МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ
ИНСТИТУТ
(государственный университет)

Элементы математической кибернетики и дискретной математики

Учебное пособие

Автор Бурцев А. А.

Москва — 2012

Оглавление

Рисунки к пособию необходимо смотреть в приложении в отдельном файле. Всего 6 рисунков. В приложении указаны номера соответствующих страниц. В тексте пособия на месте рисунков на этих страницах пропуски. Ситуация возникла по техническим причинам, но в изданной печатной книге указанный недостаток отсутствует.[1]

[1] Примечание автора.

ПРЕДИСЛОВИЕ

В данном учебном пособии излагается материал курса лекций по математической кибернетике, которые автор читает на протяжении ряда лет для студентов Московского физико-технического института (государственного университета) как спецкурс по выбору студента и как обязательный курс лекций для студентов 1-го курса ФАКИ, а также для иностранных студентов магистратуры. Пособие даёт некоторое знакомство с математической кибернетикой.

Лекции адресованы студентам 1-го курса, но могут быть полезны студентам старших курсов для написания курсовых и дипломных работ, аспирантам и научным работникам для научных исследований, проведения факультативных курсов и семинаров, учителям математики для элективных курсов.

Курс состоит из трёх частей. В первой части курса содержатся полезные для студентов сведения для изучения не только настоящего курса, но и других математических дисциплин, как-то: курсов математического анализа, алгебры и аналитической геометрии. Эти сведения можно отнести к математическому введению, обычно предваряющему курсы лекций. Во второй части излагается раздел дискретной математики булева алгебра, что необходимо для третьей, главной части – элементов математической кибернетики, относящихся к теории синтеза и сложности управляющих систем, а именно схем из функциональных элементов. Рассматриваются метод Лупанова, методы Карацубы, Тоома, дискретное преобразование Фурье, схемы для арифметики в конечных полях. Излагаются не только общеизвестные факты, необходимые для изучения математической кибернетики, но и некоторые недавно полученные научные результаты по актуальному направлению научных исследований. Наряду с математической строгостью, автор стремился к простоте изложения материала.

Я благодарю профессора кафедры дискретной математики

механико-математического факультета Московского государственного университета имени М. В. Ломоносова Сергея Борисовича Гашкова и доцента кафедры высшей алгебры механико-математического факультета Московского государственного университета имени М. В. Ломоносова Игоря Андреевича Чубарова за помощь в работе.

Отзывы

Автор учебного пособия «Элементы математической кибернетики и дискретной математики» – кандидат физико-математических наук, доцент кафедры высшей математики ФГАОУ ВПО «МФТИ (ГУ)» Бурцев Алексей Анатольевич.

Название учебного пособия соответствует его содержанию. Материал изложен логично и последовательно, на высоком научном и методическом уровне, соответствует современному развитию науки и техники, а также государственному образовательному стандарту и программе курса, читаемого автором в МФТИ. Наличествует качественный дидактический аппарат и иллюстративный материал по изучаемым темам.

Бурцев А. А. стремился, с одной стороны, к простоте изложения сложного материала, а с другой стороны, к полноте и строгости. Аналогов данному пособию в учебной литературе не имеется. Оно содержит и материалы собственных научных исследований автора.

С. Б. Гашков, И. А. Чубаров

Программа курса

1. Функции алгебры логики. Элементарные функции. Формулы. Реализация функций формулами.

2. Эквивалентность формул. Свойства элементарных функций. Принцип двойственности. Цепи эквивалентностей.

3. Разложение булевых функций по переменным. Разложение по одной переменной. Разложение по всем переменным. Конъюнктивные и дизъюнктивные нормальные формы. Совершенная дизъюнктивная нормальная форма. Совершенная конъюнктивная нормальная форма.

4. Применение к естественному языку. Сокращённые таблицы.

5. Полиномы Жегалкина.

6. Полнота и замкнутость. Базисы. Важнейшие замкнутые классы (то есть классы линейных, монотонных и самодвойственных функций, классы Т-ноль и Т-один).

7. Критерий полноты. Примеры полных и минимальных полных систем.

8. k-значные логики и их особенности. Представление о результатах Поста, Янова и Мучника (вопрос № 8 изучается ознакомительно, без доказательства теорем).

9. Схемы из функциональных элементов. Сложность и глубина схем. Элементарные методы синтеза. Функции Шеннона. Нижняя оценка для $L(n)$.

10. Метод Лупанова.

11. Метод Карацубы.

12. Метод Тоома.

13. Теорема о умножении целых чисел с почти линейной сложностью.

14. Конечные поля и их квадратичные расширения. Сложность арифметики в $GF(49)$.

15. Метод дискретного преобразования Фурье. Умножение многочленов седьмой степени над $GF(49)$ методом Фурье 16-го порядка. Метод Фурье 48-го порядка.

16. Элементы комбинаторного анализа: перестановки, размещения, сочетания, сочетания с повторениями. Группы подстановок. Индикаторы (характеристические функции) множеств. Формула включений-исключений. Бином Ньютона и его следствия. Метод производящих функций. Возвратные последовательности. Формулы Стирлинга и Валлиса. Определитель Вандермонда. Многочлен Лагранжа.

17. Множества и операции над ними. Принцип двойственности. Мощности. Теоремы Кантора и Кантора–Бернштейна. Теорема Цермело–Кантора (теорема Цермело–Кантора без доказательства). Существование собственных классов. Арифметика кардиналов. Континуум-гипотеза (в формулировке Кантора). Аксиоматические теории. Аксиомы (схемы аксиом) теории множеств по Цермело–Френкелю. Упорядоченная пара по Куратовскому и по Винеру.

18. Отношения. Бинарные отношения. Отношения эквивалентности и частичного порядка. Фактор-множество. Максимальный и наибольший элементы. Упорядоченные и вполне упорядоченные множества. Изоморфизм упорядоченных множеств. Понятие порядковых чисел (ординалов).

19. Фундированные множества. Математическая (финитная и трансфинитная) индукция.

20. Функции и их графики. Биекции, сюръекции, инъекции. Лемма о сюръективном и инъективном отображениях. Существование и единственность обратного отображения. Понятие о группе.

21. О схемах для умножения в башнях конечных полей.

Алфавиты

Опыт преподавания показывает, что студенты младших курсов недостаточно хорошо знают нижеследующие алфавиты, особенно готический. Для устранения этого пробела автор счел необходимым включить их в учебное пособие.

ЛАТИНСКИЙ АЛФАВИТ		
A, a а	J, j йот	S, s эс
B, b бэ	K, k ка	T, t тэ
C, c цэ	L, l эль	U, u у
D, d дэ	M, m эм	V, v вэ
E, e е	N, n эн	W, w дубль-вэ
F, f эф	O, o о	X, x икс
G, g гэ (же)	P, p пэ	Y, y игрек
H, h аш	Q, q ку	Z, z зет
I, i и	R, r эр	

ГОТИЧЕСКИЙ АЛФАВИТ		
$\mathfrak{A}, \mathfrak{a}$ а	$\mathfrak{J}, \mathfrak{j}$ йот	$\mathfrak{S}, \mathfrak{s}$ эс
$\mathfrak{B}, \mathfrak{b}$ бэ	$\mathfrak{K}, \mathfrak{k}$ ка	$\mathfrak{T}, \mathfrak{t}$ тэ
$\mathfrak{C}, \mathfrak{c}$ цэ	$\mathfrak{L}, \mathfrak{l}$ эль	$\mathfrak{U}, \mathfrak{u}$ у
$\mathfrak{D}, \mathfrak{d}$ дэ	$\mathfrak{M}, \mathfrak{m}$ эм	$\mathfrak{V}, \mathfrak{v}$ фау
$\mathfrak{E}, \mathfrak{e}$ э	$\mathfrak{N}, \mathfrak{n}$ эн	$\mathfrak{W}, \mathfrak{w}$ вэ
$\mathfrak{F}, \mathfrak{f}$ эф	$\mathfrak{O}, \mathfrak{o}$ о	$\mathfrak{X}, \mathfrak{x}$ икс
$\mathfrak{G}, \mathfrak{g}$ гэ	$\mathfrak{P}, \mathfrak{p}$ пэ	$\mathfrak{Y}, \mathfrak{y}$ ипсилон
$\mathfrak{H}, \mathfrak{h}$ ха	$\mathfrak{Q}, \mathfrak{q}$ ку	$\mathfrak{Z}, \mathfrak{z}$ цэт
$\mathfrak{I}, \mathfrak{i}$ и	$\mathfrak{R}, \mathfrak{r}$ эр	

ГРЕЧЕСКИЙ АЛФАВИТ		
A, α альфа	I, ι йота	P, ρ, ϱ ро
B, β бэта	K, κ каппа	$\Sigma, \sigma, \varsigma$ сигма
Γ, γ гамма	Λ, λ ламбда (лямбда)	T, τ тау
Δ, δ дельта	M, μ мю	Υ, υ ипсилон
E, ε, ϵ эпсилон	N, ν ню	Φ, ϕ фи
Z, ζ дзета	Ξ, ξ кси	X, χ хи
H, η эта	O, o омикрон	Ψ, ψ пси
$\Theta, \theta, \vartheta$ тэта	Π, π, ϖ пи	Ω, ω омега

ГЛАВА 1

МАТЕМАТИЧЕСКОЕ ВВЕДЕНИЕ

§ 1. Множества

1. Множество есть совокупность различных элементов. Запись $x \in M$ означает, что x является элементом множества M. Запись $x \notin M$ означает, что x не является элементом множества M.

2. Множество A является подмножеством множества B, если все элементы A являются элементами B:
$$(A \subset B) \Leftrightarrow \forall\, x\ (x \in A \Rightarrow x \in B).$$

3. Два множества равны тогда и только тогда, когда они состоят из одних и тех же элементов:
$$(A = B) \Leftrightarrow \forall\, x\ (x \in A \Leftrightarrow x \in B).$$

4. Пустое множество $\varnothing$ не содержит элементов и является подмножеством любого множества. Отметим, что $\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}$ – разные множества. По Нейману натуральные числа определяются следующим образом: $0 = \varnothing, 1 = \{\varnothing\}, 2 = \{\{\varnothing\}\}, 3 = \{\{\{\varnothing\}\}\}$ и так далее. $\{\ \} = \varnothing$.

5. Пересечение $A \cap B$ двух множеств A и B состоит из элементов, принадлежащих обоим множествам A и B:
$$A \cap B = \{x : x \in A \text{ и } x \in B\}.$$

6. Объединение $A \cup B$ состоит из элементов, принадлежащих хотя бы одному из множеств A и B:
$$A \cup B = \{x : x \in A \text{ или } x \in B\}.$$
Если при этом $A \cap B = \varnothing$, то говорят о дизъюнктном объединении A и B. Запись: $A \sqcup B$ или $A + B$. Если

$C = A + B$, то говорят о разбиении множества C на множества A и B.

7. Разность $A \setminus B$ состоит из элементов, принадлежащих A и не принадлежащих B:

$$A \setminus B = \{x : x \in A \text{ и } x \notin B\}.$$

Если множество B является подмножеством множества A, то разность $A \setminus B$ называется также *дополнением* B до A. Если рассматриваются лишь подмножества A, то множество A называется *универсумом рассуждения*. Тогда запись $\overline{B}$ означает дополнение B до A. Ясно, что $\overline{\overline{B}} = B$.

8. Симметрическая разность $A \triangle B$ состоит из элементов, принадлежащих ровно одному из множеств A и B:

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

9. Множество, элементами которого являются $a_1, a_2, \ldots$, обозначается $\{a_1, a_2, \ldots\}$. Например, $\{a, b\}$ есть множество, состоящее из элементов a и b. Если при этом $a \neq b$, то $\{a, b\}$ называется *неупорядоченной парой* элементов a и b. Ясно, что $\{a, b\} = \{b, a\} = \{a, a, b\}$. Множество $\{a, a\} = \{a\}$. Это одноэлементное множество с элементом a.

10. Говорят, что на множестве A задана функция (отображение) f во множество B, если всякому элементу $x \in A$ соответствует некоторый и только один элемент $y \in B$. Записи: $f : A \to B$, $y = f(x)$. Элемент y называется *образом элемента x при отображении f*.

11. Через $\{x : \Phi(x)\}$ или $\{x \mid \Phi(x)\}$ обозначается множество таких элементов x, для которых выполняется (является истинным) условие Φ. Через $\{f(x) : x \in A\}$ обозначается множество образов $f(x)$ элементов $x \in A$

при отображении (функции) f, определённом на A. Такие множества существуют для любых A, f, Φ.

12. Множества бывают конечными (содержащими не более n элементов, $n \in \mathbb{N}$) и бесконечными (содержащими бесконечно много элементов). Существует, по крайней мере, одно бесконечное множество, а именно множество натуральных чисел $\mathbb{N} = \{1, 2, 3, \ldots\}$. В математической логике 0 принято относить к натуральным числам, полагая $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\} = \mathbb{N} \cup \{0\}$ множеством натуральных чисел. Пустое множество содержит 0 элементов и считается конечным.

13. Для любого множества A существует множество $\mathcal{P}(A)$ всех подмножеств множества A (булиáн A). Например, если $A = \{1, 2\}$, то $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$. $\mathcal{P}(\varnothing) = \{\varnothing\} \neq \varnothing$.

14. Пусть $A = \{A_\alpha : \alpha \in \mathfrak{A}\}$. Тогда $\bigcup A = \bigcup\limits_{\alpha \in \mathfrak{A}} A_\alpha = \{x : \exists\, \alpha \in \mathfrak{A}\ x \in A_\alpha\}$, $\bigcap A = \bigcap\limits_{\alpha \in \mathfrak{A}} A_\alpha = \{x : \forall\, \alpha \in \mathfrak{A}\ x \in A_\alpha\}$. В частности, $\bigcup\limits_{n=1}^{\infty} A_n = \bigcup\limits_{n \in \mathbb{N}} A_n$, $\bigcap\limits_{n=1}^{\infty} A_n = \bigcap\limits_{n \in \mathbb{N}} A_n$, $\bigcup\limits_{s=1}^{n} A_s = \bigcup\limits_{s \in \overline{1,n}} A_s$, $\bigcap\limits_{s=1}^{n} A_s = \bigcap\limits_{s \in \overline{1,n}} A_s$, где $\overline{1,n} = \{1, 2, \ldots, n\}$ – начальный отрезок натурального ряда длины n.

15. Через (a, b) обозначим упорядоченную пару элементов a и b. Основное свойство упорядоченных пар: $(a_1, b_1) = (a_2, b_2) \Leftrightarrow a_1 = a_2$ и $b_1 = b_2$. По Куратовскому $(a, b) = \{a, b, \{a\}\}$. Ясно, что если так определить упорядоченную пару, то основное свойство будет выполнено. $\forall\, n \in \mathbb{N}$ можно образовать кортеж длины n (упорядоченный набор длины n, упорядоченную n-ку) $(a_1, \ldots, a_n)$ элементов $a_1, \ldots, a_n$, так что

$(a_1,\ \ldots,\ a_n) = (b_1,\ \ldots,\ b_n) \Leftrightarrow a_1 = b_1,\ \ldots,\ a_n = b_n$. Основное свойство пары будет также выполнено, если упорядоченную пару определить по Винеру: $(a,b) = \{\{\varnothing,\{a\}\},\{\{b\}\}\}$.

16. Прямым (или декартовым) произведением множеств A и B называется множество $A \times B$, состоящее из всех упорядоченных пар (a,b) таких, что $a \in A$ и $b \in B$. Аналогично, прямое произведение множеств $A_1,\ldots,A_n$ есть множество всех кортежей $(a_1,\ \ldots,\ a_n)$ таких, что $a_1 \in A_1,\ \ldots,\ a_n \in A_n$. Например, $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ есть плоскость Oxy, а $\mathbb{R}^3 = \mathbb{R}\times\mathbb{R}\times\mathbb{R}$ есть пространство $Oxyz$, $\{1,2\}\times\{2,3\} = \{(1,2),(2,2),(1,3),(2,3)\}$.

17. Принцип двойственности. *a)* $S \setminus \bigcup\limits_{\alpha\in\mathfrak{A}} A_\alpha = \bigcap\limits_{\alpha\in\mathfrak{A}} S\setminus A_\alpha$; *b)* $S \setminus \bigcap\limits_{\alpha\in\mathfrak{A}} A_\alpha = \bigcup\limits_{\alpha\in\mathfrak{A}} S\setminus A_\alpha$.

Доказательство: пусть $x \in S \setminus \bigcup\limits_{\alpha\in\mathfrak{A}} A_\alpha$. Следовательно, $x \in S$ и $x \notin \bigcup\limits_{\alpha\in\mathfrak{A}} A_\alpha$. Значит, $x \in S$ и для любого $\alpha \in \mathfrak{A}$ $x \notin A_\alpha$. Значит, для всех $\alpha \in \mathfrak{A}$ $x \in S\setminus A_\alpha$. Следовательно, $x \in \bigcap\limits_{\alpha\in\mathfrak{A}} S\setminus A_\alpha$. Ввиду произвольности x имеем: $S \setminus \bigcup\limits_{\alpha\in\mathfrak{A}} A_\alpha \subset \bigcap\limits_{\alpha\in\mathfrak{A}} S\setminus A_\alpha$. Обратно, пусть $x \in \bigcap\limits_{\alpha\in\mathfrak{A}} S\setminus A_\alpha$. Значит, x принадлежит каждому множеству $S \setminus A_\alpha$. Значит, $x \in S$ и для всех α $x \notin A_\alpha$. Отсюда вытекает, что $x \in S \setminus \bigcup\limits_{\alpha\in\mathfrak{A}} A_\alpha$. Ввиду произвольности x находим, что $\bigcap\limits_{\alpha\in\mathfrak{A}} S\setminus A_\alpha \subset S \setminus \bigcup\limits_{\alpha\in\mathfrak{A}} A_\alpha$. Утверждение *a)* доказано, поскольку установлено, что левая часть равенства есть как подмножество, так и надмножество правой части равенства. Аналогично доказывается *b)*.

18. Если $A \subset S$, то разность $S \setminus A$ называют дополнением

множества A до множества S. Иногда эта разность обозначается $\overline{A}$. Очевидно, $\overline{\overline{A}} = A$, $\overline{\varnothing} = S$, $\overline{S} = \varnothing$. Принцип двойственности можно сформулировать следующим образом: дополнение объединения множеств есть пересечение дополнений этих множеств, дополнение пересечения множеств есть объединение дополнений этих множеств. В частности, $\overline{A\cup B} = \overline{A}\cap\overline{B}$, $\overline{A\cap B} = \overline{A}\cup\overline{B}$.

19. Для любого непустого множества S попарно непересекающихся множеств существует некоторое множество, содержащее в качестве своих элементов ровно по одному элементу из каждого элемента множества S (*аксиома выбора*).

20. Не существует бесконечной убывающей последовательности $x_1 \ni x_2 \ni x_3 \ldots$ (*аксиома фундирования*).

    Следствие: $A \notin A$; если $A \in B$, а $B \in C$, то $C \notin A$ для любых множеств $A,\ B,\ C$.

21. Отметим некоторые тождества для множеств.

    $(A\cup B)\cap C = (A\cap C)\cup(B\cap C)$, $(A\cap B)\cup C = (A\cup C)\cap(B\cup C)$.

    Эти равенства суть взаимная дистрибутивность операций объединения и пересечения множеств. Каждое из этих равенств немедленно следует из другого согласно принципу двойственности. Отметим также, что

$$A\cup A = A,\ A\cap A = A,\ A\cap\varnothing = \varnothing,\ A\cup\varnothing = A,$$
$$A\ \triangle\ \varnothing = A, A\times\varnothing = \varnothing, A\ \triangle\ A = \varnothing,$$
$$(A\cup B)\cup C = A\cup(B\cup C),\ (A\cap B)\cap C = A\cap(B\cap C),$$
$$(A\ \triangle\ B)\ \triangle\ C = A\ \triangle\ (B\ \triangle\ C).$$

В изложенном кратком экскурсе содержится аксиоматика теории множеств по Цермело–Френкелю (аксиоматика ZF, 1908 г.).

§ 2. Бинарные отношения и функции, порядковые числа

Бинарным отношением между элементами множеств A и B называется любое подмножество R множества $A \times B$. Вместо $(x, y) \in R$ часто пишут xRy. *Областью (множеством) определения* бинарного отношения R называется множество δ_R, состоящее из всех таких x, что упорядоченная пара $(x, y) \in \in R$ хотя бы для одного y. *Множеством (областью) значений* ρ_R бинарного отношения R называется множество всех таких y, что пара $(x, y) \in R$ хотя бы для одного x. *Обратным отношением* для бинарного отношения R называется отношение R^{-1}, состоящее из всех таких упорядоченных наборов (x, y), что $(y, x) \in R$. Отметим, что $\delta_{R^{-1}} = \rho_R$ и $\rho_{R^{-1}} = \delta_R$. Если R_1 – отношение между элементами множеств A и B, а R_2 – отношение между элементами множеств B и C, то можно образовать произведение (композицию) отношений R_1 и R_2. *Произведением $R_1 \circ R_2$ отношений R_1 и R_2* называется отношение между элементами множеств A и C, состоящее из всех пар (x, z), для которых найдётся такой элемент $y \in B$, что $(x, y) \in R_1$ и $(y, z) \in R_2$.

Бинарное отношение f называется *функцией*, если из $(x, y) \in f$ и $(y, z) \in f$ следует $y = z$. Функция f называется функцией из A в B, если $\delta_f \subset A$ и $\rho_f \subset B$. Множество A – *область (множество) отправления* функции f, множество B – *область (множество) прибытия* функции f, множество δ_f – *область (множество) определения* функции f, множество ρ_f – *область (множество) значений* функции f. Если $\delta_f = = A$, то пишут $f : A \to B$. Если f – функция и $(x, y) \in f$, то обычно пишут $y = f(x)$ и называют y *значением* функции f при значении аргумента x. Если не существует такое y, что $(x, y) \in f$, то выражение $f(x)$ считается *неопределенным*.

Если $f : A \to B$ и $D \subset B$, то множество $f^{-1}(D) = \{x \in$

$\in A : f(x) \in D\}$ называется *полным прообразом* множества D при отображении (функции) f. Полный прообраз элемента y при отображении $f : A \to B$ есть множество $f^{-1}(y) = \{x \in \in A : f(x) = y\}$. Если $f^{-1}(y) = \{x\}$, то иногда говорят, что элемент x есть прообраз y (при отображении f). Образом подмножества $D \subset A$ при отображении $f : A \to B$ называется множество $\{f(x) : x \in D\}$. В частности, подмножество $f(A) \subset \subset B$ есть множество значений функции f. Справедливы следующие утверждения:

1. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
2. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.
3. $f(A \cup B) = f(A) \cup f(B)$.
4. $f(A \cap B) \not\equiv f(A) \cap f(B)$ в общем случае.
5. $f^{-1}(S \setminus A) = S \setminus f^{-1}(A)$.
6. $f(S \setminus A) \not\equiv S \setminus f(A)$ в общем случае.

Задача. Докажите утверждения 1–6.

Сказанное о бинарных отношениях распространяется и на функции как частный случай бинарного отношения. Функцию, кратко говоря, называют ещё *функциональным бинарным отношением*. В частности, для функций $f : X \to Y$ и $g : Y \to Z$ определено произведение (композиция) $h = g \circ f$, $h : X \to Z$, $h(x) = g(f(x))$ для любого $x \in X$. Пусть $f : X \to \to Y$, $g : X \to Z$, $h : Z \to T$. Очевидно, $(h \circ g) \circ f = h \circ (g \circ f)$.

Графиком Γ_f функции f называется множество $\{(x, y) \in \in f\} = \{(x, f(x)) : x \in \delta_f\}$. Итак, у функции есть область отправления, область прибытия, область определения, область значений и график. Сама функция суть функциональное бинарное отношение (между элементами области отправления и области прибытия).

Тождественная функция $e_A = \{(x, x) : x \in A\}$. Очевидно, $e_A(x) = x$ для любого элемента $x \in A$.

Функция f называется последовательностью, если область её определения есть множество натуральных чисел $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Среди функций можно выделить *инъекции*, *сюръекции* и *биекции*.

Отображение $f : X \to Y$ называется *инъективным*, если для любых $x_1, x_2 \in X$ выполнено $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, то есть разные точки (элементы X) переходят (отображаются при помощи f) в разные точки (элементы множества Y), или, что то же самое, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. Инъективное отображение называют иногда взаимно однозначным отображением, или $1-1$-отображением (функцией).

Отображение $f : X \to Y$ называется *сюръективным*, если $f(X) = Y$. Иначе говоря, отображение $f : X \to Y$ называется сюръективным, если для всякого элемента $y \in Y$ найдётся хотя бы один элемент $x \in X$, который перешел в этот y при отображении f, то есть такой x, что $y = f(x)$.

Отображение $f : X \to Y$ называется *биективным*, если оно сюръективно и инъективно одновременно. Иначе говоря, отображение $f : X \to Y$ называется *биективным*, если всякий элемент $y \in Y$ имеет единственный прообраз $x \in X$. Очевидно, композиция $f \circ g$ биекций f и g есть биекция. Биекцию ещё называют взаимно однозначным соответствием, или $1-1$-соответствием.

Если $f : X \to Y$, $g : Y \to X$ и $g \circ f = e_X$, то говорят, что g – левое обратное (отображение) для f, а f – правое обратное для g. Пусть, кроме того, $g' : Y \to X$ и $f \circ g' = e_Y$. Тогда $g = g'$. В самом деле, $g = g \circ e_Y = g \circ (f \circ g') = (g \circ f) \circ g' = e_X \circ g' = g'$. В таком случае f имеет двустороннее обратное (или просто обратное) отображение $f^{-1} : Y \to X$, $f^{-1} = g = g'$. Обратное отображение, если существует, то единственно: предположив

от противного, что у отображения f имеется два обратных отображения, находим, что одно из них левое обратное, а другое правое обратное, а такие отображения совпадают. Так как $f^{-1} \circ f = e_X$ и $f \circ f^{-1} = e_Y$, то в силу единственности обратного отображения $(f^{-1})^{-1} = f$. Это значит, что если отображение f^{-1} обратное для f, то f обратное для f^{-1}.

Если $g \circ f = e_X$, то отображение g – сюръекция, а отображение f – инъекция (*лемма о сюръективном и инъективном отображениях*). В самом деле, так как $\forall\, x \in X\ g(f(x)) = x$, то, положив $f(x) = y$, находим, что $\forall\, x \in X\ \exists\, y \in Y\ :\ g(y) = x$, то есть g – сюръекция. Если $f(x_1) = f(x_2)$, то $g(f(x_1)) = g(f(x_2))$, но $g(f(x_1)) = x_1$ и $g(f(x_2)) = x_2$. Значит, если $f(x_1) = f(x_2)$, то $x_1 = x_2$ и f – инъекция. Пусть отображение $f : Y \to X$ имеет обратное f^{-1}. Тогда $f^{-1} \circ f = e_X$. Значит, f – инъекция. А так как $f \circ f^{-1} = e_Y$, то f – сюръекция. Таким образом, f – биекция. Итак, чтобы отображение f имело обратное, необходимо, чтобы f было биекцией. Этого, очевидно, и достаточно, ведь если $f : X \to Y$ – биекция, то всякий элемент $y \in Y$ имеет единственный прообраз x. Тогда обратное к f отображение g можно задать правилом $g(y) = x$ (для указанных выше x и y).

Пусть $R \subset A \times A$ – бинарное отношение между элементами множества A (бинарное отношение на A). Бинарное отношение R на множестве A называется

рефлексивным, если $(x, x) \in R$ для всех A из R (диагональ множества $A \times A$ содержится в R),

иррефлексивным, если $(x, x) \notin R$ для любого $x \in A$,

симметричным, если из $(x, y) \in R$ следует $(y, x) \in R$,

антисимметричным, если из $(x, y) \in R$ и $(y, x) \in R$ следует $x = y$,

транзитивным, если из $(x, y) \in R$ и $(y, z) \in R$ следует $(x, z) \in R$.

Бинарное отношение на множестве A называется *частичным упорядочением* (или *частичным порядком*), если

это отношение рефлексивно, антисимметрично и транзитивно. Частичное упорядочение обозначается знаком $\leqslant$. Множество A с заданным на нём частичным порядком $\leqslant$ называется *частично упорядоченным* множеством и обозначается знаком $(A, \leqslant)$. Элементы x и y из A называются *сравнимыми*, если верно, что $x \leqslant y$. В таком случае говорят также, что x *предшествует* y, а y *следует* за x. Если любые два элемента частично упорядоченного множества A сравнимы, то множество A называется *линейно упорядоченным* множеством, или *совершенно упорядоченным множеством*, или *упорядоченным множеством*, а порядок – *линейным*. Если всякое непустое подмножество линейно упорядоченного множества A имеет *наименьший* элемент, то есть элемент, предшествующий всем элементам данного подмножества, то порядок называется *полным*, а само множество *вполне упорядоченным*. Наименьший элемент следует отличать от *минимального* элемента. Элемент m частично упорядоченного множества M называется минимальным, если $\forall\ x \in M\ x \leqslant \leqslant m \Rightarrow x = m$. В частично упорядоченном множестве может быть несколько минимальных элементов, но наименьший, если существует, только один. Наименьший элемент сравним со всеми элементами частично упорядоченного множества, а минимальный элемент может быть не сравним с некоторыми элементами.

Бинарное отношение на множестве A называется *строгим частичным упорядочением* (или *строгим частичным порядком*), если это отношение иррефлексивно и транзитивно (в таком случае оно и антисимметрично). Строгое частичное упорядочение обозначается обычно знаком $<$. Множество A с заданным на нём строгим частичным порядком $<$ называется *строго частично упорядоченным* и обозначается $(A, <)$. Аналогично линейному порядку определяется *строгий линейный порядок*.

Бинарное отношение на множестве A называется

отношением эквивалентности, если это отношение рефлексивно, симметрично и транзитивно. Отношение эквивалентности обычно обозначают знаком «тильда» $\sim$, например, $x \sim y$ означает, что x и y состоят в некотором данном (рассматриваемом) отношении эквивалентности. *Классом эквивалентности* элемента $a \in A$ называется множество

$$[a] = \{x \in A : x \sim a\}.$$

Для любых элементов $a,\ b \in A$ их классы эквивалентности $[a]$ и $[b]$ либо совпадают, либо не имеют общих элементов. В самом деле, пусть существует $z \in [a] \cap [b]$. Возьмём произвольный элемент $x \in [a]$. Тогда $x \sim a$ и $z \sim a$. Следовательно, $x \sim a$ и $a \sim z$. Следовательно, $x \sim \sim z$. Так как $x \sim z$ и $z \sim b$, то $x \sim b$. Значит, $x \in \in [b]$. Значит, $[a] \subset [b]$. Аналогично устанавливается, что $[b] \subset [a]$, поэтому $[a] = [b]$. Утверждение доказано. Поскольку всякий элемент $a \in A$ принадлежит $[a]$, а классы эквивалентности либо не имеют общих элементов, либо совпадают, то множество A разбивается отношением эквивалентности на классы эквивалентности: $A = \bigsqcup\limits_{a \in A} [a]$. Множество классов эквивалентности называется *фактор-множеством* и обозначается $A/\sim$. Например, равенство приложенных векторов в пространстве является отношением эквивалентности. Фактор-множество есть совокупность свободных векторов. Совокупность приложенных к одной и той же точке векторов в пространстве является линейным пространством. На фактор-множестве можно ввести аналогичную алгебраическую структуру, что и на исходном множестве, и фактор-множество также будет линейным пространством, называемым фактор-пространством. Поступать так типично в общей алгебре.

Обратно, если имеется разбиение множества на классы (подмножества), то найдётся отношение эквивалентности, которым это множество разбивается на эти классы: два

элемента объявим эквивалентными, если они принадлежат одному подмножеству. Такое бинарное отношение рефлексивно, симметрично и транзитивно, потому действительно является отношением эквивалентности.

Пример. Пусть на множестве X задано отношение эквивалентности $\sim$. Тогда отображение $p : x \mapsto p(x) = [x]$, переводящее элемент x в класс эквивалентности, которому принадлежит x, называется *канонической проекцией* (или *естественным отображением*). Очевидно, отображение $p : X \to X/\sim$ множества X в фактор-множество $X/\sim$ есть сюръекция.

Возьмём функцию $f : X \to Y$. Скажем, что $x_1 \sim x_2$, если $f(x_1) = f(x_2)$. Это отношение эквивалентности на X. Отображение f индуцирует отображение $\overline{f}([x]) = f(x)$. Отображение $\overline{f} : X/\sim \to Y$, $[x] \mapsto f(x)$ есть инъекция.

Очевидно, $\overline{f} \circ p = f$, где p – каноническая проекция. Таким образом, всякая функция может быть представлена как композиция инъекции и сюръекции.

Пример. Два частично упорядоченных множества $(A, \leqslant)$ и $(B, \leqslant)$ называются изоморфными, если между ними существует изоморфизм, то есть биекция $f : A \to B$, сохраняющая порядок: для любых элементов x, y из A выполняется $x \leqslant y \Rightarrow f(x) \leqslant f(y)$. Нетрудно видеть, что изоморфизм между вполне упорядоченными множествами есть отношение эквивалентности. Поэтому упорядоченные множества распадаются на классы эквивалентных множеств, называемые порядковыми типами (или ординалами). Например, множество натуральных чисел вполне упорядочено стандартным образом, его порядковый тип обозначается ω. Полагая по определению, что всякое нечётное число меньше всякого четного числа, а чётные и нечетные числа упорядочены стандартно, мы получим множество натуральных чисел, упорядоченное по типу $\omega + \omega$. Аналогично

можно получить порядковые типы $\omega + \omega + \omega$, $\underbrace{\omega + \omega + \cdots + \omega}_{n} = \omega \cdot n$.

§ 3. Понятие о группе

Рассмотрим множество $M = \{f : X \to X | f - \text{биекция}\}$ всех биекций из X в это же множество X. Композиция биекций есть биекция, тождественное отображение $e = e_X$ есть биекция, обратное к биекции f отображение f^{-1} есть биекция. Таким образом, на множестве M определена бинарная алгебраическая операция $\circ$ и для любых f, g, h из M справедливо:

1. $(f \circ g) \circ h = f \circ (g \circ h)$,
2. $f \circ e = e \circ f = f$,
3. $f^{-1} \circ f = f \circ f^{-1} = e$.

Множество M произвольной природы, на котором определена бинарная алгебраическая операция $\circ$ и выполнены свойства 1, 2, 3, называется *группой*. Элемент $e \in M$ называется *нейтральным элементом* группы. Элемент f^{-1} называется *обратным* (или *противоположным*) к f элементом. Если алгебраическую операцию $\circ$ обозначать $+$ и называть *сложением*, противоположный к f элемент обозначать $-f$, нейтральный элемент e называть *нулем* и обозначать 0, то аксиомы группы будут записаны в *аддитивной форме*, а сама группа будет называться *аддитивной группой*. Если алгебраическую операцию $\circ$ обозначать точкой $\cdot$ и называть *умножением*, а нейтральный элемент e называть *единицей* и обозначать 1, обратный к f элемент обозначать f^{-1}, то аксиомы группы будут записаны в *мультипликативной форме*, а сама группа будет называться *мультипликативной группой*.

Докажем, что *если для какого-нибудь элемента g группы G найден элемент e_g, удовлетворяющий одному из условий*

$$ge_g = g \text{ или } e_g g = g,$$

то

$$e_g = e.$$

Пусть $ge_g = g$. Для любого элемента g' имеем

$$g'e_g = (g'e)e_g = g'(g^{-1}g)e_g = g'g^{-1}(ge_g) = g'g^{-1}g = g'(g^{-1}g) = \\ = g'e = g'.$$

Таким образом, для любого элемента g' выполняется $g'e_g = g'$. Возьмём, в частности, $g' = e$. Получаем

$$ee_g = e.$$

С другой стороны, по определению элемента e имеем

$$ee_g = e_g.$$

Из последних двух равенств вытекает

$$e_g = e.$$

Пусть теперь для некоторого элемента g нашелся элемент e_g такой, что $e_g g = g$. Тогда для любого элемента g' имеем

$$e_g g' = e_g(eg') = e_g(gg^{-1})g' = (e_g g)g^{-1}g' = gg^{-1}g' = eg' = g'.$$

Таким образом, для любого элемента g' выполняется $e_g g' = g'$. Возьмём, в частности, $g' = e$. Получаем

$$e_g e = e.$$

С другой стороны, по определению элемента e имеем

$$e_g e = e_g.$$

Из последних двух равенств вытекает

$$e_g = e.$$

Из доказанной теоремы вытекает, во-первых, единственность нейтрального элемента в группе, а во-вторых, в аксиомах группы достаточно потребовать лишь, чтобы выполнялось какое-нибудь одно из условий $f \circ e = f$

или $e \circ f = f$ для всех f, тогда другое из этих условий будет выполняться автоматически. Таким образом, приведённая аксиоматика группы зависима: можно уменьшить список аксиом, исключив некоторые утверждения, которые будут выводиться из оставшихся в списке аксиом утверждений, то есть будут теоремами.

Замечание. Аксиоматическая теория – это множество аксиом и всех теорем, которые можно получить из этих аксиом при помощи логики – некоторых правил вывода. *Непротиворечивость* аксиоматики означает, что в теории не найдётся утверждений, каждое из которых логически исключает другое. *Независимость* аксиоматики означает, что всякая аксиома не может быть получена из других аксиом при помощи правил вывода (логического рассуждения). *Полнота* системы аксиом означает, что всякое синтаксически корректное (осмысленное в рамках понятий данной теории) утверждение можно логически либо доказать, либо опровергнуть (либо оно является аксиомой этой теории). *Категоричность* системы аксиом означает, что она определяет собой единственный (с точностью до *изоморфизма*) объект.

Докажем, что *если для данного элемента g группы G найдётся элемент g', удовлетворяющий одному из условий*

$$g'g = e \text{ или } g'g = e,$$

то

$$g' = g^{-1}.$$

Пусть

$$gg' = e,$$

тогда

$$g^{-1}(gg') = g^{-1} = (g^{-1}g)g' = eg' = g',$$

то есть

$$g' = g^{-1}.$$

Пусть

$$g'g = e,$$

тогда

$$(g'g)g^{-1} = g^{-1} = g'(gg^{-1}) = g'e = g',$$

то есть

$$g' = g^{-1}.$$

Из доказанной теоремы вытекает, во-первых, единственность обратного элемента f^{-1} к элементу f в группе, а во-вторых, в аксиомах группы достаточно потребовать лишь, чтобы выполнялось какое-нибудь одно из условий $f \circ f^{-1} = e$ или $f^{-1} \circ f = e$, тогда другое из этих условий будет выполняться автоматически.

В силу единственности обратного элемента из условия $f \circ f^{-1} = e$ имеем также

$$(f^{-1})^{-1} = f.$$

Группа $(G, \circ)$ называется *коммутативной группой*, или *абелевой группой*, если для всех элементов f и g выполнено

$$f \circ g = g \circ f.$$

§ 4. О изоморфизме двух групп

Пусть $(G, +)$ – какая-либо аддитивная группа, а $(G', \cdot)$ – какая-либо мультипликативная группа. Функция $f : G \to G'$ называется *гомоморфизмом*, если

$$\forall\, x \in G\ \forall\, y \in G'\ f(x+y) = f(x)f(y).$$

Нетрудно видеть, что $f(0) = f(0+0) = f(0)f(0)$, откуда вытекает, что $f(0) = 1$.

Также $f(0) = f(x+(-x)) = f(x)f(-x) = 1$. Следовательно, $f(-x) = (f(x))^{-1}$.

Если гомоморфизм $f : G \to G'$ есть биекция, то f называется *изоморфизмом*. Группы G и G' называются *изоморфными*, если существует изоморфизм $f : G \to G'$. Обозначение: $G \cong G'$.

Ясно, что отношение $\cong$ рефлексивно, симметрично и транзитивно. Поэтому группы распадаются на классы изоморфных групп.

Задача. Докажите, что *строго монотонная функция* $f : \mathbb{R} \to \mathbb{R}$ *осуществляет изоморфизм аддитивной группы действительных чисел и мультипликативной группы положительных действительных чисел тогда и только тогда, когда* f *есть показательная функция:* $f(x) = a^x$, *где* $a = f(1)$.

§ 5. Кардинальные числа

Множества A и B называются *равномощными* (*эквивалентными*), если существует (хотя бы одна) биекция $f : A \to B$. Запись $A \sim B$ означает, что множества A и B равномощны. Очевидно, каковы бы ни были множества A, B, C, справедливы следующие утверждения:

1) $A \sim A$,

2) если $A \sim B$, то $B \sim A$,

3) если $A \sim B$ и $B \sim C$, то $A \sim C$.

Так как отношение равномощности между множествами рефлексивно, симметрично и транзитивно, то это есть отношение эквивалентности, и множества распадаются на непересекающиеся классы равномощных множеств. Каждый такой класс называется *мощностью* множества (любого элемента – представителя данного класса), или *кардинальным числом.*

Множество M называется счетным, если оно равномощно множеству натуральных чисел $\mathbb{N}$. Таким образом, множество счетно, если его элементы можно представить в виде последовательности. Например, множество целых чисел $\mathbb{Z}$ счетно, так как элементы $\mathbb{Z}$ можно представить в виде последовательности $0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3, \ldots$

Пусть $A \subset B$, и множество B счетно. Тогда множество A конечно или счетно. Если множество A бесконечно, то оно счетно. В самом деле, так как элементы множества B можно представить в виде последовательности (b_n), то элементы бесконечного множества A образуют в этой

последовательности подпоследовательность $a_k = b_{n_k}$. Значит, A счетно.

Объединение конечного или счетного числа счетных множеств счетно. В самом деле, пусть A_1, A_2, ... – счетное число множеств, каждое из которых счетно. Выпишем элементы каждого из этих множеств A_i в виде последовательности (a_n^i) в i-й строке следующей таблицы:

$a_1^1,\ a_2^1,\ a_3^1,\ \ldots$
$a_1^2,\ a_2^2,\ a_3^2,\ \ldots$
$a_1^3,\ a_2^3,\ a_3^3,\ \ldots$
$\ldots\ldots\ldots\ldots$

Тогда элементы $B = A_1 \cup A_2 \cup A_3 \cup \ldots$ можно представить в виде последовательности $a_1^1,\ a_2^1,\ a_1^2,\ a_1^3,\ a_2^2,\ a_3^1\, a_4^1,\ a_3^2,\ a_2^3,\ a_1^4\ \ldots$ Значит, B счетно. Этот метод называется диагональной процедурой Кантора.

Например, множество рациональных чисел $\mathbb{Q}$ счетно, так как является бесконечным подмножеством множества дробей вида $\frac{m}{n}$, где m – целое число, а n – натуральное. Множество таких дробей с данным знаменателем n счетно, так как их числители образуют счетное множество целых чисел $\mathbb{Z}$. Таким образом, множество дробей вида $\frac{m}{n}$, где m – целое число, а n – натуральное число, счетно, так как является счетным объединением счетных множеств.

Множество $\mathbb{N}^k = \underbrace{\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}}_{k \text{ раз}}$ счетно. Доказать этот факт можно индукцией по k. Базис индукции: множество $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N} = \{1\} \times \mathbb{N} \cup \{2\} \times \mathbb{N} \cup \{3\} \times \mathbb{N} \cup \ldots$ счетно как объединение счетного числа счетных множеств. Шаг индукции: по предположению индукции множество $\mathbb{N}^k$ счетно. Поэтому множество $\mathbb{N}^{k+1} = \mathbb{N} \times \mathbb{N}^k = \{1\} \times \mathbb{N}^k \cup \{2\} \times \mathbb{N}^k \cup \cup\{3\}\times\mathbb{N}^k \cup \ldots$ счетно как объединение счетного числа счетных множеств.

Множество всех конечных последовательностей натуральных чисел счетно. В самом деле, достаточно

доказать, что множество $M = \bigcup_{n=1}^{\infty} \mathbb{N}^n$ счетно, а это верно, так как M есть объединение счетного числа счетных множеств.

Пусть P – конечное или счетное непустое множество (алфавит). Элементы P назовём буквами алфавита P, слово – конечная последовательность букв, P^* – множество всех слов алфавита P. Множество P^* счетно: буквы алфавита P можно занумеровать натуральными числами 1, 2, ..., n, ... , тогда P^* есть бесконечное подмножество счетного множества всех конечных последовательностей натуральных чисел и, таким образом, счетно. Например, счетно множество всех текстов, написанных на русском языке, счетно множество всех программ для ЭВМ.

Число называется алгебраическим, если оно является корнем (вообще говоря, комплексным) какого-либо многочлена с рациональными коэффициентами. Можно показать, что множество всех алгебраических чисел $\mathbb{A}$ образует алгебраическое поле. Множество всех многочленов с рациональными коэффициентами счетно. Докажем это. Множество рациональных чисел счетно, поэтому рациональные числа можно выписать в виде последовательности (q_n) и каждое рациональное число q_n из указанной последовательности кодировать последовательностью n единичек $11\ldots1$. Степень x^n полинома можно кодировать последовательностью n иксов: $xx\ldots x$. Тогда многочлен суть слово четырёхбуквенного алфавита $\{1, x, +, -\}$. Множество слов такого алфавита счетно, значит, счетно множество всех многочленов с рациональными коэффициентами как бесконечное подмножество счетного множества. Множество (комплексных) корней данного многочлена конечно. Поэтому множество всех корней всех многочленов с рациональными коэффициентами счетно как бесконечное подмножество счетного объединения конечных множеств.

Любое множество непересекающихся промежутков ненулевой длины на числовой прямой конечно или счетно. В самом деле, каждый такой промежуток содержит рациональное число, а множество рациональных чисел счетно.

Множество точек разрыва монотонной функции конечно или счетно. Как известно, разрывы монотонной функции суть скачки, а множество непересекающихся промежутков ненулевой длины на числовой прямой конечно или счетно.

Теорема 1. *Пусть множество A бесконечно, а множество B конечно или счетно. Тогда $A \cup B \sim A$.*

Доказательство. Без ограничения общности считаем $A \cap B = \varnothing$ (иначе из B удалим $A \cap B$, тогда по-прежнему B будет конечно или счетно, задача сведется к исходной). Выделим в A счетное подмножество P, остаток обозначим Q, так что $A = P + Q$. Надо доказать: $B + P + Q \sim P + Q$. Множества $B + P$ и P оба счетные, поэтому $B + P \sim P$. Очевидно, $Q \sim Q$. Теорема доказана.

Теорема 2. *Пусть множество A несчетно, а множество B конечно или счетно. Тогда $A \setminus B \sim A$.*

Доказательство. Множество $A \setminus B$ несчетно, так как в противном случае (если $A \setminus B$ счетно или конечно) множество $A = (A \setminus B) \cup (A \cap B)$ было бы конечно или счетно, что не так. Таким образом, множество $A \setminus B$ бесконечно. Тогда по предыдущей теореме $A = (A \setminus B) \cup (A \cap B) \sim A \setminus B$. Теорема доказана.

Множество всех последовательностей нулей и единиц $\{(x_n) : \{x_n\} = \{0; 1\}\}$ несчетно. Действительно, предположив, что оно счетно, можно выписать последовательности в таблицу, где в k-й строке находится k-я последовательность:

$x_1^1,\ x_2^1,\ x_3^1,\ x_4^1,\ x_5^1,\ \ldots$
$x_1^2,\ x_2^2,\ x_3^2,\ x_4^2,\ x_5^2,\ \ldots$
$x_1^3,\ x_2^3,\ x_3^3,\ x_4^3,\ x_5^3,\ \ldots$
$\ldots\ldots\ldots\ldots\ldots$

Рассмотрим последовательность (x_n) такую, что $x_n = 1$, если $x_n^n = 0$, и $x_n = 0$, если $x_n^n = 1$. Это последовательность нулей и единиц, не вошедшая в таблицу. Значит, множество всех последовательностей нулей и единиц несчетно.

В двоичной системе счисления всякое число из отрезка $[0; 1]$ можно представить в виде бесконечной дроби $\sum\limits_{n=1}^{\infty} \frac{\alpha_n}{2^n}$, где каждое $\alpha_n \in \{0; 1\}$. Дроби взаимно однозначно соответствует последовательность нулей и единиц (α_n). Запретив 1 в периоде, кроме случая всех единиц, представляющих число 1, получим взаимную однозначность представления числа из отрезка $[0; 1]$ в виде бесконечной дроби. Число последовательностей нулей и единиц, имеющих 1 в периоде, счетно (докажите это), а всех последовательностей нулей и единиц несчетно много. По теореме 2 удаление последовательностей нулей и единиц, имеющих 1 в периоде, из множества всех последовательностей нулей и единиц не повлияет на мощность множества. Таким образом, отрезок $[0; 1]$ несчетен.

Функция $f : [0; 1] \to [a; b]$, $f(x) = a + (b - a)x$ устанавливает взаимно однозначное соответствие между отрезком $[0; 1]$ и отрезком $[a; b]$. Значит, все отрезки равномощны и несчетны. По теореме 1 в таком случае $[a; b] \sim [a; b) \sim (a; b] \sim (a; b)$. Итак, все промежутки равномощны. Отображение $f(x) = \operatorname{arctg} x$ устанавливает равномощность числовой прямой с одним из конечных интервалов. Таким образом, все промежутки равномощны $\mathbb{R}$. Нетрудно видеть (проверьте), что и всякий луч равномощен $\mathbb{R}$. Говорят, что мощность множества $\mathbb{R}$ равна *континууму*.

Говорят, что мощность $|A|$ множества A меньше или равна мощности $|B|$ множества B, $|A| \leqslant |B|$, если существует инъекция из A в B. Говорят, что мощность $|A| < |B|$, если $|A| \leqslant |B|$ и $|A| \neq |B|$. Пусть $\mathcal{P}(M)$ – множество всех подмножеств множества M. Тогда $M \ni x \mapsto \{x\} \in \mathcal{P}(M)$ есть инъекция из M в $\mathcal{P}(M)$. Поэтому $|M| \leqslant |\mathcal{P}(M)|$. Если $A \subset B$, то $A \ni x \mapsto x \in B$ есть инъекция из A в B. Значит, $|A| \leqslant |B|$.

Теорема Кантора. *Для любого множества M справедливо $|M| < |\mathcal{P}(M)|$.*

Доказательство. Пусть существует биекция $f : M \to \mathcal{P}(M)$. Рассмотрим множество S таких $x \in M$, что $x \notin f(x)$. Так как f – биекция, найдётся такое $y \in M$, что $S = f(y)$. Либо $y \in S$, либо $y \notin S$. Если $y \in S$, то по определению S получается $y \notin S$. Если $y \notin S$, то по определению S получается $y \in S$. Противоречие. Значит, биекции f не существует, и $|M| \neq |P(M)|$. Поскольку всегда $|M| \leqslant |P(M)|$, получаем заключение теоремы.

Мощность множества $\mathfrak{M} = \{f : M \to \{0;1\}\}$ всех функций из множества M в множество $\{0;1\}$ равна мощности булиана $\mathcal{P}(M)$, поскольку всякая функция $f_A : M \to \{0;1\}$ есть индикатор подмножества A множества M. В самом деле, элемент $x \in M$ принадлежит подмножеству A тогда и только тогда, когда $f_A(x) = 1$. Всякое подмножество множества M имеет единственный индикатор, поэтому $|\mathfrak{M}| = |\mathcal{P}(M)|$.

По теореме Кантора $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})|$. Говорят, что множество $\mathcal{P}(\mathbb{R})$ имеет мощность *гиперконтинуум.* По теореме Кантора $|\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))|$. Говорят, что множество $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ имеет мощность *гипергиперконтинуум.* Можно продолжать так далее. Мы видим, что существует бесконечно много попарно различных бесконечностей. Ясно, что мощность $|\{f : \mathbb{R} \to \{0;1\}\}|$ есть гиперконтинуум, мощность $|\{f : \{f : \mathbb{R} \to \{0;1\}\} \to \{0;1\}\}|$ есть гипергиперконтинуум и так далее.

По теореме Кантора $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. Так как мощность $|\mathcal{P}(\mathbb{N})| = |\{f : \mathbb{N} \to \{0;1\}\}|$, а всех последовательностей нулей и единиц континуум, то мощность $|\mathcal{P}(\mathbb{N})|$ равна континууму.

Континуум-гипотеза Кантора (в формулировке Кантора) состоит в следующем: всякое подмножество отрезка числовой прямой либо конечно (пустое множество конечно), либо счетно, либо равномощно континууму. Таким образом, согласно континуум-гипотезе, континуум – наименьшая несчетная мощность, то есть наименьшая мощность,

соответствующая несчетному множеству. Предположив истинность (непротиворечивость) аксиом теории множеств, доказано, что нельзя ни доказать, ни опровергнуть континуум-гипотезу, опираясь на классическую математическую логику.

Знаменитая *теорема Гёделя о неполноте* утверждает, что каждая непротиворечивая аксиоматическая теория, содержащая аксиомы арифметики натуральных чисел (и, в частности, арифметика натуральных чисел), неполна. Это значит, что в этой теории найдётся корректно сформулированное утверждение, которое нельзя доказать, но нельзя и опровергнуть логическим рассуждением.

Теорема Кантора–Бернштейна. *Для любых множеств A и B если $|A| \leqslant |B|$ и $|B| \leqslant |A|$, то $|A| = |B|$.*

Доказательство. Если f – инъекция из A в B, а g – инъекция из B в A, то $g \circ f$ – инъекция из A в A. Пусть $A_0 = A$, $A_1 = g(B)$, $A_2 = (g \circ f)(A)$. Тогда $A_0 \subset A_1 \subset A_2$, и множества A_0 и A_2 равномощны: $(g \circ f) : A_0 \to A_2$ есть биекция. Достаточно доказать, что $A_0 \sim A_1$. Пусть $h = g \circ f$. При отображении h множество A_0 биективно отображается в A_2, меньшее множество A_1 биективно отображается в множество $A_3 \subset A_2$ и так далее. Мы имеем цепочку $A_0 \supset A_1 \supset A_2 \supset \supset A_3 \supset \dots$ Пусть $C_n = A_n \backslash A_{n-1},\ n \in \mathbb{N}$, а $C = \bigcap\limits_{n=0}^{\infty} A_n$. Тогда $A_0 = (C_0 + C_1 + C_2 + \dots + C_n + \dots) + C$, $A_1 = (C_1 + C_2 + \dots + C_n + \dots) + C$. Отображение h биективно отображает C_{2k} в C_{2k+2} и C_{2k+1} в C_{2k+3}, $k = 0,\ 1,\ 2,\ \dots$ Биекция между A_0 и A_1 строится следующим образом: элементы C и C_{2k} остаются на месте, а элементы C_{2k+1} биективно переходят при помощи h в элементы C_{2k+3}, $k = 0,\ 1,\ 2,\ \dots$ Теорема доказана.

Теорема Цермело–Кантора. *Любые два множества A и B сравнимы по мощности: либо $|A| < |B|$, либо $|A| = |B|$, либо $|B| < |A|$.*

Пусть M – множество всех множеств. Тогда $\mathcal{M} \subset P(M)$, ведь всякий элемент из $\mathcal{P}(M)$ есть множество, значит, является элементом множества всех множеств M. Тогда $|\mathcal{P}(M)| \leqslant |M|$.

Но для любого множества $|M| \leqslant |\mathcal{P}(M)|$. Тогда по теореме Кантора–Бернштейна $|M| = |\mathcal{P}(M)|$. Но по теореме Кантора $|M| < |\mathcal{P}(M)|$. Противоречие. Равенство мощностей означает, что существует биекция из M в $\mathcal{P}(M)$, а строгое неравенство означает, что такой биекции не существует. Таким образом, множества всех множеств не существует. Совокупность всех множеств является *собственным классом*. Всякое множество есть класс, но не всякий класс есть множество. Те классы, которые не являются множествами, называются *собственными классами*.

Операции с мощностями. По определению $|A + B| = |A| + |B|$, $|A \times B| = |A| \cdot |B|$, $|A|^{|B|} = |\{f : B \to A\}|$. Например, $0^0 = 1$, так как функций из пустого множества в пустое найдётся одна, а именно пустая. Пусть a, b, c – мощности (кардинальные числа). Тогда

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. $a \times b = b \times a$.
4. $(a \times b) \times c = a \times (b \times c)$.
5. $(a + b) \times c = (a \times c) + (b \times c)$.
6. $a^{b+c} = a^b \times a^c$.
7. $(a \times b)^c = a^c \times b^c$.
8. $(a^b)^c = a^{b \times c}$.
9. Если $a \leqslant b$, то $a^c \leqslant b^c$ и $a \times c \leqslant b \times c$.
10. Для бесконечных мощностей (мощностей бесконечных множеств) верно, что $a \times b = a + b = \max\{a, b\}$, $a^n = a$, $a^a = 2^a$.

Доказательство. Докажем, например, свойство 3. $a \times b = b \times a$ означает $A \times B \sim B \times A$, что верно, так как $A \ni (x; y) \mapsto (y; x) \in B$ есть биекция между A и B. Столь же просто доказываются свойства 1, 2, 4, 5, 9.

Докажем 6. Надо доказать, что $A^{B+C} \sim A^B \times A^C$. Функция $f : B + C \to A$ распадается на две функции $f_1 : B \to A$ и $f_2 : C \to A$, каждая из которых суть сужение f (на множества B и C соответственно; f_1 и f_2 действуют по тому же правилу, что и f). Таким образом, $\forall\ f \in A^{B+C}\ \exists\ f_1 \in A^B\ \exists\ f_2 \in \in A^C : f \mapsto (f_1, f_2)$. Отображение $A^{B+C} \ni f \mapsto (f_1, f_2) \in \in A^B \times A^C$ есть биекция между A^{B+C} и $A^B \times A^C$. Свойство 6 доказано.

Докажем 7. Надо доказать, что $(A \times B)^C \sim A^C \times B^C$. Элемент $(A \times B)^C$ есть функция $f : C \to A \times B$, действующая по правилу $f(c) = (a; b) \in A \times B$. Пусть $a = f_1(c)$, $b = f_2(c)$. Отображение $(A \times B)^C \ni f \mapsto (f_1, f_2) \in A^C \times B^C$ есть биекция между $(A \times B)^C$ и $A^C \times B^C$. Свойство 7 доказано.

Докажем 8. Надо доказать $(A^B)^C \sim A^{B \times C}$. Элемент $f \in A^{B \times C}$ есть функция $f : B \times C \to A$. Фиксируем $c \in C$. Рассмотрим отображение $f_c : B \to A$, $f_c(b) = = f(b, c)$. Отображение $(c \mapsto f_c) \in (A^B)^C$ взаимно однозначно соответствует элементу $f \in A^{B \times C}$. Свойство 8 доказано.

В следующих примерах приводятся формулировки свойств и их толкования.

1. $|\mathbb{N}| + n = |\mathbb{N}|$. Счетное множество плюс конечное множество есть счетное множество.
2. $|\mathbb{N}| + |\mathbb{N}| = |\mathbb{N}|$. Счетное множество плюс счетное множество есть счетное множество.
3. $|\mathbb{N}| \cdot |\mathbb{N}| = |\mathbb{N}|$. Объединение счетного числа счетных множеств есть счетное множество.
4. $2^{|\mathbb{N}|} = |\mathbb{R}|$. Множество всех подмножеств счетного множества имеет мощность континуума.

5. $|\mathbb{R}|\cdot|\mathbb{R}| = 2^{|\mathbb{N}|}\times 2^{|\mathbb{N}|} = 2^{|\mathbb{N}|+|\mathbb{N}|} = 2^{|\mathbb{N}|} = |\mathbb{R}|$. Таким образом, $\mathbb{R}\times\mathbb{R}\sim\mathbb{R}$. Плоскость имеет столько же точек, сколько прямая: континуум континуумов снова континуум.

6. $|\mathbb{R}| \leqslant |\mathbb{R}|\cdot n \leqslant |\mathbb{R}|\cdot|\mathbb{N}| \leqslant |\mathbb{R}|\cdot|\mathbb{R}| = |\mathbb{R}|$. Тогда по теореме Кантора–Бернштейна $|\mathbb{R}|\cdot n = |\mathbb{R}|\cdot|\mathbb{N}| = |\mathbb{R}|$. В частности, $|\mathbb{R}| + |\mathbb{R}| = |\mathbb{R}|$.

7. $|\mathbb{R}|^{|\mathbb{N}|} = (2^{|\mathbb{N}|})^{|\mathbb{N}|} = 2^{|\mathbb{N}|\times|\mathbb{N}|} = 2^{|\mathbb{N}|} = |\mathbb{R}|$. Мощность множества всех функций из $\mathbb{N}$ в $\mathbb{R}$, то есть всех числовых последовательностей, равна континууму. Мощность множества всех функций из счетного множества в $\mathbb{R}$ равна континууму. В частности, имеется ровно континуум функций из $\mathbb{Q}$ в $\mathbb{R}$ и столько же непрерывных функций из $\mathbb{R}$ в $\mathbb{R}$, поскольку каждая непрерывная функция однозначно определяется своими значениями в рациональных точках. Монотонных функций из $\mathbb{R}$ в $\mathbb{R}$ континуум, так как каждая из них кусочно-непрерывна, а множество точек разрыва конечно или счетно.

8. $|\mathbb{R}|^{|\mathbb{R}|} = (2^{|\mathbb{N}|})^{|\mathbb{R}|} = 2^{|\mathbb{N}|\times|\mathbb{R}|} = 2^{|\mathbb{R}|}$. Мощность множества всех функций из $\mathbb{R}$ в $\mathbb{R}$ равна гиперконтинууму. Всех функций столько же, сколько функций, принимающих значения 0 и 1.

§ 6. Фундированные множества. Математическая индукция

Теорема. *Следующие три свойства частично упорядоченного множества X равносильны:*

(а) любое непустое подмножество X имеет минимальный элемент;

(б) не существует бесконечной строго убывающей последовательности $x_1 > x_2 > \cdots > x_n > \ldots$ элементов множества X;

(в) для множества X верен принцип математической индукции: если при каждом $x \in X$ из истинности $A(y)$ для всех $y < x$ следует истинность $A(x)$, то свойство $A(x)$ верно при всех x. Формально:

$$\forall\, x(\forall\, y((y < x) \Rightarrow A(y)) \Rightarrow A(x)) \Rightarrow \forall\, x\ A(x).$$

Доказательство. Если $x_1 > x_2 > \cdots > x_n > \ldots$ – бесконечная убывающая последовательность, то, очевидно, множество её значений не имеет минимального элемента: для каждого элемента следующий ещё меньше. Поэтому из (а) следует (б). Обратно, если B – непустое подмножество, не имеющее минимального элемента, то бесконечную убывающую последовательность можно построить так. Возьмём любой элемент $b_0 \in B$. По предположению он не является минимальным, так что можно найти $b_1 \in B$, для которого $b_0 > b_1$. По тем же причинам можно найти $b_2 \in B$, для которого $b_1 > b_2$, и так далее. Получается бесконечная убывающая последовательность. Значит, из (б) следует (а).

Выведем (в) из (а). Пусть $A(x)$ – произвольное свойство элементов множества X, верное не для всех элементов x. Рассмотрим непустое множество B тех элементов, для которых свойство A не верно. Пусть x – минимальный элемент множества B. По условию меньших элементов в множестве B нет, поэтому для всех $y < x$ свойство $A(y)$ выполнено. Но тогда по предположению должно быть выполнено $A(x)$ – противоречие.

Осталось доказать, что из (в) следует (а). Пусть B – подмножество без минимальных элементов. Докажем по индукции, что B пусто. Возьмём в качестве $A(x)$ свойство $x \notin B$. Если $A(y)$ верно для всех $y < x$, то никакой элемент, меньший x, не лежит в B. Если бы x лежал в B, то он был бы там минимальным, а таких нет. Теорема доказана.

Множества, обладающие свойствами (а) – (в), называются *фундированными*.

Известно, что всякое множество можно вполне

упорядочить. Математическая индукция называется *трансфинитной*, если она применяется к несчетному множеству, и *финитной* в противном случае.

Пусть A и B – два фундированных частично упорядоченных множества. Тогда их декартово произведение $A \times B$, в котором $(a_1, b_1) \leqslant (a_2, b_2) \Leftrightarrow [(b_1 < b_2)$ или $(b_1 = b_2$, и $a_1 \leqslant a_2)]$, является фундированным. Действительно, в последовательности $(a_1, b_1) \geqslant (a_2, b_2) \geqslant \ldots$ стабилизируются сначала вторые, а затем и первые члены. В таком случае по индукции если A – фундированное множество, то и A^n – фундированное множество. Например, $\mathbb{N}^k$ – фундированное множество.

Пример. Рассмотрим олимпиадную задачу. Бизнесмен заключил сделку с чертом. Каждый день он даёт черту одну монету, и в обмен получает любой набор монет по своему выбору, но меньшего достоинства (например, за одну транзакцию тысячу рублей можно обменять на миллион по рублю). Видов монет конечное число. Менять или получать деньги в другом месте бизнесмен не может. Когда монет не останется, бизнесмен проигрывает. Докажите, что рано или поздно черт выиграет, каков бы ни был начальный набор монет у бизнесмена.

Решение. Пусть имеется k видов монет: n_1 – число монет минимального достоинства, n_2 – число следующих и так далее до n_k. Заметим, что в результате встречи с чертом набор $(n_1, \ldots, n_k)$ уменьшается. Поскольку множество $\mathbb{N}^k$ фундировано, то этот процесс должен оборваться.

ГЛАВА 2

ЭЛЕМЕНТЫ КОМБИНАТОРНОГО АНАЛИЗА

Комбинаторика является разделом дискретной математики и изучает свойства конечных множеств.

§ 7. Перестановки, размещения, сочетания, сочетания с повторениями

Перестановки. Перестановкой на n символах называется упорядоченный набор из n различных элементов множества $E_n = \{a_1, a_2, \ldots, a_n\}$. Докажем по индукции, что всего перестановок на n символах найдётся $n!$. Базис индукции. Для $n = 1$ утверждение, очевидно, верно. Шаг индукции. Пусть утверждение верно для n. Рассмотрим перестановки на $(n+1)$-символах. Поставим на k-е место элемент a_{n+1} множества E_{n+1}, зафиксируем этот элемент. По предположению индукции перестановок на $(n+1)$-символах с фиксированным элементом a_{n+1} на k-м месте найдётся $n!$. Всего мест $n+1$. Поэтому перестановок на $(n+1)$-символах оказывается $(n+1) \cdot n! = (n+1)!$. Утверждение доказано. Перестановка на пустом множестве символов одна, а именно пустая. Поэтому полученная формула верна и для $n = 0$, так как $0! = 1$.

Элементы a_i и a_j перестановки $(a_1, a_2, \ldots, a_n)$ образуют инверсию (или беспорядок), если $a_i > a_j$ при $i < j$. Если число всех инверсий $N(\tau)$ перестановки τ чётное, то перестановка τ чётная. Если число всех инверсий перестановки τ нечётное, то перестановка τ нечётная. Можно говорить, что перестановка имеет чётность N, так как по N легко определяется чётность перестановки (чётная или нечётная). Знак перестановки $\operatorname{sign} \tau = (-1)^{N(\tau)}$. При транспозиции (смене местами) элементов a_i и a_j перестановки $(a_1, a_2, \ldots, a_n)$ чётность перестановки меняется. Действительно, пусть элементы a_i и a_j соседние, тогда если между ними не

было инверсии, то она появилась, а если была инверсия, то она исчезла. Число остальных инверсий осталось без изменения. Если между элементами a_i и a_j в перестановке находится m элементов, то поменять a_i и a_j местами можно, выполнив $m+1$ транспозиций элемента a_i с соседними элементами, так чтобы a_i стал за a_j, а затем выполнив m транспозиций элемента a_j с соседними элементами, так чтобы a_j оказался на месте a_i. Всего $2m+1$ транспозиций соседних элементов изменят чётность перестановки, поскольку каждая транспозиция меняет чётность.

По индукции легко проверяется, что все перестановки на n символах можно расположить в виде последовательности, начиная с тождественной (чётной) перестановки $(1,\ 2,\ \ldots,\ n)$ так, что каждая следующая перестановка получается из предыдущей одной транспозицией элементов. Таким образом, имеется $\frac{n!}{2}$ чётных перестановок и столько же нечётных.

Размещения. Размещением из n элементов по k (элементов), $0 \leqslant k \leqslant n$, называется упорядоченный набор из k различных элементов множества $E_n = \{a_1,\ a_2,\ \ldots,\ a_n\}$. Сколько всего размещений? На первое из k мест (ящиков) элемент можно выбрать n способами. Если первый элемент уже выбран, то на второе место из оставшихся элементов элемент можно выбрать $(n-1)$ способами для каждого способа выбора первого элемента, так как элементы в размещении не повторяются, и, таким образом, для выбора остаётся $(n-1)$ элемент. Находим, что первые два элемента можно выбрать $n(n-1)$ способами. Если первые два элемента уже выбраны, то на третье место из оставшихся элементов элемент можно выбрать $(n-2)$ способами для каждого способа выбора первых двух элементов. Таким образом, первые три элемента можно выбрать $n(n-1)(n-2)$ способами. Продолжая рассуждение, находим, что всего размещений из n элементов по k найдётся $A_n^k = n(n-1)\ldots(n-(k-1)) = n(n-1)\ldots(n-k+1) = \frac{n!}{(n-k)!}$. Для $k=n$ получаем размещения из n элементов по

n, то есть перестановки на n символах. Для $k=0$ получаем одно размещение, а именно пустое.

Сочетания. Сочетанием из n элементов по k (элементов) называется произвольное подмножество из k элементов множества $E_n = \{a_1,\ a_2,\ \ldots,\ a_n\}$. Знаками C_n^k или $\binom{n}{k}$ обозначается число (количество) всех сочетаний из n элементов по k. Сколько сочетаний из n элементов по k? Каждому сочетанию из n элементов по k соответствует $k!$ размещений этих элементов (в сочетании порядок элементов не важен, а в размещении важен). Поэтому $C_n^k = \frac{A_n^k}{k!} = \frac{n(n-1)\ldots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$. Для $k=0$ получаем одно сочетание, а именно пустое. Для $k=n$ также получаем одно сочетание, а именно множество E_n. $C_n^1 = n$, так как столько существует одноэлементных подмножеств n элементного множества. $C_n^{n-1} = n$, так как выбору $n-1$ элементов из n взаимно однозначно соответствует выбор оставшегося одного элемента, а таких n. $C_n^k = C_n^{n-k}$, так как выбору k элементов n элементного множества взаимно однозначно соответствует выбор оставшихся $n-k$ элементов этого множества. $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$, так как сочетания из n элементов по k состоят из тех сочетаний, в которые входит элемент a_1, а таких C_{n-1}^{k-1} (элемент a_1 уже выбран, осталось выбрать $k-1$ элемент из оставшихся $n-1$ элементов), и тех сочетаний, в которые не входит элемент a_1, а таких C_{n-1}^k (элемент a_1 заведомо не входит, значит, из $n-1$ элементов требуется выбрать k). Сумма $C_n^0 + C_n^2 + \cdots + C_n^n = 2^n$, так как указанная сумма означает количество всех подмножеств n элементного множества, а таких 2^n. Действительно, каждому подмножеству взаимно однозначно соответствует набор нулей и единиц длины n, где на k-м месте стоит 0, если элемент a_k множества E_n не входит в выбранное подмножество, и 1, если входит. По индукции легко проверяется, что наборов нулей и единиц длины n всего 2^n.

Сочетания с повторениями. В отличие от сочетания

в сочетании с повторениями тот или иной элемент может повторяться. Число сочетаний с повторениями из n элементов по k обозначается H_n^k. Чтобы найти H_n^k, поступим следующим образом. Напишем 1 столько раз, сколько элемент a_1 входит в сочетание с повторениями (если нисколько, то ничего не пишем), потом напишем знак разделения 0. Затем напишем 1 столько раз, сколько элемент a_2 входит в сочетание с повторениями, потом напишем 0, и так далее. После того как будет рассмотрен элемент a_n, знак разделения 0 не пишем. Мы получим набор нулей и единиц длины $(k+n-1)$, в нём число единиц равно k и $(n-1)$ нулей, знаков разделения между n элементами. Каждому такому набору нулей и единиц соответствует сочетание с повторениями из n элементов по k, разным сочетаниям с повторениями из n элементов по k соответствуют разные наборы нулей и единиц. Таким образом, существует взаимно однозначное соответствие между указанными наборами нулей и единиц и сочетаниями с повторениями из n элементов по k. Значит, H_n^k равно числу построенных наборов нулей и единиц, а таких наборов C_{n+k-1}^k, так как на $n+k-1$ мест требуется разместить k единиц, что соответствует выбору k элементного подмножества мест из $(n+k-1)$ элементного множества мест, то есть сочетанию из $n+k-1$ элементов по k.

§ 8. Подстановки

Подстановкой на n символах называется биекция $f : \overline{1,n} \to \overline{1,n}$ начального отрезка натурального ряда длины n на себя. Функцию f можно задать в виде таблицы

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix},$$

где $i_k = f(k),\ k = \overline{1,n}$.

Множество всех подстановок на n символах как множество биекций множества $\overline{1,n}$ на себя образует

мультипликативную группу относительно композиции указанных функций, называемую симметрической группой S_n. Порядок симметрической группы S_n равен $n!$. Тождественная функция является тождественной подстановкой E, обратная к f функция f^{-1} является обратной подстановкой к f. Композицию $g \circ f$ подстановок f и g называют ещё произведением $g \cdot f$ подстановок f и g. Сначала выполняется f, потом g.

При транспозиции (перестановке) столбцов таблицы для функции f функция f не меняется. Поэтому таблица для f может выглядеть следующим образом:

$$\begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ j_1 & j_2 & j_3 & \dots & j_n \end{pmatrix}.$$

Первая и вторая строки этой таблицы суть перестановки с беспорядками N_1 и N_2. Тогда $N = N_1 + N_2$ – беспорядок подстановки f. Если N чётное, то подстановка f чётная, если N нечётное, то подстановка f нечётная. При транспозиции (перестановке) столбцов таблицы для f чётности N_1 и N_2 изменятся на 1, поэтому чётность числа $N = N_1 + N_2$, а значит, и чётность f не изменится (хотя само N может измениться).

Знак подстановки f, $\operatorname{sign} f = (-1)^N$.

Транспозицией (ij) элементов i и j называется подстановка

$$\tau = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix},$$

получаемая из тождественной подстановки перестановкой элементов i и j в нижней строке. Очевидно, транспозиция – нечётная подстановка, $\tau^2 = \tau \circ \tau = E,\ \tau^{-1} = E$.

Умножение подстановки

$$f = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ j_1 & j_2 & j_3 & \dots & j_n \end{pmatrix}$$

слева на транспозицию $(j_k j_s)$ меняет местами элементы j_k и j_s в нижней строке исходной подстановки f. Транспозициями

элементов нижней строки из подстановки f можно получить тождественную подстановку. В самом деле, на место j_1 одной транспозицией ставим элемент i_1 нижней строки или оставляем всё как есть, если элемент $j_1 = i_1$, что эквивалентно умножению на квадрат какой-либо транспозиции. Потом на второе место нижней строки ставим элемент i_2 и так далее:

$$\tau_s \circ \tau_{s-1} \circ \cdots \circ \tau_1 \circ f = E.$$

Отсюда получается разложение подстановки f в произведение транспозиций:

$$f = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_s \circ E.$$

Четность подстановки f совпадает с чётностью s, так как тождественная подстановка E, очевидно, чётная, а каждая транспозиция меняет чётность подстановки. Теперь легко видеть, что произведение чётных подстановок – чётная подстановка, ведь каждый из двух сомножителей раскладывается в чётное число транспозиций, значит, и произведение оказывается разложенным в чётное число транспозиций. Произведение нечётных подстановок – чётная подстановка, ведь каждый из двух сомножителей раскладывается в нечётное число транспозиций. Произведение чётной и нечётной подстановок – нечётная подстановка, ведь один из двух сомножителей раскладывается в чётное число транспозиций, а другой – в нечётное число транспозиций, значит, произведение оказывается разложенным в нечётное число транспозиций. Отсюда получается правило:

$$\operatorname{sign}(gf) = \operatorname{sign} g \cdot \operatorname{sign} f.$$

Так как $\operatorname{sign}(f^{-1} \circ f) = \operatorname{sign} E = 1 = \operatorname{sign} f \circ \operatorname{sign} f^{-1}$, то знак и чётность обратной подстановки f^{-1} совпадают с чётностью и знаком исходной подстановки f.

Теперь легко видеть, что множество всех чётных подстановок на n символах образует группу порядка $\frac{n!}{2}$ относительно взятия композиции двух функций. Группа чётных подстановок на n символах обозначается A_n и является

подгруппой симметрической группы S_n. Множество нечётных подстановок $S_n \setminus A_n$ группы относительно композиции не образует, так как произведение двух нечетных подстановок выводит за рамки этого множества.

§ 9. Бином Ньютона и его следствия

Бином Ньютона. Так называется соотношение

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k},$$

где a и b есть элементы алгебраического поля, например, вещественные или комплексные числа. По правилам раскрытия скобок $(a+b)^n = \sum\limits_{k=0}^{n} C_k a^k b^{n-k}$, где C_k – некоторые коэффициенты. Каждый множитель $a^k b^{n-k}$ получается следующим образом: k штук множителей a выбираются из n умножаемых скобок вида $(a+b)$, по одному a из каждой скобки, из остальных скобок выбираются $n-k$ множителей b, по одному b из каждой скобки. Таким образом, всего множителей вида $a^k b^{n-k}$ столько, сколькими способами можно выбрать k элементов из n без учёта порядка (k скобок из n скобок), то есть $C_k = C_n^k$. Бином Ньютона доказан.

Треугольник Паскаля. Коэффициенты C_n^k для данного n ($n = 0,\ 1,\ 2,\ \ldots$) легко находятся при помощи треугольника Паскаля:

$$\begin{array}{l}
C_0^0 \\
C_1^0\ C_1^1 \\
C_2^0\ C_2^1\ C_2^2 \\
C_3^0\ C_3^1\ C_3^2\ C_3^3 \\
C_4^0\ C_4^1\ C_4^2\ C_4^3\ C_4^4 \\
C_5^0\ C_5^1\ C_5^2\ C_5^3\ C_5^4\ C_5^5
\end{array}$$

и так далее, или в цифрах

$$\begin{array}{c} 1 \\ 1\ 1 \\ 1\ 2\ \ 1 \\ 1\ 3\ \ 3\ \ \ 1 \\ 1\ 4\ \ 6\ \ \ 4\ \ 1 \\ 1\ 5\ 10\ 10\ 5\ 1 \end{array}$$

и так далее. На ребрах треугольника Паскаля стоят единицы, так как $C_n^0 = C_n^n = 1$. Любой другой коэффициент равен сумме коэффициентов, стоящих над ним в предыдущей строке согласно тождеству $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$.

Например,

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Коэффициенты берутся из 5-й строки треугольника Паскаля, что соответствует $n = 4$. Отметим, что по биному Ньютона

$$2^n = (1+1)^n = \sum_{k=0}^{n} C_n^k, \quad 0 = (1-1)^n = \sum_{k=0}^{n} (-1)^k C_n^k.$$

Число e. Оценки для n!. Пусть $a_n = \left(1+\frac{1}{n}\right)^n$. По биному Ньютона $a_n = 1 + C_n^1\frac{1}{n} + C_n^2\frac{1}{n^2} + \cdots + C_n^n\frac{1}{n^n} = 1 + 1 + \left(1-\frac{1}{n}\right)\frac{1}{1\cdot 2} + \cdots + \left(1-\frac{1}{n}\right)\ldots\left(1-\frac{n-1}{n}\right)\frac{1}{1\cdot 2\cdot\ldots\cdot n}$. Сравним это число с $a_{n+1} = 1 + 1 + \left(1-\frac{1}{n+1}\right)\frac{1}{1\cdot 2} + \cdots + \left(1-\frac{1}{n+1}\right)\ldots\left(1-\frac{n-1}{n+1}\right)\frac{1}{1\cdot 2\cdot\ldots\cdot n} + \left(1-\frac{1}{n+1}\right)\ldots\left(1-\frac{n}{n+1}\right)\frac{1}{1\cdot 2\cdot\ldots\cdot(n+1)}$. Члены, входящие в a_{n+1}, не меньше соответствующих членов, входящих в a_n. Значит, $a_n < a_{n+1}$, и числовая последовательность (a_n) монотонно возрастает. Кроме того, $a_n = 1 + 1 + \left(1-\frac{1}{n}\right)\frac{1}{1\cdot 2} + \cdots + \left(1-\frac{1}{n}\right)\ldots\left(1-\frac{n-1}{n}\right)\frac{1}{1\cdot 2\cdot\ldots\cdot n} < 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots < 3$. Значит, числовая последовательность (a_n) ограничена сверху.

По теореме Вейерштрасса она имеет предел

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n.$$

Из доказательства следует, что при $n \geqslant 1$

$$2 < \left(1+\frac{1}{n}\right)^n < e \leqslant 3,$$

откуда

$$\frac{(n+1)^n}{e} < n^n.$$

Докажем, что

$$\left(\frac{n}{e}\right)^n < n! \leqslant 2\left(\frac{n}{2}\right)^n.$$

Первое неравенство $n! > \left(\frac{n}{e}\right)^n$ доказывается по индукции. Базис индукции: при $n = 1$ имеем $1 > \frac{1}{e}$, что верно. Шаг индукции: $(n+1)! = (n+1)\cdot n! > (n+1)\left(\frac{n}{e}\right)^n = \frac{n+1}{e^n}n^n > \frac{n+1}{e^n}\frac{(n+1)^n}{e} = \left(\frac{n+1}{e}\right)^{n+1}$, где использовано неравенство $n^n > (n+1)/e$.

Второе неравенство $n! \leqslant 2\left(\frac{n}{2}\right)^n$ доказывается при помощи хорошо известного неравенства между средним геометрическим и средним арифметическим $\sqrt{ab} \leqslant (a+b)/2$ (для положительных a и b):

$$n! = n((1\cdot(n-1))(2\cdot(n-2))\ldots) \leqslant$$

$$\leqslant 2\left(\frac{n}{2}\right)\left(\left(\frac{n}{2}\right)^2\left(\frac{n}{2}\right)^2\ldots\right) = 2\left(\frac{n}{2}\right)^n.$$

Из бинома Ньютона следует неравенство Бернулли: для любого $a > 0$ и для любого натурального $n > 1$ выполнено

$$(1+a)^n \geqslant 1 + an.$$

В самом деле, при раскрытии скобки отброшены все положительные слагаемые, за исключением первых двух.

По теореме о пределе произведения сходящихся последовательностей числовая последовательность $x_n = \left(1+\frac{1}{n}\right)^{n+1}$ сходится к e. При помощи неравенства Бернулли легко видеть, что $\frac{x_{n+1}}{x_n} > 1$. Последовательность (x_n)

монотонно убывает. По теореме Вейерштрасса $e = \lim\limits_{n\to\infty} x_n = \inf\{x_n\}$. Таким образом,

$$\left(1+\frac{1}{n}\right)^n < e < \left(1+\frac{1}{n}\right)^{n+1}.$$

Логарифмируя полученное неравенство, находим

$$\frac{1}{n+1} < \ln\left(1+\frac{1}{n}\right) < \frac{1}{n}.$$

Число Эйлера. Рассмотрим числовую последовательность

$$y_n = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{n}-\ln n.$$

Так как

$$y_{n+1}-y_n = \frac{1}{n+1}-\ln(n+1)+\ln n = \frac{1}{n+1}-\ln\left(1+\frac{1}{n}\right) < 0,$$

то числовая последовательность (y_n) убывает.

Так как $y_n = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{n}-\ln n > \ln\left(1+\frac{1}{1}\right) + \left(1+\frac{1}{2}\right)+\cdots+\left(1+\frac{1}{n}\right)-\ln n = \ln(n+1)-\ln n > 0$, то числовая последовательность (y_n) ограничена снизу. По теореме Вейерштрасса существует

$$\gamma = \lim_{n\to\infty} y_n = \inf\{x_n\}.$$

Предел γ называется *числом Эйлера.* До сих пор неизвестно, иррационально γ или рационально. Если же γ иррационально, то трансцендентно ли оно или является корнем какого-либо алгебраического уравнения с рациональными коэффициентами.

Иррациональность e. Вопрос об иррациональности числа e принадлежит области теории чисел – математической науке, родственной дискретной математике. При помощи бинома Ньютона находим: $\left(1+\frac{1}{n}\right)^n = 1+1+\frac{n(n-1)}{2!}\frac{1}{n^2}+\cdots+\frac{n(n-1)\ldots(n-(k-1))}{k!}\frac{1}{n^k}+\cdots+\frac{1}{n^n} = 1+1+\frac{1}{2!}\left(1-\frac{1}{n}\right)+\cdots+\frac{1}{k!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)+\frac{1}{n!}\left(1-\frac{1}{n}\right)\ldots\left(1-\frac{n-1}{n}\right) < 1+1+\frac{1}{2!}+\cdots+\frac{1}{n!}$. Пусть $e_n = \left(1+\frac{1}{n}\right)^n$, $s_n = 1+1+\frac{1}{2!}+\cdots+\frac{1}{n!}$.

Мы видим, что $e_n < s_n$ $(n = 1,\ 2,\ \ldots)$. Далее, $\forall\ k\ \forall\ n \geqslant k\ 1+1+\frac{1}{2!}\left(1-\frac{1}{n}\right)+\cdots+\frac{1}{k!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right) \leqslant e_n$. Фиксируем k и перейдём к пределу при $n\to\infty$, получим $1+1+\frac{1}{2!}+\cdots+\frac{1}{k!} \leqslant e$, то есть $\forall\ k\ s_k \leqslant e$. Таким образом, $\forall\ n\in\mathbb{N}\ e_n < s_n \leqslant e$. По теореме о зажатой последовательности $\exists\ \lim\limits_{n\to\infty} s_n = e$. Итак,

$$e = 1+1+\frac{1}{2!}+\frac{1}{3!}+\cdots+\frac{1}{n!}+\ldots$$

Далее, $0 < e-s_n = \frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots = \frac{1}{(n+1)!}\left(1+\frac{1}{n+2}+\frac{1}{(n+2)(n+3)}+\ldots\right) < \frac{1}{(n+1)!}\left(1+\frac{1}{n+2}+\frac{1}{(n+2)^2}+\frac{1}{(n+2)^3}+\ldots\right) = \frac{1}{(n+1)!}\frac{1}{1-\frac{1}{n+2}} = \frac{n+2}{(n+1)!(n+1)} = \frac{n+2}{n!(n+1)^2} < \frac{1}{n!n}$, ибо $\frac{n+2}{(n+1)^2} < \frac{1}{n}$, так как $n^2+2n < n^2+2n+1$. Итак, $0 < e-s_n < \frac{1}{n!n}$, что можно переписать в виде: $e = s_n+\frac{\theta_n}{n!n}$, $0 < \theta_n < 1$. Пусть $e = \frac{m}{n}$ – рациональное число. Тогда $n!e = (n-1)!m = n!\left(1+1+\frac{1}{2!}+\cdots+\frac{1}{n!}\right)+\frac{\theta_n}{n}$, откуда вытекает, что $\frac{\theta_n}{n}$ – целое число. Противоречие, так как $0 < \theta_n < 1$, а $n \geqslant 1$. Значит, число e иррациональное. Отметим, что $e = 2,7182818284590\ldots$

Суммы Гаусса. Пусть $S_m(n) = 1^m+2^m+\cdots+n^m$. При помощи бинома Ньютона находим

$(n+1)^m = n^m+\binom{m}{1}n^{m-1}+\binom{m}{2}n^{m-2}+\cdots+\binom{m}{m-1}n+\binom{m}{m}$,

$((n-1)+1)^m = (n-1)^m+\binom{m}{1}(n-1)^{m-1}+\binom{m}{2}(n-1)^{m-2}+\cdots+\binom{m}{m-1}(n-1)+\binom{m}{m}$

и так далее,

$(2+1)^m = 2^m+\binom{m}{1}2^{m-1}+\binom{m}{2}2^{m-2}+\cdots+\binom{m}{m-1}2+\binom{m}{m}$,

$(1+1)^m = 1^m+\binom{m}{1}1^{m-1}+\binom{m}{2}1^{m-2}+\cdots+\binom{m}{m-1}1+\binom{m}{m}$.

Складывая почленно эти равенства, получаем рекуррентную формулу:

$(n+1)^m = 1+\binom{m}{1}S_{m-1}(n)+\binom{m}{2}S_{m-2}(n)+\cdots+\binom{m}{m-1}S_1(n)+\binom{m}{m}S_0(n)$, где $S_0(n) = n$, $S_1(n) = 1+2+3+\cdots+n = \frac{n(n+1)}{2}$.

Отсюда постепенно можно найти $S_m(n)$. Например,

$(n+1)^3 = 1+\binom{3}{1}S_2(n)+\binom{3}{2}S_1(n)+\binom{3}{3}S_0(n)$,

$3S_2(n) = (n+1)^3 - 1 - 3\frac{n(n+1)}{2} - n = \frac{n(n+1)(2n+1)}{2}$,
или
$S_2(n) = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.
Зная $S_0(n),\ S_1(n),\ S_2(n)$, можно найти $S_3(n)$ и так далее.

§ 10. Формулы Стирлинга и Валлиса

Докажем асимптотическую **формулу Стирлинга**:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,\ n \to \infty.$$

Эта формула означает, что

$$\exists \lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} = 1,$$

что равносильно

$$\frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} = 1 + o(1),\ n \to \infty,$$

или же

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n (1 + o(1)),\ n \to \infty,$$

или

$\ln n! = \frac{1}{2}\ln(2\pi n) + n(\ln n - 1) + \ln(1 + o(1)) = n\ln n + \frac{1}{2}\ln n - n + C + o(1) == \left(n + \frac{1}{2}\right)\ln n - n + C + o(1)$, где $C = \frac{1}{2}\ln\pi = \ln\sqrt{2\pi},\ n \to \infty$.

Итак, требуется доказать, что

$$n! = \left(n + \frac{1}{2}\right)\ln n - n + C + o(1) \text{ при } n \to \infty, \text{ где } C = \ln\sqrt{2\pi}. \quad (*)$$

Рассмотрим числовую последовательность

$$c_n = \ln n! - \left(n + \frac{1}{2}\right)\ln n + n.$$

Имеем
$c_n - c_{n-1} = \ln n! - \left(n + \frac{1}{2}\right)\ln n + n - \ln(n-1)! + \left(n - \frac{1}{2}\right)\ln(n-1) - (n-1) = \ln n - n\ln n - \frac{1}{2}\ln n + n + n\ln(n-1) - \frac{1}{2}\ln(n-1) - n + 1 = \frac{1}{2}\ln n^2 + 1 + n\ln\left(1 - \frac{1}{n}\right) - \frac{1}{2}\ln n(n-1) = n\ln\left(1 - \frac{1}{n}\right) - \frac{1}{2}\ln\left(1 - \frac{1}{n}\right) + 1 = n\left(-\frac{1}{n} - \frac{1}{2n^2} - \frac{1}{3n^3} + o\left(\frac{1}{n^3}\right)\right) - \frac{1}{2}\left(-\frac{1}{n} - \frac{1}{2n^2} + o\left(\frac{1}{n^2}\right)\right) + 1 = -\frac{1}{2n} - \frac{1}{3n^2} + o\left(\frac{1}{n^2}\right) + \frac{1}{2n} + \frac{1}{4n^2} + o\left(\frac{1}{n^2}\right) = -\frac{1}{12n^2} + o\left(\frac{1}{n^2}\right)$.

Таким образом, числовой ряд $\sum\limits_{n=2}^{\infty}(c_n - c_{n-1})$ сходится по признаку сравнения в силу сходимости, например, по интегральному признаку числового ряда $\sum\limits_{n=2}^{\infty}\frac{1}{n^2}$. Тогда последовательность частичных сумм $s_n = c_n - c_{n-1} + c_{n-1} - c_{n-2} + \cdots + c_2 - c_1 = c_n - c_1$ ряда $\sum\limits_{n=2}^{\infty}(c_n - c_{n-1})$ сходится к некоторому числу $s = \lim\limits_{n\to\infty} s_n = \lim\limits_{n\to\infty} c_n - c_1$. Таким образом, $\exists\, C = \lim\limits_{n\to\infty} c_n$. Последнее равносильно тому, что

$$\ln n! - \left(n + \tfrac{1}{2}\right)\ln n + n = C + o(1) \qquad (**)$$

при $n \to \infty$. Таким образом, чтобы полностью доказать соотношение $(*)$, нам осталось найти константу C.

Пусть $W_n = \int\limits_0^{\pi/2} \sin^n x dx,\ n \geqslant 0$. Интегрируя по частям, находим
$W_n = \int\limits_0^{\pi/2} \sin^{n-1} x d(-\cos x) = -\cos x \cdot \sin^{n-1} x|_0^{\pi/2} + \int\limits_0^{\pi/2} \cos x\ d\sin^{n-1} x = (n-1)\int\limits_0^{\pi/2} \sin^{n-2} x \cdot (1 - \sin^2 x)dx = (n-1)\int\limits_0^{\pi/2} \sin^{n-2} x dx - (n-1)\int\limits_0^{\pi/2} \sin^n x$, то есть, $W_n = (n-1)W_{n-2} - (n-1)W_n,\ n \geqslant 2$, откуда вытекает

$$W_n = \frac{n-1}{n} W_{n-2},\ n \geqslant 2.$$

Тогда поскольку $W_0 = \int\limits_0^{\pi/2} \sin^0 x dx = \frac{\pi}{2},\ W_1 = \int\limits_0^{\pi/2} \sin^2 x dx = 1$, то
$W_{2k} = \frac{2k-1}{2k} W_{2k-2} = \frac{2k-1}{2k} \cdot \frac{2k-3}{2k-2} W_{2k-4} = \cdots = \frac{(2k-1)(2k-3)\cdots 1}{(2k)(2k-2)\cdots 2} W_0 = \frac{(2k-1)!!}{(2k)!!} \cdot \frac{\pi}{2}$,

$W_{2k+1} = \frac{2k}{2k+1} W_{2k-1} = \frac{2k}{2k+1} \cdot \frac{2k-2}{2k-1} W_{2k-3} = \cdots = \frac{(2k)(2k-2)\cdots 2}{(2k+1)(2k-1)\cdots 3} W_1 = \frac{(2k)!!}{(2k+1)!!}$.

Так как $\forall\ x \in \left(0; \frac{\pi}{2}\right)\ \forall\ n \in \mathbb{N} \to \sin^{2k+1} x < \sin^{2k} x < \sin^{2k-1} x$, то

$$\forall\ n \in \mathbb{N} \to W_{2k+1} < W_{2k} < W_{2k-1},$$

то есть

$$\frac{(2k)!!}{(2k+1)!!} < \frac{(2k-1)!!}{(2k)!!} \cdot \frac{\pi}{2} < \frac{(2k-2)!!}{(2k-1)!!}.$$

Следовательно,

$$a_k = \frac{((2k)!!)^2}{((2k-1)!!)^2(2k+1)} < \frac{\pi}{2} < \frac{((2k)!!)^2}{((2k-1)!!)^2(2k)} = b_k.$$

Отсюда $0 \leqslant \left|\frac{\pi}{2} - a_k\right| \leqslant |b_k - a_k| = (b_k - a_k) = \left(\frac{(2k)!!}{(2k-1)!!}\right)^2 \cdot \left(\frac{1}{2k} - \frac{1}{2k+1}\right) = \left(\frac{(2k)!!}{(2k-1)!!}\right)^2 \cdot \frac{1}{(2k)(2k+1)} < \frac{\pi}{2} \cdot \frac{1}{2k} \to 0$ при $k \to \infty$. Следовательно, $\lim\limits_{n\to\infty} a_n = \frac{\pi}{2}$ и $\lim\limits_{n\to\infty} b_n = \frac{\pi}{2}$. Таким образом, справедлива **формула Валлиса**:

$$\pi = 2 \lim_{n\to\infty} b_n = \lim_{n\to\infty} \left(\frac{(2n)!!}{(2n-1)!!}\right)^2 \cdot \frac{1}{n}.$$

Тогда поскольку $(2n)!! = 2^n n!$ и $(2n-1)!! = \frac{(2n)!}{(2n)!!} = \frac{(2n)!}{2^n n!}$, то в силу формулы Валлиса

$$\pi = \left(\frac{(2^n n!)^2}{(2n)!}\right)^2 \frac{1}{n} + o(1).$$

Из полученного равенства и формулы $(**)$ вытекает, что $\ln \pi = 2(2(n \ln 2 + \ln n!) - \ln(2n)!) - \ln n + o(1) = 4n \ln 2 + 4 \ln n! - 2 \ln(2n)! - \ln n = 4n \ln 2 - \ln n + (4n+2) \ln n - 4n + 4C + o(1) - 2((2n + \frac{1}{2}) \ln(2n) - 2n + C + o(1)) = 4n \ln 2 - \ln n + 4n \ln n + 2 \ln n - 4n + 4C - 4n \ln(2n) - \ln(2n) + 4n - 2C + o(1) = 2C + o(1) + \ln n - \ln 2 - \ln n = 2C - \ln 2 + o(1)$. Итак, $\ln \pi = 2C - \ln 2 + o(1)$, откуда следует, что $\ln \sqrt{2\pi} = C + o(1)$ и, таким образом, $C = \ln \sqrt{2\pi}$, что и требовалось доказать.

§ 11. Метод производящих функций

Пусть (a_n) – последовательность комбинаторных чисел, а $(\varphi_n(x))$ – последовательность функций. Если ряд

$$\sum_{n=0}^{\infty} a_n \varphi_n(x)$$

сходится, то на некотором множестве он задаёт функцию

$$F(x) = \sum_{n=0}^{\infty} a_n \varphi_n(x),$$

называемую производящей функцией.

Если последовательность (a_n) конечна (стабилизируется к нулю), то указанный ряд будет многочленом. Рассмотрим примеры.

Пример 1. Пусть $a_n = C_n^k$, где $k = 0, 1, \ldots, n$, а $\varphi_n(x) = x^k$. Тогда

$$F(x) = \sum_{n=0}^{\infty} a_n \varphi_n(x)$$

есть

$$(1+x)^n = \sum_{k=0}^{n} C_n^k x^k.$$

Производящая функция здесь $(1+x)^n$. С помощью производящей функции установим тождество

$$C_{2n}^n = \sum_{k=0}^{n} (C_n^k)^2.$$

Возьмём тождество

$$(1+x)^{2n} = (1+x)^n (1+x)^n.$$

Это тождество равносильно тождеству

$$\sum_{j=0}^{2n} C_{2n}^j x^j = \left(\sum_{k=0}^{n} C_n^k x^k\right) \left(\sum_{m=0}^{n} C_n^m x^m\right).$$

Сравнивая коэффициенты при x^n $(k+m=n)$, получим

$$C_{2n}^n = \sum_{k=0}^{n} C_n^k C_{n-k}^k = \sum_{k=0}^{n} \left(C_n^k\right)^2.$$

Пример 2. Рассмотрим числа Фибоначчи. Последовательность (f_n) чисел Фибоначчи задаётся рекуррентными соотношениями:

$$f_n = f_{n-1} + f_{n-2}, \quad f_0 = f_1 = 1.$$

Все числа Фибоначчи положительны. Возьмём последовательность функций $\varphi_n(x) = x^n$ $(n = 0,\ 1,\ \ldots)$. С этой последовательностью связан ряд

$$\sum_{n=0}^{\infty} f_n x^n,$$

который сходится при $|x| < \frac{1}{2}$, так как $0 < f_n \leqslant 2^n$ (поскольку $f_n \leqslant 2f_{n-1} \leqslant 2^2 f_{n-2} \leqslant \ldots \leqslant 2^n f_0$), и при $|x| < \frac{1}{2}$ определяет производящую функцию

$$F(x) = \sum_{n=0}^{\infty} f_n x^n.$$

Так как

$$xF(x) = \sum_{n=1}^{\infty} f_{n-1} x^n$$

и

$$x^2 F(x) = \sum_{n=2}^{\infty} f_{n-2} x^n,$$

то

$$xF(x)+x^2F(x) = f_0 x + \sum_{n=2}^{\infty}(f_{n-1}+f_{n-2})x^n = f_1 x + \sum_{n=2}^{\infty} f_n x^n =$$
$$= F(x) - 1,$$

откуда

$$(1 - x - x^2)F(x) = 1.$$

Отсюда находим явный вид производящей функции $F(x)$:

$$F(x) = \frac{1}{1 - x - x^2}.$$

Разложение дроби $\frac{1}{1-x-x^2}$ на простейшие дроби[2] имеет вид

$$\frac{1}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{x_1 - x} - \frac{1}{x_2 - x}\right),$$

где $x_1 = \frac{-1+\sqrt{5}}{2}$ и $x_2 = \frac{-1-\sqrt{5}}{2}$ суть корни квадратного уравнения $1 - x - x^2 = 0$. Заметим, что $x_1 x_2 = -1$. Пусть $\left|\frac{x}{x_1}\right| < 1$ и $\left|\frac{x}{x_2}\right| < 1$. Тогда

$$F(x) = \frac{1}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{x_1 - x} - \frac{1}{x_2 - x}\right) =$$
$$= \frac{1}{\sqrt{5}}\left(\frac{1}{x_1}\frac{1}{1 - \frac{x}{x_1}} - \frac{1}{x_2}\frac{1}{1 - \frac{x}{x_2}}\right) =$$
$$= \frac{1}{\sqrt{5}}\left(\frac{1}{x_1}\sum_{n=0}^{\infty}\left(\frac{x}{x_1}\right)^n - \frac{1}{x_2}\sum_{n=0}^{\infty}\left(\frac{x}{x_2}\right)^n\right) =$$
$$= \frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}\frac{x_2^{n+1} - x_1^{n+1}}{(x_1 x_2)^{n+1}}x^n = \frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}((-x_2)^{n+1} - (-x_1)^{n+1})x^n,$$

откуда

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)$$

есть явное выражение для чисел Фибоначчи (формула общего члена последовательности (f_n)).

§ 12. Определитель Вандермонда, многочлен Лагранжа, возвратные последовательности

Определитель Вандермонда. Так называется

[2] Метод разложения правильной дроби на простейшие дроби хорошо знаком читателю из курса математического анализа или из курса высшей алгебры.

определитель

$$\Delta_n = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ x_1^3 & x_2^3 & x_3^3 & \dots & x_n^3 \\ \dots & \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1} \end{vmatrix}.$$

Покажем, что

$$\Delta_n = \prod_{n \geqslant j > i \geqslant 1} (x_j - x_i).$$

Отметим вначале, что указанная формула верна, если $x_i = x_j$ для некоторых $i \neq j$, так как определитель Δ_n имеет в таком случае два одинаковых столбца. Пусть теперь все x_i, $i = \overline{1,n}$, попарно различны. Функция

$$f(t) = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ x_1 & x_2 & x_3 & \dots & t \\ x_1^2 & x_2^2 & x_3^2 & \dots & t^2 \\ x_1^3 & x_2^3 & x_3^3 & \dots & t^3 \\ \dots & \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & t^{n-1} \end{vmatrix}$$

есть многочлен степени $n-1$ со старшим коэффициентом Δ_{n-1} (чтобы понять это, достаточно разложить определитель по последнему столбцу), причём $f(x_1) = 0$, так как при $t = x_1$ определитель имеет два одинаковых столбца. Аналогично $f(x_2) = 0, \ \dots, f(x_{n-1}) = 0$. Поэтому $f(t) = \Delta_{n-1}(t - x_{n-1})(t - - x_{n-2}) \dots (t - x_1)$. Так как $\Delta_n = f(x_n)$, то

$$\Delta_n = \Delta_{n-1}(x_n - x_{n-1})(x_n - x_{n-2}) \dots (x_n - x_1).$$

Для завершения доказательства осталось многократно применить найденную рекуррентную формулу.

Многочлен Лагранжа. Пусть в прямоугольной декартовой системе координат на плоскости даны три точки

$A(x_1, y_1)$, $B(x_2, y_2)$, $C(x_3, y_3)$, абсциссы которых попарно различны. Требуется провести многочлен через эти точки, то есть найти такую функцию $y = y(x)$, что $y(x)$ является многочленом и точки A, B, C принадлежат графику функции y. Функция

$$y(x) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} y_1 + \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} y_2 + + \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)} y_3$$

есть решение поставленной задачи, поскольку, очевидно, $y(x_1) = y_1$, $y(x_2) = y_2$, $y(x_3) = y_3$ и $y(x)$ есть многочлен. Отметим, что $y(x)$ – многочлен не более второй степени (может случиться, что $y(x)$ – линейная функция и даже константа). Если точки A, B и C не лежат на одной прямой, то $y(x)$ будет многочленом второй степени, а его график – параболой. Многочлен $y(x)$ называется многочленом Лагранжа, а каждое из трёх слагаемых называется фундаментальным многочленом. Осталось доказать, что решение задачи единственно. Мы имеем: $y(x) = c + bx + ax^2$ и

$$\begin{aligned} c + bx_1 + ax_1^2 &= y_1, \\ c + bx_2 + ax_2^2 &= y_2, \\ c + bx_3 + ax_3^2 &= y_3. \end{aligned}$$

Систему из трёх линейных уравнений с тремя неизвестными a, b и c можно решить по правилу Крамера. Определитель матрицы системы

$$\begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) \neq 0$$

есть определитель Вандермонда. Так как абсциссы точек попарно различны, он отличен от нуля. Значит, система имеет единственное решение. Единственность доказана.

Совершенно аналогично в общем случае через n точек с попарно различными абсциссами можно единственным образом провести многочлен не более $(n-1)$-й степени.

Задача о двух кораблях в море. Два корабля в море двигаются с постоянными скоростями. Расстояния между ними, измеренные в 12, 14 и 15 часов, равнялись 5, 6 и 2 километра соответственно. Каким было расстояние между кораблями в 13 часов?

Решение. Движение одного корабля относительно другого описывается уравнением $\vec{r} = \vec{r_0} + \vec{v}t$. Тогда $\vec{r}^2 = \vec{r_0}^2 + 2\vec{r_0}\vec{v}t + \vec{v}^2t^2$. Таким образом, если $y = s^2$ – квадрат расстояния между кораблями, то y есть квадратичная функция от t. Многочлен Лагранжа:

$$y(t) = \frac{25(t-14)(t-15)}{(12-14)(12-15)} + \frac{36(t-12)(t-15)}{(14-12)(14-15)} + \frac{4(t-12)(t-14)}{(15-12)(15-14)},$$

откуда $y(13) = 25$.

Ответ: 5 километров.

Возвратные последовательности. Рассмотрим частный случай возвратных последовательностей, а именно возвратные последовательности степени 2. Общий случай рассматривается аналогично. Пусть последовательность (x_n) такова, что для всех n выполняется условие

$$x_{n+2} + px_{n+1} + qx_n = 0 \qquad (*)$$

и заданы x_0 и x_1. Найдём формулу общего члена последовательности (x_n). Для каждого корня λ характеристического уравнения

$$x^2 + px + q = 0$$

и любой константы C последовательность $x_n = C\lambda^n$ удовлетворяет условию $(*)$. В самом деле, $x_{n+2} + px_{n+1} + qx_n = C\lambda^{n+2} + Cp\lambda^{n+1} + qC\lambda^n = C\lambda^n(\lambda^2 + p\lambda + q) = 0$. Если последовательности (x_n) и (y_n) удовлетворяют условию $(*)$, то, очевидно, и последовательность $x_n + y_n$ удовлетворяет условию $(*)$. Таким образом, если λ_1 и λ_2 – различные (быть

может, комплексные) корни характеристического уравнения, то последовательность $x_n = C_1\lambda_1^n + C_2\lambda_2^n$ удовлетворяет условию $(*)$. Всегда найдутся такие C_1 и C_2, что

$$C_1 + C_2 = x_0,$$
$$C_1\lambda_1 + C_2\lambda_2 = x_1,$$

поскольку определитель матрицы этой системы линейных уравнений

$$\begin{vmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{vmatrix} = (\lambda_2 - \lambda_1) \neq 0.$$

Таким образом, последовательность (x_n) представляется в виде $x_n = C_1\lambda_1^n + C_2\lambda_2^n$, так как x_0, x_1 и условие $(*)$ однозначно определяют всю последовательность.

Пусть теперь характеристическое уравнение имеет один корень $\lambda = \frac{-p}{2}$. Тогда последовательность $y_n = Cn\lambda^n$ удовлетворяет условию $(*)$. В самом деле, при $C \neq 0$, и так как $p^2 - 4q = 0$, имеем

$C(n+2)\lambda^{n+2} + pC(n+1)\lambda^{n+1} + qCn\lambda^n = 0 \Leftrightarrow$

$\Leftrightarrow n\lambda^{n+2} + 2\lambda^{n+2} + pn\lambda^{n+1} + p\lambda^{n+1} + qn\lambda^n = 0 \Leftrightarrow$

$\Leftrightarrow n\lambda^2 + 2\lambda^2 + pn\lambda + p\lambda + qn = 0 \Leftrightarrow$

$\Leftrightarrow \frac{np^2}{4} + 2\frac{p^2}{4} - \frac{p^2n}{4} - \frac{p^2}{2} + qn = 0 \Leftrightarrow$

$\Leftrightarrow nq + 2q - 2qn - 2q + qn = 0 \Leftrightarrow 0 = 0.$

Таким образом, последовательность $x_n = (C_1 + C_2n)\lambda^n$ удовлетворяет условию $(*)$. Система линейных уравнений

$$C_1 = x_0,$$
$$(C_1 + C_2)\lambda = x_1$$

при $\lambda \neq 0$ имеет единственное решение. Поэтому при $\lambda \neq 0$ последовательность (x_n) представляется в виде $x_n = (C_1 + C_2n)\lambda^n$ в случае корня характеристического уравнения λ кратности 2.

Пример. Рассмотрим числа Фибоначчи. Последовательность (f_n) чисел Фибоначчи задаётся

рекуррентными соотношениями:

$$f_n = f_{n-1} + f_{n-2}, \quad f_0 = 0,\ f_1 = 1.$$

Характеристическое уравнение этой возвратной последовательности $x^2 = x + 1$. Корни характеристического уравнения $\lambda_1 = \frac{1+\sqrt{5}}{2}$ и $\lambda_2 = \frac{1-\sqrt{5}}{2}$. Тогда

$$f_n = C_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + C_2 \left(\frac{1-\sqrt{5}}{2}\right)^n,$$

$f_0 = 0 = C_1 + C_2,\ C_2 = -C_1;\ f_1 = 1 = C_1 \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) =$
$= C_1\sqrt{5},\ C_1 = \frac{1}{\sqrt{5}}$. Таким образом,

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right).$$

Задача. Решите рекуррентные соотношения, то есть найдите общий член последовательности (a_n), если

1) $a_{n+2} - 4a_{n+1} + 3a_n = 0,\ a_0 = 10,\ a_1 = 16,$

2) $a_{n+2} - 4a_{n+1} + 4a_n = 0,\ a_0 = 10,\ a_1 = 16.$

§ 13. Формула включений-исключений

Будем рассматривать подмножества некоторого конечного множества S. Обозначим $|A|$ количество элементов (мощность) конечного множества A, а $\overline{A} = S \setminus A$ – дополнение множества A до множества S. Рассмотрим характеристическую функцию χ_A множества A, задаваемую правилом:

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A; \\ 0, & \text{если } x \notin A. \end{cases}$$

Тогда, очевидно,

$$|A| = \sum_{x \in S} \chi_A(x), \quad \chi_{\overline{A}}(x) = 1 - \chi_A(x), \quad \chi_{A \cap B}(x) = \chi_A(x)\chi_B(x).$$

Так как $A \cup B = \overline{\overline{A \cup B}} = \overline{\overline{A} \cap \overline{B}}$, то

$$\chi_{A \cup B} = 1 - \chi_{\overline{A} \cap \overline{B}} = 1 - (1 - \chi_A)(1 - \chi_B) = \chi_A + \chi_B - \chi_A\chi_B.$$

Тогда

$$\sum_{x \in S} \chi_{A \cup B}(x) = \sum_{x \in S} \chi_A(x) + \sum_{x \in S} \chi_B(x) - \sum_{x \in S} \chi_{A \cap B}(x).$$

Таким образом,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Это и есть формула включений-исключений для двух множеств. Аналогично можно получить формулу включений-исключений для n множеств. Например, для трёх множеств: так как

$$\chi_{A \cup B \cup C} = 1 - (1 - \chi_A)(1 - \chi_B)(1 - \chi_C) =$$
$$= \chi_A + \chi_B + \chi_C - \chi_A\chi_B - \chi_A\chi_C - \chi_B\chi_C + \chi_A\chi_B\chi_C,$$

то

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Задача. При исследовании читательских вкусов студентов оказалось, что 60% студентов читают журнал A, 50% – журнал B, 50% – журнал C, 30% – журналы A и B, 20% – журналы B и C, 40% – журналы A и C, 10% – журналы A, B и C. Сколько процентов студентов не читают на одного из журналов?

Решение. Наряду с множествами A, B и C студентов, читающих журналы A, B и C соответственно, рассмотрим множество D студентов, не читающих ни одного из журналов и применим формулу включений-исключений для объединения этих четырех множеств. Пусть x процентов студентов не читают ни одного из журналов. По формуле включений-исключений имеем: $100 = 60 + 50 + 50 + x - 30 - 20 - 40 + 10$, откуда $x = 20$.

Ответ: 20%.

ГЛАВА 3

АЛГЕБРА ЛОГИКИ

§ 14. Алгебра логики

Алгебра логики является разделом дискретной математики.

Пусть $B = \{0,1\}$ – множество, единственными элементами которого являются 0 и 1, $B^n = \{0,1\}^n = \underbrace{B \times B \ldots \times B}_{n \text{ раз}}$ – прямое декартово произведение множества B на само себя n раз. Функция $f(x_1, \ldots, x_n)$, определённая на множестве $B^n = \{0,1\}^n$ и принимающая значения из множества $\{0,1\}$, называется функцией алгебры логики, а также булевой функцией, зависящей от n переменных.

Множество всех булевых функций обозначается P_2, множество булевых функций, зависящих от n переменных обозначается $P_2^{(n)}$. Полагают $n \geqslant 0$. Случаю $n = 0$ соответствуют константы 0 и 1.

Булеву функцию можно задать, указав, какие значения она принимает на каждом наборе значений аргументов, в виде таблицы, имеющей 2^n строк (столько существует различных наборов длины n нулей и единиц). Количество всех булевых функций, зависящих от n переменных, $\left|P_2^{(n)}\right| = 2^{2^n}$, так как каждому из 2^n наборов значений аргументов соответствует одно из двух значений функции – либо 0, либо 1.

Аргументы булевой функции бывают существенными и несущественными (фиктивными). Например, для функции $f(x,y) = x$ аргумент x – существенная переменная, а y – фиктивная. Если, например, $g(x) = x$, то говорят, что функция g получается из f удалением несущественной переменной y, а функция f получается из g добавлением несущественной переменной y. Естественно считать, что $f = g$. Таким образом, равенство функций определяется с

точностью до фиктивных переменных. Можно полагать, что две функции зависят от одного и того же количества переменных, добавив или удалив, если нужно, фиктивные переменные. Например, константы несущественно зависят от любого, наперёд заданного количества переменных.

Элементарными функциями являются константы 0 и 1, тождественная функция x и функции из следующей таблицы, называемые соответственно отрицание («не»), дизъюнкция («или»), конъюнкция («и», иначе обозначаемая $x \wedge y$), сложение по модулю 2 (исключающее «или»: исключается случай 1 или 1 равно 1, что допускает дизъюнкция), импликация[3] («из x следует y»), степень, эквивалентность (равносильность), штрих Шеффера, стрелка Пирса, экспликация:

x	y	$\overline{x}$	$x \vee y$	$x\&y$	$x+y$	$x \to y$	x^y	$x \sim y$	$x\|y$	$x \downarrow y$	$x \leftarrow y$
0	0	1	0	0	0	1	1	1	1	1	1
0	1	1	1	0	1	1	0	0	1	0	0
1	0	0	1	0	1	0	0	0	1	0	1
1	1	0	1	1	0	1	1	1	0	0	1

Рассматриваются также коимпликация

$$x \not\to y = \overline{x \to y}$$

и коэкспликация

$$x \not\leftarrow y = \overline{x \leftarrow y}.$$

Из анализа таблицы видно, что

$$x \vee y = \max\{x,y\},\ x\&y = xy = \min\{x,y\},$$
$$\overline{x} = x+1,\ x|y = \overline{xy}, x \downarrow y = \overline{x \vee y}.$$

[3] В алгебре логики 1 обозначает истину, а 0 – ложь. Заметим, что если посылка импликации ложна (0), то значение импликации – автоматически истина (1). Математический логик Льюис Кэролл, автор книги «Алиса в стране чудес», считал это свойство парадоксом импликации.

Отметим также другие тождества:

$$x \vee 0 = x,\ x \vee 1 = 1,\ x \vee x = x,\ 0x = 0,\ 1x = x,$$
$$x^2 = xx = x,\ 0 + x = x,\ x + x = 0,$$
$$x\overline{x} = 0,\ x \vee \overline{x} = 1,\ \overline{\overline{x}} = x,$$
$$(x \vee y)z = xz \vee yz,\ (xy) \vee z = (x \vee z)(y \vee z).$$

Последние два тождества означают взаимную дистрибутивность конъюнкции и дизъюнкции, при $z = 0$ они обращаются в верные равенства $0 = 0$ и $xy = xy$, а при $z = 1$ – в верные равенства $x \vee y = x \vee y$ и $1 = 1$. Так же можно доказать тождество $(x + y)z = xz + yz$.

При нахождении значения формулы, если скобки, указывающие на порядок действий, пропущены, конъюнкция выполняется раньше дизъюнкции, эквиваленция выполняется в последнюю очередь (этим, кроме обозначения и названия, она отличается от степени), операция возведения в степень имеет высокий приоритет в порядке действий.

Конъюнкция, дизъюнкция и сложение коммутативны и ассоциативны, то есть

$$x \circ y = y \circ x \text{ и } (x \circ y) \circ z = x \circ (y \circ z),$$

если кружком $\circ$ обозначить любую из этих функций. Например,

$$(x \vee y) \vee z = \max\{\max\{x, y\}, z\} = \max\{x, y, z\} =$$
$$= \max\{x, \max\{y, z\}\} = x \vee (y \vee z).$$

Столь же просто доказываются остальные тождества.

Сопоставляя таблицы для левых и правых, отделенных знаком равенства, частей следующих равенств, нетрудно видеть, что справедливы законы де Моргана:

$$\overline{x \vee y} = \overline{xy} \text{ и } \overline{xy} = \overline{x} \vee \overline{y},$$

закон контрапозиции:

$$x \to y = \overline{y} \to \overline{x},$$

а также равенства

$$x \to y = \overline{x} \vee y,\ \overline{x \to y} = x\overline{y},\ x^y = xy \vee \overline{x}\ \overline{y} = y^x,\ x^0 = \overline{x},\ x^1 = x,$$

$$x \sim y = (x \to y)(y \to x), x \to x = 1,\ \overline{x} \sim y = x \sim \overline{y} =$$
$$= x + y = \overline{x \sim y},$$

и т. д.

Пусть $\mathfrak{P}$ есть некоторое (не обязательно конечное) подмножество функций из P_2. Формулой над $\mathfrak{P}$ называется композиция функций из $\mathfrak{P}$ и, быть может, символов переменных (таких символов имеется счетный запас). Например, если

$$\mathfrak{P} = \{\&, \vee, -\},$$

то

$$\mathfrak{A} = (x_1 \vee x_2)x_3 \vee \overline{x}_4$$

есть формула над $\mathfrak{P}$, поскольку

$$(x_1 \vee x_2)x_3 \vee \overline{x}_4 = g(f(g(x_1, x_2), x_3), h(x_4)),$$

где f – конъюнкция, g – дизъюнкция, h – отрицание.

Для $\mathfrak{A}$ можно использовать также обозначения $\mathfrak{A}(x_1, x_2, x_3, x_4)$ и $\mathfrak{A}[f, g, h]$. Функции f, g и h попарно различны.

Ясно, что всякая формула реализует булеву функцию. Две формулы называются равными (или эквивалентными), если равны функции, ими реализуемые.

Подформулой формулы $\mathfrak{A}$ называется любая формула, которая использовалась для построения формулы $\mathfrak{A}$. Если подформулу некоторой формулы $\mathfrak{A}$ заменить на эквивалентную ей формулу, то формула $\mathfrak{A}$ перейдет в формулу, эквивалентную $\mathfrak{A}$. Это простое утверждение лежит в основе метода цепей эквивалентностей, позволяющего получать из известных формул новые формулы. Например, поскольку

$$x \vee xy = x \cdot 1 \vee xy = x(1 \vee y) = x \cdot 1 = x,$$

то справедливо правило поглощения произведения:

$$x \vee xy = x.$$

$$\overline{x \to y} = \overline{\overline{x} \vee y} = \overline{\overline{x}} \cdot \overline{y} = x\overline{y},$$

то

$$\overline{x \to y} = x\overline{y}.$$

Так как

$x \sim y = (x \to y)(y \to x) = (\overline{x} \vee y)(\overline{y} \vee x) = \overline{x}\ \overline{y} \vee y\overline{y} \vee \overline{x}x \vee yx =$
$= \overline{x}\ \overline{y} \vee 0 \vee 0 \vee xy = xy \vee \overline{x}\ \overline{y}$, то

$$x \sim y = xy \vee \overline{x}\ \overline{y}.$$

Функция $f^*(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n)$ называется двойственной функцией к функции $f(x_1, \ldots, x_n)$. Функция f двойственна к f^*, поскольку $f^{**} = (f^*)^* = f$ (свойство взаимности). Поэтому если $f^* = g$, то $g^* = f$.

Таблица для двойственной к f функции f^* при выбранном порядке наборов значений аргументов получается из таблицы для f инвертированием столбца функции f (то есть заменой 0 на 1 и 1 на 0) и его переворачиванием. Например,

x	y	$f(x,y)$	$f^*(x,y)$
0	0	1	0
0	1	1	1
1	0	0	0
1	1	1	0

Анализируя таблицы при помощи указанного правила, находим, что двойственны друг другу константы 0 и 1,

xy и $x \vee y$, $x + y$ и x^y, $x|y$ и $x \downarrow y$,

$x \to y$ и $\overline{x \leftarrow y}$, x и x, $\overline{x}$ и $\overline{x}$.

Указанные пары двойственных функций можно найти иначе, по определению двойственной функции, применяя свойство взаимности и цепи эквивалентностей. Например, $(x|y)^* = \overline{\overline{x}|\overline{y}} = \overline{\overline{x}\ \overline{y}} = \overline{x} \cdot \overline{y} = \overline{x \vee y} = x \downarrow y$. Значит, $(x|y)^* = x \downarrow y$ и $(x \downarrow y)^* = x|y$.

Теорема (принцип двойственности). *Если*

$$\Phi(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

то

$$\Phi^*(x_1, \ldots, x_n) = f^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n)).$$

Доказательство. $\Phi^*(x_1, \ldots, x_n) =$

$$= \overline{f}(f_1(\overline{x}_1, \ldots, \overline{x}_n), \ldots, f_m(\overline{x}_1, \ldots, \overline{x}_n)) =$$
$$= \overline{f}(\overline{\overline{f}}_1(\overline{x}_1, \ldots, \overline{x}_n), \ldots, \overline{\overline{f}}_m(\overline{x}_1, \ldots, \overline{x}_n)) =$$
$$= \overline{f}(\overline{f}_1^*(x_1, \ldots, x_n), \ldots, \overline{f}_m^*(x_1, \ldots, x_n)) =$$
$$= f^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n)).$$

Теорема доказана.

Говорят, что формулы $\mathfrak{A}[f_1, \ldots, f_s]$ и $\mathfrak{B}[g_1, \ldots, g_s]$ имеют одинаковое строение C, если функции f_i и g_i имеют одинаковые символы независимых переменных и формула $\mathfrak{B}$ получается из $\mathfrak{A}$ заменой всех вхождений f_i на g_i, где $i = 1, 2, \ldots, s$; $f_i \neq f_j$ и $g_i \neq g_j$ при $i \neq j$.

Формула $\mathfrak{A}$ однозначно определяется строением C и упорядоченной совокупностью $\{f_1, \ldots, f_s\}$, запись: $\mathfrak{A} = C[f_1, \ldots, f_s]$.

Из принципа двойственности вытекает, что

если формула $\mathfrak{A} = C[f_1, \ldots, f_s]$ реализует функцию $f(x_1, \ldots, x_n)$,

то формула $\mathfrak{A}^* = C[f_1^*, \ldots, f_s^*]$ реализует функцию $f^*(x_1, \ldots, x_n)$.

Если $\mathfrak{A}(x_1, \ldots, x_n) = \mathfrak{B}(x_1, \ldots, x_n)$, то $\mathfrak{A}^*(x_1, \ldots, x_n) = \mathfrak{B}^*(x_1, \ldots, x_n)$.

Например,

так как $\overline{x \vee y} = \overline{x}\ \overline{y}$, то $\overline{xy} = \overline{x} \vee \overline{y}$;

так как $x^y = xy \vee \overline{x}\ \overline{y}$, то $x + y = (x \vee y)(\overline{x} \vee \overline{y})$;

так как $x \to y = \overline{x} \vee y$, то $\overline{y \to x} = \overline{x}y$;

так как $x|y = \overline{xy}$, то $x \downarrow y = \overline{x \vee y}$.

Функция $h(x, y, z) = xy \vee xz \vee yz$ называется медианой. Из анализа таблиц видно, что $h(x, y, z) = h^*(x, y, z)$. Тогда согласно принципу двойственности

$$xy \vee xz \vee yz = (x \vee y)(x \vee z)(y \vee z).$$

Теорема (о разложении функций по m переменным). *Каждую функцию алгебры логики*

$f(x_1,\dots x_n)$ при любом m $(1\leqslant m\leqslant n)$ можно представить в виде

$$f(x_1,\dots,x_m,x_{m+1},\dots,x_n)=$$
$$=\bigvee_{(\sigma_1,\dots,\sigma_m)} x_1^{\sigma_1}x_2^{\sigma_2}\dots x_m^{\sigma_m}f(\sigma_1,\sigma_2,\dots,\sigma_m,x_{m+1},\dots,x_n),$$

где дизъюнкция берётся по всевозможным наборам значений переменных $x_1,\dots,x_m$.

Доказательство. Отметим, что $x^y=1$ тогда и только тогда, когда $x=y$. Возьмём произвольный набор значений переменных $(\alpha_1,\dots,\alpha_n)$. Тогда левая часть указанной формулы есть $f(\alpha_1,\dots,\alpha_n)$, а правая часть указанной формулы есть $\alpha_1^{\alpha_1}\alpha_2^{\alpha_2}\dots\alpha_m^{\alpha_m}f(\alpha_1,\alpha_2,\dots,\alpha_m,\alpha_{m+1},\dots,\alpha_n)=f(\alpha_1,\dots,\alpha_n)$, что оканчивает доказательство.

Разложение

$$f(x_1,\dots,x_n)=\bigvee_{\substack{(\sigma_1,\dots,\sigma_n)\\ f(\sigma_1,\dots,\sigma_n)=1}} x_1^{\sigma_1}x_2^{\sigma_2}\dots x_n^{\sigma_n}$$

называется совершенной дизъюнктивной нормальной формой (совершенной д. н. ф.) функции $f\neq 0$.

Напишем, например, совершенную д. н. ф. для медианы. Медиану $h(x,y,z)=xy\vee xz\vee yz$ можно задать при помощи следующей таблицы:

x	y	z	$h(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Согласно формуле для совершенной д. н. ф. в этой таблице нужно взять те строки, где значение h равно 1. Замечая, что $x^0=\overline{x}$ и $x^1=x$, по формуле для совершенной д. н. ф. находим

$$h(x,y,z)=\overline{x}yz\vee x\overline{y}z\vee xy\overline{z}\vee xyz.$$

Применим к совершенной д. н. ф.

$$f^*(x_1,\dots,x_n)=\bigvee_{\substack{(\sigma_1,\dots,\sigma_n)\\ f^*(\sigma_1,\dots,\sigma_n)=1}} x_1^{\sigma_1}x_2^{\sigma_2}\dots x_n^{\sigma_n}$$

функции $f(x_1,\dots,x_n)\neq 1$ принцип двойственности. Получим

$$f(x_1,\dots,x_n)=\bigwedge_{\substack{(\sigma_1,\dots,\sigma_n)\\ f^*(\sigma_1,\dots,\sigma_n)=1}} (x_1^{\sigma_1}\vee x_2^{\sigma_2}\vee\dots\vee x_n^{\sigma_n})=$$
$$=\bigwedge_{\substack{(\sigma_1,\dots,\sigma_n)\\ f(\overline{\sigma}_1,\dots,\overline{\sigma}_n)=0}} (x_1^{\sigma_1}\vee x_2^{\sigma_2}\vee\dots\vee x_n^{\sigma_n})=$$
$$=\bigwedge_{\substack{(\overline{\sigma}_1,\dots,\overline{\sigma}_n)\\ f(\sigma_1,\dots,\sigma_n)=0}} \left(x_1^{\overline{\sigma}_1}\vee x_2^{\overline{\sigma}_2}\vee\dots\vee x_n^{\overline{\sigma}_n}\right)=$$
$$=\bigwedge_{\substack{(\sigma_1,\dots,\sigma_n)\\ f(\sigma_1,\dots,\sigma_n)=0}} \left(x_1^{\overline{\sigma}_1}\vee x_2^{\overline{\sigma}_2}\vee\dots\vee x_n^{\overline{\sigma}_n}\right).$$

Разложение

$$f(x_1,\dots,x_n)=\bigwedge_{\substack{(\sigma_1,\dots,\sigma_n)\\ f(\sigma_1,\dots,\sigma_n)=0}} \left(x_1^{\overline{\sigma}_1}\vee x_2^{\overline{\sigma}_2}\vee\dots\vee x_n^{\overline{\sigma}_n}\right)$$

называется совершенной конъюнктивной нормальной формой (совершенной к. н. ф.) функции f.

Напишем, например, совершенную к. н. ф. для медианы h. Согласно формуле для совершенной к. н. ф. в таблице для медианы нужно взять те строки, где значение h равно 0. Замечая, что $x^0=\overline{x}$ и $x^1=x$, по формуле для совершенной к. н. ф. находим

$$h(x,y,z)=(x\vee y\vee z)\,(x\vee y\vee\overline{z})\,(x\vee\overline{y}\vee z)\,(\overline{x}\vee y\vee z)\,.$$

Пусть $\mathfrak{A}$ и $\mathfrak{P}$ – подмножества функций из P_2. Система $\mathfrak{A}$ называется $\mathfrak{P}$-полной, если всякая функция из $\mathfrak{P}$ может быть представлена формулой над $\mathfrak{A}$. Например, система $B_0 = \{\&, \vee, -\}$ P_2-полна, так как константа 1 представляется в виде $1 = x \vee \overline{x}$, константа 0 представляется в виде $0 = x\overline{x}$, а любая функция из P_2, отличная от константы, представляется в виде совершенной д. н. ф.

Ясно, что если система $\mathfrak{A}$ $\mathfrak{B}$-полна, а система $\mathfrak{B}$ $\mathfrak{P}$-полна, то система $\mathfrak{A}$ $\mathfrak{P}$-полна. Например, система $B_1 = \{\&, -\}$ P_2-полна, так как $x \vee y = \overline{\overline{x}\,\overline{y}}$, и, таким образом, B_1 B_0-полна, а B_0 P_2-полна. Система $B_2 = \{|\}$ P_2-полна, так как $\overline{x} = x|x$, $xy = \overline{x|y} = (x|y)|(x|y)$, а система $B_1 = \{\&, -\}$ P_2-полна.

$\mathfrak{P}$-полная система $\mathfrak{A}$ называется минимальной $\mathfrak{P}$-полной системой, если какое-либо собственное подмножество $\mathfrak{A}$ не является $\mathfrak{P}$-полной системой. Базисом в $\mathfrak{P}$ называется минимальная $\mathfrak{P}$-полная система.

Из принципа двойственности вытекает, что если система $\mathfrak{A}$ P_2-полна, то система $\mathfrak{A}^*$, состоящая из функций, двойственных функциям системы $\mathfrak{A}$, тоже P_2-полна. В самом деле, если $f^* = C[f_1, \ldots, f_s]$ есть формула над $\mathfrak{A}$, то $f = C[f_1^*, \ldots, f_s^*]$ есть формула над $\mathfrak{A}^*$, откуда ввиду произвольности f следует утверждение. Из этого утверждения вытекает, что если система $\mathfrak{A}$ есть базис в P_2, то система $\mathfrak{A}^*$ тоже базис в P_2, так как обе эти системы P_2-полны или не полны одновременно. Например, система $B_3 = \{\vee, -\}$ – базис в P_2, так как $B_1 = \{\&, -\}$ – базис в P_2; система $B_4 = \{\downarrow\}$ – базис в P_2, так как $B_3 = \{|\}$ – базис в P_2.

Заметим, что система $\{0, 1, \&, +\}$ P_2-полная. Это значит, что всякая функция из P_2 представляется в виде полинома от нескольких переменных. Эти полиномы называются полиномами Жегалкина. Функция $f(x_1, \ldots, x_n) \in P_2^n$ представляется в виде суммы мономов вида $x_{i_1} \ldots x_{i_s}$. Количество всех таких мономов 2^n, ведь именно столько существует подмножеств n-элементного множества

$\{x_1, \ldots, x_n\}$. Каждый моном может входить в полином Жегалкина для функции $f(x_1, \ldots, x_n)$ с коэффициентом 0 или с коэффициентом 1. Таким образом, количество всех полиномов, представляющих функции из P_2^n, равно 2^{2^n}, такое же, как и количество функций в P_2^n. Это значит, что представление булевой функции полиномом Жегалкина единственно.

Приведём примеры:

$x \vee y = xy + x + y$,

$x \to y = \overline{x} \vee y = \overline{x\overline{y}} = \overline{x(y+1)} = \overline{xy + x} = xy + x + 1$,

$x \downarrow y = \overline{x \vee y} = \overline{xy + x + y} = xy + x + y + 1$,

$x|y = \overline{xy} = xy + 1$,

$x^y = \overline{x + y} = x + y + 1$.

Полиномы Жегалкина можно находить методом неопределенных коэффициентов.[4]

Применения к естественному языку

Задача Венна (1881 г.). Существовал клуб с такими правилами: **(1)** Члены финансового комитета должны избираться среди членов общей дирекции. **(2)** Нельзя быть одновременно членом общей дирекции и членом библиотечного совета, не будучи членом финансового комитета. **(3)** Ни один член библиотечного совета не может быть членом финансового комитета. Упростите правила.

Решение. Пусть P означает: «x является членом финансового правления», Q означает: «x является членом общей дирекции», а R означает: «x является членом библиотечного совета». Тогда правила выражаются формулой

$$f = (P \to Q)\&((\overline{Q\&R}) \vee P)\&(\overline{R\&P}).$$

Составим для неё конъюнктивную нормальную форму. $f = 0$ лишь в том случае, когда какая-либо из трёх конъюнкций

[4] Метод неопределенных коэффициентов хорошо знаком читателю из курса математического анализа или из курса алгебры.

ложна (имеет значение 0), что приводит к следующей сокращенной таблице для формулы f :

P	Q	R	f
1	0		0
0	1	1	0
1		1	0

В пустых местах сокращенной таблицы можно поставить как 0, так и 1.

Эта таблица переписывается в виде следующей сокращенной таблицы:

P	Q	R	f
1	0		0
	1	1	0

,

из которой видно, что

$$f = (\overline{Q} \vee \overline{R})\&(Q \vee \overline{P}) = (Q \to \overline{R})\&(P \to Q).$$

Значит, правила попросту таковы: **(1)** и **(2a)**: Ни один член общей дирекции не может быть членом библиотечного совета.

Упражнение. (Задача Кислера.) Браун, Джонс и Смит обвиняются в подделке сведений о подлежащих налоговому обложению доходах. Они дают под присягой такие показания:

Браун: Джонс виновен, а Смит не виновен.

Джонс: Если Браун виновен, то виновен и Смит.

Смит: Я не виновен, но хотя бы один из них двоих виновен.

Обозначим соответственно B, D и C следующие высказывания: «Браун невиновен», «Джонс невиновен», «Смит невиновен». Выразите показания каждого из подозреваемых формулой. Постройте таблицы истинности трех полученных формул. Ответьте на вопросы:

(а) Совместимы ли показания всех троих подозреваемых (т. е. могут ли они быть верны одновременно)?

(б) Показания одного из подозреваемых следуют из показаний другого; о чьих показаниях идёт речь?

(в) Если все трое невиновны, то кто дал ложные показания?

(г) Предполагая, что показания всех подозреваемых верны, укажите: кто виновен, а кто невиновен?

(д) Если невиновный говорит правду, а виновный лжет, то кто виновен, а кто невиновен?

§ 15. Теорема о функциональной полноте

Замыканием $[\mathfrak{M}]$ подмножества $\mathfrak{M} \subset P_2$ функций из P_2 называется множество всех булевых функций, представимых формулами над $\mathfrak{M}$. Например,

$$[\{|\}] = P_2,\ [\{\downarrow\}] = P_2,\ [\{-, \vee, \wedge\}] = P_2,\ [P_2] = P_2.$$

Множество $\mathfrak{M}$ называется замкнутым, если оно совпадает со своим замыканием. Ясно, что замыкание множества $[\mathfrak{M}]$ замкнуто: $[[\mathfrak{M}]] = [\mathfrak{M}]$.

Пусть T_0 есть множество булевых функций, сохраняющих константу 0, то есть таких функций $f(x_1, \ldots, x_n) \in P_2$, что $f(0, \ldots, 0) = 0$.

Композиция $f(f_1(x_1, \ldots, x_n), \ldots,\ f_m(x_1, \ldots, x_n))$ функций $f, f_1, \ldots, f_m$, принадлежащих T_0, принадлежит T_0. В самом деле, для таких функций

$$f(f_1(0, \ldots, 0), \ldots, f_m(0, \ldots, 0)) = f(0, \ldots, 0) = 0.$$

Так как тождественная функция x принадлежит T_0 и композиция функций, принадлежащих T_0, принадлежит T_0, то замыкание $[T_0] = T_0$. Таким образом, T_0 есть замкнутое множество, говорят, замкнутый класс.

Пусть T_1 есть множество булевых функций, сохраняющих константу 1, то есть таких функций $f(x_1, \ldots, x_n) \in P_2$, что $f(1, \ldots, 1) = 1$.

Композиция $f(f_1(x_1, \ldots, x_n), \ldots,\ f_m(x_1, \ldots, x_n))$ функций $f, f_1, \ldots, f_m$, принадлежащих T_1, принадлежит T_1. В самом

деле, для таких функций

$$f(f_1(1,\dots,1),\dots,f_m(1,\dots,1)) = f(1,\dots,1) = 1.$$

Так как тождественная функция x принадлежит T_1 и композиция функций, принадлежащих T_1, принадлежит T_1, то замыкание $[T_1] = T_1$. Таким образом, T_1 есть замкнутый класс.

Пусть L есть множество функций, представимых формулами над $\{0,1,+\}$. Такие функции называются линейными. Линейные функции имеют вид

$$f(x_1,\dots,x_n) = a_1x_1 + \dots + a_nx_n + a_0.$$

Так как $L = [\{0,1,+\}]$, а замыкание замкнуто, то L – замкнутый класс.

Функция $f(x_1,\dots,x_n) \in P_2$ называется самодвойственной, если

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

Самодвойственны, например, тождественная функция x, отрицание $\overline{x}$, медиана $h(x,y,z) = xy \vee xz \vee yz$. Не самодвойственны константы 0 и 1, конъюнкция xy, дизъюнкция $x \vee y$, штрих Шеффера $x|y$, стрелка Пирса $x \downarrow y$, x^y, $x+y$.

Ясно, что самодвойственная функция на противоположных наборах $(\alpha_1,\dots,\alpha_n)$ и $(\overline{\alpha}_1,\dots,\overline{\alpha}_n)$ принимает противоположные значения и наоборот: если функция на противоположных наборах принимает противоположные значения, то эта функция самодвойственная.

Композиция $\Phi = f(f_1,\dots,f_m)$ самодвойственных функций $f, f_1,\dots,f_m$ самодвойственна, так как $\Phi^* = f^*(f_1^*,\dots,f_m^*) = = f(f_1,\dots,f_m) = \Phi$. Таким образом, класс S самодвойственных функций замкнут.

Пусть $\widetilde{\alpha} = (\alpha_1,\ \dots,\alpha_n)$ и $\widetilde{\beta} = (\beta_1,\ \dots,\beta_n)$ – два набора нулей и единиц. Говорят, что набор $\widetilde{\alpha}$ предшествует набору $\widetilde{\beta}$, если $\alpha_1 \leqslant \beta_1,\dots,\alpha_n \leqslant \beta_n$. Запись: $\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$. Отношение предшествования есть отношение частичного порядка на

множестве наборов нулей и единиц длины n, так как оно рефлексивно, антисимметрично и транзитивно. Не все наборы сравнимы. Например, наборы $(0,1)$ и $(1,0)$ не сравнимы.

Функция $f(x_1,\dots,x_n)$ называется монотонной, если для любых наборов $\widetilde{\alpha}$ и $\widetilde{\beta}$ длины n из того, что $\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$, следует, что $f(\widetilde{\alpha}) \leqslant f(\widetilde{\beta})$.

Монотонными являются, например, функции 0, 1, x, xy, $x \vee y$.

Композиция $\Phi = f(f_1,\dots,f_m)$ монотонных функций $f, f_1,\dots,f_m$ монотонна. Действительно, функция, равная монотонной (получающаяся из неё добавлением или удалением несущественных переменных), монотонна. Поэтому можно, как обычно, считать, что функции $f_1,\dots,f_m$ зависят от одних и тех же переменных $x_1,\dots,x_n$. Если теперь $\widetilde{\alpha} \preccurlyeq \widetilde{\beta}$, то $f_1(\widetilde{\alpha}) \leqslant f_1(\widetilde{\beta}),\ \dots, f_m(\widetilde{\alpha}) \leqslant f_m(\widetilde{\beta})$. Тогда $(f_1(\widetilde{\alpha}),\ \dots, f_m(\widetilde{\alpha})) \preccurlyeq (f_1(\widetilde{\beta}),\ \dots, f_m(\widetilde{\beta}))$ и тогда $f(\widetilde{\alpha}) \leqslant f(\widetilde{\beta})$, что завершает доказательство.

Таким образом, класс M монотонных функций замкнут.

В следующей таблице знак плюс означает, что функция содержится в указанном классе, а знак минус означает противоположное, что соответствующая функция не содержится в указанном классе.

	T_0	T_1	S	M	L
0	+	−	−	+	+
1	−	+	−	+	+
$\overline{x}$	−	−	+	−	+
x	+	+	+	+	+
$x\|y$	−	−	−	−	−

Из таблицы видно, что замкнутые классы T_0, T_1, S, M, L попарно различны, их пересечение не пусто. Указанные классы являются собственными подмножествами P_2, и их объединение является собственным подмножеством P_2.

Лемма 1 (о несамодвойственной функции). *Если $f(x_1,\dots,x_n) \notin S$, то из неё путём подстановки функций x и $\overline{x}$ можно получить несамодвойственную функцию одного переменного, то есть константу.*

Доказательство. Так как $f \notin S$, то найдётся набор $(\alpha_1,\dots,\alpha_n)$ такой, что $f(\overline{\alpha}_1,\dots,\overline{\alpha}_n) = f(\alpha_1,\dots,\alpha_n)$. Положим $\varphi(x) = f(x^{\alpha_1},\dots,x^{\alpha_2})$. Тогда $\varphi(0) = f(0^{\alpha_1}.\dots,0^{\alpha_n}) = f(\overline{\alpha}_1,\dots,\overline{\alpha}_n) = f(\alpha_1,\dots,\alpha_n) = f(1^{\alpha_1},\dots,1^{\alpha_n}) = \varphi(1)$. Лемма доказана.

Лемма 2 (о немонотонной функции). *Если $f(x_1,\dots,x_n) \notin M$, то из неё путём подстановки констант 0 и 1 и функции x можно получить функцию $\overline{x}$.*

Доказательство. Так как f немонотонна, то найдутся соседние наборы $\widetilde{\alpha} = (\alpha_1,\dots,\alpha_{i-1},0,\alpha_{i+1},\dots,\alpha_n)$ и $\widetilde{\beta} = (\alpha_1,\dots,\alpha_{i-1},1,\alpha_{i+1},\dots,\alpha_n)$ такие, что $f(\widetilde{\alpha}) > f(\widetilde{\beta})$. Пусть $\varphi(x) = f(\alpha_1,\dots,\alpha_{i-1},x,\alpha_{i+1},\dots,\alpha_n)$. Тогда $\varphi(0) = \varphi(\widetilde{\alpha}) > \varphi(\widetilde{\beta}) = \varphi(1)$. Это значит, что $\varphi(0) = 1$, $\varphi(1) = 0$. Лемма доказана.

Лемма 3 (о нелинейной функции). *Если $f(x_1,\dots,x_n) \notin L$, то из неё путём подстановки констант 0 и 1 и функций x и $\overline{x}$ и, быть может, навешиванием отрицания над f можно получить конъюнкцию x_1x_2.*

Доказательство. Без ограничения общности можно считать, что в полиноме Жегалкина для f в некотором мономе присутствуют x_1 и x_2 (если необходимо, переименуем переменные). Тогда этот полином можно преобразовать к виду $x_1x_2f_1(x_3,\dots,x_n) + x_1f_2(x_3,\dots,x_n) + x_2f_3(x_3,\dots,x_n) + f_4(x_3,\dots,x_n)$, где в силу единственности полинома $f_1(x_3,\dots,x_n) \neq 0$. Пусть $\alpha_3,\dots,\alpha_n$ таковы, что $f(\alpha_3,\dots,\alpha_n) = 1$. Тогда $\varphi(x_1,x_2) = f(x_1,x_2,\alpha_3,\dots,\alpha_n) = x_1x_2 + \alpha x_1 + \beta x_2 + \gamma$. Функция $\psi(x_1,x_2) = \varphi(x_1+\beta, x_2+\alpha) + \alpha\beta + \gamma = (x_1+\beta)(x_2+\alpha) + \alpha(x_1+\beta) + \beta(x_2+\alpha) + \gamma + (\alpha\beta+\gamma) = x_1x_2$ искомая. Лемма доказана.

Теорема (о функциональной полноте). *Для того чтобы система функций $\mathfrak{P}$ была P_2-полной, необходимо и достаточно, чтобы она целиком не содержалась ни в одном из пяти классов T_0, T_1, S, M и L.*

Доказательство. Необходимость. Пусть $\mathfrak{P}$ P_2-полна и $\mathfrak{N}$ тот из пяти указанных классов, в котором содержится $\mathfrak{P}$. Тогда $P_2 = [\mathfrak{P}] \subset [\mathfrak{N}] = \mathfrak{N} \subset P_2$. Значит, $\mathfrak{N} = P_2$, что не так. Необходимость доказана.

Достаточность. Пусть $\mathfrak{P}$ целиком не содержится ни в одном из пяти указанных классов. Выберем из $\mathfrak{P}$ функции f_0, f_1, f_s, f_m, f_l, которые не принадлежат соответственно классам T_0, T_1, S, M и L. Быть может, не все из выбранных функций различны.

I. Построим при помощи функций f_0, f_1 и f_s константы 0 и 1.

Возьмём функцию $f_0 \notin T_0$. Возможны два случая:

1. $f_0(1,\dots,1) = 1$. Тогда $\varphi(x) = f_0(x,\dots,x) = 1$, так как $\varphi(0) = f_0(0,\dots,0) = 1$, $\varphi(1) = f_0(1,\dots,1) = 1$. Вторая константа получается из $f_1 : f_1(1,\dots,1) = 0$.

2. $f_0(1,\dots,1) = 0$. Тогда $\varphi(x) = f_0(x,\dots,x) = \overline{x}$, так как $\varphi(0) = f_0(0,\dots,0) = 1$, $\varphi(1) = f_0(1,\dots,1) = 0$. Располагая $\overline{x}$ и f_s, по лемме 1 получаем константу. Располагая $\overline{x}$, находим вторую константу.

II. При помощи констант 0 и 1 и функции f_m по лемме 2 находим $\overline{x}$.

III. При помощи констант 0 и 1 и функций $\overline{x}$ и f_l по лемме 3 находим $x_1\&x_2$.

Таким образом, P_2-полная система, состоящая из отрицания $\overline{x}$ и конъюнкции $x_1\&x_2$, реализуется формулами над $\mathfrak{P}$. Достаточность доказана.

Следствие. Всякий замкнутый класс функций из P_2, отличный от P_2, содержится в одном из пяти построенных классов.

Определение. Класс $\mathfrak{N}$ функций из P_2 называется предполным (или максимальным), если $[\mathfrak{N}] \neq P_2$, и для любой функции $f \in P_2$ такой, что $f \notin \mathfrak{N}$, класс $[\mathfrak{N} \bigcup \{f\}]$ P_2-полный.

Из определения вытекает, что предполный класс является замкнутым.

Следствие. В алгебре логики существует ровно пять предполных классов, а именно классы $T_0,\ T_1,\ S,\ M$ и L.

Пример. Покажем, что система из четырех функций

$$f_1 = x_1x_2,\ f_2 = 0,\ f_3 = 1,\ f_4 = x_1 + x_2 + x_3$$

является базисом в P_2.

Имеем: $f_1 \notin L,\ f_2 \notin T_1,\ f_2 \notin S,\ f_3 \notin T_0, f_4 \notin M$. Значит, указанная система P_2-полная, так как не содержится целиком ни в одном из предполных классов. С другой стороны, удаление любой из функций приводит к неполной системе: $\{f_1,\ f_2,\ f_3\} \subset M$, $\{f_1,\ f_2,\ f_4\} \subset T_0$, $\{f_1,\ f_3,\ f_4\} \subset T_1$, $\{f_2,\ f_3,\ f_4\} \subset L$.

Теорема. *Из всякой P_2-полной системы функций $\mathfrak{P}$ можно выделить полную подсистему, содержащую не более четырех функций.*

Доказательство. При доказательстве теоремы о функциональной полноте функция $f_0 \notin T_0$ либо не самодвойственна (случай 1), либо не сохраняет 1 и не монотонна (случай 2). Поэтому P_2-полной будет либо система $\{f_0,\ f_1,\ f_m,\ f_l\}$, либо система $\{f_0,\ f_s,\ f_l\}$. Указанный выше пример показывает, что константа 4 не может быть понижена.

Упражнение. Приведите пример базиса в P_2, состоящего из трёх функций.

Замечание. Теорема о функциональной полноте позволяет в сочетании с разложением в д. н. ф. или к. н. ф. найти для произвольной булевой функции f формулу над P_2-полной системой $\mathfrak{P}$.

Аналогично P_2 можно рассматривать функции алгебры k-значной логики P_k. Имеют место следующие теоремы.

Теорема Поста. *Каждый замкнутый класс из P_2 имеет конечный базис. Мощность множества замкнутых классов в P_2 счетная.*

Теорема Янова. *Для любого $k > 2$ существует в P_k замкнутый класс, не имеющий базиса.*

Теорема Мучника. *Для любого $k > 2$ существует в P_k замкнутый класс со счетным базисом.*

Теорема. *Для любого $k > 2$ P_k содержит континуум различных замкнутых классов.*

Теорема. *Система полиномов по модулю k полна в P_k тогда и только тогда, когда $k = p$,* где *p – простое число. Система полиномов над соответствующим полем Галуа полна в P_k тогда и только тогда, когда $k = p^m$.*

ГЛАВА 4

ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ КИБЕРНЕТИКИ

§ 16. Схемы из функциональных элементов. Метод Лупанова

В математической кибернетике базисом в P_2 принято называть произвольную конечную P_2-полную систему. Такой, например, является система $Б_1 = \{\&,\ \vee,\ +,\ -\}$. Каждая функция базиса реализуется в технике функциональным элементом (Ф.Э.). Для указанного базиса это будут двухвходовые булевы элементы: соответственно конъюнктор, дизъюнктор и сумматор, и одновходовый булев элемент инвертор, который можно рассматривать как двухвходовый элемент с одним существенным и одним несущественным входом. На вход элемента поступают значения аргументов соответствующей булевой функции базиса, а на единственном выходе генерируется значение этой функции. В технике функциональные элементы не равноценны, например, по времени срабатывания, в связи с этим в математической модели им приписываются веса. В нашей математической модели будем считать элементы равноценными, а вес каждого элемента равным 1. Из функциональных элементов строятся схемы.

Формально логической схемой из функциональных элементов (СФЭ) называется ориентированная бесконтурная сеть с помеченными вершинами (то есть ориентированный граф без ориентированных циклов с выделенными вершинами, называемыми полюсами, и, кроме того, каждая вершина ещё помечена). Полюса сети делятся на входные (входы) и выходные (выходы). Входные полюса являются упорядоченными и помечаются символами переменных. Выходные полюса помечаются звездочками. На каждом

выходном полюсе реализуется та или иная булева функция, аргументы которой суть переменные, символами которых помечены входные полюса. Каждая внутренняя вершина (вершина, отличная от входа) помечается функциональным символом или символом логической связки, обозначающими функциональный элемент, расположенный в этой вершине. Непременно выполняются следующие условия: 1) полустепень захода каждого входного полюса равна нулю и 2) полустепень захода каждой внутренней вершины равна числу мест функционального символа или логической связки, которым эта вершина помечена.

Рассмотрим, например, функции $f_1 = x + y + z$ и $f_2 = xy + (x + y)z$. Эти функции реализуются в базисе $Б_1$ при помощи следующей схемы $\sum$:

Схема $\sum$ имеет три упорядоченных входа, помеченные x, y и z, два выхода, помеченные звездочками, на которых реализуются функции f_1 и f_2. Входы и выходы являются полюсами сети и обозначены кружочками. Помеченные вершины ориентированной сети схематично изображены квадратиками, внутри которых указаны символы логических связок. Часто вместо квадратиков изображают треугольники. Ориентация рёбер (проводов) показана стрелочками. Следует

иметь в виду, что рёбра не пересекаются. Двигаясь сверху вниз от входов к выходам в направлениях, указанных стрелочками, нетрудно понять, как работает схема, то есть каким образом реализуются функции f_1 и f_2.

Сложностью СФЭ в базисе Б называется количество функциональных элементов в схеме. Глубиной СФЭ в базисе Б называется максимальное число внутренних вершин (функциональных элементов) в ориентированных цепях, соединяющих входы схемы с выходами.

В нашем примере сложность $L_{\text{Б}_1}(\sum)$ схемы $\sum$ в базисе Б_1 равна 5, а глубина $D_{\text{Б}_1}(\sum)$ схемы $\sum$ в базисе Б_1 равна 3.

Глубина схемы пропорциональна времени её работы, а сложность – объёму или площади схемы, реализованной на производстве. Важной для производства задачей математической кибернетики является оптимизация (уменьшение) сложности и глубины СФЭ, реализующих заданные функции.

Рассмотрим задачу синтеза СФЭ, реализующих булевы функции от n переменных в базисе $\text{Б}_0 = \{\&,\ \vee,\ -\}$. Требуется реализовать все булевы функции от n переменных.

Обозначим $L(f)$ минимальную сложность СФЭ, реализующей функцию $f \in P_2^{(n)}$ в указанном базисе, а $L_A(f)$ – минимальную сложность СФЭ, реализующей функцию $f \in P_2^{(n)}$ при помощи алгоритма A. Такие схемы существуют, так как вообще число схем сложности не больше некоторого h конечно. В качестве h можно взять, например, сложность совершенной д. н. ф. для функции f. Перебрав все схемы сложности не более h, можно найти минимальную схему и минимальную схему для алгоритма A.

Функции $L(n) = \max\{L(f) : f \in P_2^{(n)}\}$ и $L_A(n) = \max\{L_A(f) : f \in P_2^{(n)}\}$ называются функциями Шеннона. Очевидно, $L(n) \leqslant L_A(n)$. Чем ближе $L_A(n)$ к $L(n)$ и чем дальше $L_A(n)$ от сложности алгоритма полного перебора, тем лучше (эффективнее, качественнее) алгоритм A.

Лемма. *Обозначим $S(n,h)$ число СФЭ в базисе Б_0 с n входами и одним выходом, содержащих не более h элементов. Тогда при $h > n$ справедливо неравенство $S(n,h) < (ch)^h$, где c – некоторая постоянная.*

Доказательство. Число СФЭ в базисе Б_0 с n входами и одним выходом, содержащих ровно h элементов,– $S_0(n,h) \leqslant \frac{1}{h!}3^h(n+h)^{2h+1}$. В самом деле, на каждое из h занумерованных мест элемент можно выбрать из базисных элементов тремя способами. Каждый из его входов подключается либо ко входу схемы, либо к выходу элемента. Всего для элемента имеется, таким образом, не более $3(n+h)^2$ возможностей, а для h элементов – не более $3^h(n+h)^{2h}$ возможностей. Единственный выход схемы подключается либо ко входу схемы, либо к выходу элемента. Всего для выхода имеется не более $(n+h)$ возможностей. Учитывая, что изменение нумерации мест не влияет на схему, а возможностей изменения нумерации $h!$, получаем указанную верхнюю оценку для $S_0(n,h)$. Очевидно, $S_0(n,h)$ растёт при фиксированном n с ростом h. При $h > n$ имеем

$$S(n,h) = \sum_{k=0}^{h} S_0(n,k) \leqslant \sum_{k=0}^{h} \frac{1}{k!}3^k(n+k)^{2k+1} \leqslant$$

$$\leqslant (h+1)\frac{1}{h!}3^h(n+h)^{2h+1} \leqslant \frac{1}{h!}3^h(n+h)^{2h+2} <$$

$$< \frac{3^h(2h)^{2h+2}}{(h/e)^h} = 4h^2(12e)^h h^h < (ch)^h,$$

где c – некоторая постоянная. Лемма доказана.

Теорема. *При всех достаточно больших n справедливо неравенство*

$$L(n) > \frac{2^n}{n}.$$

Доказательство. Положим $h = [2^n/n]$. Согласно лемме $S(n,h) \leqslant \left(c\frac{2^n}{n}\right)^{2^n/n}$. Условие $h > n$ выполняется для всех $n \geqslant 5$. Значит, схемами сложности не больше h может быть реализовано не более $\left(c\frac{2^n}{n}\right)^{2^n/n}$ булевых функций от n

переменных, а всего таких функций 2^{2^n}. Так как

$$\log_2 \frac{\left(c\frac{2^n}{n}\right)^{2^n/n}}{2^{2^n}} = \frac{2^n}{n}(\log_2 c + n - \log_2 n) - 2^n =$$

$$= \frac{2^n}{n}(\log_2 c - \log_2 n) \to -\infty$$

при $n \to \infty$, то при всех достаточно больших n числитель меньше знаменателя. Значит, схем сложности не более h не хватает для реализации всех булевых функций от n переменных, и найдутся функции от n переменных, которые не могут быть реализованы со сложностью меньше или равной $h = [2^n/n]$, то есть при всех достаточно больших n справедливо неравенство $L(n) > \frac{2^n}{n}$. Теорема доказана.

Следствие. Доля функций, для которых $L(n) > \frac{2^n}{n}$, стремится к 1 при $n \to \infty$.

Лемма. *В базисе $Б_0$ при каждом натуральном n сложность реализации множества всех конъюнктов $\{x_1^{\sigma_1} \,\&\, x_2^{\sigma_2} \,\&\, \ldots \,\&\, x_n^{\sigma_n}\}$ не превосходит $n2^n$.*

Доказательство. Всего конъюнктов 2^n, так как каждая компонента вида x^σ входит в конъюнкт либо с навешенным отрицанием при $\sigma = 0$, либо без отрицания при $\sigma = 1$. Отрицания переменных реализуются в схеме в самом начале раз навсегда, что требует n инверторов. Далее для реализации каждого конъюнкта требуется $(n-1)$ конъюнкций. Таким образом, сложность схемы не превосходит $n+2^n(n-1) \leqslant \leqslant n2^n$. Лемма доказана.

Теорема Лупанова. *Для СФЭ в базисе $Б_0$ можно построить асимптотически наилучший метод синтеза и*

$$L(n) \sim \frac{2^n}{n}.$$

Доказательство. Зададим булеву функцию $f(x_1, \ldots, x_n)$ при помощи следующей таблицы размера $2^k \times 2^{n-k}$.

$x_1 \ \ldots \ x_k$	$0 \ \ldots \ \sigma_{k+1} \ \ldots \ 1$ $\vdots \quad\quad \vdots \quad\quad \vdots$ $0 \ \ldots \ \sigma_n \ \ldots \ 1$	x_{k+1} $\vdots$ x_n
$0 \ \ldots \ 0$		ширина полосы́ $= s$
		по́лосы
$\sigma_1 \ \ldots \ \sigma_k$	$f(\sigma_1, \ldots, \sigma_n)$	ширина полосы́ $= s$
		по́лосы
$1 \ \ldots \ 1$		ширина полосы́ $= s' \leqslant s$

На пересечении строки с номером $(\sigma_1, \ldots, \sigma_k)$ и столбца с номером $(\sigma_{k+1}, \ldots, \sigma_n)$ находится значение $f(\sigma_1, \ldots, \sigma_n)$ функции $f(x_1, \ldots, x_n)$ на наборе значений аргументов $(\sigma_1, \ldots, \sigma_n)$. Столбец с номером $(\sigma_{k+1}, \ldots, \sigma_n)$ задаёт функцию $f(x_1, \ldots, x_k, \sigma_{k+1}, \ldots, \sigma_n)$, являющуюся компонентой разложения

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_{k+1}, \ldots, \sigma_n)} x_{k+1}^{\sigma_{k+1}} \ldots x_n^{\sigma_n} f(x_1, \ldots, x_k, \sigma_{k+1}, \ldots, \sigma_n). \tag{16.1}$$

Возьмём целое число s такое, что $1 < s < 2^k$, и разрежем таблицу на полосы ширины s. Последняя полоса имеет ширину $s' \leqslant s$. Занумеруем полосы сверху вниз числами $1, 2, \ldots, p$, где $p = \left\lceil \frac{2^k}{s} \right\rceil$, и рассмотрим полосу с номером i :

		j	
$\sigma_1(1), \ \ldots, \ \sigma_k(1)$		γ_1	
		$\vdots$	
$\sigma_1(s), \ \ldots, \ \sigma_k(s)$		γ_s	

Эта полоса распадается на короткие столбцы высоты s, или s' для последней полосы. Всего существует 2^s различных видов столбцов высоты s. Занумеруем виды столбцов, встречающиеся в i-й полосе числами $1, 2, \ldots, t(i)$. Очевидно, $t(i) \leqslant 2^s$. Пусть $(\gamma_1, \ldots, \gamma_s)$ – столбец j-го вида в i-й полосе. Он определяет булеву функцию

$$f_{ij}(x_1, \ldots, x_k) =$$

$$= \begin{cases} \gamma_l, \text{ если } (\sigma_1, \ldots, \sigma_k) = (\sigma_1(l), \ldots, \sigma_k(l)), \ l = 1, \ldots, s, \\ 0, \text{ если } (\sigma_1, \ldots, \sigma_k) \text{ не принадлежит } i\text{-й полосе.} \end{cases}$$

Столбец с номером $\sigma_{k+1}, \ldots, \sigma_n$ разрезан полосами на p столбцов. Поэтому

$$f(x_1, \ldots, x_k, \sigma_{k+1}, \ldots, \sigma_n) = f_{1j_1}(x_1, \ldots, x_k) \vee \cdots \vee f_{pj_p}(x_1, \ldots, x_k), \tag{16.2}$$

где j_i – номер вида соответствующего короткого столбца из i-й полосы.

Перейдём к описанию схемы $\sum$, на выходе которой реализуется функция $f(x_1, \ldots, x_n)$. Эта схема получается в виде соединения отдельных блоков.

1. Блок A реализует все конъюнкции вида $x_1^{\sigma_1} \ldots x_k^{\sigma_k}$. Сложность этого блока согласно лемме $L(A) \leqslant k2^k$.

2. Блок B реализует все конъюнкции вида $x_{k+1}^{\sigma_{k+1}} \ldots x_n^{\sigma_n}$. Сложность этого блока согласно лемме $L(B) \leqslant (n-k)2^{n-k} \leqslant$ $\leqslant n2^{n-k}$.

3. Блок C реализует по совершенной д. н. ф. функции $f_{ij}(x_1, \ldots, x_k)$. Так как все конъюнкции $\{x_1^{\sigma_1} \ldots x_k^{\sigma_k}\}$ реализованы в блоке A, то для реализации каждой функции осталось взять не более $(s-1)$ дизъюнкций, поскольку столбец в полосе имеет высоту не более s. Таким образом, блок C имеет оценку сложности $L(C) \leqslant (s-1)(t(1) + \cdots + t(p)) < sp2^s$.

4. Блок D реализует функции $f(x_1, \ldots, x_k, \sigma_{k+1}, \ldots, \sigma_n)$ по формуле (16.2). Всего имеется 2^{n-k} таких функций – столько, сколько наборов $(\sigma_{k+1}, \ldots, \sigma_n)$. Для синтеза каждой функции требуется $(p-1)$ дизъюнкций. Таким образом, блок D имеет оценку сложности $L(D) \leqslant (p-1)2^{n-k} < p2^{n-k}$.

5. Блок F реализует функцию $f(x_1, \ldots, x_n)$ по формуле (16.1). Формула (16.1) содержит 2^{n-k} дизъюнктов (слагаемых). Все конъюнкции $\{x_{k+1}^{\sigma_{k+1}} \ldots x_n^{\sigma_n}\}$ реализованы в блоке B. Для каждого слагаемого требуется одно умножение между конъюнктом $x_{k+1}^{\sigma_{k+1}} \ldots x_n^{\sigma_n}$ и функцией $f(x_1, \ldots, x_k, \sigma_{k+1}, \ldots, \sigma_n)$. Кроме того, требуется $(2^{n-k} - 1)$ дизъюнкций между слагаемыми. Таким образом, сложность блока $L(F) \leqslant 2^{n-k} + 2^{n-k} - 1 < 2 \cdot 2^{n-k}$.

Суммируя полученные оценки, находим

$$L(\Sigma) = L(A) + L(B) + L(C) + L(D) + L(F) \leqslant$$

$$\leqslant k2^k + n2^{n-k} + sp2^s + p2^{n-k} + 2 \cdot 2^{n-k} \leqslant$$
$$\leqslant k2^k + (n+2)2^{n-k} + (sp2^s + p2^{n-k}) \leqslant$$
$$\leqslant k2^k + (n+3)2^{n-k} + 2^{k+s+1} + \frac{2^n}{s},$$

так как $p = \left\lceil \frac{2^k}{s} \right\rceil$, $1 < s < p \leqslant 2^k$, и, таким образом, $p \leqslant \frac{2^k}{s} +$ $+ 1$, $sp \leqslant 2^k + s \leqslant 2^{k+1}$.

Положим[5]

$$k = [3\log_2 n],\ s = [n - 5\log_2 n].$$

Тогда

$$L(\Sigma) \leqslant (3\log_2 n)n^3 + (n+3)\frac{2^n}{2^{3\log_2 n - 1}} + 2^{3\log_2 n + n - 5\log_2 n + 1} +$$

$$+\frac{2^n}{n - 5\log_2 n - 1} = 3n^3\log_2 n + \frac{2(n+3)2^n}{n^3} + \frac{n^3 2^{n+1}}{n^5} +$$

$$+\frac{2^n}{n - 5\log_2 n - 1} =$$

$$= \frac{2^n}{n}\left(\left(\frac{3n^4\log_2 n}{2^n} + \frac{2(n+3)}{n^2} + \frac{2}{n}\right) + \frac{n}{n - 5\log_2 n - 1}\right) =$$

$$= \frac{2^n}{n}(1 + o(1)),\ n \to \infty,\ o(1) > 0.$$

Итак, $\forall\ f \in P_2^{(n)} \to L(f) \leqslant L_A(f) \leqslant \frac{2^n}{n}(1 + o(1)),\ n \to \infty.$ Следовательно,

$$L(n) = \max_{f \in P_2^{(n)}} L(f) \leqslant \frac{2^n}{n}(1 + o(1)).$$

Учитывая нижнюю оценку для $L(n)$, находим

$$\frac{2^n}{n} < L(n) \leqslant \frac{2^n}{n}(1 + o(1)),\ 1 < \frac{L(n)}{\frac{2^n}{n}} \leqslant (1 + o(1)).$$

Значит,

$$\exists \lim_{n\to\infty} \frac{L(n)}{\frac{2^n}{n}} = 1$$

и

$$L(n) \sim \frac{2^n}{n}.$$

Теорема доказана.

[5] $[x]$ – целая часть числа x – наибольшее целое число, не превосходящее x. Для каждого $x \in \mathbb{R}$ имеют место неравенства $[x] \leqslant x < x + 1$. В дискретной математике используются также следующие обозначения, называемые гауссовыми скобками: $\lfloor x \rfloor$ и $\lceil x \rceil$, причём $\lfloor x \rfloor = [x]$ – целая часть снизу, а $\lceil x \rceil$ – наименьшее целое число, не меньшее x, – целая часть сверху.

§ 17. Методы Карацубы и Тоома

Сумматор. Два n-разрядных двоичных целых неотрицательных числа $x = (x_n...x_1)_2$ и $y = (y_n...y_1)_2$ будем складывать столбиком:

$$\begin{array}{r} q_{n+1}q_n...q_1 \\ x_n...x_1 \\ + \quad y_n...y_1 \\ \hline z_{n+1}z_n...z_1 \end{array}$$

Числа $q_1, \ldots, q_{n+1}$ есть результаты переносов.

Очевидно, что

$$\begin{cases} q_1 = 0, \\ z_i = x_i + y_i + q_i \pmod 2, \\ q_{i+1} = x_i y_i + (x_i + y_i)q_i \pmod 2, \\ z_{n+1} = q_{n+1}, \end{cases} \quad i = 1, 2,\ \ldots, n. \quad (17.3)$$

Обозначим через B_i следующую схему:

Искомая схема $\sum_n$ получается путём последовательного соединения блоков $B_i,\ i = 1, ..., n$.

Блок B_1 осуществляет преобразование $z_1 = x_1 + y_1 \pmod 2$, $q_2 = x_1 y_1$. Таким образом, сложность СФЭ-сумматора $L\left(\sum_n\right) \leqslant 5n - 3$.

Мультипликатор. Два n-разрядных двоичных целых неотрицательных числа $x = (x_n ... x_1)_2$ и $y = (y_n ... y_1)_2$ умножим школьным методом. Пример:

$$\begin{array}{r} \times\ 11 \\ \quad\ 11 \\ \hline \quad\ 11 \\ +\ 110 \\ \hline 1001 \end{array}$$

Умножение $x_i y_i$ осуществляет одна конъюнкция &. Таким образом, требуется n^2 коньюнкций, и на каждом шаге, как видно из примера, складываются два n-разрядных двоичных числа. Всего $(n-1)$ шагов. Значит, сложность мультипликатора

$$L\left(M_n\right) \leqslant n^2 + (5n-3)(n-1) = 6n^2 - 8n + 3,\ n \geqslant 1.$$

Заметим, что при $n \geqslant 2$ можно считать $L\left(M_n\right) \leqslant 6n^2 - 8n$, учитывая ноль при первом сложении.

Инвертор двоичному числу $x = (x_n ... x_1)_2$ ставит в соответствие двоичное число $\overline{x} = (\overline{x}_n ... \overline{x}_1)_2 = e_n - x$, где $e_n = 2^n - 1 = (\underbrace{1...1}_{n \text{ раз}})_2$. Сложность инвертора $L(I_n) = n$.

Схема разности $\overline{D}_n$ вычисляет разность $z - y$ двух n-разрядных целых неотрицательных двоичных чисел z и y.

Пусть $z \geqslant y,\ z = x + y$. Так как $z_i = x_i + y_i + q_i \pmod 2$, то

$$x_i = z_i + y_i + q_i \pmod 2;$$
$$q_{i+1} = x_i y_i + (x_i + y_i) q_i = (z_i + y_i + q_i) y_i + (z_i + q_i) q_i =$$
$$= (z_i + q_i)(y_i + q_i) + y_i \pmod 2.$$

Итак,

$$\begin{cases} q_1 = 0, \\ x_i = (z_i + q_i) + y_i \pmod 2, & i = 1,\ ..., n. \\ q_{i+1} = (z_i + q_i)(y_i + q_i) + y_i \pmod 2, \end{cases} \quad (17.4)$$

Обозначим через D_i следующую схему:

Схема $\overline{D}_n$, вычисляющая $x = z - y$, получается путём последовательного соединения блоков $D_i,\ i = 1,\ \ldots, n$.

Блок D_1 осуществляет преобразование:

$$x_1 = z_1 + y_1 \pmod 2,\ q_2 = z_1 y_1 + y_1 \pmod 2.$$

Таким образом, сложность схемы $D_n,\ L(\overline{D}_n) \leqslant 5n - 2$.

Замечание. Обычно в технике используется базис из всех булевых функций двух переменных. Тогда вычисление $q_2 = z_1 y_1 + y_1 \pmod 2 = y_1 \overline{z}_1$ требует одного функционального элемента и сложность схемы $\overline{D}_n$, $L(\overline{D}_n) \leqslant 5n - 3$, оказывается такая же, как у сумматора. Отметим, что сложение или вычитание целых чисел схемно выполняются с линейной сложностью, а умножение предложенным методом (столбиком) – с нелинейной, а именно с квадратичной сложностью.

Метод Карацубы. Для умножения столбиком двух n-разрядных натуральных чисел, представленных в позиционной двоичной системе счисления, требуется приблизительно Cn^2 алгебраических операций умножения и сложения, где C – некоторая постоянная. Назовём этот способ школьным (или традиционным) методом. Метод Карацубы, начиная с некоторого n, позволяет умножать быстрее.

Суть метода Карацубы состоит в следующем. Пусть u и v – два $2n$-разрядных двоичных натуральных числа:

$u = (u_{2n-1}...u_1u_0)_2,\ v = (v_{2n-1}...v_1v_0)_2,\ u_i, v_j \in \{0,1\},\ i,j = 0,1,\ \ldots, 2n-1;$

$$u = \sum_{j=0}^{2n-1} u_j 2^j,\ v = \sum_{i=0}^{2n-1} v_i 2^i,$$

и пусть

$$U_1 = (u_{2n-1}...u_n)_2,\ V_1 = (v_{2n-1}...v_n)_2,$$
$$U_0 = (u_{n-1}...u_0)_2,\ V_0 = (v_{n-1}...v_0)_2,$$
$$U_2 = (U_1 - U_0),\ V_2 = (V_0 - V_1).$$

Тогда

$$u = 2^n U_1 + U_0,\ v = 2^n V_1 + V_0, \tag{17.5}$$
$$uv = 2^{2n}U_1V_1 + 2^n(U_1V_1 + U_2V_2 + U_0V_0) + U_0V_0. \tag{17.6}$$

Для доказательства (17.6) достаточно умножить u и v в (17.5), раскрыть скобки в (17.6) и сравнить получившиеся выражения. Таким образом, метод Карацубы сводит умножение двух $2n$-разрядных натуральных двоичных чисел к умножению трёх n-разрядных: U_0V_0, U_1V_1, U_2V_2, плюс некоторым простым операциям сложения, вычитания и «сдвига», схемно реализуемого с нулевой сложностью, и, начиная с некоторого n, оказывается проще школьного метода (то есть имеющим ме́ньшую сложность).

Рассмотрим реализацию метода Карацубы и школьного метода схемами из функциональных элементов (СФЭ) в базисе $\{\neg,\ \&,\ \vee,\ \oplus,\ 0,\ 1\}$. Обозначим $T(n)$ число элементов (сложность) СФЭ, реализующей умножение двух n-разрядных двоичных чисел. Из (17.6) следует, что

$$T(2n) \leqslant 3T(n) + Cn, \tag{17.7}$$

где C – некоторая постоянная.

Пусть $n = 2^s,\ s \in \mathbb{N}$. Из (17.7) мы имеем

1) $T(n) \leqslant 3T\left(\frac{n}{2}\right) + C\frac{n}{2}$,
$T\left(\frac{n}{2}\right) \leqslant 3T\left(\frac{n}{2^2}\right) + C\frac{n}{2^2}$,
2) $T(n) \leqslant 3^2T\left(\frac{n}{2^2}\right) + Cn\left(\frac{1}{2} + \frac{3}{2^2}\right)$,
. . . . . .
$k)$ $T(n) \leqslant 3^kT\left(\frac{n}{2^k}\right) + Cn\left(\frac{1}{2} + \frac{3}{2^2} + \cdots + \frac{3^{k-1}}{2^k}\right)$,
$T(n) \leqslant 3^kT\left(\frac{n}{2^k}\right) + Cn\left(\left(\frac{3}{2}\right)^k - 1\right)$,

$$T(n) \leqslant 3^kT\left(\frac{n}{2^k}\right) + Cn\left(\frac{3}{2}\right)^k. \tag{17.8}$$

При $k = s,\ n = 2^k,\ k = \log_2 n$ из (17.8) получается

$$T(n) \leqslant 3^k + Cn\left(\tfrac{3}{2}\right)^k,$$
$$T(n) \leqslant 3^k + C3^k,$$
$$T(n) \leqslant (C+1)3^k,$$
$$T(n) \leqslant (C+1)3^{\log_2 n},$$
$$T(n) \leqslant (C+1)n^{\log_2 3}. \tag{17.9}$$

В общем случае

$$T(n) = T\left(2^{\log_2 n}\right) \leqslant T\left(2^{\lceil \log_2 n \rceil}\right) \leqslant (C+1)3^{\lceil \log_2 n \rceil} \leqslant$$
$$\leqslant (C+1)3^{\log_2 n + 1} = 3(C+1)n^{\log_2 3}.$$

Таким образом, $T(n) = O(n^{\log_2 3})$ или, для некоторой константы C,

$$T(n) \leqslant Cn^{\log_2 3} \leqslant Cn^{1{,}586}. \tag{17.10}$$

Мы видим, что при больших n рекурсивный метод Карацубы эффективнее традиционного школьного метода умножения целых чисел.

Метод Тоома. Метод Карацубы является частным случаем при $r = 1$ более общего метода Тоома, который для произвольного фиксированного r даёт

$$T((r+1)n) \leqslant (2r+1)T(n) + Cn. \tag{17.11}$$

Этот более общий метод можно получить следующим образом. Разобьём

$$u = \left(u_{(r+1)n-1} \dots u_1 u_0\right)_2 \qquad \text{и} \qquad v = \left(v_{(r+1)n-1} \dots v_1 v_0\right)_2$$

на $r+1$ частей:

$$u = U_r 2^{rn} + \dots + U_1 2^n + U_0, \qquad v = V_r 2^{rn} + \dots + V_1 2^n + V_0,$$

где каждое U_j и каждое V_i является n-битовым числом. Рассмотрим полиномы

$$U(x) = U_r x^r + \dots + U_1 x + U_0, \qquad V(x) = V_r x^r + \dots + V_1 x + V_0$$

и положим

$$W(x) = U(x)V(x) = W_{2r} x^{2r} + \dots + W_1 x + W_0.$$

Так как $u = U(2^n)$ и $v = V(2^n)$, получаем $uv = W(2^n)$, поэтому при известных коэффициентах W_k в $W(x)$ можно легко найти uv. Задача заключается в поиске хорошего способа вычисления коэффициентов в $W(x)$, требующего только $2r+1$ умножений n-битовых чисел и несколько последующих операций, время выполнения которых пропорционально n. Это может быть достигнуто посредством вычисления

$$U(0)V(0) = W(0),\ U(1)V(1) = W(1),\ \dots,\ U(2r)V(2r) = W(2r).$$

Коэффициенты полинома степени $2r$ могут быть выражены в виде линейной комбинации значений этого полинома в $2r + 1$ различных точках. Время, необходимое для выполнения этой операции, пропорционально n. В действительности произведения $U(j)V(j)$ не являются произведениями строго n-битовых чисел, но являются произведениями $(n+t)$-битовых чисел, где t есть фиксированное значение, зависящее от r. Схема умножения $(n+t)$-битовых чисел строится легко. Для неё требуется лишь $T(n) + C_1 n$ операций (функциональных элементов), где $T(n)$ – количество операций, необходимое для умножения n-разрядов, так как при фиксированном t два произведения t и n-битовых чисел можно получить за $C_2 n$ операций.

Рассуждая так же, как при выводе неравенств (17.9) и (17.10) и учитывая неравенство (17.11), приходим к неравенствам

$$T(n) \leqslant C n^{\log_{r+1}(2r+1)} < C n^{1+\log_{r+1} 2}.$$

Так как $\varepsilon = \log_{r+1} 2 \to 0$ при $r \to \infty$, то доказана

Теорема о умножении целых чисел с почти линейной сложностью. *Для любого $\varepsilon > 0$ существуют такая постоянная $C(\varepsilon)$ и такой алгоритм умножения, что число элементарных операций $T(n)$, которое необходимо выполнить, чтобы умножить два n-битовых числа, удовлетворяет оценке*

$$T(n) \leqslant C(\varepsilon) n^{1+\varepsilon}.$$

Вопрос о том, можно ли умножить два n-битовых числа с линейной сложностью, до сих пор не решен в математике: никто не доказал и не опроверг гипотезу, что нельзя. Пока не доказана принципиальная разница умножения и сложения в контексте сложности этих операций.

§ 18. Оптимизация метода Карацубы

Улучшим метод Карацубы следующим образом. Из (17.6) следует, что

$$T(2n) \leqslant 3T(n) + Cn + C'. \tag{18.12}$$

Оценим константы C и C'.

Схема разности D_n вычисляет модуль разности $|z-y|$ двух n-разрядных натуральных двоичных чисел z и y и знак разности

$$\operatorname{sign}(z-y) = \begin{cases} 0, z \geqslant y, \\ 1, z < y. \end{cases}$$

Если в схеме разности $\overline{D}_n$, рассмотренной выше, $z \geqslant y$, то $s = q_{n+1} = \operatorname{sign}(z-y) = 0,\ (x_n \dots x_1)_2 = x = |x| \geqslant 0$. В случае

$z < y,\ s = \operatorname{sign}(z-y) = 1,\ x = (x_n \dots x_1)_2 - 2^n < 0,\ |x| = -x = 2^n - (x_n \dots x_1)_2 = ((2^n - 1) - (x_n \dots x_1)_2) + 1 = (e_n - (x_n \dots x_1)_2) + 1 = (\overline{x}_n \dots \overline{x}_1)_2 + 1 > 0.$

Таким образом, всегда $s = \operatorname{sign}(z-y),\ |z-y| = (x_n \oplus s,\ \dots, x_1 \oplus s)_2 + s.$

Блок C осуществляет преобразование

$$\hat{x}_1 = \tilde{x}_1 \oplus s, \dots, \hat{x}_n = \tilde{x}_n \oplus s,$$

где $s = \operatorname{sign}(z-y)$, со сложностью n.

Блок $\sum$ осуществляет преобразование

$$(x_n, \dots, x_1)_2 = (\hat{x}_n, \dots, \hat{x}_1)_2 + s$$

со сложностью $(2n-1)$, как это следует из формул (17.4), учитывая, что $q_{n+1} = 0$. Видно, что

$$x = (x_n ... x_1)_2 = |z-y|,\ \operatorname{sign}(z-y) = s.$$

Сложность схемы D_n :

$$L(D_n) \leqslant L(\overline{D}_n) + L(C) + L\left(\sum\right) \leqslant (5n-2) + n + (2n-1) = 8n-3.$$

Таким образом, сложность вычисления $U_2 = (U_1 - U_0), V_2 = (V_0 - V_1)$ и знака $\operatorname{sign}(U_2 V_2) = \operatorname{sign}(U_2) \oplus \operatorname{sign}(V_2)$

$$L_0 \leqslant 2(8n-3) + 1 = 16n - 5.$$

Схема разности D_n :

Пусть $U_1 V_1,\ U_0 V_0$ и $|U_2| \cdot |V_2|$ уже вычислены со сложностью $3T(n) + L_0,\ L_0 \leqslant 16n - 5$, и представляют собой $2n$-разрядные двоичные числа. Потребуется синтезировать $t = x + y$, где $x,\ x+y,$ – $(2n+1)$-разрядные, а y – $(2n)$-разрядное двоичные натуральные числа, причем $x \geqslant 0$, а y может быть меньше нуля. Это делается с помощью следующей **схемы** A:

Здесь $s = \operatorname{sign}(y),\ x = (x_{2n+1} \dots x_1)_2,\ y = (y_{2n} \dots y_1)_2.$

Блок C_1 вычисляет $\tilde{x}_1 = x_1 \oplus s,\ \dots, \tilde{x}_{2n+1} = x_{2n+1} \oplus s.$

Блок $\sum_{2n}$ складывает столбиком $(\tilde{x}_{2n+1},\ \dots, \tilde{x}_1)_2$ и $(y_{2n},\ \dots, y_1)_2$.

Блок C_2 вычисляет $t = (t_{2n+1} \dots t_1)_2$, где $t_1 = z_1 \oplus s,\ \dots, t_{2n+1} = z_{2n+1} \oplus s.$

Таким образом, если $s = 0$, вычисляется $t = x + y$, а если $s = 1$, вычисляется $t = \overline{\overline{x} + y} = e_n - ((e_n - x) - y) = x - y$.

Сложность схемы A:

$$L(A) \leqslant L(C_1) + L\left(\sum_{2n}\right) + L(C_2) \leqslant$$

$$\leqslant (2n+1) + (5 \cdot 2n - 3 + 1) + (2n+1) = 14n.$$

Мы учли «разрядность» (число бит) x, y и t.

Заметим, что

$$U_1V_1 + U_2V_2 + U_0V_0 = U_1V_1 + (U_1 - U_0)(V_0 - V_1) + U_0V_0 =$$

$$= U_1V_0 + U_0V_1 \geqslant 0.$$

Сумма $U_1V_1 + U_0V_0$ вычисляется со сложностью, не превосходящей $5{\cdot}2n{-}3 = 10n{-}3$, получается $(2n{+}1)$-разрядное число. Далее вычисляется $(U_1V_1 + U_0V_0) + U_2V_2$ по схеме A. Таким образом, $S_0 = 2^n(U_1V_1 + U_2V_2 + U_0V_0)$ вычисляется со сложностью

$$L(S_0) \leqslant (10n - 3) + 14n = 24n - 3$$

в предположении, что соответствующие произведения уже вычислены. Очевидно, «сдвиг» – умножение на 2^n – не требует в СФЭ никаких затрат. Остаётся вычислить $S_0 + S_1$, где $S_1 = 2^{2n}U_1V_1 + U_0V_0$ вычисляется с нулевой сложностью, если произведения U_1V_1 и U_0V_0 уже вычислены. Число бит S_1, $R(S_1) = 4n$. Число бит S_0, $R(S_0) = 3n + 1$, причём в S_0 последние n знаков – нули. С учётом этого сложность соответствующего сумматора будет

$$L_1 \leqslant 5(2n + 1) - 3 + 2(n - 1) - 1 = 12n - 1.$$

Суммируя оценки сложности, находим

$$T(2n) \leqslant 3T(n) + L_0 + L(S_0) + L_1 \leqslant$$

$$\leqslant 3T(n) + (16n - 5) + (24n - 3) + (12n - 1) = 3T(n) + 52n - 9.$$

Итак,

$$T(2n) \leqslant 3T(n) + 52n - 9. \qquad (18.13)$$

Соотношение (18.13) позволяет найти чётные значения n, при которых хотя бы один ход рекурсивного метода Карацубы с последующим переходом в вычислениях на школьный метод оказывается проще непосредственного применения школьного метода. Эти значения $n = 2k,\ k \in \mathbb{N}$, следуют из решения неравенства

$$6 \cdot (2k)^2 - 8 \cdot (2k) \geqslant 3 \cdot (6k^2 - 8k) + 52k - 9.$$

Мы видим, что при всех чётных $n \geqslant 16$ метод Карацубы лучше школьного метода. Покажем, что это справедливо и для всех нечётных $n \geqslant 16$.

Пусть u и v – $(n + q)$-разрядные двоичные натуральные числа, причём $n \geqslant q \geqslant 0$. Представим u и v в виде

$$u = 2^qU_1 + U_0,\ v = 2^qV_1 + V_0, \qquad (18.14)$$

где U_0, V_0 – q-разрядные двоичные натуральные числа, а U_1, V_1 – n-разрядные двоичные натуральные числа. Аналогично (17.6) имеем

$$uv = 2^{2q}U_1V_1 + 2^q(U_1V_1 + V_2U_2 + U_0V_0) + U_0V_0, \qquad (18.15)$$

где $U_2 = (U_1{-}U_0)$, $V_2 = (V_0{-}V_1)$. Аналогично (18.13) получаем соотношение

$$T(n + q) \leqslant 2T(n) + T(q) + 40n + 12q - 9. \qquad (18.16)$$

При $n = q$ это соотношение совпадает с (18.13). Согласно 18.16 имеем

$$T(2k + 1) \leqslant 2T(k + 1) + T(k) + 40(k + 1) + 12k - 9. \qquad (18.17)$$

Соотношение (18.17) позволяет найти нечётные значения n, при которых хотя бы один ход рекурсивного метода Карацубы с последующим переходом в вычислениях на школьный метод оказывается проще непосредственного применения школьного метода. Эти значения $n = 2k + 1,\ k \in \mathbb{N}$, следуют из решения неравенства

$$6{\cdot}(2k{+}1)^2{-}8{\cdot}(2k{+}1) \geqslant 2{\cdot}(6(k{+}1)^2{-}8(k{+}1)){+}6k^2{-}8k{+}52k{+}31.$$

Мы видим, что при всех нечётных $n \geqslant 17$ метод Карацубы лучше школьного метода. Таким образом, при всех натуральных $n \geqslant 16$ метод Карацубы лучше школьного метода.

Покажем, что в методе Карацубы наиболее эффективно производить разбиение m-битовых множителей примерно

пополам каждый множитель на каждом шаге рекурсии. Полагая $m = n + q$, перепишем соотношение 18.16 в виде

$$T(m) \leqslant f(x), \text{ где } f(x) = 2T(m-q)+T(q)+40(m-q)+12q-9. \tag{18.18}$$

Функция $T(x)$ представляется как

$$T(x) = Cx^{\alpha} + C_1 x + C_2,\ C > 0,\ \alpha > 1.$$

Её вторая производная

$$T''(x) = C\alpha(\alpha-1)x^{\alpha-2} > 0.$$

Следовательно её первая производная $T'(x)$ строго возрастает, и тогда

$$f'(q) = -2T'(m-q) + T'(q) - 28 < 0,$$

ведь $T'(m-q) \geqslant T'(q)$, так как $m - q \geqslant q$. Значит, f строго убывает, и для получения минимальной оценки сложности требуется взять $q = \frac{m}{2}$ при чётном m и $q = \lfloor \frac{m}{2} \rfloor$ при нечётном m, что и требовалось показать.

Для $n < 16$ школьный метод, по нашим оценкам, лучше метода Карацубы. Однако нижние оценки сложности метода Карацубы не найдены. Поэтому, улучшив верхние оценки сложности метода Карацубы, возможно, можно уменьшить те n, при которых метод Карацубы лучше традиционного школьного метода умножения двоичных натуральных чисел.

Оптимизация в случае $n = 2^s$.

Рассмотрим формулу (18.13). Пусть $n = 2^s,\ s \in \mathbb{N}$. Мы имеем

1) $T(n) \leqslant 3T\left(\frac{n}{2}\right) + 52\frac{n}{2} - 9,$
$T\left(\frac{n}{2}\right) \leqslant 3T\left(\frac{n}{2^2}\right) + 52\frac{n}{2^2} - 9,$

2) $T(n) \leqslant 3^2 T\left(\frac{n}{2^2}\right) + 52n\left(\frac{1}{2} + \frac{3}{2^2}\right) - 9(1+3),$

. . . . . .

$k)$ $T(n) \leqslant 3^k T\left(\frac{n}{2^k}\right) + 52n\left(\frac{1}{2} + \frac{3}{2^2} + \cdots + \frac{3^{k-1}}{2^k}\right) -$
$-9(1+3+\cdots+3^{k-1}),$
$T(n) \leqslant 3^k T\left(\frac{n}{2^k}\right) + 52n\left(\left(\frac{3}{2}\right)^k - 1\right) - 9\frac{3^k-1}{2},$

$$T(n) \leqslant 3^k T\left(\frac{n}{2^k}\right) + 52n\left(\frac{3}{2}\right)^k - 52n - 4{,}5 \cdot 3^k + 4{,}5. \tag{18.19}$$

При $k = s,\ n = 2^k,\ k = \log_2 n$, имеем

$$T(n) \leqslant 3^k + 52n\left(\tfrac{3}{2}\right)^k - 52n - 4{,}5 \cdot 3^k + 4{,}5,$$

$$T(n) \leqslant 3^{\log_2 n} + 52n\left(\tfrac{3}{2}\right)^{\log_2 n} - 52n - 4{,}5 \cdot 3^{\log_2 n} + 4{,}5,$$

$$T(n) \leqslant n^{\log_2 3} + 52n^{\log_2 3} - 52n - 4{,}5n^{\log_2 3} + 4{,}5,$$

$$T(n) \leqslant 48{,}5n^{\log_2 3} - 52n + 4{,}5. \tag{18.20}$$

Такова оценка сложности неоптимизированного метода Карацубы для двоичных чисел, когда рекурсия выполнена полностью. С целью его оптимизации рассмотрим другую возможность: при некотором $k < s$ прекратим рекурсию и перейдём в вычислениях на школьный метод. В таком случае

из формулы (18.19) следует, что

$$T(n) \leqslant 3^k(6\tfrac{n^2}{2^{2k}} - 8\tfrac{n}{2^k}) + 52n\left(\tfrac{3}{2}\right)^k - 52n - 4{,}5\cdot 3^k + 4{,}5. \tag{18.21}$$

Обозначим

$$f(k) = 6n^2\left(\frac{3}{2}\right)^k \cdot \frac{1}{2^k} + 44n\left(\frac{3}{2}\right)^k - 52n - 4{,}5\cdot 3^k + 4{,}5. \tag{18.22}$$

Исследуем $f(k)$ на экстремум:

$$f'(k) = 6n^2\left(\frac{3}{2}\right)^k \cdot \frac{1}{2^k}\ln\frac{3}{4} + 44n\left(\frac{3}{2}\right)^k \ln\frac{3}{2} - 4{,}5\cdot 3^k \ln 3,$$

$f'(k) \geqslant 0$ тогда и только тогда, когда

$$\begin{gathered}
-6n^2\tfrac{1}{2^k}\ln\tfrac{4}{3} + 44n\ln\tfrac{3}{2} - 4{,}5\ln 3\cdot 2^k \geqslant 0 \;\Leftrightarrow \\
\Leftrightarrow -6n^2\ln\tfrac{4}{3} + 44n\ln\tfrac{3}{2}\cdot 2^k - 4{,}5\ln 3\cdot 2^{2k} \geqslant 0 \;\Leftrightarrow \\
\Leftrightarrow 4{,}5\ln 3\cdot 2^{2k} - 44n\ln\tfrac{3}{2}\cdot 2^k + 6n^2\ln\tfrac{4}{3} \leqslant 0 \Leftrightarrow \\
\Leftrightarrow 4{,}5\ln 3\cdot t^2 - 44n\ln\tfrac{3}{2}\cdot t + 6n^2\ln\tfrac{4}{3} \leqslant 0,\ t = 2^k, \\
\tfrac{D}{4} = \left(\left(22\ln\tfrac{3}{2}\right)^2 - 27\ln 3\cdot\ln\tfrac{4}{3}\right)n^2 > 0, \\
t_{0,1} = \tfrac{22\cdot\ln\frac{3}{2}n \pm\sqrt{\frac{D}{4}}}{4{,}5\ln 3}, \\
2^{k_0} = t_0 \approx 0{,}09949n, \qquad 2^{k_1} = t_1 \approx 3{,}5n.
\end{gathered}$$

Мы видим, что $f'(k) > 0$ при $k_0 < k < k_1$ и $f'(k) < 0$ при $k < k_0$ и при $k > k_1$. Значит, $f(k_0)$ есть строгий локальный минимум функции $f(k)$, а $f(k_1)$ – её строгий локальный максимум. Но $2^{k_1} = t_1 > n$, в то время как $2^k \leqslant n$, поэтому значение $k = k_1$ не достигается.

Далее, $k_0 = \log_2 t_0 \approx \log_2 n - \varepsilon$, $\varepsilon \approx |\log_2 0{,}09949| \approx 3{,}33$. Значит, минимум дискретной функции $f(k)$ достигается либо при $k = s-3$, либо при $k = s-4$, причём глобальный минимум ввиду того,что $1 \leqslant k \leqslant s$.

Из (18.22), учитывая, что $n = 2^s$, находим

$$\begin{gathered}
f(s-3) = \tfrac{731{,}5}{27}\cdot 3^s - 52n + 4{,}5, \\
f(s-4) > 27{,}5\cdot 3^s - 52n + 4{,}5.
\end{gathered}$$

Итак, оптимальное значение $k = s - 3 \geqslant 0$, и сложность оптимизированного метода Карацубы для двоичных чисел при $n = 2^s,\ s \geqslant 4$, составляет

$$T(n) \leqslant \frac{731{,}5}{27}\cdot n^{\log_2 3} - 52n + 4{,}5. \tag{18.23}$$

При $s = 3,\ n = 2^s = 8$ происходит переход на школьный метод.

Оценка (18.23) лучше, чем в соотношении (18.20) примерно в 2 раза.

§ 19. Некоторые частные случаи метода Тоома. Оптимизация метода Тоома

Рассмотрим частный случай метода Тоома, состоящий в следующем.

Пусть u и v – два $4n$-разрядных двоичных натуральных числа: $u = (u_{4n-1}\dots u_1u_0)_2,\ v = (v_{4n-1}\dots v_1v_0)_2,\ u_i, v_j \in \{0,1\},\ i,j = 0,1,\ \dots, 4n-1$;

$$u = \sum_{j=0}^{4n-1} u_j 2^j,\ v = \sum_{i=0}^{4n-1} v_i 2^i.$$

Пусть

$$\begin{gathered}
U_3 = (u_{4n-1}\dots u_{3n})_2,\ U_2 = (u_{3n-1}\dots u_{2n})_2, \\
U_1 = (u_{2n-1}\dots u_n)_2,\ U_0 = (u_{n-1}\dots u_0)_2; \\
V_3 = (v_{4n-1}\dots v_{3n})_2,\ V_2 = (v_{3n-1}\dots v_{2n})_2, \\
V_1 = (v_{2n-1}\dots v_n)_2,\ V_0 = (v_{n-1}\dots v_0)_2.
\end{gathered}$$

Тогда

$$\begin{aligned}
u &= 2^{3n}U_3 + 2^{2n}U_2 + 2^nU_1 + U_0, \\
v &= 2^{3n}V_3 + 2^{2n}V_2 + 2^nV_1 + V_0.
\end{aligned} \tag{19.24}$$

Рассмотрим полиномы

$$\begin{aligned}
U(x) &= U_3x^3 + U_2x^2 + U_1x + U_0, \\
V(x) &= V_3x^3 + V_2x^2 + V_1x + V_0
\end{aligned} \tag{19.25}$$

и положим

$$W(x) = U(x)V(x) = W_6x^6 + W_5x^5 + W_4x^4 + W_3x^3 + W_2x^2 + W_1x + W_0. \tag{19.26}$$

Так как $u = U(2^n), v = V(2^n)$, то $uv = W(2^n)$. Поэтому при известных коэффициентах W_k в $W(x)$, $k = \overline{0,6}$, можно легко вычислить uv.

Для нахождения коэффициентов W_k найдём

$$\begin{aligned} b_0 &= W(-3) = U(-3)V(-3), \\ b_1 &= W(-2) = U(-2)V(-2), \\ b_2 &= W(-1) = U(-1)V(-1), \\ b_3 &= W(0) = U(0)V(0), \\ b_4 &= W(1) = U(1)V(1), \\ b_5 &= W(2) = U(2)V(2), \\ b_6 &= W(3) = U(3)V(3). \end{aligned} \tag{19.27}$$

Как известно, коэффициенты полинома $W(x)$ степени 6 могут быть выражены в виде линейной комбинации значений этого полинома в семи различных точках, например, в точках b_i, $i = \overline{0,6}$. Каждое b_i есть произведение $(n+t)$-битовых двоичных чисел и при фиксированном t вычисляется со сложностью

$$T(n+t) \leqslant T(n) + 6t^2 - 4t - 4 + (12t+2)n. \tag{19.28}$$

Таким образом,

$$T(4n) \leqslant 7T(n) + Cn + C'. \tag{19.29}$$

Рассмотрим реализацию метода Тоома схемами из функциональных элементов в базисе $\{\neg, \&, \vee, \oplus, 0, 1\}$.

Обозначим через $L(x)$ сложность вычисления x, $R(x)$ – число бит в двоичной записи x. Обозначим через $L(n+t)$ сложность умножения двух $(n+t)$-разрядных двоичных чисел.

Если умножать двоичное n-разрядное число U_0 столбиком на число x, имеющее в двоичном представлении q единиц, то потребуется $(q-1)$ раз сложить не более чем n-разрядные числа. Таким образом,

$$L(xU_0) \leqslant (q-1)(5n-3), \quad q \geqslant 1. \tag{19.30}$$

Например, $L(3U_0) = L(11_2 U_0) \leqslant 1 \cdot (5n-3)$.

Так как $W(x) = U(x)V(x)$, а коэффициенты многочленов $U(x)$ и $V(x)$ суть n-разрядные двоичные числа, то можно дать некоторые верхние оценки числа бит для коэффициентов многочлена $W(x)$, а именно:

$$R(W_0) = R(W_6) = 2n, \ R(W_1) = R(W_5) = 2n+1,$$
$$R(W_2) = R(W_3) = R(W_4) = 2n+2$$

и далее для b_i, $i = \overline{0,6}$:

$$R(b_0) = 2n+12, \ R(b_1) = 2n+8, \ R(b_2) = 2n+4, \ R(b_3) = 2n,$$
$$R(b_4) = 2n+5, \ R(b_5) = 2n+8, \ R(b_6) = 2n+12.$$

Полином $U(x)$ можно записать в виде

$$U(x) = U_e(x^2) + xU_o(x^2). \tag{19.31}$$

Полиномы $V(x)$ и $W(x)$ могут быть выражены аналогично. Для $j = 1,\ 2,\ 3$ вычисляем

$$W(j) = (U_e(j^2) + jU_o(j^2))(V_e(j^2) + jV_o(j^2)),$$
$$W(-j) = (U_e(j^2) - jU_o(j^2))(V_e(j^2) - jV_o(j^2)).$$

Тогда

$$W_e(j^2) = \frac{1}{2}(W(j) + W(-j)), \ W_o(j^2) = \frac{1}{2}(W(j) - W(-j)).$$

Вычисляем также $W_e(0) = U(0)V(0)$. Затем строим таблицы разностей для полиномов W_e и W_o.[6]

b_3	$b_3 = U_0 V_0, \ L(b_3) \leqslant T(n), \ R(b_3) = 2n$
b_4	$b_4 = (\underbrace{(U_0+U_2)+(U_1+U_3)}_{I})(\underbrace{(V_0+V_2)+(V_1+V_3)}_{II}),$
	$L(I) = L(II) \leqslant 15n-4,$
	$R(I) = R(II) \leqslant n+2,$
	$L(n+2) \leqslant 12 + 26n + T(n),$
	$L(b_4) \leqslant 2(15n-4) + 12 + 26n + T(n) = 4 + 56n + T(n),$
	$R(b_4) \leqslant 2n+4.$

[6] Этот способ для метода Тоома предложил К. Бейкер.

b_2	$b_2 = (\underbrace{(U_0+U_2)-(U_1+U_3)}_{I})(\underbrace{(V_0+V_2)-(V_1+V_3)}_{II}),$ $L(I) = L(II) \leqslant 8(n+1)-3 = 8n+5,$ $R(I) = R(II) \leqslant n+1,$ $L(n+1) \leqslant -2+14n+T(n),$ $L(b_2) \leqslant 2(8n+5)-2+14n+T(n)+1 = 9+30n+T(n),$ $R(b_2) \leqslant 2n+2.$
b_5	$(\underbrace{(U_0+2^2U_2)+2(U_1+2^2U_3)}_{I})(\underbrace{(V_0+2^2V_2)+2(V_1+2^2V_3)}_{II}),$ $L(I) = L(II) \leqslant 2(5n-9)+(5n+8) = 15n-10,$ $R(I) = R(II) \leqslant n+4,$ $L(n+4) \leqslant 76+50n+T(n),$ $L(b_5) \leqslant 2(15n-10)+76+50n+T(n) = 56+80n+T(n),$ $R(b_5) \leqslant 2n+8.$
b_1	$(\underbrace{(U_0+2^2U_2)-2(U_1+2^2U_3)}_{I})(\underbrace{(V_0+2^2V_2)-2(V_1+2^2V_3)}_{II}),$ $L(I) = L(II) \leqslant 8(n+4)-3-2-3 = 8n+24,$ $R(I) = R(II) \leqslant n+4,$ $L(n+4) \leqslant 76+50n+T(n),$ $L(b_1) \leqslant 2(8n+24)+76+50n+T(n)+1 = 125+66n+T(n),$ $R(b_1) \leqslant 2n+8.$
b_6	$(\underbrace{(U_0+3^2U_2)+3(U_1+3^2U_3)}_{I})(\underbrace{(V_0+3^2V_2)+3(V_1+3^2V_3)}_{II}),$ $L(I) = L(II) \leqslant 2(10n-7)+5(n+5)-2 = 25n-9$ $R(I) = R(II) \leqslant n+6,$ $L(n+6) \leqslant 188+74n+T(n),$ $L(b_6) \leqslant 2(25n-9)+188+74n+T(n) = 170+124n+T(n)$ $R(b_6) \leqslant 2n+12.$

b_0	$(\underbrace{(U_0+3^2U_2)-3(U_1+3^2U_3)}_{I})(\underbrace{(V_0+3^2V_2)-3(V_1+3^2V_3)}_{II}),$ $L(I) = L(II) \leqslant 8(n+6)-3-2 = 8n+43,$ $R(I) = R(II) \leqslant n+6,$ $L(n+6) \leqslant 188+74n+T(n),$ $L(b_0) \leqslant 275+90n+T(n),$ $R(b_0) \leqslant 2n+12.$

При вычислении b_2 в (I) и (II) используется, что уменьшаемые и вычитаемые соответствующих разностей уже вычислены при нахождении b_4; вычисляются модули разностей и их знаки, причём в вычислениях разностей учитываются «дополнительно возникающие нули» за счёт нулей в конце или в начале чисел; найденные модули разностей умножаются (вычисляется $L(n+1)$), и при нахождении b_2 добавляется один элемент для вычисления знака произведения: 0, если произведение неотрицательно, и 1, если оно отрицательно. Аналогично производятся дальнейшие вычисления.

Для b_6 при вычислении $3(U_1 + 3^2U_3)$ и $3(V_1 + 3^2V_3)$ использовалась схема Горнера, но при подсчёте разрядности, то есть предполагаемого числа битов в двоичном представлении получающихся чисел, схема Горнера не использовалась: так получаются лучшие результаты. Суммарно

$$L(b_i,\ i=\overline{0,6}) \leqslant 639+386n+7T(n). \qquad (19.32)$$

Далее требуется вычислить $W_e(1) = \frac{1}{2}(b_4+b_2)$ и $W_o(1) = \frac{1}{2}(b_4-b_2)$. Заметим, что эти числа неотрицательны. Можно поступить так. Вычисляем $\tilde{W}_e(1) = \frac{1}{2}(b_4+|b_2|)$ и $\tilde{W}_o(1) = \frac{1}{2}(b_4-|b_2|)$. Если $s = \operatorname{sign}(b_2) = 0$, то есть $b_2 \geqslant 0$, то $W_e = \tilde{W}_e$, $W_o = \tilde{W}_o$. Если же $s = \operatorname{sign}(b_2) = 1$, то есть $b_2 < 0$, то $W_e = \tilde{W}_o$, $W_o = \tilde{W}_e$. Такая операция осуществима с помощью следующей схемы: возьмём два экземпляра $\tilde{W}_e$

и два экземпляра $\tilde{W}_o$ ($\tilde{W}_e$ и $\tilde{W}_o$ суть двоичные числа) и выполним поэлементную конъюнкцию первого экземпляра $\tilde{W}_e$ с $\overline{s}$ и первого экземпляра $\tilde{W}_o$ с $\overline{s}$; выполним аналогично поэлементную конъюнкцию вторых экземпляров $\tilde{W}_e$ и $\tilde{W}_o$ с s, после чего выполняется поэлементная дизъюнкция первого экземпляра изменённого $\tilde{W}_e$ и второго экземпляра изменённого $\tilde{W}_o$, в результате получается W_e, и поэлементная дизъюнкция первого экземпляра изменённого $\tilde{W}_o$ и второго экземпляра изменённого $\tilde{W}_e$, в результате получается W_o. Сложность указанных вычислений оценивается следующим образом:

$L_1 = L(W_e(1),\ W_o(1)) \leqslant (20n{+}20){+}(8n{+}13){+}2(2n{+}2) = 32n{+}37.$

Кроме того, $R_1 = R(W_e(1)) = R(W_o(1)) = 2n + 4$.

Аналогично вычисляются пары

$W_e(2) = \frac{1}{2}(b_5 + b_1)$ и $W_o(2) = \frac{1}{2}(b_5 - b_1)$,

$W_e(3) = \frac{1}{2}(b_6 + b_0)$ и $W_o(3) = \frac{1}{2}(b_6 - b_0)$, для которых справедливо

$$L_2 := L(W_e(2),\ W_o(2)) \leqslant (20n + 70) + (8n + 33) + 2(2n + 8) = \\ = 32n + 119,$$

$$R_2 := R(W_e(2)) = R(W_o(2)) = 2n + 8,$$

$$L_3 := L(W_e(3),\ W_o(3)) \leqslant (20n + 110) + (8n + 49) + 2(2n + 12) = \\ = 32n + 183,$$

$$R_3 := R(W_e(3)) = R(W_o(3)) = 2n + 12.$$

Суммарно

$$L_0 = L(b_i,\ i = \overline{0,6}){+}L_1{+}L_2{+}L3 \leqslant 978{+}482n{+}7T(n). \quad (19.33)$$

$W_o(x) = W_1x + W_3x^3 + W_5x^5$.

Рассмотрим многочлен

$$\hat{W}_o(x) = W_o(x)/x = W_1 + W_3x^2 + W_5x^4.$$

$\hat{W}_o(1) = W_o(1) =: c_1, \quad R(c_1) = 2n + 3\ L(c_1) = 0,$

$\hat{W}_o(2) = W_o(2)/2 =: c_2,\ R(c_2) = 2n + 6\ L(c_2) = 0,$

$\hat{W}_o(3) = W_o(3)/3 =: c_3,\ R(c_3) = 2n + 9\ L(c_3) = 10n + 50.$

Имеем

$$\begin{cases} W_1 + \ W_3 + \ \ W_5 \ = c_1 \\ W_1 + 4W_3 + 16W_5 \ = c_2 \\ W_1 + 9W_3 + 81W_5 = c_3. \end{cases} \quad (19.34)$$

Решаем систему (19.34):

$$\begin{cases} d_1 := (c_2 - c_1)/3 = W_3 + 5W_5 \geqslant 0, \\ L(d_1) = 20n + 38, \\ R(d_1) = 2n + 5, \\ d_2 := (c_3 - c_2)/5 = W_3 + 13W_5 \geqslant 0, \\ L(d_2) = 20n + 78, \\ R(d_2) = 2n + 6. \end{cases}$$

$f := (d_2 - d_1)/8 = W_5 \geqslant 0,$

$L(f) \leqslant 10n + 15,$

$R(f) = 2n + 1,$

$g := W_3 = d_1 - 5W_5 = d_1 - 5f \geqslant 0,$

$L(g) \leqslant 20n + 1,$

$R(g) = 2n + 2,$

$h := W_1 = c_1 - g - f \geqslant 0,$

$L(h) \leqslant 20n + 19,$

$R(h) = 2n + 1.$

Суммируя оценки сложности, находим, что сложность вычислений

$$L(W_1,\ W_3,\ W_5) \leqslant 100n + 201. \quad (19.35)$$

$W_e(x) = W_0 + W_2x^2 + W_4x^4 + W_6x^6.$

Рассмотрим многочлен

$$\hat{W}_e(x) = (W_e(x) - W_0)/x^2 = W_2 + W_4x^2 + W_6x^4.$$

$$\hat{W}_e(1) = W_e(1) - W_0 =: e_1,$$
$$R(e_1) = 2n + 4,$$
$$L(e_1) = 10n + 5,$$
$$\hat{W}_e(2) = (W_e(2) - W_0)/4 =: e_2,$$
$$R(e_2) = 2n + 6,$$
$$L(e_2) = 10n + 13,$$
$$\hat{W}_e(3) = (W_e(3) - W_0)/9 =: e_3,$$
$$R(e_3) = 2n + 8$$
$$L(e_3) = 20n + 81.$$

Имеем

$$\begin{cases} W_2 + W_4 + W_6 = e_1 \\ W_2 + 4W_4 + 16W_6 = e_2 \\ W_2 + 9W_4 + 81W_6 = e_3. \end{cases} \tag{19.36}$$

Решаем систему (19.36):

$$\begin{cases} d_1 := (e_2 - e_1)/3 = W_4 + 5W_6 \geqslant 0, \\ L(d_1) = 20n + 41, R(d_1) = 2n + 4, \\ d_2 := (e_3 - e_2)/5 = W_4 + 13W_6 \geqslant 0, \\ L(d_2) = 20n + 71, \\ R(d_2) = 2n + 5. \end{cases}$$

$$f := (d_2 - d_1)/8 = W_6 \geqslant 0,$$
$$L(f) \leqslant 10n + 10,$$
$$R(f) = 2n,$$
$$g := W_4 = d_1 - 5W_6 = d_1 - 5f \geqslant 0,$$
$$L(g) \leqslant 20n - 4,$$
$$R(g) = 2n + 2,$$
$$h := W_2 = e_1 - g - f \geqslant 0,$$
$$L(h) \leqslant 20n + 12,$$
$$R(h) = 2n + 2.$$

Суммируя оценки сложности, находим, что сложность

вычислений

$$L(W_2,\ W_4,\ W_6) \leqslant 130n + 229. \tag{19.37}$$

Таким образом, найдены все коэффициенты $W_j,\ j = \overline{0,6}$, и

$$L(W_j,\ j = \overline{0,6}) \leqslant 1069 + 616n + 7T(n). \tag{19.38}$$

Далее,

$$uv = W(2^n) = W_e(2^n) + W_o(2^n);$$
$$W_e(2^n) = W_6 2^{6n} + W_4 2^{4n} + W_2 2^{2n} + W_0,$$
$$W_o(2^n) = (W_5 2^{4n} + W_3 2^{2n} + W_1)2^n.$$

Все коэффициенты многочлена $W_e(x)$ – не менее чем $2n$-разрядные двоичные неотрицательные целые числа (допускаются нули в старших разрядах). Поэтому $W_e(2^n)$ – не менее чем $8n$-разрядное число. Но $W_e(2^n)$ – не более чем $8n$-разрядное число, так как произведение uv суть $8n$-разрядное число. Поэтому $W_e(2^n)$ – $8n$-разрядное число (допускаются нули в старших разрядах). Мы знаем, что $R(W_0) = R(W_6) = 2n,\ R(W_2) = R(W_4) = 2n + 2$. Отщепим от W_2 и W_4 два «лишних» старших разряда, представив W_2 и W_4 в виде $W_2 = (e_2, e_1)_2 \cdot 2^{2n} + \hat{W}_2,\ W_4 = (e_3, e_4)_2 \cdot 2^{2n} + \hat{W}_4$. Аналогично, $W_1 = (e_5)_2 \cdot 2^{2n} + \hat{W}_1,\ W_3 = (e_7, e_6)_2 \cdot 2^{2n} + + \hat{W}_3,\ W_5 = (e_8)_2 \cdot 2^{2n} + \hat{W}_5$. Тогда $\hat{W}_e(2^n) := W_6 \cdot 2^{6n} + + \hat{W}_4 \cdot 2^{4n} + \hat{W}_2 \cdot 2^{2n} + W_0$ есть двоичное представление $8n$-разрядного числа. Прибавим к нему разреженное нулями число, составленное из отщепленных разрядов коэффициентов $W_j,\ j = \overline{1,5}$, на соответствующих им местах. К полученному вновь $8n$-разрядному числу прибавим $\hat{W}_0(2^n) = (\hat{W}_5 2^{4n} + + \hat{W}_3 2^{2n} + \hat{W}_1)2^n$, которое есть двоичное представление $7n$-разрядного числа с n нулями в конце, получим $W(2^n)$. Таким образом, для получения ответа требуется произвести два сложения трёх чисел, полученных с нулевой сложностью (все W_j вычислены ранее).

Указанная процедура имеет сложность $L \leqslant 46n + 16$, и алгоритм Тоома с учётом (19.38) имеет оценку сложности

$$T(4n) \leqslant 7T(n) + 662n + 1085. \tag{19.39}$$

Пусть сомножители u и v имеют $n = q^s$ бит. Тогда (см. [13])

$$T(n) \leqslant (2q-1)T\left(\frac{n}{q}\right) + C\frac{n}{q} + C', \tag{19.40}$$

что на k-м шаге рекурсии приводит к соотношению

$$T(n) \leqslant (2q-1)^k T\left(\frac{n}{q^k}\right) + \frac{Cn}{q-1}\left(\left(\frac{2q-1}{q}\right)^k - 1\right) + \\ + \frac{C'}{2(q-1)}((2q-1)^k - 1). \tag{19.41}$$

Подставляя в (19.41) значения $C = 662,\ C' = 1085,\ q = 4$ из 19.39, получаем соотношение

$$T(n) \leqslant 7^k T\left(\frac{n}{4^k}\right) + \frac{662}{3}n\left(\frac{7}{4}\right)^k - \frac{662}{3}n + \frac{1085}{6}\cdot 7^k - \frac{1085}{6}. \tag{19.42}$$

При $k = s,\ n = q^k,\ k = \log_q n$, из (19.41) получаем оценку сложности неоптимизированного случая метода Тоома для двоичных чисел (когда рекурсия выполнена полностью):

$$T(n) \leqslant \left(1 + \frac{C}{q-1} + \frac{C'}{2(q-1)}\right) n^{\log_q(2q-1)} - \frac{Cn}{q-1} - \frac{C'}{2(q-1)}. \tag{19.43}$$

В данном случае для $q = 4,\ C = 662,\ C' = 1085$ имеем

$$T(n) \leqslant 402{,}5 n^{\log_4 7} - \frac{662}{3}n - \frac{1085}{6}. \tag{19.44}$$

С целью оптимизации рассмотренного случая метода Тоома и улучшения оценки (19.44) рассмотрим другую возможность: при некотором $k < s$ прекратим рекурсию и перейдём в вычислениях на оптимизированный метод Карацубы. Из соотношения (19.42) и соотношения (18.23) следует, что $T(n) \leqslant f(k)$, где

$$f(k) = 7^k\left(\tfrac{731{,}5}{27}\left(\tfrac{n}{4^k}\right)^{\log_2 3} - 52\left(\tfrac{n}{4^k}\right) + 4{,}5\right) + \\ + \tfrac{662}{3}n\left(\tfrac{7}{4}\right)^k - \tfrac{662}{3}n + \tfrac{1085}{6}\cdot 7^k - \tfrac{1085}{6}. \tag{19.45}$$

Исследуем $f(k)$ на экстремум:

$$f'(k) = \left(-\frac{731{,}5}{27}\ln\frac{9}{7}\left(\frac{n}{4^k}\right)^{\log_2 3} + \frac{506}{3}\ln\frac{7}{4}\left(\frac{n}{4^k}\right) + \frac{556}{3}\ln 7\right)\cdot 7^k.$$

Положим $4^k = nt,\ 0 < t < 1$. Тогда имеем: $f'(k) \geqslant 0 \Leftrightarrow$

$$\Leftrightarrow g(t) = \left(\frac{556}{3}\cdot\ln 7\right)t^{\log_2 3} + \left(\frac{506}{3}\ln\frac{7}{4}\right)t^{\log_2\frac{3}{2}} - \frac{731{,}5}{27}\ln\frac{9}{7} \geqslant 0. \tag{19.46}$$

Функция $g(t)$ непрерывна и строго возрастает на отрезке $[0;\ 1]$, а на концах этого отрезка имеет значения разных знаков: в нуле она отрицательна, а при $t = 1$ положительна. Численно решая уравнение $g(t) = 0$ на отрезке $[0;\ 1]$, находим корень уравнения: $t_0 \approx 9{,}8766 \cdot 10^{-3}$. Учитывая знаки производной, заключаем, что функция $f(t)$ достигает минимума при $t = t_0$.

Так как $k = \log_4 n + \log_4 t \approx s - 3{,}29$ при $t = t_0$, то минимум дискретной функции $f(k)$ достигается либо при $k = s-3$, либо при $k = s-4$. Сравнивая с помощью соотношений (19.45) $f(s-3)$ и $f(s-4)$, находим, что в оптимизированном методе $k = s - 3 \geqslant 0$ и

$$T(n) \leqslant \frac{92\ 191{,}5}{1029}n^{\log_4 7} - \frac{662}{3}n - \frac{1085}{6}. \tag{19.47}$$

Примерно в 4,5 раза лучше неоптимизированного случая (19.44).

Как только рекурсия достигнет чисел разряда 64 (при $n = 4^s,\ s = 3$), переходим на оптимизированный метод Карацубы. Таким образом, метод Тоома для $q = 4,\ n = 4^s$ лучше метода Карацубы при $n \geqslant 4^4 = 256$.

Заметим, что оптимизированный метод Тоома можно применять для чисел разрядности $n = 4^s \cdot 2$. Тогда $k = s + \\ + 0{,}5 + \log_4 t \approx s - 2{,}8$ при $t = t_0$. То есть минимум дискретной функции достигается либо при $k = s-3$, либо при $k = s-2$.

Сравнивая с помощью соотношений (19.45) значения функций $f(s-2)$ и $f(s-3)$, находим, что в оптимизированном

случае при $n = 4^s \cdot 2$ значение $k = s - 3$. Тогда согласно (19.45)

$$T(n) \leqslant \frac{243078{,}5}{1029\sqrt{7}} n^{\log_4 7} - \frac{662}{3} n - \frac{1085}{6}. \qquad (19.48)$$

Как только рекурсия достигнет чисел разряда 128 (при $n = 2 \cdot 4^s$, $s = 3$), переходим на оптимизированный метод Карацубы. Таким образом, метод Тоома для $q = 4, n = 2 \cdot 4^s$ лучше метода Карацубы при $n \geqslant 4^4 \cdot 2 = 512$.

Соотношение (19.44), выражающее случай полной рекурсии, также можно переписать при помощи (19.42) для $n = 4^s \cdot 2$:

$$T(n) \leqslant \frac{91}{\sqrt{7}} n^{\log_4 7} - \frac{662}{3} n - \frac{1085}{6}. \qquad (19.49)$$

На последнем шаге рекурсии здесь получается $T(2) \leqslant 8$.

Замечание. Согласно соотношению (19.47) для умножения 1024-битовых целых двоичных чисел имеем следующую оценку схемной сложности:

$$T(1024) \leqslant 1\ 279\ 651. \qquad (19.50)$$

Этажи рекурсии в алгоритме умножения устроены следующим образом: вначале дважды применяется метод Тоома, в котором множители разбиваются на 4 части, затем трижды применяется метод Карацубы, а потом школьный метод. В чистом методе Карацубы согласно (18.20) получается оценка сложности $T_0(n) \leqslant 2\ 810\ 633$ (вдвое хуже (19.50)). В оптимизированном варианте метода Карацубы согласно 18.23 получается оценка $T_1(n) \leqslant 1\ 546\ 547$ (на 21% хуже (19.50)).

Замечание. Можно рассмотреть метод Тоома для $q = 8$, $n = 8^s$, в котором множители разбиваются на 8 частей на каждом шаге рекурсии, и получить рекуррентную верхнюю оценку:

$$T(8n) \leqslant 15T(n) + 5762n + 63\ 589. \qquad (19.51)$$

Для оптимизированного варианта (состоящего из каскада методов Тоома, Карацубы и школьного) можно получить

оценку

$$T(n) \leqslant 257{,}05 n^{\log_8 15} - 823n - 4542. \qquad (19.52)$$

Это приблизительно в 21 раз лучше неоптимизированного случая, когда рекурсия выполнена полностью. Можно показать, что при $n \geqslant 8^5 = 32\ 768$ этот метод эффективнее метода Тоома для $q = 4$. Для $n \leqslant 8^4 = 4\ 096$ эффективнее оптимизированный вариант метода Тоома для $q = 4$. Как только рекурсия достигнет чисел разряда 4096, переходим на оптимизированный метод Тоома для $q = 4$.

Случай $n = 2^s - 1$.

Пусть $n = 2^s - 1$. Рассмотрим умножение n-битовых двоичных целых чисел. Согласно соотношению (18.17)

$$T(2^s - 1) \leqslant 2T(2^{s-1}) + 2T(2^{s-2}) + \cdots + 2T(2^4) + \\ + T(15) + 40 \cdot 2^4 + 12 \cdot 15 - 9. \qquad (19.53)$$

Так как $T(15) \leqslant 1230$ по школьному алгоритму, то (19.53) перепишем в виде

$$T(2^s - 1) \leqslant 2T(2^{s-1}) + 2T(2^{s-2}) + \cdots + 2T(2^4) + 2041. \qquad (19.54)$$

Для $s = 8$ имеем

$$T(2^8 - 1) \leqslant 2T(2^7) + 2T(2^6) + 2T(2^5) + 2T(2^4) + 2041. \qquad (19.55)$$

Согласно (18.23) справедливы оценки:

$$T(2^4) \leqslant 1367,\ T(2^5) \leqslant 4924,\ T(2^6) \leqslant 16\ 427,\ T(2^7) \leqslant 52\ 600.$$

Тогда согласно (19.55) и (19.47)

$$T(255) \leqslant 152\ 677,\ \ T(256) \leqslant 158\ 442. \qquad (19.56)$$

Отметим, что $T(256) - T(255) = 5765$ (приблизительно $3{,}8\%$ от $T(255)$), причём для получения оценки $T(255)$ применялся метод Карацубы, а для получения оценки $T(256)$ применялся метод Тоома (было показано, что он эффективнее метода Карацубы для $n = 2^s \geqslant 256$). Указанный способ (19.54) неэффективен для $s > 8$, так как при таких значениях s метод Карацубы уступает методу Тоома, но при $4 < s < 8$ достигается экономия порядка 10%.

§ 20. Схемы для арифметики по модулю 7

Нам понадобятся некоторые сведения из алгебры.

Говорят, что на множестве F задана бинарная алгебраическая операция f, если каждой упорядоченной паре (x, y) из $F \times F$ соответствует и только один элемент z из F. Таким образом, бинарная алгебраическая операция f есть функция $f : F \times F \to F$. Вместо $z = f(x, y)$ пишут $z = xfy$.

Непустое множество F называется алгебраическим полем, если на нём определены две бинарные алгебраические операции сложение и умножение и выполнены следующие аксиомы:

1. $(x + y) + z = x + (y + z)$.
2. $0 + x = x$.
3. $(-x) + x = 0$.
4. $x + y = y + x$.
5. $(xy)z = x(yz)$.
6. $1x = x$.
7. $x^{-1}x = 1$, если $x \neq 0$.
8. $xy = yx$.
9. $(x + y)z = xz + yz$.
10. $0 \neq 1$.

Мощность $|F|$ множества F называется порядком алгебраического поля. Поле называется конечным, если его порядок конечен. Запись $GF(q)$ означает конечное поле порядка q. Примером конечного поля может служить поле

$GF(p) = \{0,\ 1,\ \ldots,\ p-1\}$, где p – простое число, а сложение и умножение элементов осуществляются по модулю p. Число $a = b$ по модулю p, если разность $a - b$ делится нацело на p. Например, $8 = 2 \pmod 3$. Известно, что для любого натурального числа n и простого числа p существует поле $GF(p^n)$ порядка p^n.

Пусть p – минимальное натуральное число, такое что $\underbrace{1+1+\cdots+1}_{p} = 0$. Это число p называется характеристикой поля F. Характеристика поля всегда простое число. Например, поле $GF(p^n)$ имеет характеристику p. Бесконечные поля имеют характеристику 0.

Рассмотрим поле $GF(7)$ и построим для него квадратичное расширение $GF(7^2)$. Элементами поля $GF(7^2)$ являются всевозможные упорядоченные пары (x, y) элементов x и y из F. Сложение и умножение определяются следующим образом: $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, $(x_1, y_1)(x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. Если пару $(x, 0)$ отождествить с x, а пару $(0, 1)$ обозначить σ, то $(x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0)(0, 1) = x + y\sigma$. Кроме того, $\sigma^2 = (0, 1)(0, 1) = (-1, 0) = -1$. Построен аналог комплексных чисел. Роль мнимой единицы играет σ. Нетрудно видеть, что аксиомы алгебраического поля выполняются для $GF(7^2)$. Важно обратить внимание при проверке выполнения аксиом на обратимость всякого ненулевого элемента (существование для него мультипликативного обратного). Так как $\frac{1}{x+\sigma y} = \frac{x-\sigma y}{(x+\sigma y)(x-\sigma y)} = \frac{x-\sigma y}{x^2+y^2}$, то надо проверить, что если x и y не равны нулю одновременно, то $x^2 + y^2 \not\equiv 0$. В данном случае это легко проверить перебором. Так как $1^1 = 1,\ 2^2 = 4,\ 3^2 = 2,\ 4^2 = 2,\ 5^2 = 4,\ 6^2 = 1$ и $1+1 = 2,\ 1+2 = 3,\ 1+4 = 5,\ 2+2 = 4,\ 2+4 = 6,\ 4+4 = 1$, то сумма $x^2 + y^2$ не обращается в ноль, если x и y не равны нулю одновременно.

Поле $GF(7^{2n})$ может быть представлено как множество всех многочленов степени не более чем $n-1$ с коэффициентами

из $GF(7^2)$, где сложение и умножение многочленов осуществляются по модулю некоторого неприводимого многочлена (такого, который не разлагается на множители в этом поле).

Поле $GF(7^n)$ может быть представлено как множество всех многочленов степени не более чем $n-1$ с коэффициентами из $GF(7)$, где сложение и умножение многочленов осуществляются по модулю некоторого неприводимого многочлена.

Лемма. *Умножение в $GF(7)$ выполняется схемой сложности* 25.

Доказательство. Заметим, что умножение числа $(x_2x_1x_0)_2$ по модулю 7 на числа $4=(100)_2$, $2=(010)_2$ равносильно циклическим сдвигам битов x_i, умножение на $1=(001)_2$ – это тождественное преобразование, умножение на числа

$$3=(011)_2=-4,\ 5=(101)_2=-2,\ 6=(110)_2=-1$$

делается точно так же, но у результата меняется знак на противоположный, что равносильно прибавлению по модулю два ко всем битам результата знакового бита σ. Очевидно, этот бит можно вычислить по формуле

$$m(y_2,y_1,y_0)=(y_0+y_1)(y_0+y_2)+y_0.$$

Умножение на числа $(000)_2$ и $(111)_2$ дает в результате $(000)_2$. Рассмотрим линейный оператор $u_1=y_0\oplus y_1\oplus 1, u_0=y_0\oplus y_2\oplus 1$. Очевидно, он принимает значение 11 на противоположных наборах $000,111$, значение 10 на противоположных наборах $011,100$, значение 01 на противоположных наборах $010,101$, значение 00 на противоположных наборах $001,110$. Рассмотрим оператор

$$d_2=\neg u_1\&\neg u_0,\ d_1=u_1\&\neg u_0,\ d_0=\neg u_1\&u_0.$$

На наборах $000,111$ он принимает значение 000, на наборах $100,011$ – значение 010, на наборах $010,101$ – значение 001, на

наборах $001,110$ – значение 100. Рассмотрим оператор

$$a_2=d_2x_2\vee d_1x_0\vee d_0x_1,\ a_1=d_2x_1\vee d_1x_2\vee d_0x_0,$$

$$a_0=d_2x_0\vee d_1x_1\vee d_0x_2.$$

На наборах $000x_2x_1x_0$, $111x_2x_1x_0$ он принимает значение 000, на наборах $001x_2x_1x_0$, $110x_2x_1x_0$ – значение $x_2x_1x_0$, на наборах $010x_2x_1x_0$, $101x_2x_1x_0$ – значение $x_1x_0x_2$, $(x_1x_0x_2)_2=2(x_2x_1x_0)_2 \pmod 7$, на наборах $100x_2x_1x_0$, $011x_2x_1x_0$ – значение $x_0x_2x_1$, $(x_0x_2x_1)_2=4(x_2x_1x_0)_2 \pmod 7$. Тогда умножение чисел $(x_2x_1x_0)_2$, $(y_2y_1y_0)_2$ по модулю 7 реализуется оператором

$$z_2=a_2\oplus m,\ z_1=a_1\oplus m,\ z_0=a_0\oplus m.$$

Действительно, если $(y_2y_1y_0)_2=0$, то $m=0$ и он принимает значение $(000)_2=(000)_2\cdot(x_2x_1x_0)_2 \pmod 7$, если $(y_2y_1y_0)_2=7$, то $m=1$ и он принимает значение $(111)_2=7=0 \pmod 7=(111)_2\cdot(x_2x_1x_0)_2 \pmod 7$, если $(y_2y_1y_0)_2=a=1,2,4$, то $m=0$ и он принимает значение $a(x_2x_1x_0)_2 \pmod 7$, если $(y_2y_1y_0)_2=a=3,5,6$, то $-a \pmod 7=b=4,2,1$, $m=1$ и он принимает значение $-b(x_2x_1x_0)_2 \pmod 7=a(x_2x_1x_0)_2 \pmod 7$. Сложность схемы для оператора m,d_2,d_1,d_0 равна 7. Сложность схемы для оператора a_2,a_1,a_0 равна $15+7=22$, глубина равна 5. Сложность схемы для оператора z_2,z_1,z_0 равна $22+3=25$. Если в схеме для a_2,a_1,a_0 заменить $\vee$ на $\oplus$, то оператор z_2,z_1,z_0 можно реализовать формулами

$$z_2=(d_2x_2\oplus d_1x_0)\oplus(d_0x_1\oplus m),\ z_1=(d_2x_1\oplus d_1x_2)\oplus(d_0x_0\oplus m),$$

$$z_0=(d_2x_0\oplus d_1x_1)\oplus(d_0x_2\oplus m)$$

с той же сложностью 25.

Отождествим набор $(111)_2$ с набором $(000)_2$, так как $7=0 \pmod 7$.

Лемма. *Сложение в $GF(7)$ выполняется схемой сложности* 17.

Доказательство. Действительно, складываем два трёхзначных двоичных числа при помощи схемы, построенной по формулам 17.3 со сложностью 12, получаем сумму

$(\sigma, \varepsilon_2, \varepsilon_1, \varepsilon_0)_2$. Приведение по модулю $(\sigma, \varepsilon_2, \varepsilon_1, \varepsilon_0)_2 =$

$$= 2^3\sigma + (\varepsilon_2, \varepsilon_1, \varepsilon_0)_2 = (\varepsilon_2, \varepsilon_1, \varepsilon_0)_2 + \sigma = (z_2 z_1 z_0)_2 \pmod 7$$

по формулам (17.3) имеет сложность 5, так как при прибавлении однобитового числа формулы (17.3) приобретают вид

$$z_1 = x_1 + y_1,\ z_2 = x_2 + (x_1 y_1),\ z_3 = x_3 + x_2(x_1 y_1) \pmod 2.$$

Таким образом, схема сложения в $GF(7)$ имеет сложность 17. Лемма доказана.

Схемы для вычитания получаются путем навешивания отрицаний на биты, составляющие вычитаемое число. Поэтому сложность схемы для вычитания такая же, как у схемы сложения.

Умножение на $1, 2, 4$ бесплатно в $GF(7)$, так как бесплатно умножение на 2. В самом деле, умножение на 2 произвольного элемента в $GF(7)$ сводится к циклической перестановке двоичной записи этого элемента, действительно умножение на 2 представляется сдвигом двоичной записи влево, приписыванием нуля справа и приведением по модулю 7. Смена знака также бесплатна в этих полях, так как вместо сложения можно делать в соответствующих местах вычитание и наоборот, а сложение и вычитание имеют одинаковую схемную сложность в $GF(7)$. Поэтому умножение на любую константу из $GF(7)$ бесплатно в любом поле $GF(7^n)$.

Стандартная схема для умножения в поле $GF(7^2)$, основанная на формуле

$$(a + b\sigma)(c + d\sigma) = (ac - bd) + \sigma(ad + bc),$$

имеет сложность $4M(7) + 2A(7) = 134$, так как требуются 4 умножения и два сложения (вычитания) в поле $GF(7)$. Здесь $M(7)$ – схемная сложность умножения в поле $GF(7)$, $A(7)$ – схемная сложность сложения (вычитания) в поле $GF(7)$.

§ 21. Схемы для умножения в поле $GF(7^{14n})$

Используются следующие обозначения: $GF(q)$ – конечное поле порядка q, n – произвольное натуральное число, p – простое, $M(G)$ – схемная сложность умножения в поле G, $A(p)$ – сложность сложения в поле $GF(p)$, $M(p)$ – сложность умножения в поле $GF(p)$, $M(n)$ – сложность умножения многочленов степени, меньшей n, над $GF(7^2)$.

Теорема. *Умножение элементов поля $GF(7^{14n})$ может быть выполнено схемой сложности*

$$M(GF(7^{14n})) \leqslant 13M(GF(7^{2n})) + 258nA(7).$$

В частности, при $n = 31$

$$M(GF(7^{14\cdot 31})) \leqslant 698\ 554.$$

Доказательство. Построим схему для умножения двух многочленов шестой степени: $f_0 + f_1 x + \ldots + f_6 x^6$ и $g_0 + g_1 x + \ldots + g_6 x^6$ с коэффициентами из $GF(7^{2n})$ методом Тоома. Выберем узлы интерполяции: $0, \pm 1, \pm 2, \pm 3, \pm\sigma, \pm 2\sigma, \pm \pm 3\sigma$. Значения в узлах многочлена f представим следующим образом:

$f(0) = f_0,$
$f(1) = ((f_0 + {}_1 f_4) + {}_3(f_2 + {}_2 f_6)) + {}_6((f_1 + {}_4 f_5) + {}_5 f_3),$
$f(-1) = ((f_0 + f_4) + (f_2 + f_6)) - {}_7((f_1 + f_5) + f_3),$
$f(\sigma) = ((f_0 + f_4) - {}_8(f_2 + f_6)) + {}_{10}((f_1 + f_5) - {}_9 f_3)\sigma,$
$f(-\sigma) = ((f_0 + f_4) - (f_2 + f_6)) - {}_{11}((f_1 + f_5) - f_3)\sigma,$
$f(2) = ((f_0 + {}_{12}2f_4) + {}_{14}(4f_2 + {}_{13}f_6)) + {}_{17}((2f_1 + {}_{15}4f_5) + {}_{16}f_3),$
$f(-2) = ((f_0 + 2f_4) + (4f_2 + f_6)) - {}_{18}((2f_1 + 4f_5) + f_3),$
$f(2\sigma) = ((f_0 + 2f_4) - {}_{19}(4f_2 + f_6)) + {}_{21}((2f_1 + 4f_5) - {}_{20}f_3)\sigma,$
$f(-2\sigma) = ((f_0 + 2f_4) - (4f_2 + f_6)) - {}_{22}((2f_1 + 4f_5) - f_3)\sigma,$
$f(3) = f(-4) =$

$= ((f_0 + {}_{23}4f_4) + {}_{25}(2f_2 + {}_{24}f_6)) + {}_{28}((4f_1 + {}_{26}2f_5) - {}_{27}f_3),$

$f(-3) = f(4) = ((f_0 + 4f_4) + (2f_2 + f_6)) - {}_{29}((4f_1 + 2f_5) - f_3),$

$f(3\sigma) = f(-4\sigma) =$

$= ((f_0 + 4f_4) - {}_{30}(2f_2 + f_6)) + {}_{32}((4f_1 + 2f_5) + {}_{31}f_3)\sigma,$

$f(-3\sigma) = f(4\sigma) =$

$= ((f_0 + 4f_4) - (2f_2 + f_6)) - {}_{33}((4f_1 + 2f_5) + f_3)\sigma.$

Сложность этих вычислений, учитывая указанные скобками разбиения (порядок действий занумерован индексами), равна $33A(GF(7^{2n})) = 66nA(7)$. В этом равенстве учтено, что $A(GF(7^{2n})) = 2nA(7)$. Те же вычисления необходимо проделать и для многочлена g. Суммарная сложность их равна $132nA(7)$.

Найдём значения многочлена $h(x) = f(x) \cdot g(x)$, $h(x) = h_0 + h_1x + \cdots + h_{12}x^{12}$ в выбранных узлах a_j, $j = 0, \ldots, 12$. Сложность вычисления $h_j = h(a_j) = f(a_j)g(a_j)$, $j = 0, \ldots 12$ при $p = 7$ составляет

$$13(3M(GF(7^n)) + 4A(GF(7^n))) = 39M(GF(7^n)) + 52nA(7).$$

Оценим сложность схемы для интерполяции. Пусть

$$d_0 = -h(0),\ d_1 = -4h(1),\ d_2 = -4h(-1), \ldots,$$

$$d_{11} = -4h(3\sigma),\ d_{12} = -4h(-3\sigma).$$

Фундаментальные многочлены (после некоторой перестановки) есть

$-4x(x^4-4)(x^4-2)(x^2-1)(x+\sigma)h(\sigma),$

$-4x(x^4-4)(x^4-2)(x^2-1)(x-\sigma)h(-\sigma),$

$-(x^4-4)(x^4-2)(x^4-1)h(0) = -(x^8+x^4+1)(x^4-1)h(0),$

$-4x(x^8+x^4+1)(x^2+1)(x+1)h(1),$

$-4x(x^8+x^4+1)(x^2+1)(x-1)h(-1),$

$-4x(x^4-1)(x^4-4)(x^2+4)(x+2)h(2),$

$-4x(x^4-1)(x^4-4)(x^2+4)(x-2)h(-2),$

$-4x(x^4-1)(x^4-4)(x^2-4)(x+2\sigma)h(2\sigma),$

$-4x(x^4-1)(x^4-4)(x^2-4)(x-2\sigma)h(-2\sigma),$

$-4x(x^4-1)(x^4-2)(x^2-2)(x+4\sigma)h(3\sigma),$

$-4x(x^4-1)(x^4-2)(x^2-2)(x-4\sigma)h(-3\sigma),$

$-4x(x^4-1)(x^4-2)(x^2+2)(x+4)h(-3),$

$-4x(x^4-1)(x^4-2)(x^2+2)(x-4)h(3),$

так как для получения k-го фундаментального многочлена нужно из произведения $x(x-1)(x+1)(x-\sigma)(x+\sigma)\times$

$$\times(x-2)(x+2)(x-3)(x+3)(x-2\sigma)(x+2\sigma)(x-3\sigma)(x+3\sigma)$$

удалить $(x-k)$, $k = \pm1, \pm2, \pm3, \pm\sigma, \pm2\sigma, \pm3\sigma$, умножить оставшиеся скобки, результат умножить на $h(k)$ и разделить на значение от k полученного многочлена (оно равно -2, за исключением случая $k = 0$, где оно равно -1).

Вычисление коэффициентов многочлена $h(x)$ по его значениям в 13 узлах можно представить в следующем виде:

$h(x) = (x^8+x^4+1)^2[d_0(x^4-1) + {}^1x(x^2-1)(d_7(x+\sigma) + {}^2$

$+{}^2d_8(x-\sigma)) + {}^4 + {}^4x(x^2+1)(d_1(x+1) + {}^2d_2(x-1))] + {}^{12}$

$+{}^{12}x(x^4-1)^4[(x^4-2)((x^2-2)(d_{11}(x+4\sigma) + {}^2d_{12}(x-4\sigma)) + {}^4$

$+{}^4(x^2+2)(d_5(x+4) + {}^2d_6(x-4))) + {}^8$

$+{}^8(x^4-4)((x^2+4)(d_4(x-2) + {}^2$

$+{}^2d_3(x+2)) + {}^4(x^2-4)(d_9(x-2\sigma) + {}^2d_{10}(x+2\sigma)))].$

Индексы сверху над каждой операцией указывают ее сложность в виде $kA(GF(7^{2n}))$. Отсутствие индекса означает, что сложность равна нулю. Поэтому сложность этих вычислений равна

$$A(GF(7^{2n}))[(2+2+4+1)+1+1)+12+4+((2+2+4)\cdot2+8)] =$$

$$= 2nA(7) \cdot 51 = 102nA(7).$$

Суммируя полученные оценки, находим, что сложность умножения многочленов степени $\leqslant 6$ над $GF(7^{2n})$ есть

$$L = 132nA(7) + 13M(GF(7^{2n})) + 102nA(7) =$$

$$= 13M(GF(7^{2n})) + 234nA(7).$$

Приведение по модулю $x^7 - x + 2$ многочлена двенадцатой степени

$$d_0 + d_1x + \ldots + d_{12}x^{12} = c_0 + c_1x + \cdots + c_6x^6 \pmod{x^7 - x + 2}$$

выполняется по формулам $c_6 = d_6 + d_{12},\ c_5 = d_5 - 2d_{12} + d_{11},$

$$c_4 = d_4 - 2d_{11} + d_{10}, \ldots,\ c_1 = d_1 - 2d_8 + d_7,\ c_0 = d_0 - 2d_7.$$

Эти формулы содержат 12 сложений-вычитаний (в $GF(7^{2n})$) и 6 удвоений (а они бесплатны при схемной реализации). Таким образом, приведение по модулю $x^7 - x + 2$ имеет сложность $12A(GF(7^{2n})) = 24nA(7)$ и тогда, учитывая полученную оценку сложности умножения многочленов шестой степени с коэффициентами из $GF(7^{2n})$, имеем

$$M(GF(7^{14n})) = 13M(GF(7^{2n})) + 258nA(7).$$

Оценка для $n = 31$ вычисляется с учётом полученных далее оценок.

§ 22. Метод дискретного преобразования Фурье

Рассмотрим подробно дискретное преобразование Фурье (ДПФ) 16-го порядка. ДПФ n-го порядка будем обозначать F_n.

Пусть множители – многочлены 7-й степени над $GF(7^{2n})$. Коэффициенты каждого такого многочлена можно рассматривать как многочлены степени $(n-1)$ с коэффициентами из $GF(7^2)$.

Для простоты изложения рассмотрим вначале случай $n = 1$, то есть многочлены будем рассматривать с коэффициентами из $GF(7^2)$.

Произведение этих многочленов есть многочлен 14-й степени $h(x) = h_0 + h_1x + \cdots + h_{14}x^{14}$. Для нахождения его коэффициентов потребуется вычислить значения $h(x)$ в 15-ти различных точках, «узлах интерполяции». Узлами интерполяции выберем $w^k,\ k = \overline{0,15},\ w^{16} = 1,\ w = 2 + 4\sigma$

– первообразный корень из единицы порядка 16, σ – «мнимая единица» квадратичного расширения поля $GF(7)$, то есть поля $GF(7^2)$. Действительно,

$$(2 + 4\sigma)^2 = 4 + 16\sigma - 16 = -12 + 16\sigma = 2 + 2\sigma \pmod 7,$$

$$(2 + 4\sigma)^4 = ((2 + 4\sigma)^2)^2 = (2 + 2\sigma)^2 = 4 + 8\sigma - 4 = \sigma \pmod 7,$$

$$(2 + 4\sigma)^{16} = ((2 + 4\sigma)^4)^4 = \sigma^4 = 1 \pmod 7.$$

Вычисления будем производить в стандартном базисе $\{1, \sigma\}$.

Идея метода состоит в том, чтобы привести многочлены f и g по 16-ти различным линейным модулям вида $(x - w^k)$ к многочленам нулевой степени:

$$f(x) = f \pmod{x - w^k},\ g(x) = g \pmod{x - w^k},\ k = \overline{0,15}.$$

Тогда по теореме Безу́

$$f(w^k) = f \pmod{x - w^k},\ g(w^k) = g \pmod{x - w^k},\ k = \overline{0,15}.$$

Указанное приведение осуществляется в несколько шагов, которые схематично представляются в виде бинарного дерева. Это есть прямое ДПФ. Далее вычисляется $h(w^k) = f(w^k)g(w^k),\ k = \overline{0,15}$, и затем по полученным значениям $h(w^k),\ k = \overline{0,15}$, находятся коэффициенты многочлена 14-й степени $h(x)$ (обратное ДПФ).

Очевидно, $f_4 + f_5x + f_6x^2 + f_7x^3 \equiv f_4x^4 + f_5x^5 + f_6x^6 + f_7x^7 \pmod{x^4-1}$. Действительно, разность этих многочленов делится на $(x^4 - 1)$. Поэтому

$$\begin{aligned} &f_0 + f_1x + f_2x^2 + \cdots + f_7x^7 \pmod{x^4 - 1} = \\ &= (f_0 + f_1x + f_2x^2 + f_3x^3) + (f_4 + f_5x + f_6x^2 + f_7x^3) = \\ &= (f_0 + f_4) + (f_1 + f_5)x + (f_2 + f_6)x^2 + (f_3 + f_7)x^3. \end{aligned}$$

Аналогично, $f_4 + f_5x + f_6x^2 + f_7x^3 = -f_4x^4 - f_5x^5 - f_6x^6 - f_7x^7 \pmod{x^4+1}$. Действительно, разность этих многочленов делится на $(x^4 + 1)$. Поэтому

$$\begin{aligned} &f_0 + f_1x + f_2x^2 + \cdots + f_7x^7 \pmod{x^4 + 1} = \\ &= (f_0 + f_1x + f_2x^2 + f_3x^3) - (f_4 + f_5x + f_6x^2 + f_7x^3) = \\ &= (f_0 - f_4) + (f_1 - f_5)x + (f_2 - f_6)x^2 + (f_3 - f_7)x^3. \end{aligned}$$

Таким образом, для вычисления $f \pmod{x^4+1}$, $f \pmod{x^4-1}$ требуется 8 сложений или вычитаний в $GF(7^2)$. При этом из многочлена 7-й степени получаются многочлены 3-й степени. Аналогично,

$f_2x^2 + f_3x^3 = f_2 + f_3x \pmod{x^2-1}$, так как разность этих многочленов делится на (x^2-1);

$f_2x^2 + f_3x^3 = -(f_2 + f_3x) \pmod{x^2+1}$, так как разность этих многочленов делится на (x^2+1). Поэтому

$f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) + (f_2 + f_3x) \pmod{x^2-1} = (f_0 + f_2) + (f_1 + f_3)x$,

$f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) - (f_2 + f_3x) \pmod{x^2+1} = (f_0 - f_2) + (f_1 - f_3)x$.

Эти вычисления требуют 4 сложения или вычитания в $GF(7^2)$. При этом из многочлена третьей степени получаются многочлены первой степени. Аналогично,

$f_2x^2 + f_3x^3 = w^4(f_2 + f_3x) \pmod{x^2 - w^4}$, так как разность этих многочленов делится на $(x^2 - w^4)$;

$f_2x^2 + f_3x^3 = -w^4(f_2 + f_3x) \pmod{x^2+1}$, так как разность этих многочленов делится на (x^2+1). Поэтому

$f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) + w^4(f_2 + f_3x) \pmod{x^2-1} = (f_0 + f_2w^4) + (f_1 + f_3w^4)x$,

$f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) - w^4(f_2 + f_3x) \pmod{x^2+1} = (f_0 - f_2w^4) + (f_1 - f_3w^4)x$.

Эти вычисления требуют 4 сложения или вычитания в $GF(7^2)$, так как умножение на w^4 осуществляется в $GF(7^2)$ с нулевой сложностью. При этом из многочлена третьей степени получаются многочлены первой степени.

Вычисления делаются по схеме:

1)	f	$f \pmod{x^8-1}$	$f \pmod{x^8+1}$
2)	$f \pmod{x^8-1}$	$f \pmod{x^4-1}$	$f \pmod{x^4+1}$
3)	$f \pmod{x^4-1}$	$f \pmod{x^2-1}$	$f \pmod{x^2+1}$
	$f \pmod{x^4+1}$	$f \pmod{x^2-\omega^4}$	$f \pmod{x^2+\omega^4}$
4)	$f \pmod{x^2-1}$	$f \pmod{x+1}$	$f \pmod{x-1}$
	$f \pmod{x^2+1}$	$f \pmod{x-\omega^4}$	$f \pmod{x+\omega^4}$
	$f \pmod{x^2-\omega^4}$	$f \pmod{x-\omega^2}$	$f \pmod{x+\omega^2}$
	$f \pmod{x^2+\omega^4}$	$f \pmod{x-\omega^6}$	$f \pmod{x+\omega^6}$

«Вход» каждой следующей по номеру системы строк есть «выход» предыдущей системы строк, многочлен левой колонки, приведённый по указанному модулю, приводится к многочленам в правых колонках по указанным модулям, так что степени многочленов каждый раз понижаются, а сама схема представляет бинарное дерево. Сложность вычисления второй строки в этой схеме составляет $8A(GF(7^2))$. Сложность вычисления третьей серии двух строк составляет $4 + 4 = 8$ сложений или вычитаний в $GF(7^2)$.

В четвёртой серии указанной схемы вычислений, состоящей из четырёх строк, каждая из первых двух вычисляется со сложностью 2 сложения в $GF(7^2)$. Действительно, $f_0 + f_1x = f_0 + f_1 \pmod{x-1}$, так как разность этих многочленов есть $f_1(x-1)$, что делится на $(x-1)$. Аналогично, $f_0 + f_1x = f_0 - f_1 \pmod{x+1}$, $f_0 + f_1x = f_0 + f_1w^4 \pmod{x-w^4}$, $f_0 + f_1x = f_0 - f_1w^4 \pmod{x+w^4}$, а умножение элемента из $GF(7^2)$ на w^4 производится с нулевой сложностью.

Каждая из двух последних строк четвёртой серии вычисляется со сложностью 3 сложения или вычитания в $GF(7^2)$. Действительно, $f_0 + f_1x = f_0 + f_1w^2 \pmod{x - w^2}$, так как разность левого и правого многочленов есть $f_1(x - w^2)$, что делится на $(x - w^2)$. Но умножение f_1w^2 элемента f_1 из $GF(7^2)$ на w^2 производится со сложностью

$2A(7) = 1A(GF(7^2))$. Таким образом, данное приведение по модулю $(x - w^2)$ происходит со сложностью $2A(GF(7^2))$. При приведении $f_0+f_1x = f_0-f_1w^2 \pmod{x+w^2}$ можно сэкономить один функциональный элемент ввиду того, что умножение f_1w^2 уже выполнено ранее при приведении по модулю $(x - w^2)$. Таким образом, здесь требуется лишь одно вычитание в $GF(7^2)$, а сложность вычисления рассматриваемой строки схемы алгоритма составляет $3A(GF(7^2))$.

Для последней строки мы имеем: $f_0 + f_1x = f_0 + f_1w^6 \pmod{x - w^6}$, $f_0 + f_1x = f_0 - f_1w^6 \pmod{x + w^6}$. Умножение f_1w^6 имеет ту же сложность, что и умножение f_1w^2. Значит, сложность строки составляет $3A(GF(7^2))$.

Суммируя оценки, находим, что сложность вычислений по этой схеме составляет

$$26A(GF(7^2)) = 52A(7).$$

В общем случае при рассмотрении многочленов f и g с коэффициентами из $GF(7^{2n})$ сложность вычислений по указанной схеме составляет $52nA(7)$, ведь каждый коэффициент в таком случае есть многочлен $(n-1)$-й степени с n коэффициентами из $GF(7^2)$.

Далее производим вычисления по схеме, являющейся продолжением предыдущей, только что рассмотренной схемы, и составляющей вместе с ней общую схему вычислений:

2)	$f \pmod{x^8+1}$	$f \pmod{x^4-\omega^4}$	$f \pmod{x^4+\omega^4}$
3)	$f \pmod{x^4-\omega^4}$	$f \pmod{x^2-\omega^2}$	$f \pmod{x^2+\omega^2}$
	$f \pmod{x^4+\omega^4}$	$f \pmod{x^2-\omega^6}$	$f \pmod{x^2+\omega^6}$
4)	$f \pmod{x^2-\omega^2}$	$f \pmod{x+\omega}$	$f \pmod{x-\omega}$
	$f \pmod{x^2+\omega^2}$	$f \pmod{x-\omega^5}$	$f \pmod{x+\omega^5}$
	$f \pmod{x^2-\omega^6}$	$f \pmod{x-\omega^3}$	$f \pmod{x+\omega^3}$
	$f \pmod{x^2+\omega^6}$	$f \pmod{x-\omega^7}$	$f \pmod{x+\omega^7}$

Найдём сложность вычислений по этой схеме вначале для частного случая многочлена f с коэффициентами из $GF(7^2)$.

Строка 2). $f_4x^4 + f_5x^5 + f_6x^6 + f_7x^7 = w^4(f_4 + f_5x + f_6x^2 + f_7x^3) \pmod{x - w^4}$. Действительно, разность этих многочленов делится на $(x - w^4)$. Следовательно, $f_0 + f_1x + \cdots + f_7x^7 = (f_0+f_1x+f_2x^2+f_3x^3)+w^4(f_4+f_5x+f_6x^2+f_7x^3) \pmod{x-w^4} = (f_0+w^4f_4)+(f_1+w^4f_5)x+(f_2+w^4f_6)x^2+(f_3+w^4f_7)x^3$.

Как было показано ранее, умножение на w^4 производится с нулевой сложностью в $GF(7^2)$. Поэтому приведение по модулю $(x - w^4)$ требует $4A(GF(7^2))$ функциональных элементов.

Аналогично, приведение $f_0 + f_1x + \cdots + f_7x^7 = (f_0 + f_1x + f_2x^2 + f_3x^3) - w^4(f_4 + f_5x + f_6x^2 + f_7x^3) \pmod{x + w^4} = (f_0 - w^4f_4) + (f_1 - w^4f_5)x + (f_2 - w^4f_6)x^2 + (f_3 - w^4f_7)x^3$ имеет схемную сложность $4A(GF(7^2))$. Вычисление строки 2) указанной таблицы имеет таким образом схемную сложность $8A(GF(7^2))$.

Серия строк 3). $f_2x^2 + f_3x^3 = w^2(f_2 + f_3x) \pmod{x^2 - w^2}$, так как разность этих многочленов, очевидно, делится на $(x - w^2)$. Поэтому $f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) + w^2(f_2 + f_3x) \pmod{x^2 - w^2} = (f_0 + f_2w^2) + (f_1 + f_3w^2)x$. Аналогично $f_2x^2 + f_3x^3 = -w^2(f_2 + f_3x) \pmod{x^2 + w^2}$. Следовательно, $f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) - w^2(f_2 + f_3x) \pmod{x^2 + w^2} = (f_0 - f_2w^2) + (f_1 - f_3w^2)x$.

Умножение на w^2 в $GF(7^2)$ имеет сложность $1A(GF(7^2))$. Таким образом, приведение по модулю $(x^2 - w^2)$ имеет сложность $4A(Gf(7^2))$, а приведение по модулю $(x^2 + w^2)$ имеет сложность $2A(GF(7^2))$, так как произведения f_2w^2 и f_3w^2 оказываются уже вычисленными ранее при приведении по модулю $(x^2 - w^2)$. Таким образом, эта строка алгоритма имеет сложность $6A(GF(7^2))$.

$f_2x^2 + f_3x^3 = w^6(f_2 + f_3x) \pmod{x^2 - w^6}$. Следовательно, $f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) + w^6(f_2 + f_3x) \pmod{x^2 - w^6} = (f_0 + f_2w^6) + (f_1 + f_3w^6)x$.

$f_2x^2 + f_3x^3 = -w^6(f_2 + f_3x) \pmod{x^2 + w^6}$. Следовательно,

$f_0 + f_1x + f_2x^2 + f_3x^3 = (f_0 + f_1x) - w^6(f_2 + f_3x) \pmod{x^2 + w^6} = (f_0 - f_2w^6) + (f_1 - f_3w^6)x$.

Умножение на w^6 в $GF(7^2)$ имеет сложность $A(GF(7^2))$. Таким образом, указанное приведение по модулю $(x^2 - w^6)$ имеет сложность $4A(GF(7^2))$, а приведение по модулю $(x^2 + w^6)$ имеет сложность $2A(GF(7^2))$, так как произведения f_2w^6 и f_3w^6 оказываются уже вычисленными ранее. Таким образом, эта строка алгоритма имеет сложность $6A(Gf(7^2))$, а серия строк 3) имеет сложность $12A(GF(7^2))$.

Серия строк 4). $f_0 + f_1x = f_0 + f_1w \pmod{x - w}$, $f_0 + f_1x = f_0 - f_1w \pmod{x + w}$, $f_0 + f_1x = f_0 + f_1w^7 \pmod{x - w^7}$, $f_0 + f_1x = f_0 - f_1w^7 \pmod{x + w^7}$, $f_0 + f_1x = f_0 + f_1w^3 \pmod{x - w^3}$, $f_0 + f_1x = f_0 - f_1w^3 \pmod{x + w^3}$.

Так как умножение на w, w^3 и w^7 в $GF(7^2)$ имеет схемную сложность $A(GF(7^2))$, то сложность вычислений каждой строки этой серии составляет $3A(GF(7^2))$ – по $2A(GF(7^2))$ на каждое приведение двучлена по модулю $(x - w)$, $(x - w^7)$, $(x - w^3)$ и по $1A(GF(7^2))$ на каждое приведение двучлена по модулю $(x + w)$, $(x + w^7)$, $(x + w^3)$ ввиду экономии $1A(GF(7^2))$ на вычисленных к этому моменту f_1w, f_1w^7, f_1w^3. Сложность вычисления всех строк этой серии составляет таким образом $12A(GF(7^2))$.

Складывая оценки сложности, находим, что суммарная сложность вычислений по указанной схеме составляет $32A(GF(7^2)) = 64A(7)$. Если коэффициенты многочлена f берутся из $GF(7^{2n})$, то есть представляют собой многочлены степени $(n - 1)$ с n коэффициентами из $GF(7^2)$, сложность вычислений составляет $64nA(7)$.

Суммируя оценки сложности, находим окончательную оценку сложности вычислений по приведённым схемам в общем случае, то есть с коэффициентами f из $GF(7^{2n})$, а именно $116nA(7)$.

Проделанные для многочлена f вычисления означают, что получены следующие тождества: $f(x) = f \pmod{x - w^k}$, $k = \overline{0,15}$. По теореме Безу $f \pmod{x - w^k} = f(w^k)$, $k = \overline{0,15}$. Действительно, например, $f(1)$ получается следующим образом: $f = f_1 \pmod{x^8 - 1}$, $f_1 = f_2 \pmod{x^4 - 1}$, $f_2 = f_3 \pmod{x^2 - 1}$, $f_3 = f_4 \pmod{x - 1}$. Следовательно, $f = g_1(x^8 - 1) + f_1 = g_1(x^8 - 1) + g_2(x^4 - 1) + f_2 = g_1(x^8 - 1) + g_2(x^4 - 1) + g_3(x^2 - 1) + f_3 = g_1(x^8 - 1) + g_2(x^4 - 1) + g_3(x^2 - 1) + g_4(x - 1) + f_4$, где g_1, g_2, g_3, g_4 – некоторые многочлены. Но $g_1(x^8 - 1) + g_2(x^4 - 1) + g_3(x^2 - 1) + g_4(x - 1)$ делится на $(x - 1)$. Значит, $f \pmod{x - 1} = f_4 = f(1)$. Точно так же получаются все остальные значения $f(w^k)$. Пусть $f_3 = f_4 \pmod{x - w^k}$, $f_2 = f_3 \pmod{x^2 - w^{2k}}$, $f_1 = f_2 \pmod{x^4 - w^{4k}}$, $f = f_1 \pmod{x^8 - w^{8k}}$. Тогда $f = g_1(x^8 - w^{8k}) + f_1 = g_1(x^8 - w^{8k}) + g_2(x^4 - w^{4k}) + f_2 = g_1(x^8 - w^{8k}) + g_2(x^4 - w^{4k}) + g_3(x^2 - w^{2k}) + f_3 = g_1(x^8 - w^{8k}) + g_2(x^4 - w^{4k}) + g_3(x^2 - w^{2k}) + g_4(x - w^k) + f_4$, где g_1, g_2, g_3, g_4 – некоторые многочлены. Но многочлен $g_1(x^8 - w^{8k}) + g_2(x^4 - w^{4k}) + g_3(x^2 - w^{2k}) + g_4(x - w^k)$, очевидно, делится на $(x - w^k)$. Значит, $f \pmod{x - w^k} = f_4 = f(w^k)$, $k = \overline{0,15}$.

Таким образом, сложность вычисления $f(w^k)$, $g(w^k)$, $k = \overline{0,15}$ составляет $116nA(7) + 116nA(7) = 232nA(7)$. Вычисление значений $h(w^k) = f(w^k)g(w^k)$, $k = \overline{0,15}$ требует $16M(GF(7^{2n}))$ функциональных элементов. Таким образом, нахождение значений многочлена $h(x)$ 14-й степени, $h(x) = f(x)g(x)$, с коэффициентами из $GF(7^{2n})$ в шестнадцати различных точках при помощи двух ДПФ имеет оценку сложности $232nA(7) + 16M(GF(7^{2n}))$.

Найти коэффициенты многочлена $h(x)$ по его значениям в узлах w^k, $k = \overline{0,15}$, можно при помощи схемы ДПФ, читаемой в обратном порядке («обратное ДПФ»). Действительно, если $a + bx = a + bw^k \pmod{x - w^k} = c$, $a + bx = a - bw^k \pmod{x + w^k} = d$, то $a = (c + d)/2$, $b = (c - d)w^{-k}/2$. Коэффициенты a, b, c, d можно рассматривать как многочлены от y степени $(n - 1)$ над $GF(7^2)$, $x = y^n$. Мы видим, что обратное ДПФ

существует и имеет ту же сложность, что и прямое ДПФ (см. [16]).

Значит, сложность интерполяции $h(x)$ равна $116nA(7) + 32nA(7)$, и окончательная оценка сложности умножения многочленов 7-й степени с полиномиальными коэффициентами составляет

$$3 \cdot 116nA(7) + 32nA(7) + 16M(GF(7^{2n})) = \\ = 380nA(7) + 16M(GF(7^{2n})).$$

§ 23. Некоторые эффективные схемы умножения многочленов над полем $GF(7^2)$

Используем следующие обозначения: $M(fg)$ – схемная сложность умножения многочленов f и g, $A(fg)$ – сложность сложения многочленов f и g, $M_o(n)$ – сложность умножения многочленов n-й степени над $GF(7^2)$, $M(7^2)$ – сложность умножения в поле $GF(7^2)$, $A(7^2)$ – сложность сложения в этом поле.

Будем применять методы Карацубы, Тоома, Фурье и школьный, их композиции и модификации с целью найти оптимальный вариант.

Напомним, что метод Карацубы заключается в умножении двух многочленов f и g согласно тождеству

$$(f_0+f_1y)(g_0+g_1y) = f_1g_1y^2+((f_0+f_1)(g_0+g_1)-f_0g_0-f_1g_1)y+f_0g_0,$$

имеющему оценку сложности $M(fg) =$

$$= 2M(f_0g_0)+M(f_1g_1)+A(f_0g_0)+A(f_1g_1)+2A(f_0+f_1)+C, \quad (*)$$

где C – сложность приведения полученного многочлена к обычному виду (аналог переносов при умножении чисел), $\deg f_0 \geqslant \deg f_1$, $\deg g_0 \geqslant \deg g_1$, $\deg f_0 = \deg g_0$, $\deg f_1 = \deg g_1$.

Стандартная схема для умножения в поле $GF(7^2)$, основанная на формуле

$$(a + b\sigma)(c + d\sigma) = (ac - bd) + \sigma(ad + bc),$$

имеет сложность

$$M(GF(7^2)) = 4M(7) + 2A(7) = 4 \cdot 26 + 2 \cdot 17 = 138.$$

Умножение многочленов малых степеней

Умножение многочленов малых степеней служит для эффективного умножения многочленов более высоких степеней.

Многочлены 1-й степени. Умножим многочлены первой степени над $GF(7^2)$ школьным методом. Это умножение $fg = (f_0 + f_1y)(g_0 + g_1y)$ имеет оценку сложности

$$M(fg) = 4M(GF(7^2)) + 1 \cdot A(GF(7^2)) = \\ = 4 \cdot 138 + 1 \cdot 17 = 569.$$

Для умножения многочленов первой степени можно применить метод Карацубы. Тогда согласно $(*)$

$$M(fg) = 3M(GF(7^2)) + 4A(GF(7^2)) = 3 \cdot 138 + 8 \cdot 17 = 550.$$

Эта оценка лучше школьной.

Многочлены 2-й степени. Можно показать, что метод Тоома в этом случае лучше, чем метод Карацубы, но хуже школьного, а лучшим оказывается метод ДПФ. Метод ДПФ, как было показано, можно представить в виде бинарного поддерева в виде таблицы.

Таблица 1

3)	$h \pmod{x^4-1}$	$h \pmod{x^2-1}$	$h \pmod{x^2+1}$
	$h \pmod{x^4+1}$	$h \pmod{x^2-\omega^4}$	$h \pmod{x^2+\omega^4}$
4)	$h \pmod{x^2-1}$	$h \pmod{x+1}$	$h \pmod{x-1}$
	$h \pmod{x^2+1}$	$h \pmod{x-\omega^4}$	$h \pmod{x+\omega^4}$
	$h \pmod{x^2-\omega^4}$	$h \pmod{x-\omega^2}$	$h \pmod{x+\omega^2}$
	$h \pmod{x^2+\omega^4}$	$h \pmod{x-\omega^6}$	$h \pmod{x+\omega^6}$

Приведём сомножители – многочлены 2-й степени – по модулю $(x^2 - 1)$. Так как

$$f_0 + f_1x + f_2x^2 = (f_0 + f_2) + f_1x \pmod{x^2-1},$$

то эта операция имеет схемную сложность $2A(7^2)$ для двух сомножителей, где $A(7^2) = A(GF(7^2))$. Вместо поддерева таблицы 1 рассмотрим его поддерево, представленное таблицей 2, по которой произведём вычисления, как в ДПФ. Сложность вычислений по таблице 2 составляет (как было показано) $3 \cdot 2A(7^2) = 6A(7^2)$ и ещё 2 умножения в $GF(7^2)$.

Таблица 2

4)	$h \pmod{x^2-1}$	$h \pmod{x+1}$	$h \pmod{x-1}$

Произведением многочленов 2-й степени является многочлен 4-й степени $a_0+a_1x+\cdots+a_4x^4$. Его коэффициенты

$$a_0 = f_0g_0,\ a_4 = f_2g_2,\ a_1 = (f_0g_1 + f_1g_0)$$

находятся со сложностью $4M(7^2) + A(7^2)$, где f_i и g_i - соответствующие коэффициенты исходных сомножителей. Очевидно,

$$a_0 + a_1x + \cdots + a_4x^4 = (a_0 + a_4 + a_2) + (a_1 + a_3)x \pmod{x^2-1}.$$

В результате вычислений по таблице 2 становятся известны $(a_0 + a_4 + a_2)$, $(a_1 + a_3)$, откуда находим a_2 и a_3 со сложностью $3A(7^2)$. Суммируя оценки, находим сложность метода:

$$12A(7^2) + 6M(7^2) = 24A(7) + 6M(7^2) = 24 \cdot 17 + 6 \cdot 138 = 1236.$$

Многочлены 3-й степени. Можно показать, что самым лучшим в этом случае из методов Карацубы, Тоома, Фурье и школьного оказывается метод Фурье, некоторую модификацию которого рассмотрим.

Метод ДПФ для многочлена h 6-й степени, как было показано, можно представить в виде бинарного дерева в виде таблицы 1 (см. выше). Приведём сомножители – многочлены 3-й степени – по модулю (x^2-1) и по модулю (x^2+1). Так как

$$f_0 + f_1x + \cdots + f_3x^3 = (f_0 + f_2) + (f_1 + f_3)x \pmod{x^2-1},$$
$$f_0 + f_1x + \cdots + f_3x^3 = (f_0 - f_2) + (f_1 - f_3)x \pmod{x^2+1},$$

то эта операция имеет схемную сложность $2 \cdot 4A(7^2) = 8A(7^2)$.

Вместо поддерева таблицы 1 рассмотрим его поддерево, представленное следующей таблицей 3, по которой произведём

вычисления, как в ДПФ. Сложность этих вычислений составляет (как было показано) $3 \cdot 4A(7^2) + 4A(7^2) = 16A(7^2)$ и ещё 4 умножения в $GF(7^2)$.

Таблица 3

3)	h $\pmod{x^4-1}$	$h \pmod{x^2-1}$	$h \pmod{x^2+1}$
4)	$h \pmod{x^2-1}$	$h \pmod{x+1}$	$h \pmod{x-1}$
	$h \pmod{x^2+1}$	$h \pmod{x-\omega^4}$	$h \pmod{x+\omega^4}$

Произведением многочленов 3-й степени является многочлен 6-й степени $a_0+a_1x+\cdots+a_6x^6$. Его коэффициенты

$$a_0 = f_0g_0,\ a_6 = f_3g_3,\ a_1 = (f_0g_1 + f_1g_0)$$

находятся со сложностью $(4M(7^2) + A(7^2))$, где $M(7^2) = M(GF(7^2))$, а f_i и g_i – соответствующие коэффициенты исходных сомножителей. Очевидно,

$$a_0 + a_1x + \cdots + a_6x^6 =$$
$$= (a_0 + a_4) + (a_1 + a_5)x + (a_2 + a_6)x^2 + a_3x^3 \pmod{x^4-1}.$$

В результате вычислений по таблице 3 становятся известны $(a_0 + a_4)$, $(a_1 + a_5)$, $(a_2 + a_6)$, a_3, откуда находим a_4, a_5, a_2 со сложностью $3A(7^2)$. Суммируя оценки, находим сложность метода:

$$28A(7^2) + 8M(7^2) = 56A(7) + 8M(7^2) = 56 \cdot 17 + 8 \cdot 138 = 2\,056.$$

Умножение многочленов более высоких степеней. ДПФ 48-го порядка

Для умножения многочленов более высоких степеней рассмотрим ДПФ 48-го порядка F_{48}. В $GF(7^2)$ существует элемент ε такой, что $\varepsilon^3 = 1$; $\varepsilon = 2$, так как $2^3 = 1 \pmod 7$. Если w – первообразный корень из единицы порядка 16 в $GF(7^2)$ (все такие корни были указаны ранее), то $(\varepsilon w)^{48} = 1$ и никакая меньшая степень с натуральным показателем $(\varepsilon w)^k \neq 1$ ввиду взаимной простоты чисел 3 и 16. Поэтому εw – первообразный корень порядка 48 в $GF(7^2)$, и каждый

ненулевой элемент из $GF(7^2)$, а таких элементов ровно 48, представляется в виде $(\varepsilon w)^k$ для некоторого натурального $k \in \overline{1,48}$, единственного для данного элемента. Это даёт возможность применить ДПФ 48-го порядка F_{48}.

ДПФ 3-го порядка F_3 для трёхчлена $f = f_0 + f_1 x + f_2 x^2$ определяется равенствами

$$y_0 = f_0 + f_1 + f_2,$$

$$y_1 = f_0 + \varepsilon f_1 + \varepsilon^2 f_2,$$
$$y_2 = f_0 + \varepsilon^2 f_1 + \varepsilon^4 f_2.$$

В самом деле, по теореме Безу

$$f \pmod{x-1} = f(1),$$

$$f \pmod{x-\varepsilon} = f(\varepsilon),\ f \pmod{x-\varepsilon^2} = f(\varepsilon^2).$$

Решая систему указанных уравнений относительно $f_0,\ f_1,\ f_2$, находим равенства, определяющие обратное ДПФ F_3 :

$$f_2 = \frac{1}{1-\varepsilon^2}\left(\frac{y_0 - y_1}{1-\varepsilon} - \frac{y_1 - y_2}{\varepsilon - \varepsilon^2}\right),$$
$$f_1 = \frac{y_0 - y_1}{1-\varepsilon} - (1+\varepsilon) f_2,$$
$$f_0 = y_0 - \varepsilon f_1 - \varepsilon^2 f_2.$$

Отсюда видно, что как прямое, так и обратное ДПФ F_3 имеют сложность $6A(7^2)$ для $GF(7^2)$, так как умножения и деления на $\pm 1,\ \pm 2,\ \pm 3,\ \pm 4$ происходят с нулевой сложностью. Если же $f_0,\ f_1,\ f_2$ – многочлены степени $(n-1)$ над $GF(7^2)$, то прямое и обратное ДПФ F_3 имеют сложность $6A(7^{2n}) = 6nA(7^2)$. Рассмотрим F_{48}. Многочлен 47-й степени представим в виде $f(y) = f_0 + f_1 y + f_2 y^2$, $y = x^{16}$, $f_0 = a_0 + a_1 x + \cdots + a_{15} x^{15}$, $f_1 = = a_{16} + a_{17} x + \cdots + a_{31} x^{15}$, $f_2 = a_{32} + a_{33} x + \cdots + a_{47} x^{15}$ и выполним F_3 над кольцом. F_3 можно схематично представить в виде таблицы 0. Сложность вычислений по таблице 0 составляет $16 \cdot 6A(7^2) = 96A(7^2)$. Далее выполняются три ДПФ F_{16}, каждое из которых представим в виде пары таблиц.

Таблица 1.1

1)	$h \pmod{x^{16}-1}$	$\to$	$h \pmod{x^8-1}$	
2)	$h \pmod{x^8-1}$	$\to$	$h \pmod{x^4-1}$	$h \pmod{x^4+1}$
3)	$h \pmod{x^4-1}$	$\to$	$h \pmod{x^2-1}$	$h \pmod{x^2+1}$
	$h \pmod{x^4+1}$	$\to$	h $\pmod{x^2-\omega^4}$	$h \pmod{x^2+\omega^4}$
4)	$h \pmod{x^2-1}$	$\to$	$h \pmod{x+1}$	$h \pmod{x-1}$
	$h \pmod{x^2+1}$	$\to$	$h \pmod{x-\omega^4}$	$h \pmod{x+\omega^4}$
	$h \pmod{x^2-\omega^4}$	$\to$	$h \pmod{x-\omega^2}$	$h \pmod{x+\omega^2}$
	$h \pmod{x^2+\omega^4}$	$\to$	$h \pmod{x-\omega^6}$	$h \pmod{x+\omega^6}$

Таблица 1.2

1)	$h \pmod{x^{16}-1}$	$\to$	$f \pmod{x^8+1}$	
2)	$h \pmod{x^8+1}$	$\to$	$h \pmod{x^4-\omega^4}$	$h \pmod{x^4+\omega^4}$
3)	$h \pmod{x^4-\omega^4}$	$\to$	$h \pmod{x^2-\omega^2}$	$h \pmod{x^2+\omega^2}$
	$h \pmod{x^4+\omega^4}$	$\to$	$h \pmod{x^2-\omega^6}$	$h \pmod{x^2+\omega^6}$
4)	$h \pmod{x^2-\omega^2}$	$\to$	$h \pmod{x+\omega}$	$h \pmod{x-\omega}$
	$h \pmod{x^2+\omega^2}$	$\to$	$h \pmod{x-\omega^5}$	$h \pmod{x+\omega^5}$
	$h \pmod{x^2-\omega^6}$	$\to$	$h \pmod{x-\omega^3}$	$h \pmod{x+\omega^3}$
	$h \pmod{x^2+\omega^6}$	$\to$	$h \pmod{x-\omega^7}$	$h \pmod{x+\omega^7}$

Таблица 2.1

1)	$h \pmod{x^{16}-2}$	$\to$	$h \pmod{x^8-4}$	
2)	$h \pmod{x^8-4}$	$\to$	$h \pmod{x^4-2}$	$h \pmod{x^4+2}$
3)	$h \pmod{x^4-2}$	$\to$	$h \pmod{x^2-4}$	$h \pmod{x^2+4}$
	$h \pmod{x^4+2}$	$\to$	$h \pmod{x^2-4\omega^4}$	$h \pmod{x^2+4\omega^4}$
4)	$h \pmod{x^2-4}$	$\to$	$h \pmod{x-2}$	$h \pmod{x+2}$
	$h \pmod{x^2+4}$	$\to$	$h \pmod{x-2\omega^4}$	$h \pmod{x+2\omega^4}$
	$h \pmod{x^2-4\omega^4}$	$\to$	$h \pmod{x-2\omega^2}$	$h \pmod{x+2\omega^2}$
	$h \pmod{x^2+4\omega^4}$	$\to$	$h \pmod{x-2\omega^6}$	$h \pmod{x+2\omega^6}$

Таблица 2.2

1)	$h \pmod{x^{16}-2}$	$\to$	$f \pmod{x^8+4}$	
2)	$h \pmod{x^8+4}$	$\to$	$h \pmod{x^4-2\omega^4}$	$h \pmod{x^4+2\omega^4}$
3)	$h \pmod{x^4-2\omega^4}$	$\to$	$h \pmod{x^2-4\omega^2}$	$h \pmod{x^2+4\omega^2}$
	$h \pmod{x^4+2\omega^4}$	$\to$	$h \pmod{x^2-4\omega^6}$	$h \pmod{x^2+4\omega^6}$
4)	$h \pmod{x^2-4\omega^2}$	$\to$	$h \pmod{x+2\omega}$	$h \pmod{x-2\omega}$
	$h \pmod{x^2+4\omega^2}$	$\to$	$h \pmod{x-2\omega^5}$	$h \pmod{x+2\omega^5}$
	$h \pmod{x^2-4\omega^6}$	$\to$	$h \pmod{x-2\omega^3}$	$h \pmod{x+2\omega^3}$
	$h \pmod{x^2+4\omega^6}$	$\to$	$h \pmod{x-2\omega^7}$	$h \pmod{x+2\omega^7}$

Таблица 3.1

1)	$h \pmod{x^{16}-4}$	$\to$	$h \pmod{x^8-2}$	
2)	$h \pmod{x^8-2}$	$\to$	$h \pmod{x^4-4}$	$h \pmod{x^4+4}$
3)	$h \pmod{x^4-4}$	$\to$	$h \pmod{x^2-2}$	$h \pmod{x^2+2}$
	$h \pmod{x^4+4}$	$\to$	$h \pmod{x^2-2\omega^4}$	$h \pmod{x^2+2\omega^4}$
4)	$h \pmod{x^2-2}$	$\to$	$h \pmod{x+4}$	$h \pmod{x-4}$
	$h \pmod{x^2+2}$	$\to$	$h \pmod{x-4\omega^4}$	$h \pmod{x+4\omega^4}$
	$h \pmod{x^2-2\omega^4}$	$\to$	$h \pmod{x-4\omega^2}$	$h \pmod{x+4\omega^2}$
	$h \pmod{x^2+2\omega^4}$	$\to$	$h \pmod{x-4\omega^6}$	$h \pmod{x+4\omega^6}$

Таблица 3.2

1)	$h \pmod{x^{16}-4}$	$\to$	$f \pmod{x^8+2}$	
2)	$h \pmod{x^8+2}$	$\to$	$h \pmod{x^4-4\omega^4}$	$h \pmod{x^4+4\omega^4}$
3)	$h \pmod{x^4-4\omega^4}$	$\to$	$h \pmod{x^2-2\omega^2}$	$h \pmod{x^2+2\omega^2}$
	$h \pmod{x^4+4\omega^4}$	$\to$	$h \pmod{x^2-2\omega^6}$	$h \pmod{x^2+2\omega^6}$
4)	$h \pmod{x^2-2\omega^2}$	$\to$	$h \pmod{x+4\omega}$	$h \pmod{x-4\omega}$
	$h \pmod{x^2+2\omega^2}$	$\to$	$h \pmod{x-4\omega^5}$	$h \pmod{x+4\omega^5}$
	$h \pmod{x^2-2\omega^6}$	$\to$	$h \pmod{x-4\omega^3}$	$h \pmod{x+4\omega^3}$
	$h \pmod{x^2+2\omega^6}$	$\to$	$h \pmod{x-4\omega^7}$	$h \pmod{x+4\omega^7}$

Таблица 0

$h \to$	$h \pmod{x^{16}-1}$	$h \pmod{x^{16}-2}$	$h \pmod{x^{16}-4}$

Так как умножение на 2 и на 4 имеет нулевую сложность в $GF(7^2)$, то все указанные пары деревьев имеют одинаковую сложность, такую, как у обычного F_{16}, представленного таблицами 1.1 и 1.2, равную, как было показано, $74A(7^2) + 16M(7^2)$. Таким образом, сложность вычислений трёх ДПФ F_{16} составляет

$$3 \cdot (74A(7^2) + 16M(7^2)) = 222A(7^2) + 48M(7^2),$$

а сложность полного ДПФ F_{48} составляет

$$96A(7^2) + 222A(7^2) + 48M(7^2) = 318A(7^2) + 48M(7^2).$$

Многочлены 24-й степени. Приведём каждый из сомножителей, многочленов 24-й степени над $GF(7^2)$, по модулю $(x^{16}-1)$, $(x^{16}-2)$, $(x^{16}-4)$, произведём ДПФ и обратное ДПФ F_{48} по полной схеме. Эти операции имеют сложность

$$2 \cdot 27A(7^2) + 3 \cdot (74 \cdot 3)A(7^2) + 96A(7^2) + 48M(7^2) =$$

$$= 816A(7^2) + 48M(7^2).$$

Произведением многочленов 24-й степени является многочлен 48-й степени вида $a_0 + a_1x + \cdots + a_{48}x^{48}$. Очевидно, $a_0 + a_1x + \cdots + a_{48}x^{48} = (a_0 + a_{48}) + a_1x + \cdots + a_{47}x^{47} \pmod{x^{48}-1} = b_0 + b_1x + \cdots + b_{47}x^{47}$. В результате вычислений стали известны коэффициенты b_i, $i = 0, \ldots, 47$, откуда a_0 и a_{48} находятся со сложностью $M(7^2) + A(7^2)$. Суммируя оценки, находим сложность метода умножения многочленов 24-й степени:

$$49M(7^2) + 817A(7^2) = 49 \cdot 138 + 817 \cdot 34 = 34\ 540.$$

Многочлены 30-й степени. Приведём каждый из сомножителей, многочленов 30-й степени над $GF(7^2)$, по

модулю $(x^{16}-1)$, $(x^{16}-2)$, $(x^{16}-4)$, произведём ДПФ и обратное ДПФ F_{48}. Эти операции имеют сложность

$$2\cdot(15+15+15)A(7^2)+3\cdot 222A(7^2)+96A(7^2)+48M(7^2)=$$
$$=852A(7^2)+48M(7^2).$$

Произведением многочленов 30-й степени является многочлен 60-й степени вида $a_0+a_1x+\cdots+a_{60}x^{60}$. Очевидно, $a_0+a_1x+\cdots+a_{60}x^{60}=(a_0+a_{48})+(a_1+a_{49})x+\cdots+(a_{12}+$ $+a_{60})x^{12}+\cdots+a_{47}x^{47} \pmod{x^{48}-1}=b_0+b_1x+\cdots+b_{47}x^{47}$. В результате вычислений становятся известны коэффициенты $b_i,\ i=0,\ \ldots,47$, откуда, зная $a_i,\ i=0,\ \ldots,5$ и $a_j,\ j=$ $=\ 54,\ \ldots,60$, можно найти остальные коэффициенты $a_k,\ k=6,\ldots,53$ со сложностью $13A(7^2)$.

Найти коэффициенты

$$a_0=f_0g_0,\ a_1=(f_0g_1+f_1g_0),\ a_2=(f_0g_2+f_1g_1+f_2g_0),\ \ldots,a_5$$

всё равно, что умножить многочлены $(f_0+f_1x+\cdots+f_5x^5)(g_0+$ $+g_1x+\cdots+g_5x^5)$ и взять первые 6 коэффициентов результата умножения, начиная со свободного члена.

Для умножения многочленов 5-й степени по модулю x^6 поступим следующим образом:

$$(f_0+f_1x+\cdots+f_5x^5)(g_0+g_1x+\cdots+g_5x^5) \pmod{x^6}=$$
$$=(f_0+f_1x+f_2x^2)(g_0+g_1x+g_2x^2)+$$
$$+[(f_0+f_1x+f_2x^2)(g_3+g_4x+g_5x^2)+$$
$$+(f_3+f_4x+f_5x^2)(g_0+g_1x+g_2x^2) \pmod{x^3}]x^3,$$

$$(f_0+f_1x+f_2x^2)(g_0+g_1x+g_2x^2) \pmod{x^3}=$$
$$=(f_0+f_1x)(g_0+g_1x)+$$
$$+[(f_0+f_1x)g_2+(g_0+g_1x)f_2 \pmod{x}]x^2=$$
$$=(f_0+f_1x)(g_0+g_1x)+(f_0g_2+g_0f_2)x^2,$$

откуда видно, что сложность умножения многочленов 5-й

степени по модулю x^6 составляет

$$M_o(2)+5A(7^2)+2(M_o(1)+2M(7^2)+2A(7^2))=$$
$$=M_o(2)+2M_o(1)+4M(7^2)+9A(7^2)=(6M(7^2)+12A(7^2))+$$
$$+2(3M(7^2)+4A(7^2))+4M(7^2)+9A(7^2)=16M(7^2)+29A(7^2).$$

Аналогично, найти коэффициенты $a_i,\ i=54,\ \ldots,60$ (их семь) всё равно, что умножить многочлены 6-й степени и взять первые 7 коэффициентов результата умножения, начиная со свободного члена.

Для умножения многочленов 6-й степени по модулю x^7 поступим следующим образом:

$$(f_0+f_1x+\cdots+f_6x^6)(g_0+g_1x+\cdots+g_6x^6) \pmod{x^7}=$$
$$=(f_0+f_1x+f_2x^2+f_3x^3)(g_0+g_1x+g_2x^2+g_3x^3)+$$
$$+[(f_0+f_1x+f_2x^2+f_3x^3)(g_4+g_5x+g_6x^2)+$$
$$+(f_4+f_5x+f_6x^2)(g_0+g_1x+g_2x^2+g_3x^3) \pmod{x^3}]x^4,$$

$$(f_0+f_1x+f_2x^2+f_3x^3)(g_0+g_1x+g_2x^2) \pmod{x^3}=$$
$$=(f_0+f_1x+f_2x^2)(g_0+g_1x+g_2x^2)=$$
$$=(f_0+f_1x)(g_0+g_1x)+$$
$$+[(f_0+f_1x)g_2+(g_0+g_1x)f_0 \pmod{x}]x^2=$$
$$=(f_0+f_1x)(g_0+g_1x)+[(f_0g_2+g_0f_0]x^2,$$

откуда видно, что сложность умножения многочленов 6-й степени по модулю x^7 составляет

$$M_o(3)+6A(7^2)+2(M_o(1)+2A(7^2)+2M(7^2))=$$
$$=M_o(3)+2M_o(1)+4M(7^2)+10A(7^2)=$$
$$=(8M(7^2)+28A(7^2))+2(3M(7^2)+4A(7^2))+4M(7^2)+$$
$$+10A(7^2)=18M(7^2)+46A(7^2).$$

Суммируя оценки, находим сложность метода умножения многочленов 30-й степени:

$$82M(7^2)+940A(7^2)=82\cdot 138+940\cdot 34=43\ 276.$$

Теорема. *Умножение в поле* $GF(7^{14\cdot 31})$ *имеет оценку сложности*

$$M(GF(7^{14\cdot 31})) \leqslant 698\ 554.$$

Доказательство. $M(GF(7^{14n})) \leqslant$

$$\leqslant 13M(GF(7^{2n})) + 129nA(7^2) = 13M(GF(7^{2n})) + 4386n.$$

Эта оценка была получена при рассмотрении умножения многочленов 6-й степени над $GF(7^2)$ методом Тоома. Ровно такая же оценка сложности получается с помощью метода ДПФ, но ухудшается глубина схемы.

Подставляя в указанную оценку $n = 31$ и полагая $M(GF(7^{2n})) = M_o(30)$, находим, что

$$M(GF(7^{14\cdot 31})) \leqslant 13M_o(30) + 129 \cdot 31A(7^2) =$$
$$= 13 \cdot (82M(7^2) + 940A(7^2)) + 129 \cdot 31A(7^2) =$$
$$= 1066M(7^2) + 16219A(7^2) = 1066 \cdot 138 + 16219 \cdot 34 = 698\ 554.$$

Этот результат касается арифметики в поле $GF(7^{14\cdot 31})$ и применим в криптографии, так как порядок алгебраического поля $GF(7^{14\cdot 31})$ приблизительно равен 2^{1000}, что обеспечивает необходимый уровень криптографической надёжности согласно современным стандартам.

Можно рассмотреть алгоритмы умножения для многочленов других степеней. В правой колонке следующей таблицы 4 указано условное название наилучшего алгоритма умножения (при поиске такого алгоритма рассматривались, кроме стандартного, методы Тоома, Карацубы, метод, основанный на применении ДПФ, а также их композиции и модификации). $M_o(n \times m)$ обозначает сложность умножения многочленов степени n и m над $GF(7^2)$.

Можно получить оценку сложности умножения многочленов 49-й степени:

$$M_o(49) \leqslant 94\ 984, \quad \text{ДПФ},$$

и оценку сложности умножения многочленов 47-й степени:

$$M_o(47) \leqslant 95\ 826, \quad \text{ДПФ}.$$

Асимптотические оценки умножения n-членов

Опираясь на полученные результаты, можно получить асимптотические оценки умножения многочленов степени $(n-1)$ над $GF(7^2)$, причём, как показывают непосредственные вычисления, наилучшие асимптотические оценки получаются при использовании умножения многочленов 24-й степени: именно при умножении многочленов 24-й степени максимально реализуются возможности ДПФ 48-го порядка F_{48} и алгебраического поля $GF(7^2)$, мультипликативная группа которого имеет также 48-й порядок.

Теорема. *Многочлены степени* $n-1$ *над* $GF(7^2)$ *могут быть умножены со сложностью* $M(n) \lesssim \frac{12\ 443}{8}\, n^{\log_5 7}$ *при* $n = 25^s$, *в случае произвольного* n, $M(n) \lesssim \frac{609\ 707}{8}\, n^{\log_5 7}$.

Доказательство. Пусть $M(7^{2n}) = M(n)$ – сложность умножения многочленов степени $n-1$ над $GF(7^2)$, а $A(7^{2n})$ – сложность их сложения. Следуя указанному выше способу умножения многочленов 24-й степени, имеем

$$M(25n) = 49M(7^{2n}) + 319A(7^{2(2n-1)}) + 498A(7^{2n}) + C =$$
$$= 49M(7^{2n}) + 319(2n-1)A(7^2) + 498nA(7^2) + C =$$
$$= 49M(n) + (1136n - 319)A(7^2) + C =$$
$$= 49M(n) + 40256n - 12478,$$

где $C = 48(n-1)A(7^2)$ – сложность приведения полученного многочлена к обычному виду – аналог переносов при умножении целых чисел. Таким образом,

$$M(n) \leqslant 49M\left(\tfrac{n}{25}\right) + 40256\tfrac{n}{25} - 12478,\ n = 25^s,$$
$$M(n) \leqslant 49^k M\left(\tfrac{n}{25^k}\right) + 40256\left(\tfrac{n}{25} + \tfrac{49n}{25^2} + \cdots + \tfrac{49^{k-1}n}{25^k}\right) -$$
$$-12478\left(1 + 49 + 49^2 + \cdots + 49^{k-1}\right),$$
$$M(n) \leqslant 49^k M\left(\tfrac{n}{25^k}\right) + \tfrac{5032n}{3}\left(\left(\tfrac{49}{25}\right)^k - 1\right) - \tfrac{6239}{24}\left(49^k - 1\right).$$

При $k = s$, $n = 25^s$ имеем

$$M(25^s) \leqslant 49^s M(GF(7^2)) + \tfrac{5032}{3}\left(49^s - 25^s\right) - \tfrac{6239}{24}49^s + \tfrac{6239}{24},$$
$$M(25^s) \leqslant 49^s \left(M(GF(7^2)) + \tfrac{5032}{3} - \tfrac{6239}{24}\right) - \tfrac{5032}{3}25^s + \tfrac{6239}{24},$$
$$M(n) \leqslant \left(M(GF(7^2)) + \tfrac{11339}{8}\right) n^{\log_{25} 49} - \tfrac{5032}{3}n + \tfrac{6239}{24}.$$

Полагая $M(GF(7^2)) = 138$, имеем

$$M(n) \leqslant \left(\tfrac{12443}{8}\right) n^{\log_5 7} - \tfrac{5032}{3}n + \tfrac{6239}{24},$$
$$M(n) \lesssim \left(\tfrac{12443}{8}\right) n^{\log_5 7}.$$

Для каждого натурального n, начиная с некоторого, найдётся такое натуральное число s, что $25^s < n \leqslant 25^{s+1}$. Следовательно, $\frac{n}{25} \leqslant 25^s < n \leqslant 25^{s+1} = 25 \cdot 25^s < 25n$, и полученные оценки, таким образом, переписываются в виде

$$M(n) \leqslant \left(\tfrac{12443}{8}\right)(25n)^{\log_5 7} - \tfrac{5032}{3\cdot 25}n + \tfrac{6239}{24} =$$
$$= \left(\tfrac{609707}{8}\right) n^{\log_5 7} - \tfrac{5032}{75}n + \tfrac{6239}{24},$$
$$M(n) \lesssim \left(\tfrac{609707}{8}\right) n^{\log_5 7}.$$

Теорема доказана.

Таблица 4.1

$M_o(0) =$	$M(7^2)$	$=$	138	
$M_o(1) =$	$3M(7^2) +$	$4A(7^2) =$	550	Карацуба
$M_o(2) =$	$6M(7^2) +$	$12A(7^2) =$	1236	ДПФ
$M_o(3) =$	$8M(7^2) +$	$28A(7^2) =$	2056	ДПФ
$M_o(4) =$	$12M(7^2) +$	$38A(7^2) =$	2948	ДПФ
$M_o(5) =$	$12M(7^2) +$	$74A(7^2) =$	4172	ДПФ
$M_o(6) =$	$16M(7^2) +$	$86A(7^2) =$	5132	ДПФ
$M_o(7) =$	$22M(7^2) +$	$100A(7^2) =$	6436	ДПФ
$M_o(8) =$	$20M(7^2) +$	$154A(7^2) =$	7996	ДПФ
$M_o(11) =$	$30M(7^2) +$	$228A(7^2) =$	11 892	ДПФ

Таблица 4.2

$M_o(12) =$	$37M(7^2) +$	$246A(7^2) =$	13 470	ДПФ
$M_o(6\times 3) =$	$10M(7^2) +$	$67A(7^2) =$	3 658	ДПФ
$M_o(6\times 4) =$	$10M(7^2) +$	$73A(7^2) =$	3 862	ДПФ
$M_o(15) =$	$38M(7^2) +$	$369A(7^2) =$	17 790	ДПФ
$M_o(22) =$	$66M(7^2) +$	$605A(7^2) =$	29 678	ДПФ
$M_o(23) =$	$76M(7^2) +$	$637A(7^2) =$	32 146	ДПФ
$M_o(24) =$	$49M(7^2) +$	$817A(7^2) =$	34 540	ДПФ
$M_o(25) =$	$52M(7^2) +$	$826A(7^2) =$	35 260	ДПФ
$M_o(30) =$	$82M(7^2) +$	$940A(7^2) =$	43 276	ДПФ
$M_o(31) =$	$92M(7^2) +$	$972A(7^2) =$	45 744	ДПФ

ГЛАВА 5

УМНОЖЕНИЕ В БАШНЯХ КОНЕЧНЫХ ПОЛЕЙ

В этой главе доказывается, что для любого $\varepsilon > 0$ при любом m, $n = m^s$ и $s \geqslant s_\varepsilon$ можно выбрать в поле $GF(2^n)$ базис, для которого схемная сложность умножения меньше $n^{1+\varepsilon/2}$, а сложность инвертирования меньше $n^{1+\varepsilon}$. При $n = 2 \cdot 3^k$ для некоторого базиса получаются для умножения оценки сложности $n(\log_3 n)^{(\log_2 \log_3 n)/2+O(1)}$, и по порядку такие же оценки получаются для инвертирования.

Известно (см. [1], [2]), что при использовании стандартных базисов в полях $GF(2^n)$ сложность булевой схемы для умножения, построенной из двухвходовых элементов, равна $O(n \log n \log\log n)$. Для инвертирования (т.е вычисления мультипликативного обратного в данном поле) известен быстрый алгоритм Евклида с оценкой сложности $O(n \log^2 n \log\log n)$ (см. [1], [3]). Однако мультипликативная константа в этой оценке велика (несколько сотен), и при реальных значениях n стандартный алгоритм Евклида работает быстрее. Кроме того, этот алгоритм затруднительно применить при построении булевой схемы для инвертирования. Методом [4] можно построить такую схему сложности $I(n) = O(n^{(\omega+1)/2} \log_2 n)$, где ω – экспонента матричного умножения. Однако величина мультипликативной константы здесь с трудом поддается оценке, также трудно оценить глубину этой схемы. Используя [5], можно построить схему для инвертирования глубины $O(\log_2^2 n)$ и сложности $O(n^{\log_2 \sqrt{14}} (\log_2 n)^{\log_2 8/7})$, где мультипликативные константы сравнительно невелики, но и эта схема при реальных значениях n представляется неэффективной.

При использовании в поле $GF(2^n)$ нормального базиса можно построить схему для умножения сложности $O(n^2/\log n)$ (см. [6]). Если для инвертирования применить метод [7] (основанный на методе Шольца–Брауэра для вычисления

$2^n - 1$ аддитивными цепочками [13]), то можно построить схему сложности $O(M_N(n) \log n) = O(n^2)$ с небольшой мультипликативной константой в оценке, где $M_N(n)$ – сложность умножения в данном базисе. Для некоторых специальных нормальных базисов (существующих не при всех n) можно построить более эффективные схемы для умножения и, как следствие, для инвертирования. В [6] показано, что для оптимальных нормальных базисов первого типа можно построить мультиплер сложности $M(n) + O(n)$, где $M(n)$ – сложность умножения двоичных многочленов степени $n - 1$. Для оптимальных нормальных базисов второго типа в [6] указана оценка $3M(n)) + \frac{3n}{2} \log_2 n + O(n)$. В [6] также показано, что если $n = mk$, $m, k \geqslant n^C, C \leqslant 1/2$, $(m, k) = 1$, то для некоторого нормального базиса сложность умножения равна $O(n(m+k)/\log n) = O(n^{2-C}/\log n)$, откуда следует, что если n – достаточно гладкое число, то для некоторого нормального базиса сложность умножения равна $O(n^{2-C})$ при $C > 0$, характеризующем гладкость числа n. В [4] доказано, что для гауссовых нормальных базисов типа k в поле $GF(2^n)$ сложность умножения равна $O(M(nk))$, а в [8] подобный результат получен в более общем случае.

§ 24. Схемы в поле $GF(2^n)$ при $n = m^s$

К упомянутым результатам можно добавить также следующие.

Теорема 1. *Для любого $\varepsilon > 0$ при любом m для $n = m^s$ и $s \geqslant s_\varepsilon$ можно указать в поле $GF(2^n)$ базис (не стандартный и не нормальный), для которого можно построить схему умножения сложности $M(m^s) < n^{1+\varepsilon/2}$ и схему инвертирования сложности $I(m^s) < n^{1+\varepsilon}$.*

Доказательство. Пусть $k < s$ параметр, значение которого укажем позднее. Выберем наименьшее r такое, что

$2^{m^r} \geqslant 2m^k - 1$ и $r = s \bmod k$. Тогда $r = O(k)$. Поле

$$GF\left(2^{m^s}\right) = GF\left(q^{m^{s-r}}\right) = GF\left(q^{m^{kl}}\right), q = 2^{m^r}$$

представим в виде башни расширений

$$GF(q) \subset GF\left(q^{m^k}\right) \subset GF\left(\left(q^{m^k}\right)^{m^k}\right) =$$

$$= GF\left(q^{m^{2k}}\right) \subset \ldots \subset GF\left(q^{m^{kl}}\right).$$

Для каждого этажа башни

$$GF(q_i) = GF\left(q^{m^{ik}}\right) \subset GF\left(\left(q^{m^{ik}}\right)^{m^k}\right) =$$

$$= GF\left(q^{m^{(i+1)k}}\right) = GF(q_{i+1})$$

выберем стандартный базис $\{1, \alpha, \ldots, \alpha^{m^k-1}\}$, определяемый неприводимым над полем $GF(q_i)$ многочленом $p_i(x)$ степени m^k таким образом, чтобы элемент α порождал нормальный базис $\{\alpha, \alpha^Q \ldots, \alpha^{Q^{m^k-1}}\}$, где $Q = q_i$. Тогда произвольный элемент поля $GF(q_{i+1})$ можно представить в виде m^k-мерного вектора с компонентами из поля $GF(q_i)$ и в виде $m^{k(i+1)}-$мерного вектора с компонентами из поля $GF(q)$. Умножение в поле $GF(q_{i+1})$ можно свести к умножению по модулю многочлена p_i двух многочленов степени $t = m^k - 1$ над полем $GF(q_i)$. Известно [1], что умножение в поле $GF(q_{i+1})$ сводится к трем умножениям многочленов степени t над полем $GF(q_i)$ и t сложениям в этом поле. Для умножения двух многочленов f, g степени t над полем $GF(q_i)$ можно сначала вычислить значения $f(a_i), g(a_i)$ на произвольных $2t + 1$ элементах его подполя $GF(q)$, выполнить $2t + 1$ умножение в поле $GF(q_i)$ и потом, используя интерполяционную формулу, восстановить по значениям $h(a_i) = f(a_i)g(a_i)$ коэффициенты произведения $h(x) = f(x)g(x)$. Для выполнения всех этих операций с помощью схемы Горнера и формулы Лагранжа требуется $O(t^2)$ операций сложения и умножения на элементы подполя $GF(q)$

в поле $GF(q_i)$. Поэтому сложность умножения в поле $GF(q_{i+1})$ оценивается как

$$M(GF(q_{i+1})) \leqslant 3(2m^k - 1)M(GF(q_i)) + O(m^{2k})m^{ik}(\log_2 q)^{\log_2 3},$$

так как сложение в поле $GF(q_i)$ выполняется со сложностью $\log_2 q_i = m^{ik} \log_2 q$, а сложность умножения на элементы подполя $GF(q)$ равна $M(GF(q))m^{ik} = O(\log_2 q)^{\log_2 3} m^{ik}$, потому что это умножение сводится к m^{ik} умножениям в поле $GF(q)$. Если обозначить $M(GF(q_i))$ через $M(i)$, а $3(2m^k - 1)$ через a, то полученное рекуррентное неравенство переписывается в виде $M(i + 1) \leqslant aM(i) + bm^{(i+1)k}$, где $b = O(a)(m^k m^{r \log_2 3}) = O(a)m^{O(k)}$, $M(0) = M(GF(q)) = O(\log_2 q)^{\log_2 3}$. Применяя индукцию, имеем

$$M(l) \leqslant a^l M(0) + b\left(a^{l-1}m^k + a^{l-2}m^{2k} + \ldots + m^{lk}\right),$$

следовательно,

$$M(l) \leqslant a^l M(0) + a^l b\frac{1 - (m^k/a)^{l+1}}{1 - m^k/a} \leqslant a^l M(0) + \frac{a^l b}{1 - m^k/a} \leqslant$$

$$\leqslant a^l M(0) + 3a^l b/2 = O(a^{l+1})m^{O(k)} = O(a)m^{O(k)}2^{l \log_2 3(2m^k-1)}.$$

Поэтому, так как $q_l = q^{m^{kl}}$, имеем $l = (\log_2 \log_q q_l)/\log_2 m^k$, $\log_2 q_l = n$,

$$M(GF(2^n)) = M(GF(q_l)) = O(m^{r \log_2 3})2^{l \log_2 3(2m^k-1)} =$$

$$= m^{O(k)}2^{\frac{\log_2 \log_q q_l \log_2 3(2m^k-1)}{\log_2 m^k}} = m^{O(k)}(\log_q q_l)^{\log_{m^k} 3(2m^k-1)} =$$

$$= m^{O(k)}(\log_2 q_l)^{\log_{m^k} 3(2m^k-1)} = m^{O(k)}n^{\log_{m^k} 3(2m^k-1)}.$$

Так как $\log_{m^k} 3(2m^k - 1) \to 1$ при $m^k \to \infty$, то для любого $\varepsilon > 0$ при любом m, $n = m^s$ и $s \geqslant s_\varepsilon$ имеем $M\left(GF(2^n)\right) = M\left(GF(2^{m^s})\right) = n^{1+\varepsilon/2}$. Умножение на каждом этаже башни можно выполнять и в нормальном базисе, если выполнить переход к стандартному базису, произвести умножение в нем и вернуться опять в нормальный базис. Грубая оценка сложности переходов между базисами равна

$$m^{2k}M(GF(q_i)) + (m^{2k} - m^k)m^{ik+r},$$

так как для выполнения как прямого, так и обратного преобразования координат требуется не более m^{2k} умножений и не более $m^{2k} - m^k$ сложений в поле $GF(q_i)$, имеющем размерность m^{ik+r}. С помощью циклических сдвигов вычислим в нормальном базисе систему степеней

$$x^Q, x^{Q^2}, \ldots, x^{Q^{m^k-1}},\ Q = q_i.$$

Возьмем кратчайшую линейную аддитивную цепочку (см. [13]) для числа $t = m^k - 1$ $a_0 = 1, a_1 = 2, a_2, \ldots, a_L = t$ длины $L = L(t)$, т.е. такую последовательность, что каждый ее член a_n при $n > 0$ равен $a_{n-1} + a_k$, $k < n$ (если $k = n - 1$, то операция вычисления a_n называется шагом удвоения, а если $k < n - 1$– линейным шагом). Построим линейную аддитивную цепочку, содержащую подпоследовательность

$$\frac{Q^{a_1} - 1}{Q - 1}, \frac{Q^{a_2} - 1}{Q - 1}, \ldots, \frac{Q^t - 1}{Q - 1},$$

между соседними членами которой производятся несколько последовательных шагов удвоения и один линейный шаг, пользуясь формулами

$$\frac{Q^{a_i} - 1}{Q - 1} = \frac{Q^{a_j + a_h} - 1}{Q - 1} = Q^{a_h}\frac{Q^{a_j} - 1}{Q - 1} + \frac{Q^{a_h} - 1}{Q - 1}.$$

Так как возведение в степень Q^n в нормальном базисе делается бесплатно, а $x^{(Q^{a_0}-1)/(Q-1)} = x$, то для вычисления $K(x) = x^{(Q^{t+1}-Q)/(Q-1)}$ требуется только $L = L(m^k - 1)$ операций умножения. Еще одно умножение требуется для вычисления $N(x) = xK(x)$. Поэтому сложность совместного вычисления $K(x), N(x)$ оценивается как $LM(GF(q_{i+1})) \leqslant$

$$\leqslant L\left(3(m^{2k} + 2m^k - 1)M(GF(q_i)) + O(m^{2k})m^{ik}(m^r)^{\log_2 3}\right).$$

Используя формулу $x^{-1} = K(x)/N(x)$, получаем рекуррентную оценку сложности инвертирования:

$$I(\log_2 q_{i+1}) = I\left(m^{(i+1)k+r}\right) \leqslant I\left(m^{ik+r}\right) + m^k M(GF(q_i)) +$$

$$+L(m^k - 1)\left(3(m^{2k} + 2m^k - 1)M(GF(q_i)) + \right.$$
$$\left. +O(m^{2k})m^{ik}(m^r)^{\log_2 3}.\right.$$

Очевидно, $L(t) \leqslant \lambda_2(t) + \nu_2(t) - 1 \leqslant 2\log_2 t \leqslant 2k\log_2 m$, где $\lambda_2(t)$ – длина двоичной записи числа t, а $\nu_2(t)$ – число единиц в ней (см. [13], где приведены и более точные оценки). Из полученных выше оценок по индукции с помощью неравенства $aM(n) \leqslant M(an)$ выводим оценку

$$I(m^s) = I\left(m^{lk+r}\right) = I(\log_2 q_l) \leqslant$$

$$\leqslant I(m^r) + O(km^{2k}\log_2 m)M(\log_2 q_{l-1}) =$$
$$= I(m^r) + O(km^k \log_2 m)M(m^s) = O(km^k \log_2 m)M(m^s).$$

Теорема доказана.

Укажем конкретный пример применения данного метода. Пусть $m = 2, n = m^s$. Выберем $k = 8$, тогда $\log_{m^k} 3(2m^k - 1) = \log_{256} 1533 < 1,33$. Получаем, как следствие, в некотором базисе поля $GF(2^{2^n})$ оценку сложности умножения $O(2^{n^{1,33}})$ и оценку сложности инвертирования $I(n) = O(M(n))$. Эти оценки асимптотически лучше оценок [9] (полученных для другого базиса).

§ 25. Схемы в поле $GF(2^n)$ при $n = 2 \cdot 3^k$

При $m = 3$ можно уточнить доказанную теорему следующим образом.

Теорема 2. *При $n = 2 \cdot 3^k$ в поле $GF(2^n)$ можно указать некоторый (не стандартный и не нормальный) базис, для которого можно построить схемы умножения и инвертирования сложности:*

$$M(n) = n(\log_3 n)^{(\log_2 \log_3 n)/2 + O(1)}, I(n) = O(M(n)).$$

Доказательство. Положим $q_i = 2^{a_i}, a_i = 2 \cdot 3^{b_i}, b_i = 2^i$ и рассмотрим башню полей

$$GF(q_0) \subset GF(q_1) \subset \ldots \subset GF(q_k).$$

Так как $q_i - 1 = 2^{a_i} - 1$ кратно $3^{b_i+1} = 3n_i$, то в поле $GF(q_i)$ найдется элемент порядка $3^{b_i+1} = 3n_i$, и, значит, определено дискретное преобразование Фурье порядка $3^{b_i+1} = 3n_i$. Как следует из [10], многочлены степени меньше $n_i = 3^{b_i} = a_i/2$ над полем $GF(q_i)$ могут быть перемножены с помощью $24n_i \log_3 n_i + O(n_i)$ умножений и $68n_i \log_3 n_i + O(n_i)$ сложений в этом поле. Если обозначить сложность умножения в поле $GF(q_i)$ через $M(GF(q_i))$, то сложность умножения многочленов степени меньше n_i над полем $GF(q_i)$ будет оцениваться как

$$(24n_i \log_3 n_i + O(n_i))M(GF(q_i)) + (68n_i \log_3 n_i + O(n_i))n_i.$$

Обозначим далее эту оценку через M_i. Выберем в этом поле примитивный элемент α_i, тогда двучлен $f_i = x^{n_i} - \alpha_i$ будет неприводимым согласно теореме 3.75 [11], так как $n_i = 3^{b_i}$ делит $q_i - 1$, а значит, и $q_{i+1} - 1 = 2^{a_{i+1}} - 1$. Выбирая в расширении $GF(q_{i+1})$ поля $GF(q_i)$ стандартный базис, соответствующий двучлену f_i, и замечая, что умножение в этом базисе сводится к умножению многочленов степени меньше n_i над полем $GF(q_i)$ и приведению результата по модулю f_i (которое выполняется школьным алгоритмом деления с помощью n_i операций умножения и n_i операций сложения в поле $GF(q_i)$), имеем

$$M(GF(q_{i+1})) \leqslant M_i + n_i M(GF(q_i)) + a_{i+1} \leqslant$$
$$\leqslant (24n_i \log_3 n_i + O(n_i))M(GF(q_i)) + (68n_i \log_3 n_i + O(n_i))n_i + a_{i+1} \leqslant$$
$$\leqslant (12a_i \log_3 a_i + O(a_i))M(GF(q_i)) + (17a_i^2 \log_3 a_i + O(a_i^2)) + a_{i+1} \leqslant$$
$$\leqslant (12a_i \log_3 a_i + O(a_i))M(GF(q_i)) + (17a_i^2 \log_3 a_i + O(a_i^2)) \leqslant$$
$$\leqslant (12a_i b_i + O(a_i))M(GF(q_i)).$$

Отсюда по индукции следует, что

$$\log_2 M(GF(q_n)) \leqslant \sum_{i=1}^{n-1} \log_2 12a_i b_i + O(1) =$$
$$= \sum_{i=1}^{n-1} ((\log_2 3)2^i + i \log_2 24) + O(1) \leqslant$$

$$\leqslant (\log_2 3)2^n + n^2/2 + (2\frac{1}{2} + \log_2 3)n + O(1),$$

значит,

$$M(GF(q_n)) \leqslant O\left(3^{2^n+n} 2^{(n^2+5n)/2}\right), q_n = 2^{2 \cdot 3^{2^n}}.$$

Обозначая для краткости $a_n = 2 \cdot 3^{2^n}$ через N, имеем

$$M(GF(2^N)) \leqslant N(\log_3 N)^{n/2+O(1)} = N(\log_3 N)^{(\log_2 \log_3 N)/2+O(1)}.$$

Получим теперь оценку для сложности инвертирования. В расширении $GF(q_{i+1})$ поля $GF(q_i)$ выполняем инвертирование по формуле

$$x^{-1} = K(x)N(x)^{-1}, K(x) = x^{q_i} x^{q_i^2} \dots x^{q_i^{n_i-1}}, N(x) = xK(x).$$

Так как

$$N(x)^{q_i} = x^{q_i} x^{q_i^2} \dots x^{q_i^{n_i}} = x^{q_i} x^{q_i^2} \dots x^{q_i^{n_i-1}} x = N(x),$$

то $N(x) \in GF(q_i)$, поэтому для инвертирования нужно вычислить $K(x), N(x)$, потом выполнить инвертирование в подполе $GF(q_i)$ и n_i раз выполнить умножение в поле $GF(q_i)$.

Для вычисления $N(x), K(x)$ сначала найдем $y = xx^{q_i^{n_i/3}} x^{q_i^{2n_i/3}}$, а потом

$$N(x) = yy^{q_i} \dots y^{q_i^{n_i/3-1}}, K(x) = y^{q_i} \dots y^{q_i^{n_i/3-1}} x^{q_i^{n_i/3}} x^{q_i^{2n_i/3}}.$$

Так как

$$y^{q_i^{n_i/3}} = x^{q_i^{n_i/3}} x^{q_i^{2n_i/3}} x^{q_i^{n_i}} = xx^{q_i^{n_i/3}} x^{q_i^{2n_i/3}} = y,$$

то $y \in GF(q_i^{n_i/3})$. Значит, для вычисления y можно сделать 2 умножения в поле $GF(q_{i+1})$ и 2 операции возведения в степени $q_i^{n_i/3}, q_i^{2n_i/3}$ в том же поле, потом вычислить

$$N(x) = yy^{q_i} \dots y^{q_i^{n_i/3-1}}$$

и для вычисления $K(x)$ сделать одно умножение в поле $GF(q_{i+1})$ на элемент подполя $GF(q_i^{n_i/3})$. Так как произвольный элемент поля $GF(q_{i+1})$ можно представить в виде

$$X_0 + X_1\gamma_i + X_2\gamma_i^2,$$

где $X_j = x_j + x_3\gamma_i^{3+j} + x_{3(n_i/3-1)+j}\alpha_i^{3(n_i/3-1)} \in GF(q_i^{n_i/3}), j = = 0,1,2$, то умножение в поле $GF(q_{i+1})$ на элемент подполя $GF(q_i^{n_i/3})$ сводится к трем умножениям в этом подполе. Поле $GF(q_i^{n_i/3})$ является расширением степени $n_i/3 = = 3^{b_i-1}$ подполя $GF(q_i)$, и в нем можно выбрать базис $\{1,\beta_i,\ldots,\beta_i^{n_i/3-1}\}$, где $\beta_i^{n_i/3} = \alpha_i$. Умножение в этом базисе совпадает с умножением многочленов степени $n_i/3$ по модулю неприводимого над полем $GF(q_i)$ многочлена $x^{n_i/3} + \alpha_i$. В расширении $GF(q_i) \subset GF(q_{i+1})$ ранее был выбран базис $\{1,\gamma_i,\ldots,\gamma_i^{n_i-1}\}$, где $\gamma_i^{n_i} = \alpha_i$. Положим $\beta_i = \gamma_i^3$. Тогда произвольный элемент подполя $GF(q_i^{n_i/3})$ имеет относительно базиса $\{1,\beta_i,\ldots,\beta_i^{n_i/3-1}\}$ координаты, которые совпадают с $n_i/3$ координатами этого элемента относительно базиса $\{1,\alpha_i,\ldots,\alpha_i^{n_i-1}\}$ (а остальные его координаты в этом базисе равны нулю). Поэтому сложность умножения элементов этого подполя оценивается неравенством

$$M(GF(q_i^{n_i/3})) \leqslant M(a_{i+1}/3) + (n_i/3)M(GF(q_i)) + a_{i+1}/3 \leqslant$$
$$\leqslant (8n_i\log_3 n_i + O(n_i))M(GF(q_i)) + ((68/3)n_i\log_3 n_i + O(n_i))n_i + +a_{i+1}/3 \leqslant (4a_ib_i + O(a_i))M(GF(q_i)).$$

Оценим сложность возведения в степени $q_i^{n_i/3}, q_i^{2n_i/3}$ в поле $GF(q_{i+1})$. Так как произвольный элемент x поля $GF(q_{i+1})$ можно представить в виде

$$X_0 + X_1\gamma_i + X_2\gamma_i^2,$$

где $X_j \in GF(q_i^{n_i/3}), j = 0,1,2$, то

$$x^{q_i^{n_i/3}} = X_0^{q_i^{n_i/3}} + X_1^{q_i^{n_i/3}}\gamma_i^{q_i^{n_i/3}} + X_2^{q_i^{n_i/3}}\gamma_i^{2\cdot q_i^{n_i/3}} =$$
$$= X_0 + X_1\gamma_i^{q_i^{n_i/3}} + X_2\gamma_i^{2\cdot q_i^{n_i/3}}.$$

Так как $q_i^{n_i/3} - 1$ делится на $q_i - 1$, а значит, кратно n_i, то

$$\gamma_i^{q_i^{n_i/3}} = \gamma_i(\alpha_i)^{(q_i^{n_i/3}-1)/n_i} = a_i\gamma_i, \gamma_i^{2\cdot q_{i-1}^3} = \gamma_i^2(\alpha_i)^{2(q_{i-1}^3-1)/9} =$$
$$= b_i\gamma_i^2, a_i, b_i \in GF(q_i),$$

поэтому $x^{q_i^{n_i/3}} = X_0 + X_1\gamma_i^{q_i^{n_i/3}} + X_2\gamma_i^{2\cdot q_i^{n_i/3}} = X_0 + X_1a_i\gamma_i + + X_2b_i\gamma_i$, значит, возведение в степень $q_i^{n_i/3}$ в поле $GF(q_{i+1})$ сводится к двум умножениям в подполе $GF(q_i^{n_i/3})$ на элементы подполя $GF(q_i)$. Следовательно, его сложность оценивается как $(2n_i/3)M(GF(q_i))$. Точно так же оценивается сложность возведения в степень $q_i^{2n_i/3}$. Поэтому суммарная сложность всех выполненных операций равна

$$L_i = 2M(GF(q_{i+1})) + 3M(GF(q_i^{n_i/3})) + (4n_i/3)M(GF(q_i)) \leqslant$$
$$\leqslant (36a_ib_i + O(a_i))M(GF(q_i)).$$

Для вычисления

$$yy^{q_i}\ldots y^{q_i^{n_i/3-1}},$$

где $y \in GF(q_i^{n_i/3})$, применяем тот же прием, вычисляя сначала

$$z = yy^{q_i^{n_i/9}}y^{q_i^{2n_i/9}}.$$

Так как $y^{q_i^{n_i/3}} = y$, то $z^{q_i^{n_i/9}} = z$, значит, $z \in GF(q_i^{n_i/9})$. Для вычисления z нужно выполнить два умножения в поле $GF(q_i^{n_i/3})$ и возведения в степени $q_i^{n_i/9}, q_i^{2n_i/9}$ в том же поле. Аналогично предыдущим рассуждениям, оцениваем их сложность как

$$2M(GF(q_i^{n_i/3})) + (4n_i/9)M(GF(q_i)) \leqslant$$
$$\leqslant (24a_{i-1}b_i + O(a_{i-1}))M(GF(q_i)).$$

Так как

$$yy^{q_i}\ldots y^{q_i^{n_i/3-1}} = zz^{q_i}\ldots z^{q_i^{n_i/9-1}},$$

то остается вычислить

$$zz^{q_i}\ldots z^{q_i^{n_i/9-1}}, z \in GF(q_i^{n_i/9}).$$

Применяя тот же прием, сводим это вычисление со сложностью

$$2M(GF(q_i^{n_i/9})) + (4n_i/27)M(GF(q_i)) \leqslant$$
$$\leqslant (24a_{i-2}b_i + O(a_{i-2}))M(GF(q_i))$$

к вычислению

$$ww^{q_i}\ldots w^{q_i^{n_i/27-1}}, w \in GF(q_i^{n_i/27})$$

и т.д. Так как $n_i = 3^{b_i}$, этот процесс закончится через b_i шагов. На каждом шаге требуемая сложность уменьшается асимптотически в три раза, поэтому сложность вычисления $N(x)$ оценивается как

$$\left(24\frac{3}{2}a_{i-1}b_i + O(a_i)\right) M(GF(q_i)),$$

значит, сложность вычисления $N(x), K(x)$ оценивается как

$$(44a_ib_i + O(a_i))M(GF(q_i)).$$

Отсюда следует рекуррентная оценка сложности инвертирования:

$$I(a_{i+1}) \leqslant I(a_i) + n_iM(GF(q_i)) + (44a_ib_i + O(a_i))M(GF(q_i)) \leqslant$$
$$\leqslant I(a_i) + (44a_ib_i + O(a_i))M(GF(q_i)).$$

Из нее по индукции получаем, что

$$I(a_n) \leqslant \sum_{i=1}^{n-1}(44a_ib_i + O(a_i))M(GF(q_i)) + I(a_0) =$$
$$= (44a_{n-1}b_{n-1} + O(a_{n-1}))M(GF(q_{n-1})).$$

Так как $M(GF(q_{i+1})) \leqslant (12a_ib_i + O(a_i))M(GF(q_i))$, то, предполагая, что

$$M(GF(q_{i+1})) = (12a_ib_i + O(a_i))M(GF(q_i)),$$

получаем асимптотическую оценку:

$$I(a_n) \leqslant \left(\frac{11}{3} + o(1)\right) M(GF(q_n)).$$

Так как $M(GF(q_n)) = O\left(3^{2^n+n}2^{(n^2+5n)/2}\right)$, во всех случаях имеем $I(a_n) =$

$$= (44a_{n-1}b_{n-1} + O(a_{n-1}))M(GF(q_{n-1})) = O\left(3^{2^n+n}2^{(n^2+5n)/2}\right).$$

Поэтому при $N = a_n$ справедливо равенство $I(N) = O(M(GF(2^N)))$. Такие же оценки можно получить и для любого $N = 2 \cdot 3^n$. Для этого выберем k так, чтобы $2^{k-1} \leqslant n < 2^k$, и определим последовательность $a_k = N, a_{i-1} = 2 \cdot 3^{\lceil \log_3(a_i/2))/2 \rceil}$, положим $q_i = 2^{a_i}$ и рассмотрим башню полей $GF(q_0) \subset GF(q_1) \subset \ldots \subset GF(q_k)$. Теорема доказана.

Для практического построения схем для умножения и инвертирования в полях $GF(2^n)$ произвольной размерности можно разложить n на множители, равные степеням простых чисел, построить эти схемы для полей, размерности которых равны указанным множителям, сводя их построение к построению схем для полей простой размерности, а потом применить метод построения схем для полей составной размерности при условии взаимной простоты сомножителей. Для инвертирования в полях простой размерности применяется метод [7]. Вместо простых чисел, при возможности, можно применять размерности, для которых существуют оптимальные нормальные базисы, или гауссовы базисы малой сложности (см., например, [8]).

ЗАКЛЮЧЕНИЕ

Конечные поля возникли в исследованиях Гаусса и Галуа. Современное изложение теории появилось в работах Мура и Диксона. Схемы для арифметических операций в конечных полях используются в криптографии, кодировании, цифровой передаче сигналов и других областях. В указанных применениях в основном использовались поля сравнительно малой размерности ($n \leqslant 32$), но с развитием криптографии с открытым ключом поля большой размерности ($n \geqslant 1000$) нашли применение в криптографических протоколах, основанных на предположении о трудности задачи дискретного логарифмирования[7,8]. Благодаря развитию криптографии на эллиптических кривых появилась возможность использовать поля размерности порядка двухсот[9,10].

Теория сложности схем для булевых функций была развита в работах К. Э. Шеннона и О. Б. Лупанова. Схемы обычно строятся из элементов, реализующих двухместные булевы функции. Под сложностью схемы понимается количество составляющих схему функциональных элементов. Понятие схемной сложности, по существу, совпадает с понятием битовой сложности. При конструировании логических схем стремятся уменьшить не только их сложность, но и глубину — максимальное число элементов в любой цепи, соединяющей входы схемы с её выходами, так как практически важно увеличить быстродействие схемы. Операции сложения и вычитания просты, поэтому наибольший

[7] Diffie W., Hellman M., *New directions in cryptography // IEEE Trans. Inform. Theory*, **IT-22**, (1976).

[8] Coppersmith D. *Fast evaluation of logarithms in fields of characteristic two // IEEE Trans.Inform.Theory*, **IT30**, 4,(1984), 587–594.

[9] Miller V. *Uses elliptic curves in cryptography . – CRYPTO-85*, (1986), 417–426.

[10] Koblitz N. *Elliptic curve cryptosystems // Mathematics of computation.* 48 (1987), 203–209.

интерес представляет умножение и инвертирование ненулевых элементов (инвертирование есть нахождение мультипликативного обратного). Деление сводится к инвертированию и умножению. Умножение элементов конечного поля в стандартном базисе сводится к умножению представляющих эти элементы многочленов по модулю некоторого неприводимого многочлена, поэтому существенное значение имеет разработка эффективных схем для умножения многочленов над конечными полями.

Используя методы дискретной математики, математической кибернетики и алгебры, в частности теории синтеза и сложности управляющих систем и теории конечных полей, можно получать эффективные верхние оценки сложности и глубины схем из двухвходовых булевых элементов для арифметики в конечных полях различной структуры, а также для умножения многочленов в конечных полях.

Эти теоретические исследования приводят к построению схемной реализации арифметики в конечных полях, что может найти применение в кодировании, криптографии, цифровой обработке сигналов и других областях, а также может быть использовано для программной реализации арифметических операций в конечных полях в компьютерной алгебре.

Методы умножения в конечных полях зависят от типа базисов, используемых для представления элементов поля. Чаще всего применяются стандартные полиномиальные базисы, в которых элементы поля размерности n представляются в виде многочленов степени $n-1$, операции над которыми выполняются по модулю данного неприводимого многочлена. Очевидные оценки сложности и глубины таких схем равны $O(n^2)$, $O(\log n)$. Методом Карацубы можно для тех же базисов построить схемы сложности $O(n^{\log_2 3})$. Вопросы практического использования метода Карацубы для умножения в поле $GF(2^n)$ рассмотрены,

в частности, в диссертации К. Паара[11]. Известно[12,13], что в стандартных базисах в полях $GF(2^n)$ сложность схемы для умножения равна $O(n \log n \log\log n)$. Для инвертирования в компьютерных вычислениях можно использовать быстрый алгоритм Евклида[9] с оценкой сложности $O(n \log^2 n \log\log n)$. Однако мультипликативная константа в этой оценке велика (несколько сотен), и при актуальных для приложений значениях n стандартный алгоритм Евклида лучше. Кроме того, этот алгоритм затруднительно применить при построении схемы для инвертирования.

Автором учебного пособия были построены схемы для умножения и инвертирования в башнях конечных полей вида $GF(2^n)$, $n = m^s$. Далее приводятся формулировки результатов при помощи следующих обозначений: $L(M(n))$, $M(n)$ – сложность схемы для умножения, $L(I(n))$, $I(n)$ – сложность схемы для инвертирования, $L(S(n))$ – сложность схемы для возведения в квадрат, $D(M(n))$ – глубина схемы для умножения, $D(I(n))$ – глубина схемы для инвертирования, $D(S(n))$ – глубина схемы для возведения в квадрат в конечном поле $GF(2^n)$.

Для расширения $GF((2^n)^4)$ поля $GF(2^n)$ при нечетном n и выборе в поле $GF(2^4)$ нормального базиса

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}, \quad 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0,$$

и произвольного нормального базиса в поле $GF(2^n)$ можно построить схемы для умножения и инвертирования со следующими рекуррентными оценками сложности и глубины:

$$L(M(4n)) \le 10L(M(n)) + 21n, \quad D(M(4n)) \le D(M(n)) + 3,$$

[11] Paar C. *Effective VLSI architectures for bit paralel computation in Galois fields*, Ph. D. Thesis, Universität GH Essen, Germany, 1994.

[12] Gathen J. von zur , Gerhard J. Modern computer algebra. – Cambridge University Press, 1999.

[13] Schonhage A. Schnelle Multiplication von Polynomen ueber Koerpern der Charakteristik 2 // Acta Informatica (1977). Vol. 7, 395–398.

$$L(I(4n)) \le L(I(n)) + 19L(M(n)) + 13n,$$
$$D(I(4n)) \le 3D(M(n)) + 2 + \max\{D(I(n)), 2\}.$$

Можно также построить схемы для инвертирования с оценками

$$L(I(4n)) \le L(I(n)) + 18L(M(n)) + 15n,$$
$$D(I(4n)) \le 3D(M(n)) + 2 + \max\{D(I(n)), 3\}.$$

Для расширения $GF((2^n)^6)$ поля $GF(2^n)$, где n взаимно просто с 6, при выборе в подполе $GF(2^6)$ нормального базиса

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}\}, \quad 1 + \alpha + \alpha^4 + \alpha^5 + \alpha^6 = 0,$$

и произвольного нормального базиса в поле $GF(2^n)$ можно построить для умножения и инвертирования схемы со следующими рекуррентными оценками сложности и глубины:

$$L(M(6n)) \le 21L(M(n)) + 60n, \quad D(M(6n)) \le D(M(n)) + 4,$$
$$L(I(6n)) \le L(I(n)) + 42L(M(n)) + 65n,$$
$$D(I(6n)) = 4D(M(n)) + 4 + \max\{D(I(n)), 4\}.$$

В башне расширений $GF((((2^n)^2)^2))^2$ поля $GF(2^n)$ при нечетном n можно выбрать базис так, что справедливы следующие рекуррентные оценки сложности и глубины умножения и возведения в квадрат:

$$L(M(8n)) \le 27L(M(n)) + 80n, \quad D(M(8n)) \le D(M(n)) + 7,$$
$$L(S(8n)) \le 10n + 4L(S(n)), \quad D(S(8n)) \le 5 + D(S(4n)).$$

Если в поле $GF(2^n)$ выбрать нормальный базис, то для инвертирования справедливы следующие рекуррентные оценки сложности и глубины:

$$L(I(8n)) \le L(I(n)) + 45L(M(n)) + 101n,$$
$$D(I(8n)) \le 4D(M(n)) + 8 + \max\{D(I(n)), 6\}.$$

В башне расширений $GF(((2^n)^4)^2)$ поля $GF(2^n)$ при нечетном n можно выбрать базис так, что справедливы следующие рекуррентные оценки сложности и глубины умножения и инвертирования:

$$L(M(8n)) \le 30L(M(n)) + 82n, \quad D(M(8n)) \le D(M(n)) + 5,$$
$$L(I(8n)) \le L(I(n)) + 52L(M(n)) + 88n,$$

$$D(I(8n)) \le 4D(M(n)) + 6 + \max\{D(I(n)), 2\}.$$

Интерес к эффективной схемной реализации арифметики в *полях большой характеристики* возник в связи с возможными применениями в криптографии на эллиптических кривых. С этой целью было предложено в работе[14] использовать поля с характеристикой, относительно мало отличающейся от степени двойки (такие простые числа названы псевдомерсенновскими), в которых существуют полиномиальные базисы, соответствующие неприводимым двучленам (такие представления этих полей названы в указанной работе оптимальными расширениями простых полей). В работе[15] среди таких расширений выделены расширения размерности 2^n, 3^n и представлены в виде башен полей, построенных из квадратичных и кубических расширений. С помощью этих башен (названных оптимальными башнями полей) была указана для оптимальных расширений эффективная реализация операций умножения и инвертирования.

Используем следующие обозначения: $M(q)$ – сложность умножения в $GF(q)$, $A(q)$ – сложность сложения в $GF(q)$, $M(C, q)$ – сложность умножения на константу C в $GF(q)$. В цитированной работе получен результат, который можно сформулировать следующим образом.

Умножение в башне полей $GF(q^{2^k})$ имеет рекуррентную верхнюю оценку сложности

$$M(q^{2^k}) \leqslant 3^k M(q) + 5(3^k - 2^k)A(q) + \frac{1}{2}(3^k - 1)M(\alpha_0, q),$$

где многочлен $x^2 - \alpha_0$ неприводим над $GF(q)$, $\alpha_0 \in GF(q)$. Умножение в башне полей $GF(q^{3^k})$ имеет рекуррентную

[14]Bailey D.V., Paar C. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography // J. of Cryptology, 14:3(2001), 156–173.

[15]Baktir S., Sunar B. Optimal tower fields. // IEEE Trans. Comp. V. 53, N 10 (2004), 1231–1243.

верхнюю оценку сложности

$$M(q^{3^k}) \leqslant 6^k M(q) + 5(6^k - 3^k)A(q) + \frac{2}{5}(6^k - 1)M(\alpha_0, q),$$

где многочлен $x^3 - \alpha_0$ неприводим над $GF(q)$, $\alpha_0 \in GF(q)$.

Эти результаты можно улучшить следующим образом. Используем обозначения: w_k – примитивный корень k-й степени из единицы в $GF(q)$, $\varepsilon = w_3$; n, k_i – неотрицательные целые, p – простое.

Умножение в башне полей $GF(q^3)$, $q = p^n$, имеет оценку сложности

$$M(q^3) \le 5M(q) + 21A(q) + 6M(2, q) +$$
$$+2(M(4, q) + M(1/2, q) + M(1/6, q)) + 2M(\alpha_0, p)$$

в предположении, что $q-1$ кратно 3, двучлены $x^n - \alpha_0$ и $x^{3n} - \alpha_0$ неприводимы над $GF(p)$.

Умножение в башне полей $GF(q^4)$, $q = p^n$, имеет оценку сложности

$$M(q^4) \le 7M(q) + 6M(\omega_3, q) + 54A(q) + 6M(1/6, q) + 3M(\alpha_0, p)$$

в предположении, что $q - 1$ кратно 12 и многочлены $x^n - \alpha_0$ и $x^{4n} - \alpha_0$ неприводимы над $GF(p)$.

Умножение в башне полей $GF(q^6)$, $q = p^n$, имеет оценку сложности

$$M(q^6) \le 12M(q) + 121A(q) + 6M(\alpha_0, p) + M(1/12, q) +$$
$$+2(M(-3/2, q) + M(\frac{\varepsilon - \varepsilon^2}{2}, q) + M(-1/8, q) + M(\frac{\varepsilon - \varepsilon^2}{24}, q)) +$$
$$+2(M(\omega_4, q) + M(-3\omega_4/2, q) + M(\omega_4\frac{\varepsilon - \varepsilon^2}{2}, q)) +$$
$$+M(\frac{\omega_4}{12}, q) + M(-\omega_4/8, q) + M(\omega_4\frac{\varepsilon - \varepsilon^2}{24}, q)$$

в предположении, что $q - 1$ кратно 12, многочлены $x^n - \alpha_0$ и $x^{6n} - \alpha_0$ неприводимы над $GF(p)$.

Для $q = p^n$, $p = 2^{13} - 1$, $n = 2^{k_0} \cdot 3^{k_1} \cdot 5^{k_2} \cdot 7^{k_3} \cdot 13^{k_4}$, $k_0 = 0, 1$, умножение в поле $GF(q^5)$ имеет оценку сложности $M(q^5) \leqslant$ $\leqslant 77A(q) + 11M(q)$, умножение в поле $GF(q^7)$ имеет оценку

сложности $M(q^7) \le 13M(q) + 344A(q) + 6A(p)$, умножение в поле $GF(q^{13})$ имеет оценку сложности $M(q^{13}) \le 26M(q) + 1026A(q) + 12A(p)$, умножение в поле $GF(q^{14})$ имеет оценку сложности $M(q^{14}) \le 26M(q) + 1032A(q) + 13A(p)$.

Для $q = p^n$, $p = 2^{17} - 1$, $n = 2^{k_0} \cdot 3^{k_1} \cdot 5^{k_2} \cdot 17^{k_3}$, $k_0 = 0, 1$, умножение в поле $GF(q^9)$ имеет оценку сложности $M(q^9) \le 17M(q) + 578A(q) + 6A(p)$, умножение в поле $GF(q^{18})$ имеет оценку сложности $M(q^{18}) \le 35M(q) + 1825A(q) + 17A(p)$.

Умножение в поле $GF(q^{2^k})$, $k \le 4$, $q = p^n$, $n = 2^m$, $p = 2^{16} + 1$, имеет оценки сложности

$$M(q^4) \le 7M(q) + 59A(q) + 3M(3,p),$$
$$M(q^8) \le 15M(q) + 193A(q) + 7M(3,p),$$
$$M(q^{16}) \le 31M(q) + 558A(q) + 15M(3,p).$$

Далее используются также следующие обозначения: $I(q)$ – сложность инвертирования, $S(q)$ – сложность возведения в квадрат, $D(I(q))$ – глубина схемы инвертирования, $D(S(q))$ – глубина схемы возведения в квадрат, $D(M(C,q))$ – глубина схемы умножения на константу C в поле $GF(q)$, $M(2^s,q) = \max\{M(C,q) : C = 2^s, s = 1,2,3,\dots\}$, $D(M(2^s,q)) = \max\{D(M(C,q)) : C = 2^s, s = 1,2,3,\dots\}$.

В поле $GF(p^{2^m}), p = 2^{16} + 1$, существует схема для инвертирования, у которой сложность рекуррентно оценивается как

$$I_{2^m} = I_{2^{m-1}} + 6S_{2^{m-1}} + 12M_{2^{m-1}} + 15A_{2^{m-1}} + 5M(3,p) + M(6,p) + (2^{m-1} - 1)M(2,p),$$

где I_k есть сокращение для $I(p^k)$, и аналогично определяются M_k, S_k, A_k. Глубина этой схемы рекуррентно оценивается как

$$D(I_{2^m}) = D(I_{2^{m-1}}) + 2D(M_{2^{m-1}}) + D(S_{2^{m-1}}) + 2(D(A(p)) + D(M(3,p))).$$

Для инвертирования в поле $GF(q^{16})$, $q = p^n$, $n = 2^m$, $p = 2^{16} + 1$, может быть построена схема сложности

$$I(q) + 410M(q) + 24S(q) + 2173A(q) + 735M(2^s,q) +$$

$$+119M(3,p) + M(6,p).$$

Если $D(M(q)) + 2(D(A(p)) + D(M(3,p))) \le D(I(q))$, то глубина этой схемы не больше

$$D(I(q)) + 4D(M(q)) + D(S(q)) + 19D(A(p)) + 10D(M(2^s,p)) + 3D(M(3,p)).$$

В противном случае она не превосходит

$$5D(M(q)) + D(S(q)) + 21D(A(p)) + 10D(M(2^s,p)) + 5D(M(3,p)).$$

Инвертирование в поле $GF(p^{10n})$, $p = 1 \pmod{10n}$, может быть выполнено схемами, имеющими оценки сложности

$$I(p^{10n}) \le I(p^{2n}) + 28M(p^{2n}) + 143nA(p) + (16n + 2)M(\alpha_0,p) + 6n(M(\omega_5,p) + M(\omega_5^2,p) + M(\omega_5^3,p) + M(\omega_5^4,p)),$$
$$I(p^{10n}) \le I(p^n) + 445nA(p) + 76M(p^n) + 34M(\alpha_0,p) + 6n(M(\omega_5,p) + M(\omega_5^2,p) + M(\omega_5^3,p) + M(\omega_5^4,p)),\ \alpha_0 \in GF(p).$$

Умножение в поле $GF(q^n)$ для $q = p^2$, $p = 2^{13} - 1$, $n = 5^m$, $m = 1, 2$, имеет оценку сложности

$$M(q^5) \leqslant 27M(p) + 121A(p), \quad M(q^{25}) \leqslant 1462A(p) + 243M(p).$$

Умножение в поле $GF(p^{2n})$ для $p = 2^k - 1$ при $n \le 2^{k-1}$, имеющем только простые нечетные делители, делящие $p - 1$, может быть выполнено с помощью схемы сложности

$$M(p^{2n}) \le (15 \cdot 2^{m-2} + 9(2^{m-1}(m-2) + 1))M(p) + ((12m + 7)2^{m-1} + 9(2^{m-1}(m-2) + 1))A(p),$$

где $2^{m-1} \le 2n - 2 < 2^m, m \le k$. Если $2n - 2 = 2^m, m \le k$, тогда к указанной оценке сложности прибавляется $M(p^2) + A(p^2)$.

В заключение я выражаю благодарность читателю за проявленный интерес к предмету. Желаю успехов.

Литература

1. Gathen J. von zur, Gerhard J. Modern computer algebra. – Cambridge University Press, 1999.
2. Schonhage A. Schnelle Multiplication von Polynomen über Körpern der Charakteristik 2 // Acta Informatica. 1977. Vol. 7. P. 395–398.
3. Schonhage A. Schnelle berechnung von kettenbruchentwicklungen // Acta Informatica. 1971. 1. P. 139–144.
4. Gao S., Gathen J. von zur, Panario D., Shoup V. Algorithm for exponentiation in finite field // J. of Symbolic Computation. 2000. Vol. 29. P. 879–889.
5. Штрассен Ф. Алгоритм Гаусса не оптимален // Кибернетический сборник. Вып. 7. – М.: Мир, 1971.
6. Болотов А. А., Гашков С. Б. О быстром умножении в нормальных базисах конечных полей // Дискретная математика. 2001. Т. 13. № 3. С. 3–31.
7. Itoh T., Tsujii S. A fast algorithm for computing multiplicative inverses in $GF(2^n)$ using normal bases // Inform. And Comp. 1988. V. 78. P. 171–177.
8. Gathen J. von zur, Nöcker. Fast arithmetic with general Gauss period // Theor. Comp. Sci. 2004. 315. P. 419–452.
9. Paar C., Fan J.L. Efficient inversion in tower fields of characteristic two // ISIT, Ulm, Germany, 1997.
10. Гашков С. Б. Замечания о быстром умножении многочленов, преобразовании Фурье и Хартли // Дискретная математика. 2000. Т. 12. N 3. 124–153.
11. Лидл Р., Нидеррейтер Х. Конечные поля. – М.: Мир, 1988.
12. Яблонский С. В. Введение в дискретную математику. – М.: Высшая школа, 2001.
13. Кнут Д. Э. Искусство программирования. Т. 2. – М.: Вильямис, 2000.
14. Верещагин Н. К., Шень А. Начала теории множеств. – М.: МЦНМО, 2002.
15. Кострикин А. И. Введение в алгебру. – М.: Наука, 1977.
16. Ноден П., Китте К. Алгебраическая алгоритмика. – М.: Мир, 1999.

17. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. – М.: МГУ, 1984.
18. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. – М.: Физматлит, 2004.
19. Клини С. Математическая логика. – М.: Мир, 1973.
20. Лавров И. А., Максимова Л. Л. Задачи по теории множеств, математической логике и теории алгоритмов. – М.: Физматлит, 2004.
21. Успенский В. А., Верещагин Н. К., Плиско В. Е. Вводный курс математической логики. – М.: Физматлит, 2004.
22. Виленкин Н. Я. Рассказы о множествах. – М.: МЦНМО, 2005.
23. Дискретная математика и математические вопросы кибернетики / под общей редакцией С. В. Яблонского и О. Б. Лупанова. – М.: Наука, 1974.
24. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1., Т. 2. – М.: Мир, 1987.
25. Болотов А. А, Фролов А. Б., Гашков С. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию. – М.: КомКнига, 2006.
26. Алфутова Н. Б., Устинов А. В. Алгебра и теория чисел: сборник задач. – М.: МЦНМО, 2005.
27. Гашков С. Б. Современная элементарная алгебра в задачах и упражнениях. – М.: МЦНМО, 2006.
28. Колмогоров А. Н., Фомин С. В. Теория функций, функциональный анализ. – М.: Физматлит, 2004. Гл. 1 (Введение).

Получено