \inf A^{\triangle}$ и двойственно,
если $\inf A$ или $\sup A^{\triangledown}$ существует, то $\inf A = \sup A^{\triangledown}$.

Разделы

Булевы многочлены: определение

Определение

Пусть $X_n = \{x_1, \ldots, x_n\}$ — n-элементное множество *неизвестных* или *переменных*.

Булевыми многочленами над X_n называют строки символов, удовлетворяющие следующим условиям:

1) $x_1, \ldots, x_n, 0, 1$ — булевы многочлены;
2) если p и q — булевы многочлены, то таковыми являются и $(p \sqcup q)$, $(p \sqcap q)$, (p').

Таким образом, булевы многочлены — формулы из переменных и констант 0 и 1 над множеством символов $\{\sqcup, \sqcap, '\}$.

Множество всех булевых многочленов над X_n обозначаем M_n.

Булевы многочлены: синтаксическое тождество

Запись $p = q$ (читается: данные многочлены равны) означает синтаксическое тождество многочленов p и q, т.е. они совпадают как строки символов.

Далее пользуемся известными правилами экономии скобок (опускаем внешние скобки, учитываем приоритет операций) и считаем, что многочлены равны, если они совпадают при восстановлении всех скобок.

Булев многочлен над n (далее $n \geqslant 1$) переменными можно рассматривать как многочлен над $n+1$ переменной, поэтому

$$M_1 \subset M_2 \subset \ldots \subset M_n \subset M_{n+1} \subset \ldots.$$

M_n не есть булева алгебра, т.к., например, $x_1 \sqcup x_2 \neq x_2 \sqcup x_1$.

Для отождествления подобных выражений введём понятие полиномиальной функции.

Полиномиальная функция булева многочлена

Определение

Пусть $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ — булева алгебра и p — булев многочлен из M_n.
Обозначим через $p_{\mathcal{B}}(b_1, \ldots, b_n)$ элемент из B, который получается из p заменами $x_i \mapsto b_i \in B,\ i = 1, \ldots, n,\ 0 \mapsto o$, $1 \mapsto \iota$. Тогда отображение

$$p_{\mathcal{B}} : B^n \to B$$

называется *полиномиальной функцией* (п.ф.), *индуцированной булевым многочленом* p *на* $\mathcal{B}$.

Пример. Пусть $p = x_1 \sqcup x_2$ и $\mathcal{B} = \mathbf{2}^3$ с носителем $\{0, a, b, c, ab, ac, bc, 1\}$.

Тогда

$p_{\mathcal{B}}(a, b) = a \vee b = ab;\ p_{\mathcal{B}}(a, 1) = a \vee 1 = 1;\ p_{\mathcal{B}}(a, ab) = a \vee ab = ab.$

Полиномиальная функция булева многочлена: пример

Разные булевы многочлены могут индуцировать одну и ту же полиномиальную функцию.

Пример (везде $n = 2$)

1. Пусть $p = x_1 \sqcup x_2$, $q = x_2 \sqcup x_1$ и $\mathcal{B} = \mathbf{2}$. Тогда $p \neq q$, $p_{\mathcal{B}} = a \vee b$, $q_{\mathcal{B}} = b \vee a$, $a, b \in \{0, 1\}$, т.е. $p_{\mathcal{B}} = q_{\mathcal{B}}$, поскольку при любой замене в этих выражениях букв a и b элементами $\{0, 1\} = \mathbf{2}$ получим один и тот же элемент.

2. Пусть $p = (x_1 \sqcup x_2)'$, $q = x_1' \sqcap x_2'$ и $\mathcal{B} = \mathcal{P}(A)$, $A \neq \varnothing$. Тогда опять
$$p \neq q, \text{ и } p_{\mathcal{B}} = \overline{X \cup Y}, \quad q_{\mathcal{B}} = \overline{X} \cap \overline{Y},$$
где $X, Y \subseteq A$, и снова $p_{\mathcal{B}} = q_{\mathcal{B}}$.

Булевы многочлены: эквивалентность

Определение

Два булевых многочлена $p, q \in M_n$ называются *эквивалентными*, символически $p \sim q$, если равны их полиномиальные функции на $\mathbf{2}$: $p \sim q \Leftrightarrow p_{\mathbf{2}} = q_{\mathbf{2}}$.

$\sim$ — отношение эквивалентности на M_n (легко проверяется).

Пример (предыдущий, $n = 2$; $a, b \in \{0, 1\} = \mathbf{2}$)

1. Если $p = x_1 \sqcup x_2$, $q = x_2 \sqcup x_1$, то
$$p_{\mathbf{2}} = a \vee b = b \vee a = q_{\mathbf{2}} \text{ и } p \sim q.$$

2. Если $p = (x_1 \sqcup x_2)'$, $q = x_1' \sqcap x_2'$, то
$$p_{\mathbf{2}} = \overline{a \vee b} = \overline{a} \cdot \overline{b} = q_{\mathbf{2}} \text{ и снова } p \sim q.$$

Множество полиномиальных функций

Обозначим через $P_n(\mathcal{B}) = \{\, p_{\mathcal{B}} \mid p \in M_n \,\}$ множество полиномиальных функций, индуцированных всеми многочленами из M_n на $\mathcal{B}$.

Например, пусть $\mathcal{B} = \mathbf{2}^3 = \left\langle \{0,1\}^3, \vee, \cdot, {}^-, 0, 1 \right\rangle$.
Тогда $P_n(\mathbf{2}^3)$ — все функции, выражающиеся формулами от аргументов $x_1, \ldots, x_n$ над множеством связок $\{\, \vee, \cdot, {}^- \,\}$, причём каждый аргумент может принимать любое из 8 значений $\{0,1\}^3$.

Обозначим для булевой алгебры $\mathcal{B}$ с носителем B через $F_n(\mathcal{B})$ множество всех функций из B^n в B : $F_n(\mathcal{B}) \stackrel{\text{def}}{=} B^{B^n}$.
Ясно, что это есть булева алгебра и $|P_n(\mathcal{B})| \subset F_n(\mathcal{B})$.

Тогда, например, $\left|F_1(\mathbf{2}^3)\right| = 8^8 = 16\,777\,216$, а $P_1(\mathbf{2}^3) = \{\, [0]_\sim, [1]_\sim, [x]_\sim, [\bar{x}]_\sim \,\}$, т.е. $\left|P_1(\mathbf{2}^3)\right| = 4$.

Фактормножество п.ф. — булева алгебра

Теорема

Если $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ *— булева алгебра, то*

$$1.\ P_n(\mathcal{B}) \leqslant F_n(\mathcal{B}); \qquad 2.\ P_n(\mathcal{B})/\sim\ \cong_b\ P_n(\mathbf{2}).$$

Доказательство.

1. Убедимся в устойчивости множества функций $P_n(\mathcal{B})$ относительно операций $\sqcup, \sqcap, '$, а также в принадлежности ему постоянных функций $f_0 \equiv o$ и $f_1 \equiv \iota$.

Для $\sqcup$ и $b = (b_1, \ldots, b_n) \in B^n$ имеем

$$(p_{\mathcal{B}} \sqcup q_{\mathcal{B}})(b) = p_{\mathcal{B}}(b) \sqcup q_{\mathcal{B}}(b) = (p \sqcup q)_{\mathcal{B}}(b) \in P_n(\mathcal{B})$$

для произвольного $b \in B^n$ и аналогично для $\sqcap$ и $'$.

Кроме того, $p_{\mathcal{B}}(0) = o$, $p_{\mathcal{B}}(1) = \iota$.

Фактормножество п.ф. — булева алгебра...

Доказательство (продолжение)

2. Определим отображение $\varphi\colon P_n(\mathbf{2}) \to P_n(\mathbf{2})/\sim$, переводящее п.ф. $p_{\mathbf{2}}$ в класс эквивалентности $[p]_\sim \in P_n(\mathbf{2})/\sim$.

Данное определение корректно, т.к.

$$p_{\mathbf{2}} = q_{\mathbf{2}} \Rightarrow p \sim q \Rightarrow [p]_\sim = [q]_\sim.$$

Легко проверить, что φ и есть искомый булев изоморфизм.

С помощью теоремы Стоуна показывается, что полиномиальные функции, соответствующие эквивалентным многочленам, совпадают на любой булевой алгебре, а не только на $\mathbf{2}$, то есть справедлива

Теорема

Пусть $p, q \in M_n$ и $p \sim q$. Тогда для произвольной булевой алгебры $\mathcal{B}$ справедливо $p_{\mathcal{B}} = q_{\mathcal{B}}$.

Полиномиальная полнота алгебры Буля $\mathbf{2}$

Следствия

1. $F_n(\mathbf{2}) = P_2$ *и* $|P_n(\mathbf{2})/\sim| = 2^{2^n}$.
   Это означает, что любая булева функция (из $\mathbf{2}^n$ *в* $\mathbf{2}$*) является полиномальной функцией.*
   Поэтому говорят, что алгебра $\mathbf{2}$ *полиномиально полна.*

2. *Если* $\mathcal{B} \not\cong_b \mathbf{2}$ *и мощность носителя* $\mathcal{B}$ *есть* m *(в конченом случае* $m = 2^k$*), то*
   $$|P_n(\mathcal{B})| = |P_n(\mathcal{B})/\sim| = 2^{2^n} < m^{m^n} = |F_n(\mathcal{B})|,$$
   т.е. $P_n(\mathcal{B}) \subset F_n(\mathcal{B})$.
   Это означает, что $\mathbf{2}$ *— единственная полиномиально полная алгебра.*

Традиционное для дискретной математики обозначение $F_n(\mathbf{2}) = P_2$ или P_2^n.

Эквивалентные многочлены стандартного вида

Часто возникает потребность заменить данный многочлен эквивалентным ему более простым многочленом.

Для этого вводят т.н. нормальные формы многочленов: ДНФ, КНФ и, аналогично, АНФ (полиномы Жегалкина) для булева кольца соответствующей булевой алгебры.

Совокупность нормальных форм обеспечивает наличие системы представителей для каждого класса эквивалентности множества M_n.

Разложение Шеннона булевой функции $f(x) \in P_2$

$$f(x) = ax \vee b\overline{x} = f(1)x \vee f(0)x$$

Разделы

Булевы уравнения: определение

Будем решать «*булевы уравнения*» задаваемые полиномами.
Равенство $p = q$ говорит, что многочлены p и q идентичны.

Определение

Пару (p, q), где $p, q \in M_n$, назовём (булевым) уравнением.

Пусть $\mathcal{B}$ — булева алгебра с носителем B.
Элемент $(b_1, \ldots, b_n) \in B^n$ называется решением уравнения (p, q) в булевой алгебре $\mathcal{B}$, если

$$p_{\mathcal{B}}(b_1, \ldots, b_n) = q_{\mathcal{B}}(b_1, \ldots, b_n).$$

Множество $\{ (p_i, q_i) \mid i = \overline{1, m} \}$ образует систему уравнений.
Решением системы называют общее решение всех её уравнений.

Уравнение (p, q) допустимо записывать в виде $p = q$.

Например, $\overline{x}_1 x_2 \vee x_3 = x_1(x_2 \vee x_3)$ — уравнение в $\mathbf{2}$, а (101) — его решение, поскольку в $(\overline{1} \cdot 0) \vee 1 = 1 \cdot (0 \vee 1)$.

Преобразование уравнения $p = q$ к виду $r = 0$

Теорема (о преобразовании булевых уравнений)
Уравнения $p = q$ *и* $(p \sqcap q') \sqcup (p' \sqcap q) = 0$, *где* p *и* q — *булевы многочлены, имеют одни и те же решения.*

Доказательство.
Пусть $p, q \in M_n$, $\mathcal{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ — булева алгебра и $(b_1, \ldots, b_n) \in B^n$.
Положим $a = p_{\mathcal{B}}(b_1, \ldots, b_n)$ и $b = q_{\mathcal{B}}(b_1, \ldots, b_n)$. Тогда

$$a = b \Rightarrow (a \sqcap b') \sqcup (a' \sqcap b) = (a \sqcap a') \sqcup (a' \sqcap a) = o \sqcup o = o,$$

и

$$(a \sqcap b') \sqcup (a' \sqcap b) = o \Leftrightarrow \begin{cases} a \sqcap b' = o \\ a' \sqcap b = o \end{cases} \overset{DeM1}{\Longleftrightarrow} \begin{cases} a \sqcap b' = o \\ a \sqcup b' = \iota \end{cases} \Leftrightarrow$$

$$\Leftrightarrow a = b'' \Leftrightarrow a = b\,.$$

Преобразование уравнения $p = q$ к виду $r = 0$

Следствия

1. *Уравнения* $p = q$ *и* $(p \sqcap q) \sqcup (p' \sqcap q') = 0$ *имеют одни и те же решения в любой булевой алгебре.*
   Уравнение будем, как правило, сразу записывать в сигнатуре указанной булевой алгебры и считать переменные $x_1, \ldots$ *её элементами.*
2. *Любое булево уравнение (или систему), заданную в алгебре логики* $\mathbf{2}$ *можно привести к эквивалентным видам* $p = 0$ *и* $q = 1$, *где* p, q *— ДНФ и/или КНФ.*
   Справедливость утверждения следует из полиномиальной полноты алгебры $\mathbf{2}$.
3. *Система* $\left\{ (p_i, q_i) \mid i = \overline{1, m} \right\}$ *эквивалентна одному уравнению*
$$p_1 q_1' \vee p_1' q_1 \vee p_2 q_2' \vee p_2' q_2 \vee \ldots \vee p_m q_m' \vee p_m' q_m = 0.$$

Решение булевых уравнений: примеры

① Решим булево уравнение $x_1 = x_2$ в $\mathbf{2}$.

Преобразуем уравнение

$$x_1 = x_2 \Leftrightarrow (x_1\overline{x}_2) \vee (\overline{x}_1 x_2) = 0 \Leftrightarrow$$
$$\Leftrightarrow (x_1 \vee \overline{x}_1) \cdot (x_1 \vee x_2) \cdot (\overline{x}_1 \vee \overline{x}_2) \cdot (x_2 \vee \overline{x}_2) \Leftrightarrow$$
$$\Leftrightarrow (x_1 \vee x_2) \cdot (\overline{x}_1 \vee \overline{x}_2) = 0.$$

В $\mathbf{2}$ это эквивалентно условиям

$$\left[\begin{array}{l} x_1 \vee x_2 = 0, \\ x'_1 \vee x'_2 = 0, \end{array}\right. \quad \text{откуда} \quad \left[\begin{array}{l} x_1 = x_2 = 0, \\ x_1 = x_2 = 1. \end{array}\right.$$

Т.о. решениями исходного уравнения будут наборы (00) и (11) из $\mathbf{2}^2$.

Решение булевых уравнений: примеры

② Решим булево уравнение $x_1 \cdot x_2 = x_3$ в $\mathbf{2}$.

Преобразуем уравнение

$$x_1 \cdot x_2 = x_3 \Rightarrow (\overline{x}_1 \vee x_2 \vee x_3)(x_1 \vee \overline{x}_2 \vee x_3)(\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3) = 0$$

Отсюда получаем искомые решения: (000), (010), (100), (111).

Замечание: получение для данной формулы эквивалентной КНФ, вообще говоря, сопряжено со столь значительными вычислительными трудностями, что может оказаться практически невозможным.

Решение булевых уравнений: примеры...

③ Решить заданную в $\mathbf{2}$ систему БУ

$$\{\,(x_1x_2,\, x_1x_3 \vee x_2),\, (x_1 \vee \overline{x}_2,\, x_3)\,\}.$$

Перепишем систему в привычном виде

$$\begin{cases} x_1x_2 & = x_1x_3 \vee x_2, \\ x_1 \vee \overline{x}_2 & = x_3. \end{cases}$$

По теореме о преобразовании булевых уравнений эта система эквивалентна единственному уравнению

$$x_1x_2\overline{(x_1x_3 \vee x_2)} \vee \overline{(x_1x_2)}(x_1x_3 \vee x_2) \vee (x_1 \vee \overline{x}_2)\overline{x}_3 \vee \overline{(x_1 \vee \overline{x}_2)}x_3 = 0.$$

Преобразуя левую часть в СКНФ, получим эквивалентное заданной системе уравнение

$$(x_1 \vee x_2 \vee \overline{x}_3)(\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3) = 0,$$

т.е. решениями системы будут наборы (001) и (111) из $\mathbf{2}^3$.

Важное замечание

Когда решение ищется не в простейшей алгебре $\mathbf{2}$, а в произвольной булевой алгебре, следование

$$D_1 \sqcap \ldots \sqcap D_l = o \;\Rightarrow\; \left[\begin{array}{l} D_1 = o, \\ \ldots \\ D_l = o \end{array}\right.$$

не имеет места.

Поэтому, например, в произвольной булевой алгебре $\mathcal{B} = \langle\, B, \sqcup, \sqcap, ', o, \iota \,\rangle$ решением уравнения

$$x_1 \sqcap x_2 = o$$

будет $(\, b, (b')^{\triangledown} \,) \in B^2$ и для $\mathcal{B} = \mathbf{2}^3$ подходит пара ненулевых элементов

$$(\,(100), (010)\,) \in (\mathbf{2}^3)^2.$$

Разделы

Параметры БУ

Далее нас будет интересовать зависимость значений одних неизвестных решения БУ от других.

- Пусть (p, q) — уравнение в булевой алгебре $\mathcal{B}$ и $p, q \in M_{n+m},\ n, m \geqslant 0,\ n + m \geqslant 1.$
- Множество неизвестных с индексами $m, m + 1, \ldots, n + m$ назовём параметрами.
- Элементы носителя $\mathcal{B}$, соответствующие аргументам-параметрам полиномиальных функций $p_{\mathcal{B}}$ и $q_{\mathcal{B}}$ будем обозначать символами a, b, ...
- Формулу вида $p_{\mathcal{B}}(x_1, \ldots, x_n, a, \ldots) = q_{\mathcal{B}}(x_1, \ldots, x_n, a, \ldots)$ будем называть булевым уравнением с параметрами и n неизвестными (в алгебре $\mathcal{B}$).

Алгоритм решения БУ с одним неизвестным

Пусть дано БУ $p = q$ с одним неизвестным x в булевой структуре $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \rangle$.

Алгоритм 1

Шаг ① Приводим уравнение $p = q$ к равносильному с o в правой части: $r = 0$.

Шаг ② Приводим уравнение $r = 0$ к равносильному уравнению вида

$$(a \sqcap x) \sqcup (b \sqcap x') = o,$$

где элементы B a и b — параметры.

Алгоритм решения БУ с одним неизвестным...

Шаг ③ Заменяем полученное уравнение на эквивалентную систему

$$\begin{cases} a \sqcap x = o, \\ b \sqcap x' = o. \end{cases}$$

Шаг ④ Если $b \not\sqsubseteq a'$, то исходное уравнение решений не имеет.

Иначе $\boxed{b \sqsubseteq a' \Leftrightarrow a \sqcap b = o}$ — *условие разрешимости уравнения* и его решение — любой элемент x из B такой, что

$b \sqsubseteq x \sqsubseteq a'$ — решение в *интервальной форме* $\left(\Leftrightarrow x \in b^{\triangle} \cap (a')^{\triangledown}\right)$

или

$x = (b \sqcup u) \sqcap a' = (a' \sqcap u) \sqcup b$, u — произвольный элемент B

— решение в *функциональной форме* $(=$

$= (a' \sqcap u) \sqcup (b \sqcap u')$ — *симметричная функциональной форма*$)$.

Основная теорема о решении булевых уравнений

Теорема (основная о решении булевых уравнений)
Результатом выполнения Алгоритма 1 является решение булева уравнения относительно единственного неизвестного.

Доказательство.
Проведём обоснование шагов алгоритма.

Шаг ① Основанием для равносильной замены $p = q \Rightarrow r = 0$ служит теорема о преобразовании булевых уравнений.

Шаг ② Приведение уравнения вида $r = 0$ к равносильному $(a \sqcap x) \sqcup (b \sqcap x') = o$ основано на разложении Шеннона по переменной x.

Выражение последнего вида назовём канонической формой булева уравнения.

Основная теорема о решении булевых уравнений...

Доказательство (продолжение)

Шаг ③ Замена уравнение в канонической форме на эквивалентную систему $a \sqcap x = o,\ b \sqcap x' = o$ основывается на лемме об основных свойствах элементов булевой алгебры.

Шаг ④ Обоснование:

1. Имеем $b \sqsubseteq x \sqsubseteq a'$,

$$a \sqcap x = o \Leftrightarrow (a \sqcap x) \sqcup a' = a' \Leftrightarrow (a \sqcup a') \sqcap (x \sqcup a') = a' \Leftrightarrow$$

$$\Leftrightarrow x \sqcup a' = a' \Leftrightarrow x \sqsubseteq a' \quad \text{и аналогично } b \sqcap x' = 0 \Leftrightarrow b \sqsubseteq x.$$

2. $b \sqsubseteq a' \Leftrightarrow b \sqcap a' = b \Leftrightarrow a \sqcap b = o$ — условие существования решения.

Основная теорема о решении булевых уравнений...

Доказательство (продолжение)

3. Справедливость формулы решения в функциональной форме следует из

$$\left\{\begin{array}{l} b \sqsubseteq x \\ x \sqsubseteq a' \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x = b \sqcup u \quad \text{для некоторого } u \in B \\ x \sqcap a' = x \end{array}\right. \Leftrightarrow$$

$$\Leftrightarrow \; x = (b \sqcup u) \sqcap a'.$$

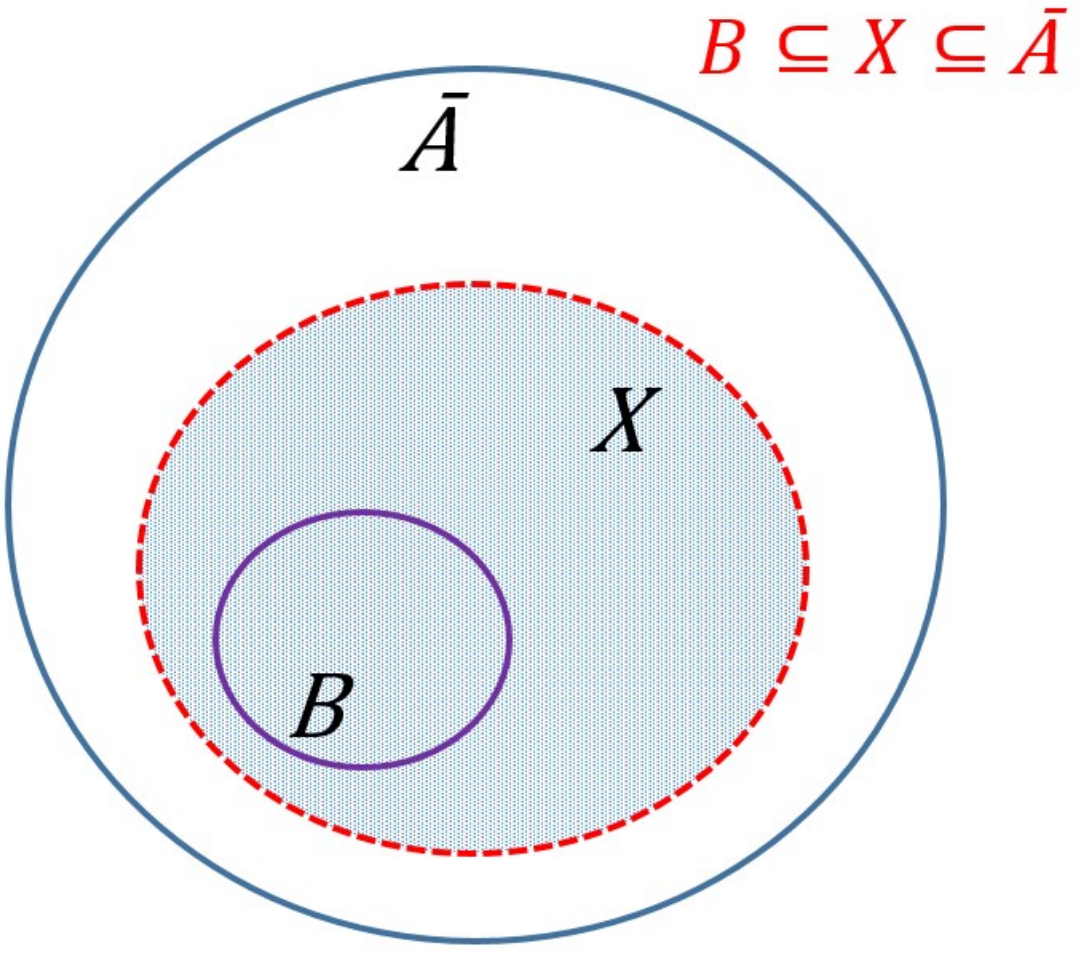
Равенство $x = (b \sqcup u) \sqcap a' = (a' \sqcap u) \sqcup b$ при $b \sqsubseteq a'$ выражает модулярный закон.

Симметричная функциональной форма:

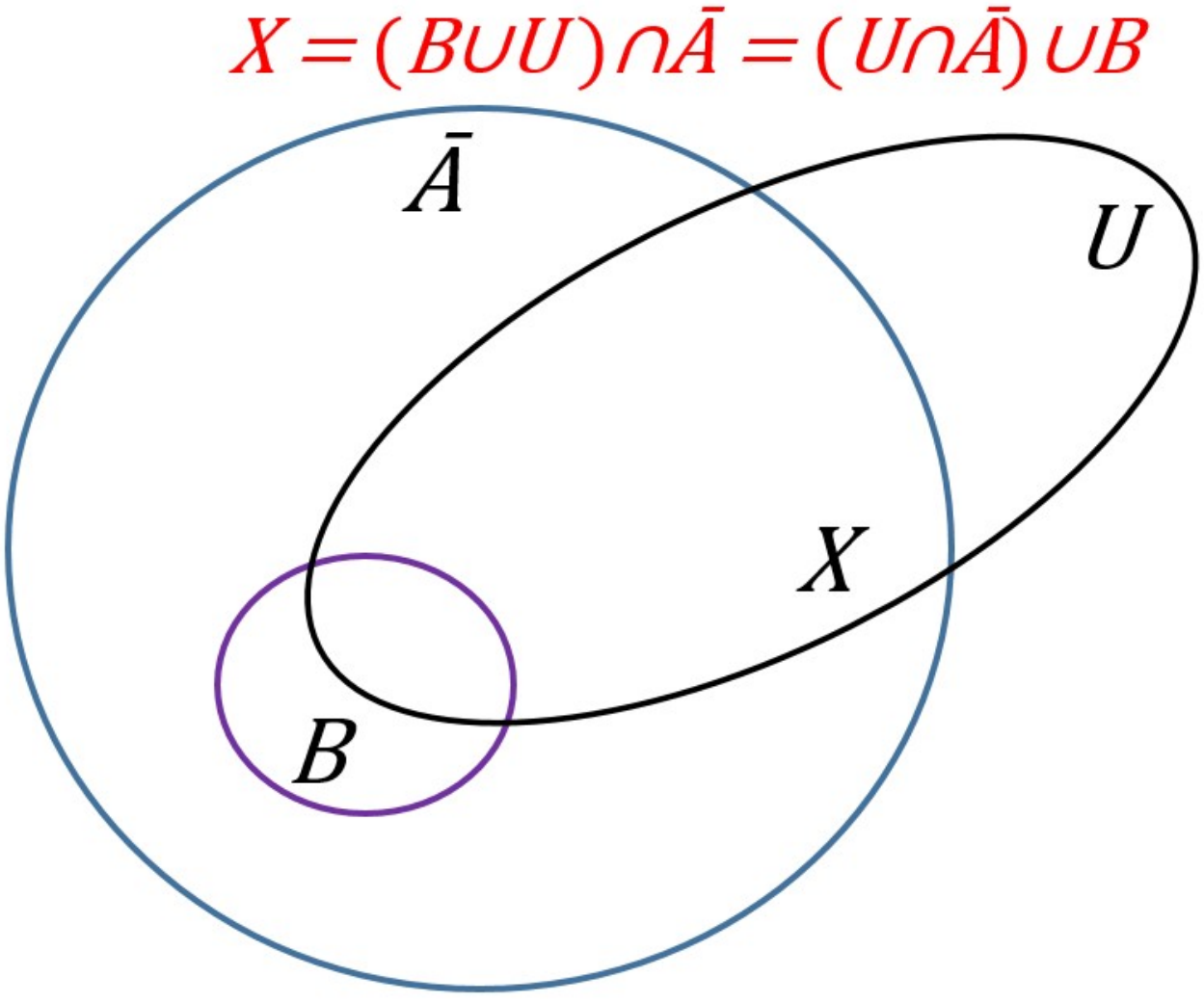
$$x = (a' \sqcap u) \sqcup b = (a' \sqcap u) \sqcup (b \sqcap (u \sqcup u') = (a' \sqcap u) \sqcup (b \sqcap u'),$$

поскольку $b \sqcap u' \sqsubseteq b \sqsubseteq a' \sqsubseteq x$.

Решение БУ $(A \cap X) \cup (B \cap \overline{X})$: диаграмма Венна



Решение БУ $(A \cap X) \cup (B \cap \overline{X})$: диаграмма Венна



Решение БУ $ax \vee b\overline{x}$ в $\mathbf{2}$

В частном случае $\mathcal{B} = \mathbf{2}$ по интервальной формуле получим решения:

a	b	x
0	0	$\{0,1\}$
0	1	1
1	0	0
1	1	$\varnothing$

Эти решения, естественно, совпадают с решениями по функциональной формуле, если положить $u = 0$ и $u = 1$:

$$b \leqslant \overline{a} \;\Rightarrow\; b \leqslant x \leqslant \overline{a} \;\Leftrightarrow\; \left[\begin{array}{l} x = \overline{a}, \\ x = b. \end{array}\right.$$

Решение БУ $\widetilde{\alpha} \cdot \widetilde{x} \vee \widetilde{\beta} \cdot \overline{\widetilde{x}}$ в $\mathbf{2}^n$

Если $B = \mathbf{2}^n$, то имеем многомерный вариант предыдущего случая:

- интервальная форма при $\widetilde{\beta} \preccurlyeq \overline{\widetilde{\alpha}}$ задаёт булев подкуб $\mathbf{2}^n$, натянутый на вершины $\widetilde{\beta}$ и $\overline{\widetilde{\alpha}}$ (при $\widetilde{\beta} \succcurlyeq \overline{\widetilde{\alpha}}$ решений нет);
- в функциональной форме $\widetilde{x} = (\widetilde{\beta} \vee \widetilde{\upsilon}) \cdot \overline{\widetilde{\alpha}}$ полагаем $\upsilon = (- \ldots -)$, операции $\vee$ и $\cdot$ применяем к векторам из $\mathbf{2}^n$ покомпонентно по правилам

  $$\widetilde{\alpha} \vee \widetilde{\beta} = \max\left\{\widetilde{\alpha}, \widetilde{\beta}\right\}, \quad \widetilde{\alpha} \cdot \widetilde{\beta} = \min\left\{\widetilde{\alpha}, \widetilde{\beta}\right\}, \quad 0 \leqslant - \leqslant 1,$$

  и в полученном векторе $\widetilde{x}$ символы $(-)$ заменяем на 0 и 1 всевозможными способами.

Например, если в $\mathbf{2}^4$ имеем $\widetilde{\alpha} = (0001)$ и $\widetilde{\beta} = (1000)$, то $\widetilde{x} = (1 - -0)$ и решениями исходного уравнения будет любой из векторов (1000), (1010), (1100), (1110).

Решение БУ с одним неизвестным: пример

Решим булево уравнение $x \sqcup c = d$ в произвольной булевой структуре $\mathcal{B} = \langle B, \sqcup, \sqcap, ', \sqsubseteq, o, \iota \rangle$.

Шаг ① $x \sqcup c = d \Leftrightarrow ((x \sqcup c)' \sqcap d) \sqcup ((x \sqcup c) \sqcap d') = o.$

Шаг ② $((x \sqcup c)' \sqcap d) \sqcup ((x \sqcup c) \sqcap d') =$

$= (x' \sqcap c' \sqcap d) \sqcup (x \sqcap d') \sqcup (c \sqcap d') =$

$= (x' \sqcap c' \sqcap d') \sqcup (x \sqcap d') \sqcup (x \sqcap c \sqcap d') \sqcup (x' \sqcap c \sqcap d') =$

$= (x \sqcap \underbrace{(d' \sqcup (c \sqcap d'))}_{d'}) \sqcup \big(x' \sqcap ((c' \sqcap d) \sqcup (c \sqcap d'))\big) = o.$

Шаг ③ Имеем

$$\begin{cases} d' \sqcap x = o, \\ ((c' \sqcap d) \sqcup (c \sqcap d')) \sqcap x' = o \end{cases}.$$

Решение БУ с одним неизвестным: пример...

Шаг ④ Исходное уравнение имеет решение, если и только если

$$(c' \sqcap d) \sqcup (c \sqcap d') \sqsubseteq d.$$

Покажем, что данное условие эквивалентно $c \sqsubseteq d$:

$$((c' \sqcap d) \sqcup (c \sqcap d')) \sqsubseteq d \Leftrightarrow (c' \sqcap d) \sqcup (c \sqcap d') \sqcup d = d \Leftrightarrow$$
$$\Leftrightarrow d \sqcup (c \sqcap d') = d \Leftrightarrow (d \sqcup (c \sqcap d')) \sqcap c = d \sqcap c \Leftrightarrow$$
$$\Leftrightarrow (c \sqcap d) \sqcup (c \sqcap d') = d \sqcap c \Leftrightarrow c = c \sqcap d \Leftrightarrow c \sqsubseteq d.$$

Общее решение исходного уравнения —

$$x = ((c' \sqcap d) \sqcup (c \sqcap d') \sqcup u) \sqcap d = (c' \sqcap d) \sqcup (u \sqcap d) = d \sqcap (c' \sqcup u),$$

где u — произвольный элемент B.

Булевы «неравенства»

Методы решения уравнений в булевой алгебре позволяют решать и «неравенства»

Теорема

Следование $p \sqsubseteq q$ *и уравнение* $p \sqcap q' = o$ *имеют одни и те же решения.*

Доказательство.

$$p \sqsubseteq q \;\Leftrightarrow\; p \sqcap q = p \;\Leftrightarrow\; \overbrace{\big((p \sqcap q) \sqcap p'\big)}^{=o} \sqcup \big((p \sqcap q)' \sqcap p\big) = o \;\Leftrightarrow$$
$$\Leftrightarrow\; \big(p' \sqcup q'\big) \sqcap p = o \;\Leftrightarrow\; p \sqcap q' = o.$$

Разделы

Метод исключения неизвестных

Идея метода — многократное применение Алгоритма 1 при последовательном исключении булевых неизвестных.

Опишем метод для уравнений в булевой структуре

$$\mathbf{2} = \langle \{0,1\}, \vee, \cdot, {}^{-}, \leqslant, 0, 1 \rangle.$$

Пусть БУ задано в виде $f(x_1, \ldots, x_n) = 0$ $(*)$,
где f — полином.

Определим формулы

$$f_p(x_1, \ldots, x_p) = \mathop{\&}_{(\alpha_{p+1}, \ldots, \alpha_n)} f(x_1, \ldots, x_p, \alpha_{p+1}, \ldots, \alpha_n), \quad (**)$$

$$\alpha_i \in \{0,1\},\ i = \overline{p+1, n},\ p = \overline{1, n},$$

где конъюнкция берётся по всем двоичным наборам $(\alpha_{p+1}, \ldots, \alpha_n)$.

Итерционный алгоритм исключения переменных

Алгоритм 2

Шаг 1. Записываем исходное уравнение в форме $f_n = 0$, к которой применяем разложение Шеннона по переменной x_n:

$$f_n(x_1, \ldots, x_{n-1}, 1) \cdot x_n \vee f_n(x_1, \ldots, x_{n-1}, 0) \cdot \overline{x}_n = 0.$$

Из обоснования Алгоритма 1 следует, что это равенство эквивалентно

$$f_n(x_1, \ldots, x_{n-1}, 0) \leqslant x_n \leqslant \overline{f_n(x_1, \ldots, x_{n-1}, 1)}$$

при условии выполнения соотношения

$$\underbrace{f_n(x_1, \ldots, x_{n-1}, 1) \cdot f_n(x_1, \ldots, x_{n-1}, 0)}_{f_{n-1}(x_1, \ldots, x_{n-1})} = 0.$$

На следующем шаге решаем уравнение $f_{n-1}(x_1, \ldots, x_{n-1}) = 0$.

Итерционный алгоритм исключения переменных...

Шаг $n - p + 1$. Рассматривается уравнение

$$f_p(x_1, \ldots, x_p) = 0\,, \quad p \in \{\, n, n-1, \ldots, 1 \,\},$$

которое можно записать в форме (разложение по x_p)

$$f_p(x_1, \ldots, x_{p-1}, 1) \cdot x_p \vee f_p(x_1, \ldots, x_{p-1}, 0) \cdot \overline{x}_p = 0.$$

В свою очередь, данное уравнение эквивалентно соотношению

$$f_p(x_1, \ldots, x_{p-1}, 0) \leqslant x_p \leqslant \overline{f_p(x_1, \ldots, x_{p-1}, 1)},$$

при условии справедливости

$$\underbrace{f_p(x_1, \ldots, x_{p-1}, 1) \cdot f_p(x_1, \ldots, x_{p-1}, 0)}_{f_{p-1}(x_1, \ldots, x_{p-1})} = 0\,.$$

На следующем шаге решаем уравнение $f_{p-1}(x_1, \ldots, x_{p-1}) = 0$.

Итерционный алгоритм исключения переменных...

Шаг n. Решается уравнение

$$f_1(x_1) = 0,$$

откуда получаем

$$f_1(0) \leqslant x_1 \leqslant \overline{f_1(1)}$$

и условие его разрешимости

$$f_0 = f_1(0) \cdot f_1(1) = 0.$$

Из обоснования описанного алгоритма вытекает

Теорема

Если $f_0 \neq 0$, *то уравнение* $(*)$ *не имеет решений.*
Иначе, его решение описывается рекуррентным соотношением $(p = n, n-1, \ldots, 1)$

$$f_p(x_1, \ldots, x_{p-1}, 0) \leqslant x_p \leqslant \overline{f_p(x_1, \ldots, x_{p-1}, 1)}.$$

Алгоритм 2: обсуждение...

Применяя Алгоритм 2 к уравнению $(*)$: для

определения разрешимости — необходимо вычислить f_0;

нахождения хотя бы одного решения — из последнего неравенства $f_1(0) \leqslant x_1 \leqslant \overline{f_1(1)}$ необходимо найти одно значение $b_1 = x_1$, по которому из предпоследнего неравенства найти одно значение b_2 и т.д.

В результате будет получен набор $(b_1, \ldots, b_n)$ — решение исходного уравнения.

нахождения всех решений — из последнего неравенства находят все допустимые значения $b_1 = x_1$, затем для каждого из найденных b_1 из предпоследнего неравенства находят все допустимые значения b_2 и т.д.

Алгоритм 2: обсуждение

Разделение задач нахождения хотя бы одного решения БУ и всех его связано с тем, что БУ может иметь очень большое число корней. Например, для систем БУ вида

$$\text{ДНФ}_i = 1, \quad i = \overline{1, m},$$

у которых число переменных равно n, число элементарных конъюнкций во всех ДНФ одинаково и равно t, число букв во всех элементарных конъюнкциях одинаково и равно r среднее число решений равно $2^n(1-(1-2^{-r})^t)^m$.

Эти задачи в конечных булевых алгебрах могут быть решены тривиальной проверкой всех комбинаций значений переменных, однако это требует чрезвычайно большого перебора.

Все существующие универсальные методы решения систем БУ не позволяют элиминировать этот перебор. Причём остаётся открытым вопрос о принципиальной возможности такой элиминации.

Алгоритм 2: пример 1

Найти все решения уравнения $\underline{x_1 \supset x_2 = 1}$ в структуре $\mathbf{2}$.

Шаг ① Записываем исходное уравнение в форме

$$f_2(x_1, x_2) = x_1 \cdot \overline{x}_2 = 0.$$

Применяем разложение Шеннона по переменной x_2 имеем

$$x_1 \cdot \overline{x_2} = f_2(x_1, 1) \cdot x_2 \vee f_2(x_1, 0) \cdot \overline{x}_2 = 0,$$

откуда $f_2(x_1, 1) = 0$ и $f_2(x_1, 0) = x_1$.

Полученное уравнение эквивалентно «двойному неравенству»

$$f_2(x_1, 0) \leqslant x_2 \leqslant \overline{f_2(x_1, 1)}$$

или

$$x_1 \leqslant x_2 \leqslant 1. \tag{1}$$

при условии $f_1(x_1) = \underbrace{f_2(x_1, 0) \cdot f_2(x_1, 1)}_{\equiv 0} = 0$, которое

тривиально выполняется.

Алгоритм 2: пример $x_1 \cdot \overline{x}_2 = 0$...

Шаг ② Уравнение

$$f_1(x_1) = f_2(x_1, 0) \cdot f_2(x_1, 1) = 0,$$

записывается в форме

$$f_1(1) \cdot x_1 \vee f_1(0) \cdot \overline{x}_1 = 0,$$

где $f_1(1) = f_1(0) = 0$, а его решение в интервальной форме записывается как

$$f_1(0) \leqslant x_1 \leqslant \overline{f_1(1)}$$

или

$$0 \leqslant x_1 \leqslant 1 \qquad (2)$$

при тривиальной выполнимости условия

$$f_0 = \underbrace{f_1(1) \cdot f_1(0)}_{\equiv 0} = 0.$$

Алгоритм 2: пример $x_1 \cdot \overline{x}_2 = 0,\ x_1 \leqslant x_2 \leqslant 1\ (*)$**...**

Найдём решения исходного уравнения.

Из соотношения (2) получаем значения для x_1:

$$x_1^{(0)} = 0, \quad \text{и} \quad x_1^{(1)} = 1.$$

Их необходимо подставить в (1) для определения x_2.

Подставляя $x_1^{(0)}$, получаем соотношение

$$0 \leqslant x_2 \leqslant 1,$$

откуда $x_2^{(00)} = 0$ и $x_2^{(01)} = 1$, а подставляя $x_1^{(1)}$ —

$$1 \leqslant x_2 \leqslant 1,$$

откуда $x_2^{(1)} = 1$.

Т.о. решениями исходного уравнения будут векторы (00), (01), (11) из $\mathbf{2}^2$, что соответствует строкам с единичным значением функции в таблице операции импликации.

Алгоритм 2: пример 2

Найти все решения уравнения $\underline{x_1 \cdot x_2 = x_3}$ в алгебре логики.

Шаг ① Преобразовываем исходное уравнение:

$$f_3(x_1, x_2, x_3) = x_1x_2\overline{x}_3 \vee \overline{(x_1x_2)}x_3 =$$
$$= x_1x_2\overline{x}_3 \vee (\overline{x}_1 \vee \overline{x}_2)x_3 = x_1x_2\overline{x}_3 \vee \overline{x}_1x_3 \vee \overline{x}_2x_3 = 0$$

и применяем разложение Шеннона по переменной x_3:

$$f_3(x_1, x_2, x_3) = \underbrace{(\overline{x}_1 \vee \overline{x}_2)}_{f_3(x_1,x_2,1)} \cdot x_3 \vee \underbrace{x_1x_2}_{f_3(x_1,x_2,0)} \cdot \overline{x}_3 = 0.$$

Решение полученного уравнения в интервальном виде:

$$x_1x_2 \leqslant x_3 \leqslant \overline{\overline{x}_1 \vee \overline{x}_2} = x_1x_2. \qquad (1)$$

Алгоритм 2: пример 2...

Условие такого представления —

$$f_2(x_1, x_2) = f_3(x_1, x_2, 1) \cdot f_3(x_1, x_2, 0) = (\overline{x}_1 \vee \overline{x}_2)x_1x_2 = 0$$

выполняется.

Шаг ② Подставляя в $f_2(x_1, x_2)$ вместо x_2 значения 0 и 1, получаем

$$f_2(x_1, 1) = f_2(x_1, 0) = 0\,.$$

Это влечёт

$$0 \leqslant x_2 \leqslant 1 \qquad (2)$$

при тривиально выполняемом условии

$$f_1(x_1) = f_2(x_1, 1) \cdot f_2(x_1, 0) = 0$$

такого представления.

Алгоритм 2: пример 2...

Шаг ③ Для x_1 получаем интервальное решение

$$0 \leqslant x_1 \leqslant 1 \qquad (3)$$

при $f_0 = f_1(1) \cdot f_1(0) = 0$.

Т.о. исходное уравнение имеет решение и из (3) и (2) получаем $x_1, x_2 \in \{0, 1\}$, а из (2.1) — $x_1 \cdot x_2 \leqslant x_3 \leqslant x_1 \cdot x_2$.

Отсюда решения: (000), (010), (100), (111), совпадающие с ранее найденными.

Алгоритм 2'

Алгоритм 2 может быть модифицирован: на $(n-p+1)$-м шаге проводить разложение Шеннона возможно по любой переменной с индексом $1, 2, \ldots, p$ и не обязательно по x_p.

Для этого определим функции

$$f_p(\widetilde{x}) = \mathop{\&}_{\widetilde{\alpha}} f(\widetilde{x}, \widetilde{\alpha}), \quad p = \overline{1,n}, \qquad (**')$$

где $\widetilde{x} = (x_{j_1}, \ldots, x_{j_p})$, $\widetilde{\alpha} = (\alpha_{i_{p+1}}, \ldots, \alpha_{i_n}) \in \mathbf{2}^{n-p}$ и

$$f_{p,k}(\widetilde{x}', 1) = f_p(\widetilde{x})\big|_{x_k=1}, \quad f_{p,k}(\widetilde{x}', 0) = f_p(\widetilde{x})\big|_{x_k=0}.$$

Алгоритм, получающийся из алгоритма Алгоритм 2 заменой определения функций f_p с $(**)$ на $(**')$, выбором тем или иным способом на каждом, кроме последнего, шаге индекса $k \in \{j_1, \ldots, j_p\}$ и заменами $f_p(x_1, \ldots, x_{p-1}, 1) \mapsto f_{p,k}(\widetilde{x}', 1)$ $f_p(x_1, \ldots, x_{p-1}, 0) \mapsto f_{p,k}(\widetilde{x}', 0)$, назовём Алгоритмом 2'.

Алгоритм 2': пример

Найти по Алгоритму 3' все решения (уже решённого) уравнения $\underline{x_1 \cdot x_2 = x_3}$ в $\mathbf{2}$.

Шаг ① Для уравнения $x_1x_2\overline{x}_3 \vee \overline{x}_1x_3 \vee \overline{x}_2x_3 = 0$ применим разложение Шеннона по переменной x_1 $(k = 1)$:

$$f_3(x_1, x_2, x_3) = (x_2 \vee x_3)(\overline{x}_2 \vee \overline{x}_3) \cdot x_1 \vee (x_2 \vee x_3)(\overline{x}_2 \vee x_3) \cdot \overline{x}_1 = 0,$$

откуда

$$f_{3,1}(x_2, x_3, 1) = x_2\overline{x}_3 \vee \overline{x}_2x_3, \quad f_{3,1}(x_2, x_3, 0) = x_3.$$

Записываем решение данного уравнения в интервальном виде:

$$x_3 \leqslant x_1 \leqslant \overline{x_2\overline{x}_3 \vee \overline{x}_2x_3} = x_2x_3 \vee \overline{x}_2\overline{x}_3.$$

Условие такого представления —

$$f_2(x_1, x_2) = f_3(x_1, x_2, 1) \cdot f_3(x_1, x_2, 0) = \overline{x}_2x_3 = 0.$$

Алгоритм 2': пример...

Шаг ② Подставляя в $f_2(x_2, x_3)$ вместо x_2 $(k = 2)$ значения 0 и 1, получаем

$$f_{2,2}(x_3, 1) = 0\,, \quad f_{2,2}(x_3, 0) = x_3\,.$$

Это влечёт

$$x_3 \leqslant x_2 \leqslant 1$$

при тривиально выполняемом условии

$$f_1(x_3) = f_{2,2}(x_3, 1) \cdot f_{2,2}(x_3, 0) = 0.$$

такого представления.

Шаг ③ Для x_3 получаем интервальное решение

$$0 \leqslant x_3 \leqslant 1$$

при $f_0 = 0$.

Алгоритм 2': пример...

Рассматривая значения x_3, x_2 и x_1 (в данном порядке) с учётом условия $(*)$, получаем их возможные значения

$$\begin{aligned} x_3 &= 1 \Rightarrow x_2 = 1 \Rightarrow x_1 = 1, \\ x_3 &= 0 \Rightarrow x_2 = 0 \Rightarrow x_1 \in \{0, 1\}, \\ x_3 &= 0 \Rightarrow x_2 = 1 \Rightarrow x_1 = 0. \end{aligned}$$

т.е. решения исходного уравнения суть те же векторы (000), (010), (100) и (111).

Наиболее трудоёмкой процедурой данного метода является построение формул f_p. В процессе их построения необходимо производить подстановки наборов значений переменных в f_p. В частности при построении f_0 надо подставить 2^n наборов и общее число операций будет порядка $\omega \cdot 2^n$, где ω — сложность подстановки одного набора.

Разделы

Алгебраические полиномы: определение

Определение

Константу 1 и выражения вида $x_{i_1} \cdot \ldots \cdot x_{i_r}$, где $\varnothing \neq \{i_1, \ldots, i_r\} \subseteq \{1, \ldots n\}$ называют *элементарными монотонными конъюнкциями* над $X_n = \{0, 1, x_1, \ldots, x_n\}$.

Алгебраический полином над X_n есть либо 1 (полином длины 0), либо выражение вида

$$K_1 + \ldots + K_s,$$

где K_i — попарно различные элементарные монотонные конъюнкции над X_n; $i = 1, \ldots, s$, s — *длина полинома*.

Под записью $p = q$ понимают *синтаксическое тождество* полиномов p и q.

Pl_n — множество всех алгебраических полиномов над X_n.

Ясно, что $Pl_1 \subset Pl_2 \subset \ldots \subset Pl_n \subset Pl_{n+1} \subset \ldots$.

Полиномиальная функция алгебраических полиномов

Заметим, что Pl_n не является кольцом, поскольку, например, $x_1 \cdot x_1 \neq x_1$, $x_1 \cdot x_2 \neq x_2 \cdot x_1$ и $K_1 + K_2 \neq K_2 + K_1$.

Для отождествления подобных выражений воспользуемся понятием полиномиальной функции.

Определение

Пусть $\mathcal{R} = \langle R, +, \cdot, 0, 1 \rangle$ — булево кольцо и p — полином из Pl_n.
Обозначим через $p_{\mathcal{R}}(r_1, \ldots, r_n)$ элемент из R, который получается из p заменами $x_i \mapsto r_i \in R$, $i = 1, \ldots, n$, $0 \mapsto o$, $1 \mapsto \iota$. Тогда отображение

$$p_{\mathcal{R}} : R^n \to R$$

назовём *полиномиальной функцией, индуцированной алгебраическим полином* p *на* $\mathcal{R}$.

Алгебраические полиномы: эквивалентность

Определение

Два многочлена $p, q \in Pl_n$ называются эквивалентными (символически $p \sim q$), если равны их полиномиальные функции на $\{0,1\} = \mathbf{2}$, т.е. $p \sim q \Leftrightarrow p_{\mathbf{2}} = q_{\mathbf{2}}$.

Обозначим $P_n(\mathcal{R}) = \{p_{\mathcal{R}} \mid p \in Pl_n\}$ — множество всех полиномиальных функций, индуцированных полиномами из Pl_n на R.

Теорема

$Pl_n/\sim$ есть булево кольцо, и $Pl_n/\sim \cong P_n(\mathbf{2})$.

Элементы $Pl_n/\sim$ называют полиномами Жегалкина (ПЖ).

Теорема Жегалкина и разложение Рида

Теорема (И.И.Жегалкин)
Всякая булева функция единственным образом представима в виде полинома Жегалкина.

Разложение Рида булевой функции $f \in P_2$

$$f(x) = a \cdot x + b = (f(0) + f(1)) \cdot x + f(0)$$

Уравнения в булевом кольце

Рассмотрим в булевом кольце уравнение вида

$$a_1 Q_1(x_1, \ldots, x_n) + \ldots + a_r Q_r(x_1, \ldots, x_n) = b, \qquad (*)$$

где $a_1, \ldots, a_r, b \in \{0, 1\}$ — известные коэффициенты, $Q_1(x_1, \ldots, x_n), \ldots, Q_r(x_1, \ldots, x_n)$ — попарно различные монотонные конъюнкции над

Для упрощения записи будем пользоваться сокращением

$$\overline{a} = a + 1.$$

Теорема (о существовании решения уравнения в булевом кольце)

Уравнение $(*)$ *имеет хотя бы одно решение, если*

$$b \cdot \overline{a}_1 \cdot \ldots \cdot \overline{a}_r = 0. \qquad (**)$$

Уравнения в булевом кольце... $b \cdot \overline{a}_1 \cdot \ldots \cdot \overline{a}_r = 0$

Доказательство.

Необходимость. Пусть уравнение $(*)$ имеет корни, а условие $(**)$ не выполняется.
Подставив корни в $(*)$, получим тождество

$$a_1 Q_1 \cdot \ldots \cdot a_r Q_r = b,$$

умножив которое на $\overline{a}_1 \cdot \ldots \cdot \overline{a}_r$, получим $(**)$, что противоречит допущению.

Достаточность. Рассмотрим уравнение с одним неизвестным

$$a \cdot x + b = 0. \qquad (1)$$

Пусть условие $a \cdot b \equiv 0$ выполняется.
Тогда $x = b$ есть корень уравнения (1): действительно, имеем $a \cdot b + b = \overline{a} b$.

Уравнения в булевом кольце... $b \cdot \overline{a}_1 \cdot \ldots \cdot \overline{a}_r = 0$

Доказательство (продолжение)

Пусть условие $a \cdot b = 0$ выполняется.

Тогда $x = b$ есть корень уравнения (1): действительно, имеем

$$a \cdot b + b = \overline{a}b.$$

Пусть условие теоремы справедливо для уравнения вида $(*)$ с n неизвестными. Покажем, что в этом случае оно справедливо и для уравнения вида $(*)$ с $n+1$ неизвестными.

Представим уравнение с $n+1$ неизвестными в виде:

$$(a_0 + a_1 Q_1(x_1, \ldots, x_n) + \ldots + a_r Q_r(x_1, \ldots, x_n))\, x_{n+1} + b_0 + \\ + b_1 P_1(x_1, \ldots, x_n) + \ldots + b_k Q_k(x_1, \ldots, x_n) = 0\,.$$

Запишем условие $(**)$ относительно неизвестных $x_1, \ldots, x_n$:

$$\overline{a_0 x_{n+1}} \cdot \ldots \cdot \overline{a_r x_{n+1}} \cdot b_0 \overline{b}_1 \ldots \overline{b}_k = 0. \qquad (2)$$

Уравнения в булевом кольце... $b \cdot \overline{a}_1 \cdot \ldots \cdot \overline{a}_r = 0$

Доказательство (продолжение)

Ясно, что булеву функцию $f(x)$ от переменной x можно представить в виде

$$f(x) = x(f(0) + f(1)) + f(0)\,. \tag{3}$$

Из (2) и (3) получим

$$x_{n+1}(b_0\overline{b}_1 \ldots \overline{b}_k + a_0\overline{a}_1 \ldots \overline{a}_r \cdot b_0\overline{b}_1 \ldots \overline{b}_k) + b_0\overline{b}_1 \ldots \overline{b}_k = 0\,.$$

Используя условие, полученное для (1), получаем

$$\overline{a}_0\overline{a}_1 \ldots \overline{a}_r \cdot b_0\overline{b}_1 \ldots \overline{b}_k = 0\,.$$

Решение уравнения $ax + b = 0$ в булевом кольце

Теорема (о решении уравнения в булевом кольце)
Если уравнение (1) *имеет решение, то все они описываются соотношением*

$$x = b + \overline{a} \cdot \lambda(x), \qquad (4)$$

где $\lambda(x)$ *— произвольная функция от переменной* x*.*

Доказательство.

Покажем сначала, что (4) является корнем (1).

Перепишем (1) в виде $ax = b$.

По $(**)$ это уравнение имеет решение, если $b\overline{a} \equiv 0$. Подставив (4) в (1), получим $ab + b = 0$ или $ab = b$, что, по лемме об основных свойствах элементов булевой алгебры эквивалентно $0 = b\overline{a}$.

Т.о. выполнение необходимого условие существования решений влечёт справедливость того, что (4) есть корень (1).

Решение уравнения $ax + b = 0$ в булевом кольце...

Доказательство (продолжение)

Докажем теперь, что (4) описывает все корни (1).
Пусть существует такой корень β, что

$$\beta \neq b + \overline{a} \cdot \lambda(x) \tag{5}$$

ни при каких значениях функции $\lambda(x)$.
Это означает, что выполняется условие $(\beta + b)a \neq 0$.

В этом случае можно найти такое $\epsilon \not\equiv 0$, что $(\beta + b) \cdot a = \epsilon$, откуда

$$\beta \cdot \overline{a} = b \cdot a + \epsilon\,. \tag{6}$$

Решение уравнения $ax + b = 0$ в булевом кольце...

Доказательство (продолжение)

Подставляя β в (1) мы должны получить тождество

$$(\beta + b) \cdot a = \epsilon\,,$$

или, используя (6) — $b \cdot a + \epsilon + b \equiv 0\,, \qquad b \cdot \overline{a} + \epsilon \equiv 0.$

Но, согласно теореме о существовании решения уравнения в булевом кольце, $b\overline{a} \equiv 0$ и тогда $\epsilon \equiv 0$, что противоречит (5). Значит, β не является корнем уравнения (1).

Итерационно применяя формулу для решения уравнения с одним неизвестным, можно получить алгоритм решения уравнений вида $(*)$ со многими неизвестными.

Решение уравнения в булевом кольце: пример

Пример. Решим уравнение с тремя неизвестными

$$a_0 + a_1x_1x_2x_3 + a_2x_3 = 0. \tag{7}$$

Пусть условие $(**)$ выполняется, т.е. $a_0\overline{a}_1\overline{a}_2 = 0$.
Запишем условие разрешимости относительно x_3 —

$$a_0(a_1x_1x_2 + \overline{a}_2) = 0 \tag{8}$$

и разрешимости полученного условия относительно x_2 —

$$a_0\overline{a}_2(a_0a_1x_1 + 1) = 0\,.$$

Отсюда находим x_1:

$$x_1 = a_0\overline{a}_2 + \overline{a_0a_1\overline{a}_2}\cdot\lambda_1, \tag{9}$$

где $\lambda \in \{0, 1\}$.

Решение уравнения в булевом кольце: пример...

Из (8) и (9) получаем x_2:

$$x_2 = a_0\overline{a}_2 + \overline{a_0a_1\overline{a}_2 + a_0a_1a_2\lambda_1} \cdot \lambda_2, \qquad (10)$$

а из (9), (10) и (7) — x_3:

$$x_3 = a_0 + \overline{a_0a_1\overline{a}_2 + \overline{a}_0\lambda_1\lambda_2} \cdot \lambda_3.$$