**Федеральное государственное автономное образовательное учреждение высшего профессионального образования**

**КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ**

**ИНСТИТУТ МАТЕМАТИКИ И МЕХАНИКИ ИМ. Н.И. ЛОБАЧЕВСКОГО**

**КАФЕДРА АЛГЕБРЫ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ**

Направление: 01.03.01: Математика,бакалавр математики.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

(Бакалаврская работа)

# Многочлены над булевыми алгебрами.

**Работа завершена:**

«___»_____2015 г. _____Э.И. Сафина

**Работа проверена:**

Научный руководитель
кандидат физико-математических наук,
доцент кафедры алгебры и математической логики
«___»_____2015 г. _____С.Н. Ильин

Заведующий кафедрой алгебры и математической логики
доктор физико-математических наук, профессор
«___»_____2015 г. _____М. М. Арсланов

Казань — 2015 г.

# ОГЛАВЛЕНИЕ

# Введение

Булевы алгебры, в частности, двухэлементная булева алгебра $\mathbb{B}_2$, встречаются в различных разделах математики, в том числе, математической логике, дискретной математике, теории решеток и др. ([1], [4]). Впервые булевы алгебры появились в трудах английского математика Дж. Буля в 50-х годах XIX-го века и использовались как аппарат математической логики. При этом элементы булевой алгебры трактовались как высказывания, а операциями в ней являлись, в частности, дизъюнкция и конъюнкция.

Таким образом, булевы алгебры можно рассматривать как алгебраические системы с двумя бинарными операциями: сложением – дизъюнкцией и умножением – конъюнкцией, а следовательно, над такими системами можно вводить стандартные алгебраические конструкции, такие как матрицы, многочлены и т.п., можно изучать их свойства и решать задачи, аналогичные классическим задачам. Так, например, в разделе 5 книги [2] рассматриваются многочлены над булевыми алгебрами применительно к задачам о разрешимости в булевых алгебрах полиномиальных уравнений и систем таких уравнений. Данная выпускная квалификационная работа посвящена изучению алгебраических свойств многочленов от одной переменной над произвольными булевыми алгебрами.

Работа содержит четыре параграфа. В первом параграфе приведены начальные определения и некоторые теоретические сведения о булевых алгебрах, используемые в работе. Во втором параграфе изучаются свойства степеней многочленов, а также ряд вопросов о неприводимых многочленах. В третьем параграфе излагается алгоритм проверки делимости одного многочлена на другой, дается теоретическое обоснование алгоритма и рассматриваются примеры его работы. Четвертый параграф посвящен изучению свойств наибольшего общего делителя и наименьшего общего кратного многочленов. В

конце работы приведен список используемой литературы.

# §1 Основные определения и понятия.

***Определение 1***. *Булевой алгеброй* называется непустое множество $A$ с двумя бинарными операциями: конъюнкцией $\wedge$, дизъюнкцией $\vee$, унарной операцией отрицания $\neg$ и двумя выделенными элементами 0 и 1, такими что для всех $a, b, c \in A$ выполнены следующие аксиомы:

(1) *ассоциативные законы*

$a \vee (b \vee c) = (a \vee b) \vee c$ $\qquad$ $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

(2) *коммутативные законы*

$a \vee b = b \vee a$ $\qquad$ $a \wedge b = b \wedge a$

(3) *законы поглощения*

$a \vee (a \wedge b) = a$ $\qquad$ $a \wedge (a \vee b) = a$

(4) *дистрибутивные законы*

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ $\qquad$ $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

(5) *свойства дополнения*

$a \vee \neg a = 1$ $\qquad$ $a \wedge \neg a = 0$

Для всех $a, b \in A$ верны также следующие равенства:

$a \vee a = a$ $\qquad$ $a \wedge a = a$

$a \vee 0 = a$ $\qquad$ $a \wedge 1 = a$

$a \vee 1 = 1$ $\qquad$ $a \wedge 0 = 0$

$\neg 0 = 1$ $\qquad$ $\neg 1 = 0$

$\neg\neg a = a$ $\qquad$ $a \wedge \neg a = 0$

Ниже для упрощения записи вместо $\vee$ и $\wedge$ будем писать $+$ и $\cdot$, соответственно.

Наиболее простым примером булевой алгебры может служить двухэлементная булева алгебра $\mathbb{B}_2 = \{0, 1\}$, в которой сложение и умножение задаются следующими таблицами:

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Как обычно, *конечная булева алгебра* — это алгебра, содержащая конечное число элементов. С помощью хорошо известных результатов о булевых алгебрах (см., например, [4, Теорема 7 и Следствие из нее, стр. 149–150], а также [4, Упражнение 9, стр. 144]) нетрудно показать справедливость следующих двух утверждений:

***Утверждение 1.1***. Любая конечная булева алгебра изоморфна прямому произведению конечного числа двухэлементных алгебр $\mathbb{B}_2$.

***Утверждение 1.2***. Подалгебра булевой алгебры, порожденная конечным числом элементов, конечна.

Хорошо известны примеры и бесконечных булевых алгебр, например, такой алгеброй является алгебра всех подмножеств произвольного бесконечного множества.

Многочлены над булевыми алгебрами формально определяются точно так же, как и многочлены над кольцами и полями. Множество всех многочленов от переменной $x$ над булевой алгеброй $B$ будем, как обычно, обозначать через $B[x]$. Основная цель работы состоит в том, чтобы исследовать, в какой мере известные результаты о многочленах над полями и кольцами могут быть перенесены на случай многочленов над булевыми алгебрами.

# §2 Неприводимые многочлены.

Как уже было отмечено выше, алгебра $\mathbb{B}_2 = \{0, 1\}$ является наиболее простым и в то же время достаточно важным примером булевой алгебры, поэтому изучение многочленов над булевыми алгебрами естественно начать именно с изучения многочленов над алгеброй $\mathbb{B}_2$.

Прежде всего исследуем свойства степеней многочленов. Как известно, в случае колец степень суммы многочленов не превышает максимума из степеней слагаемых. Легко видеть, что для многочленов над $\mathbb{B}_2$ справедливо более сильное свойство:

***Утверждение 2.1***. $\deg(f + g) = \max(\deg f, \deg g)$.

Далее, очевидно, что алгебра $\mathbb{B}_2$ не содержит делителей нуля, поэтому следующее утверждение легко доказывается по аналогии с соответствующим свойством для многочленов над кольцами без делителей нуля (о свойствах многочленов над кольцами без делителей нуля и, в частности, полями, см., например [3, глава 5]):

***Утверждение 2.2*** $\deg(f \cdot g) = \deg f + \deg g$.

Нетрудно заметить, что в случае, когда коэффициенты многочленов $f$ и $g$ лежат в произвольной булевой алгебре $B$, Утверждение 2.1 остается справедливым, а равенство в Утверждении 2.2 следует заменить неравенством $\deg(f \cdot g) \leq \deg f + \deg g$.

В самом деле, пусть $B$ — это изображенная ниже на рис. 1 четырехэлементная булева алгебра:

Тогда для $f = ax + 1$ и $g = a'x + 1$ имеем $fg = (ax + 1)(a'x + 1) = aa'x^2 + (a + a')x + 1 = x + 1$, так что $\deg(fg) = 1 < 2 = \deg f + \deg g$.

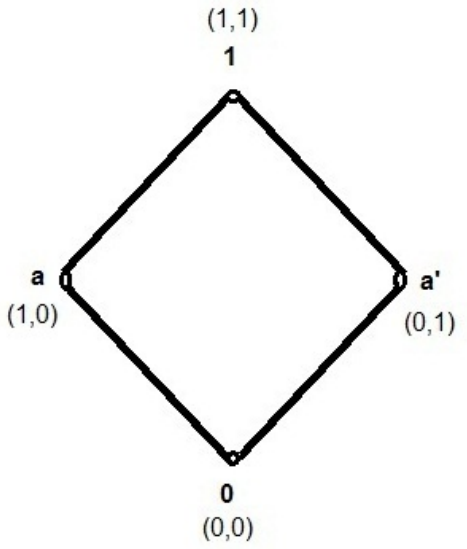


Рис. 1: Четырехэлементная булева алгебра

Для многочленов над булевыми алгебрами полезным оказывается также понятие минимальной степени. А именно, пусть дан многочлен $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$ степени $n$. Его *минимальной степенью* (обозначение: $\operatorname{mindeg} f$) будем называть число $n - i$, где $i$ — наибольший индекс, такой что $a_i \neq 0$. Другими словами, $\operatorname{mindeg} f$ — это наименьший из показателей степеней переменной $x$, входящих в многочлен $f$. Справедливы следующие свойства:

***Утверждение 2.1'***. $\operatorname{mindeg}(f + g) = \min(\operatorname{mindeg} f, \operatorname{mindeg} g)$.

***Утверждение 2.2'***. Если $f, g \in \mathbb{B}_2[x]$, то

$$\operatorname{mindeg}(f \cdot g) = \operatorname{mindeg} f + \operatorname{mindeg} g,$$

а в случае многочленов над произвольной булевой алгеброй верно

$$\operatorname{mindeg}(f \cdot g) \geq \operatorname{mindeg} f + \operatorname{mindeg} g.$$

Вполне очевидно также следующее

***Утверждение 2.3***. Каждый ненулевой многочлен $f \in B[x]$ можно единственным способом представить в виде

$$f = x^{\operatorname{mindeg} f}\tilde{f}, \quad \text{где } \operatorname{mindeg}\tilde{f} = 0. \tag{2.1}$$

Перейдем теперь к изучению неприводимых многочленов. Напомним, что *неприводимый многочлен* — это такой многочлен $f$, что $\deg f \geq 1$ и $f$ нельзя представить в виде $f = gh$, где $\deg g$, $\deg h \geq 1$. Как и при изучении свойств степеней многочленов, будем рассматривать сначала многочлены над $\mathbb{B}_2$.

Как известно, в кольце многочленов $K[x]$, где $K$ — это одно из полей $\mathbb{R}$ или $\mathbb{C}$, каждый неприводимый многочлен имеет степень 1 или 2. В случае двухэлементной алгебры $\mathbb{B}_2$ это утверждение не выполняется, так как существуют неприводимые многочлены бóльших степеней.

Действительно, неприводимыми являются, например, многочлены вида $x^n + 1$ при любом $n \geq 1$. При $n = 1$ это очевидно. Предположим теперь, что $n \geq 2$ и $x^n + 1 = gh$, где $\deg g$, $\deg h \geq 1$. Тогда $g = x^k + a_1x^{k-1} + \ldots + a_k$, $h = x^l + b_1x^{l-1} + \ldots + b_l$, $k + l = n$. Так как $a_kb_l = 1$, то $a_k = b_l = 1$, следовательно, раскрывая скобки в произведении $gh = (x^k + a_1x^{k-1} + \ldots + 1)(x^l + b_1x^{l-1} + \ldots + 1) = x^n + x^k + x^l + \ldots + 1$, приходим к противоречию с равенством $x^n + 1 = gh$.

Все неприводимые многочлены малых степеней можно найти методом перебора. Ниже выписаны все неприводимые многочлены степени не больше чем 4:

$$\{x, x+1, x^2+1, x^3+1, x^3+x+1, x^3+x^2+1,$$
$$x^4+1, x^4+x^3+1, x^4+x^3+x^2+1, x^4+x^2+x+1, x^4+x+1\}$$

Так как степень любого неприводимого многочлена больше или равна 1, то с учетом Утверждения 2.2, всякий многочлен $f \in \mathbb{B}_2[x]$, $\deg f \geq 1$, можно разложить в произведение неприводимых многочленов. Однако, в отличие

от многочленов над полями, необходимо отметить неоднозначность такого разложения. Продемонстрируем это на примере.

***Пример 2.1.*** Пусть $f = x^3 + x^2 + x + 1$. Этот многочлен над $\mathbb{B}_2$ может быть разложен в произведение неприводимых многочленов $x + 1$ и $x^2 + 1$, а также можно заметить, что $x^3 + x^2 + x + 1 = (x + 1)^3$. Таким образом, для $f$ имеется два различных способа разложения в произведение неприводимых многочленов: $f = (x + 1)(x^2 + 1)$ и $f = (x + 1)^3$.

Возможность разложения в произведение неприводимых многочленов сохраняется для многочленов над конечными булевыми алгебрами. В самом деле, согласно Утверждению 1.1 конечная булева алгебра $B$ изоморфна прямому произведению некоторого конечного числа $n$ двухэлементных булевых алгебр, поэтому любой многочлен $f \in B[x]$ можно рассматривать как набор $(f_1, \ldots, f_n)$, где $f_i \in \mathbb{B}_2[x]$ при любом $i$. Ясно, что $f = gh$ в точности тогда, когда $f_i = g_i h_i$ для всех $i = 1, \ldots, n$. Следовательно, при любом $i$ верно $\deg f_i \geq \deg g_i$ и $\deg f_i \geq \deg h_i$, а если $\deg g, \deg h \geq 1$, то найдутся (не обязательно различные) индексы $i$ и $j$, такие что $\deg f_i > \deg g_i$ и $\deg f_j > \deg h_j$. Поскольку степень каждого многочлена $f_i$ — конечное число, процесс разложения очередного сомножителя в разложении $f$ в произведение двух других сомножителей не может продолжаться бесконечно, и значит, на некотором шаге все сомножители будут уже неразложимыми многочленами.

Таким образом, верна

***Теорема 2.1***. Если булева алгебра $B$ конечна, то каждый многочлен $f \in B[x]$, $\deg f \geq 1$, можно разложить в произведение конечного числа неприводимых многочленов. Такое разложение, в общем случае, необязательно единственно.

Нетрудно понять, что описанные выше рассуждения не годятся для мно-

гочленов над бесконечными булевыми алгебрами. Действительно, если булева алгебра $B$ бесконечна, то существует бесконечная убывающая цепь подалгебр $B \supset a_1B \supset a_2B \supset \ldots$, так что даже многочлен $x+1$ нельзя представить требуемым образом:

$$x+1 = (a_1x+1)(a_1'x+1) = (a_2x+1)(a_2'a_1x+1)(a_1'x+1) = \ldots =$$

$$(a_nx+1)(a_n'a_{n-1}x+1)\ldots(a_2'a_1x+1)(a_1'x+1) = \ldots$$

# §3 Делимость многочленов.

Пусть $B$ — булева алгебра и $f, g \in B[x]$. Как обычно, будем говорить, что $g$ *делит* $f$ (обозначение $g \mid f$), если $f = gq$ для некоторого $q \in B[x]$. Как уже было показано в предыдущем параграфе (см. Пример 2.1), частное $q$ в этом случае может быть определено, вообще говоря, неоднозначно.

Основная задача данного параграфа состоит в том, чтобы выяснить, как по заданным многочленам $f, g \in B[x]$ определить, делится ли $f$ на $g$, и если да, то как найти все такие многочлены $q \in B[x]$, что $f = gq$.

Ясно, что если $g = 0$, то единственный многочлен $f$, который делится на $g$, — это нулевой многочлен, и тогда в качестве $q$ годится любой многочлен. Если $f = 0$, а $g \neq 0$, то, очевидно, $g \mid f$ и единственное частное $q = 0$. Поэтому в дальнейшем будем предполагать, что $f \neq 0$ и $g \neq 0$.

Рассмотрим сначала случай, когда $B = \mathbb{B}_2$.

***Утверждение 3.1.*** Пусть $f = x^{\operatorname{mindeg}(f)}\tilde{f}$ и $g = x^{\operatorname{mindeg}(g)}\tilde{g}$ — разложения вида (2.1) для $f$ и $g$. Тогда условие, что $g$ делит $f$, равносильно тому, что $\operatorname{mindeg}(g) \leq \operatorname{mindeg}(f)$ и $\tilde{g} \mid \tilde{f}$.

Доказательство. Пусть $f = gq$. Тогда $q \neq 0$ и, значит, согласно Утверждению 2.3 имеем $q = x^{\operatorname{mindeg}(q)}\tilde{q}$. Подставляя в равенство $f = gq$, получаем $f = x^{\operatorname{mindeg}(g)+\operatorname{mindeg}(q)}\tilde{g}\tilde{q}$, причем с учетом Утверждения 2.2' верно $\operatorname{mindeg}(\tilde{g}\tilde{q}) = \operatorname{mindeg}(\tilde{g}) + \operatorname{mindeg}(\tilde{q}) = 0+0 = 0$. Следовательно, учитывая единственность разложения вида (2.1) для $f$, получаем $\operatorname{mindeg}(f) = \operatorname{mindeg}(g)+\operatorname{mindeg}(q) \geq \operatorname{mindeg}(g)$ и $\tilde{f} = \tilde{g}\tilde{q}$, так что $\tilde{g} \mid \tilde{f}$.

Обратная импликация очевидна.

Итак, в силу Утверждения 3.1 проверка делимости $f$ на $g$ равносильна проверке неравенства $\operatorname{mindeg}(g) \leq \operatorname{mindeg}(f)$ и делимости $\tilde{f}$ на $\tilde{g}$.

**Замечание 3.1.** С учетом того, что $\tilde{q} \neq 0$ и $\operatorname{mindeg}(\tilde{q}) = 0$, получаем $\tilde{q} = c_0x^k + c_1x^{k-1} + \ldots + c_{k-1}x + 1 = q_1 + 1$, где $q_1 = c_0x^k + c_1x^{k-1} + \ldots + c_{k-1}x$. Следовательно, $q_1 = 0$ или $\operatorname{mindeg}(q_1) \geq 1$.

***Утверждение 3.2.*** $\tilde{g} \mid \tilde{f}$ тогда и только тогда, когда существует такой $h \in \mathbb{B}_2[x]$, что 1) $\tilde{f} = h + \tilde{g}$, 2) $\tilde{g} \mid h$ и 3) либо $h = 0$, либо $\operatorname{mindeg}(h) \geq 1$.

Доказательство. Пусть $\tilde{f} = \tilde{g}\tilde{q}$. Тогда согласно Замечанию 3.1 получаем $\tilde{f} = \tilde{g}(q_1 + 1) = \tilde{g}q_1 + \tilde{g}$. Нетрудно убедиться в том, что многочлен $h = \tilde{g}q_1$ удовлетворяет всем требуемым условиям.

Справедливость обратной импликации немедленно вытекает из условий 1) и 2).

***Утверждение 3.3.*** Пусть $\tilde{f} = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + 1$, $\tilde{g} = x^m + b_1x^{m-1} + \ldots + b_{m-1}x + 1$, $n \geq m \geq 1$. Если существует $h \in \mathbb{B}_2[x]$, удовлетворяющий условиям 1)–3) Утверждения 3.2, то $\tilde{f} + \tilde{g} = \tilde{f}$ и многочлен $h$ имеет вид

$$\sum_{i:\, b_i = 0} a_i x^i + \sum_{k \in K} x^k, \tag{3.1}$$

где $K$ — произвольное (в том числе, пустое) подмножество множества $J = \{i > 0 : b_{m-i} = 1\}$. Таким образом, если указанный многочлен $h$ существует, то всего их будет не более чем $2^{|J|}$.

Доказательство. Пусть многочлен $h$ удовлетворяет условиям 1)–3). Согласно условию 1) имеем: $\tilde{f} = h + \tilde{g} = h + \tilde{g} + \tilde{g} = \tilde{f} + \tilde{g}$, так что $\tilde{f} = \tilde{f} + \tilde{g}$.

Далее, при $n = m$ из условий 1) и 2) получаем, что либо $h = 0$ — этот многочлен имеет требуемый вид (3.1), либо $\deg h = m$, но в последнем случае имеем $h = \tilde{g}$, что противоречит условию 3), так как $0 = \operatorname{mindeg}(\tilde{g}) = \operatorname{mindeg}(h) > 0$.

Если $n > m$, то в $h$, очевидно, должны входить все мономы $a_i x^{n-i}$ при $b_i = 0$, поскольку они отсутствуют в многочлене $\tilde{g}$. Но тогда $h$ снова имеет требуемый вид (3.1).

Опираясь на Утверждения 3.1–3.3, опишем следующий

**Алгоритм проверки делимости:**

Пусть $f, g \neq 0$.

Шаг 1. Проверяем неравенство $\operatorname{mindeg}(g) \leq \operatorname{mindeg}(f)$. Если оно не выполнено, то $g \nmid f$. Если выполнено, то переходим к Шагу 2.

Шаг 2. Проверяем делимость $\tilde{f}$ на $\tilde{g}$. Для этого проверяем равенство $\tilde{f} = \tilde{f}+\tilde{g}$. Если оно не выполняется, то многочленов $h$, удовлетворяющих условиям 1)–3) из формулировки Утверждения 3.2 не существует и, следовательно, $g \nmid f$. Если они есть, то находим все многочлены вида (3.1) и переходим к Шагу 3.

Шаг 3. Для каждого многочлена $h$, найденного на Шаге 2, проверяем делимость $h$ на $\tilde{g}$, пользуясь при $h \neq 0$ данным алгоритмом. Если хотя бы один из многочленов $h$ делится на $\tilde{g}$, то $g \mid f$, иначе — $g \nmid f$. Заметим, что в первом случае для подходящего $\hat{h} \in \mathbb{B}_2[x]$ верно $h = \hat{h}\tilde{g}$, откуда $\tilde{f} = \hat{h}\tilde{g}+\tilde{g} = (\hat{h}+1)\tilde{g}$. Тем самым, найдено одно из возможных частных $\tilde{q} = \hat{h} + 1$.

Обоснование алгоритма. Корректность работы алгоритма обеспечивается Утверждениями 3.1–3.3. Нужно лишь убедиться в том, что алгоритм не может работать бесконечно долго. Докажем это индукцией по $n = \deg f$.

Пусть $n = 0$. При $\operatorname{mindeg}(g) > 0$ алгоритм закончит работу на Шаге 1, при $\operatorname{mindeg}(g) = 0$ и $\deg g > 0$ — на Шаге 2. Наконец, при $\deg g = 0$ получаем $f = 1 = g$, так что единственный многочлен $h$, который будет найден на Шаге 2, — это $h = 0$. Следовательно, алгоритм закончит работу на Шаге 3.

Пусть $n \geq 1$ и для всех многочленов степени строго меньше $n$ остановка алгоритма за конечное число шагов уже доказана.

Ясно, что алгоритм не может "зациклиться" на Шаге 1. Далее, с учетом Утверждения 3.3 алгоритм не может работать бесконечно долго и на Шаге 2. Наконец, для Шага 3 проверка делимости многочлена $h = 0$ на $\tilde{g}$ тривиальна, а если $h \neq 0$, то такая проверка сводится к проверке делимости $\tilde{h}$ на $\tilde{g}$, которая заканчивается за конечное число шагов по предположению индукции, поскольку $\deg \tilde{h} < \deg h \leq n$.

Рассмотрим примеры.

***Пример 3.1.*** Проверить делимость многочлена $f = x^5 + x^4 + x^3 + x^2 + x + 1$ на многочлен $g = x^3 + x + 1$.

Шаг 1. Имеем $\operatorname{mindeg}(g) = 0 \leq 0 = \operatorname{mindeg}(f)$, тем самым, требуемое неравенство выполнено, следовательно, переходим к Шагу 2.

Шаг 2. Проверяем делимость $\tilde{f}$ на $\tilde{g}$. Для этого проверяем равенство $\tilde{f} = \tilde{f} + \tilde{g}$ :

$$x^5 + x^4 + x^3 + x^2 + x + 1 = (x^5 + x^4 + x^3 + x^2 + x + 1) + (x^3 + x + 1),$$

равенство выполняется. Находим все многочлены $h$, вида (3.1):

$h_1 = x^5 + x^4 + x^2$,

$h_2 = x^5 + x^4 + x^3 + x^2$,

$h_3 = x^5 + x^4 + x^2 + x$,

$h_4 = x^5 + x^4 + x^3 + x^2 + x$.

Переходим к Шагу 3.

Шаг 3. Для каждого многочлена $h$, проверяем делимость $h$ на $\tilde{g}$, используя данный алгоритм.

**Для** $h_1$. Шаг 1.1 Неравенство $\operatorname{mindeg}(\tilde{g}) = 0 \leq 2 = \operatorname{mindeg}(h_1)$ выполняется, следовательно переходим к следующему Шагу.

Шаг 2.1 Равенство $\tilde{h_1} = \tilde{h_1} + \tilde{g}$ неверно, так как $x^3 + x^2 + 1 \neq (x^3 + x^2 + 1) + (x^3 + x + 1)$, следовательно, приступаем к проверке следующего $h$.

**Для $h_2$.** Шаг 1.2 Неравенство $\mathrm{mindeg}\,(\tilde{g}) = 0 \leq 2 = \mathrm{mindeg}\,(h_2)$ выполняется, следовательно переходим к следующему Шагу.

Шаг 2.2 Равенство $\tilde{h_2} = \tilde{h_2} + \tilde{g}$ выполнено, так как $x^3 + x^2 + x + 1 = (x^3 + x^2 + x + 1) + (x^3 + x + 1)$. Находим все многочлены $h_{2i}$ вида (3.1):

$h_{21} = x^2$,

$h_{22} = x^3 + x^2$,

$h_{23} = x^2 + x$,

$h_{24} = x^3 + x^2 + x$,

и переходим к следующему Шагу.

Шаг 3.2 Для каждого многочлена $h_{2i}$, найденного на Шаге 2.2 проверка делимости $h_{2i}$ на $\tilde{g}$, заканчивается отрицательным ответом на Шаге 2.2.$i$, где $i \in [1, 4]$. Продолжим наш алгоритм для следующего $h$.

**Для $h_3$.** Шаг 1.3 Неравенство $\mathrm{mindeg}\,(\tilde{g}) = 0 \leq 1 = \mathrm{mindeg}\,(h_3)$ выполняется, следовательно, переходим к следующему Шагу.

Шаг 2.3 Равенство $\tilde{h_3} = \tilde{h_3} + \tilde{g}$ выполняется: $x^4 + x^3 + x + 1 = (x^4 + x^3 + x + 1) + (x^3 + x + 1)$. Находим все многочлены $h_{3i}$ вида (3.1):

$h_{31} = x^4$,

$h_{32} = x^4 + x^3$,

$h_{33} = x^4 + x$,

$h_{34} = x^4 + x^3 + x$,

и переходим к следующему Шагу.

Шаг 3.3 Для каждого многочлена $h_{3i}$, найденного на Шаге 2.3 проверка делимости $h_{3i}$ на $\tilde{g}$, заканчивается отрицательным ответом на Шаге 2.3.$i$, где $i \in [1, 4]$. Продолжим наш алгоритм для следующего $h$.

**Для $h_4$.** Шаг 1.4 Неравенство $\mathrm{mindeg}\,(\tilde{g}) = 0 \leq 1 = \mathrm{mindeg}\,(h_4)$ выполняется, следовательно, переходим к следующему Шагу.

Шаг 2.4 Равенство $\tilde{h_4} = \tilde{h_4} + \tilde{g}$ выполняется: $x^4 + x^3 + x^2 + x + 1 = (x^4 + x^3 + x^2 + x + 1) + (x^3 + x + 1)$. Находим все многочлены $h_{4i}$ вида (3.1):

$h_{41} = x^4 + x^2$,

$h_{42} = x^4 + x^3 + x^2$,

$h_{43} = x^4 + x^2 + x$,

$h_{44} = x^4 + x^3 + x^2 + x$,

и переходим к следующему Шагу.

Шаг 3.4 Для многочленов $h_{41}, h_{42}$ проверка делимости на $\tilde{g}$, заканчивается отрицательным ответом на Шаге 2.4.$i$, где $i = 1, 2$, а $\tilde{h}_{44} = \tilde{h}_2$— делимость этого многочлена на $\tilde{g}$ проверялась на Шаге 2.2. Выполним проверку для многочлена $h_{43}$.

Для $h_{43}$. Шаг 1.4.3 Неравенство $\mathrm{mindeg}\,(\tilde{g}) = 0 \leq 1 = \mathrm{mindeg}\,(h_{43})$ выполняется, следовательно, переходим к следующему Шагу.

Шаг 2.4.3 В этом случае $\tilde{h_{43}} = x^3 + x + 1 = \tilde{g}$, так что $\tilde{g} \mid h_{43}$, и следовательно, $g$ ДЕЛИТ $f$.

***Пример 3.2.*** Проверить делимость многочлена $f = x^5 + x^3 + x + 1$ на многочлен $g = x^3 + x$.

Шаг 1. Проверяем неравенство $\mathrm{mindeg}\,(g) = 1 \not\leq 0 = \mathrm{mindeg}\,(f)$, неравенство не выполнено, следовательно, $g$ НЕ ДЕЛИТ $f$.

Заметим, что описанный выше алгоритм можно перенести на случай многочленов над произвольными булевыми алгебрами. Сначала рассмотрим случай конечных булевых алгебр.

Пусть $B$ — конечная булева алгебра. По аналогии с расуждениями, приведенными перед Теоремой 2.1, в этом случае каждый многочлен $f \in B[x]$

можно понимать как набор $f = (f_1, f_2, \ldots, f_n)$, где $f_i \in \mathbb{B}_2[x]$ при любом $i$, причем для $g \in B[x]$ верно $f = gq$ тогда и только тогда, когда $f_i = g_i q_i$ для всех $i = 1, 2, \ldots, n$. Пусть $Q_i = \{q_i : f_i = g_i q_i\}$ — множество всех частных многочлена $f_i$. Тогда множество $Q = \{(q_1, \ldots, q_n), q_i \in Q_i\}$ — конечное множество частных для многочлена $f$.

Пусть теперь $B$ — бесконечная булева алгебра. И пусть даны два многочлена $f, g \in B[x]$, $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$ и $g = b_0x^m + b_1x^{m-1} + \ldots + b_m$. Множество $Y = \{a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m\}$ конечно, следовательно, из Утверждения 1.2 вытекает, что булева алгебра, порожденная множеством $Y$, конечна. Значит, $f$ и $g$ можно рассматривать как многочлены над конечной булевой алгеброй и применять к ним описанный выше алгоритм.

# §4 НОД и НОК.

В этом параграфе рассматриваются примеры нахождения наибольшего общего делителя и наименьшего общего кратного для многочленов над булевой алгеброй $\mathbb{B}_2$.

***Определение.*** Многочлен $d \in \mathbb{B}_2[x]$ называется *наибольшим общим делителем* многочленов $f$ и $g$ (обозначение: $d = \text{НОД}(f, g)$), если

1) $d|f$, $d|g$;

2) $c|f$, $c|b \Rightarrow c|d$.

Для нахождения наибольшего общего делителя $f$ и $g$ можно воспользоваться следующим способом. Поскольку существует лишь конечное число многочленов, степени которых не превышают $\deg f$, для многочлена $f$ можно найти все способы его разложения на неприводимые множители, и аналогично, для многочлена $g$. Следовательно, можно в явном виде найти все общие делители для $f$ и $g$. Если среди них существует многочлен $d$, удовлетворяющий свойству 2) из определения НОД, то этот многочлен и будет наибольшим общим делителем для $f$ и $g$. Продемонстрируем этот способ на конкретных примерах:

***Пример 4.1.*** Найти НОД двух многочленов $f = x^6 + x^4 + x^3 + x + 1$, $g = x^5 + x^4 + x^3 + x^2 + 1$.

Найдем всевозможные разложения многочленов $f$ и $g$ на неприводимые сомножители:

$f = x^6 + x^4 + x^3 + x + 1 = (x^3 + 1)(x^3 + x + 1)$

$g = x^5 + x^4 + x^3 + x^2 + 1 = (x^3 + x^2 + 1)(x^2 + 1)$

Получаем, что общих делителей, кроме 1, у многочленов $f$ и $g$ нет. Следовательно, $\text{НОД}(f, g) = 1$.

***Определение.*** Многочлены $f, g \in \mathbb{B}_2[x]$, для которых НОД$(f, g) = 1$, называются *взаимно простыми*.

***Пример 4.2.*** Найти НОД двух многочленов $f = x^4 + x^3 + x + 1$, $g = x^5 + x^4 + x^2 + x + 1$.

Найдем всевозможные разложения многочленов $f$ и $g$ на неприводимые сомножители:

$f = x^4 + x^3 + x + 1 = (x + 1)(x^3 + 1)$

$g = x^5 + x^4 + x^2 + x + 1 = (x + 1)(x^4 + x + 1)$

Получаем, что общими делителями многочленов $f$ и $g$ являются многочлены $x + 1$ и 1, следовательно, НОД$(f, g) = x + 1$.

***Определение.*** Многочлен $m \in \mathbb{B}_2[x]$ называется *наименьшим общим кратным* многочленов $f$ и $g$ (обозначение: $m = \text{НОК}(f, g)$), если

1) $f|m$, $g|m$;

2) $f|c$, $g|c \Rightarrow m|c$.

Покажем на примере, что наименьшее общее кратное многочленов $f, g$ существует не всегда.

***Пример 4.3.*** $f = x^3 + x^2 + 1$, $g = x^2 + 1$.

Предположим, что $h$ является наименьшим общим кратным многочленов $f$ и $g$. Поскольку $f$ и $g$ не делятся друг на друга, то $\deg h > \max(\deg f, \deg g) = 3$. Заметим, что одним из общих кратных для $f$ и $g$ является многочлен $p = x^4 + x^3 + x^2 + x + 1$, так как $p = f(x + 1)$ и $p = g(x^2 + x + 1)$, причем других общих кратных степени 4 для $f$ и $g$ не существует, поэтому $h = p$. С другой стороны, еще одним общим кратным для $f$ и $g$ является их произведение $fg = x^5 + x^4 + x^3 + x^2 + 1$. Но $h$ его не делит, что нарушает свойство 2)

из определения НОК. Следовательно, НОК многочленов $f$ и $g$ не существует.

# Список литературы

[1] Альпин Ю.А., Ильин С.Н. Дискретная математика: Графы и автоматы. Учебное пособие. — Казань: Казанский государственный университет, 2007. — 78 с.

[2] Гуров С.И. Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. —М.: Либроком, 2013. — 352 с.

[3] Кострикин А.И. Введение в алгебру. Часть I. Основы алгебры. Учебник для ВУЗов. 3-е изд. — М.: ФИЗМАТЛИТ, 2004. — 272 с.

[4] Скорняков Л.А. Элементы теории структур. — М.: Наука, 1982. — 160 с.