

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ  
ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМ. П.Г. ДЕМИДОВА

В.Г. ДУРНЕВ, М.А. БАШКИН, О.П. ЯКИМОВА

# ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

## ЧАСТЬ I

УЧЕБНОЕ ПОСОБИЕ

*Рекомендовано Научно-методическим советом по математике и механике  
Учебно-методического объединения по классическому университетскому  
образованию Российской Федерации в качестве учебного пособия  
для студентов высших учебных заведений, обучающихся по группе  
математических и механических направлений и специальностей*

Чит. зал

ЯРОСЛАВЛЬ 2007

275474

2/3

УДК 519.854  
ББК В 174 я 73  
Д 84

*Рекомендовано  
Редакционно-издательским советом университета  
в качестве учебного издания. План 2007 года*

Рецензенты:

кафедра алгебры и геометрии Тульского государственного педагогического  
университета им. Л.Н. Толстого;

кафедра алгебры Ярославского государственного педагогического  
университета им. К.Д. Ушинского;

доктор физ.-матем. наук, профессор В.Н. Безверхний;

доктор физ.-матем. наук, профессор А.С. Тихомиров

Д 84 **Дурнев, В.Г.** Элементы дискретной математики: учебное пособие /  
В.Г. Дурнев, М.А. Башкин, О.П. Якимова; Ярославский гос. ун-т  
им. П.Г. Демидова. — Ярославль: ЯрГУ, 2007. — Часть I. — 168 с.

ISBN 978-5-8397-0531-9

В учебном пособии рассматриваются основные математические понятия, традиционно включаемые в программу дисциплины “Дискретная математика”: булевы и  $k$ -значные функции, комбинаторика, графы, алфавитное кодирование, регулярные выражения и регулярные языки, конечные автоматы и автоматные языки.

Пособие предназначено для студентов, обучающихся по направлению подготовки 010100 Математика и по специальностям 010101 Математика и 090102 Компьютерная безопасность, очной и заочной форм обучения. Оно может быть использовано при изучении дисциплины “Дискретная математика” (блок ЕН, ОПД), а также базирующихся на ней специальных дисциплин.

Библиогр.: 56 назв.

УДК 519.854  
ББК В 174 я 73

ISBN 978-5-8397-0531-9

© Ярославский государственный университет  
им. П.Г. Демидова, 2007

© В.Г. Дурнев, М.А. Башкин, О.П. Якимова,  
2007



# Оглавление

Предисловие	5
<b>Глава 1. Булевы функции</b>	<b>9</b>
1. Булевы функции	9
2. Нормальные формы	12
3. Замыкание классов функций	14
4. Теорема Э. Поста о полноте	16
5. Сложность некоторых задач	23
6. Спектральное разложение булевых функций	25
7. Некоторые приложения булевых функций	31
<b>Глава 2. Комбинаторика</b>	<b>41</b>
1. Выборки, перестановки, сочетания и размещения	41
2. Полиномиальная теорема	51
3. Биномиальная теорема. Биномиальные коэффициенты и их свойства	53
4. Формула включений и исключений	57
5. Производящие функции	61
5.1. Основные определения	61
5.2. Применение аппарата производящих функций к задаче о составах слов	65
5.3. Свойства производящих функций	67
6. Рекуррентные уравнения	70
6.1. Линейные однородные рекуррентные уравнения с постоянными коэффициентами	71
6.2. Линейные неоднородные рекуррентные уравнения с постоянными коэффициентами	74
6.3. Применение линейных рекуррентных последовательностей в радиолокации и криптографии	78
6.4. Рекуррентные уравнения и производящие функции	80
6.5. Асимптотика	83
7. Разбиения. Числа Стирлинга и их свойства	85
8. Системы представителей	91
9. Латинские прямоугольники и квадраты	95

## ОГЛАВЛЕНИЕ

---

10.	Матрицы Адамара . . . . .	102
11.	Блок-схемы . . . . .	108
12.	Конечные проективные плоскости . . . . .	111
13.	Генерация комбинаторных объектов . . . . .	114
13.1.	<i>Порождение перестановок</i> . . . . .	114
13.2.	<i>Порождение подмножеств множества</i> . . . . .	118
13.3.	<i>Порождение размещений с повторениями</i> . . . . .	118
13.4.	<i>Порождение сочетаний</i> . . . . .	119
Глава 3. Функции $k$ -значной логики. Схемы из функциональных элементов . . . . .		121
1.	$k$ -значные функции . . . . .	121
2.	Замыкание классов $k$ -значных функций . . . . .	123
3.	Полнота систем $k$ -значных функций . . . . .	126
4.	О сложности схем из функциональных элементов . . . . .	147
Биографическая справка . . . . .		155
Литература . . . . .		163



*Светлой памяти  
Олега Борисовича Лупанова  
посвящается*

## ПРЕДИСЛОВИЕ

Трудно переоценить значение вклада в развитие и преподавание как дискретной математики, так и математики в целом, в разработку ее приложений, в подготовку математических кадров скоропостижно скончавшегося 3 мая 2006 года Олега Борисовича Лупанова, доктора физико-математических наук, профессора, академика РАН, создателя кафедры дискретной математики на механико-математическом факультете МГУ им. М.В. Ломоносова и его бессменного заведующего, декана механико-математического факультета МГУ на протяжении последних 26 лет, председателя Учебно-методического совета по математике и механике Учебно-методического объединения по классическому университетскому образованию РФ, заведующего отделом дискретной математики Института прикладной математики им. М.В. Келдыша. Более чем 20-летнее общение с Олегом Борисовичем старшего из авторов оказало огромное влияние на формирование многих его взглядов и убеждений. Светлой памяти Олега Борисовича Лупанова посвящаем мы наш скромный труд.

В учебное пособие включен основной, по мнению его авторов, материал, который традиционно последние 35–40 лет включается в программы дисциплины “Дискретная математика”. Содержание программы этой дисциплины на сегодняшний день вряд ли можно считать столь же однозначно определившимся и устоявшимся, как, например, содержание программы дисциплины “Математический анализ”. Кроме того, содержание программы, конечно, существенно зависит от специальности, на которую она ориентирована. Если первоначально, 40 лет тому назад, дисциплина “Дискретная математика” рассматривалась, в определенной мере, как раздел прикладной математики, база для математической кибернетики и преподавалась прежде всего для студентов специальности “Прикладная математика”, о чем наглядно свидетельствует очень емкое по содержанию предисловие С.В. Яблонского к его замечательной книге “Введение в дискретную математику”, то со временем “Дискретная математика” была включена в учебные планы ряда других специальностей, причем весьма различных по уровню математических требований. Если при введении этой дисциплины в учебные планы таких специальностей, как “Математика” и “Компьютерная безопасность”, произошло усиление ее математической составляющей, то при включении в учебные планы технических специальностей неизбежно произошло расширение объема рассматриваемых математических понятий, например, включение в программу дисциплины “Дискретная математика” таких разделов, как “Элементы теории множеств”, “Алгебраические системы”, “Формальные и логические исчисления”, которые в учебных планах для специальностей “Математика” и “Компьютерная безопасность” выделены в самостоятельные дисциплины. Такое расширение программы дисциплины “Дискретная математика” убедительно подтверждает справедливость утверждения С.В. Яблонского:

“Чрезмерная детализация и привязывание программы к специальным фактам опасно тем, что ...появятся новые факты, а старые частично утратят свою значимость. Ввиду этого главная задача курса — это обучение методам и мышлению, характерным для дискретной математики”.

В предлагаемом вниманию читателя пособии содержится, на наш взгляд, некоторое ядро дисциплины: булевы функции — комбинаторика — графы — алфавитное кодирование — регулярные языки — конечные автоматы.

По ряду причин авторы сочли целесообразным разбить пособие на две части, первая из которых включает главы 1, 2, 3, а вторая 4, 5 и 6.

Первая глава посвящена булевым функциям, теория которых чрезвычайно богата как с точки зрения самой математики, так и с точки зрения ее приложений. Не вдаваясь в подробности, напомним лишь, что список “Проблемы III тысячелетия” открывает вопрос о совпадении классов  $NP$  и  $P$ , который может быть сформулирован как проблема существования полиномиального алгоритма для решения вопроса выполнимости для булевых функций. Основное содержание этой главы составляет доказательство теоремы Э. Поста о полноте для систем булевых функций. Завершается глава обсуждением вычислительной сложности ряда задач, связанных с булевыми функциями.

Во вторую главу включен основной материал по комбинаторике: рассматриваются важнейшие соединения комбинаторики, полиномиальная теорема, биномиальные коэффициенты и формула включений и исключений. Особое внимание уделено рекуррентным уравнениям и производящим функциям, латинским квадратам, блок-схемам и конечным проективным плоскостям. Этот материал особенно важен с точки зрения приложений к построению различных кодов. Завершается глава рассмотрением чрезвычайно важного вопроса о перечислении (генерации) комбинаторных объектов.

Следующая глава по ряду причин намеренно сделана достаточно краткой — в ней дается представление об особенностях класса  $k$ -значных функций при  $k > 2$ , рассмотрены начальные вопросы, связанные с построением схем из функциональных элементов.

Четвертая глава посвящена графам. В нее включены основные вопросы, изучаемые на начальном этапе работы с графами: маршруты и связность, деревья, построение остова минимального веса. Рассматриваются важные вопросы о планарности графа, эйлеровых и гамильтоновых циклах. Значительное внимание уделено независимым множествам и кликам, раскраске графов. Завершается глава рассмотрением ряда алгоритмов, связанных с графами.

Пятая глава посвящена алфавитному кодированию. Ее ядро — теорема Ал.Ал. Маркова. Здесь же рассмотрен вопрос об оптимальном кодировании.

Заключительная шестая глава содержит, на наш взгляд, базовый материал по регулярным выражениям и регулярным языкам, конечным автоматам и автоматным языкам. Ее ядро — теорема С. Клини и недетерминированные автоматы. Заканчивается глава, а вместе с ней и пособие, рассмотрением некоторых алгоритмических проблем для автоматных языков, приводится пример алгоритмически неразрешимой проблемы для конечных автоматов. Дается пред-

ставление об использовании конечных автоматов в качестве моделей шифраторов.

Авторы намеренно придерживались разной степени полноты и глубины при изложении различных вопросов — по возможности старались осветить большую часть вопросов, традиционно включаемых в программу дисциплины “Дискретная математика”, однако определенное предпочтение отдавалось математической точке зрения, может быть в ущерб кибернетической. Оправданием может служить ориентация на студентов математических факультетов.

На формирование взглядов авторов в области дискретной математики значительное влияние оказали изданные у нас в стране книги по этой тематике, включенные в список литературы. Если некоторые из книг оказались пропущены, то сделано это было по незнанию, а не преднамеренно. За каждый такой случай авторы приносят свои искренние глубокие извинения.

Нам кажется, что пособие может несколько облегчить нашим студентам изучение “Дискретной математики”. Если же мы кому-то из них своим скромным трудом создали дополнительные проблемы, то сделали это неумышленно.

Первым из авторов написаны главы 1, 3, 5 и 6, второму принадлежит глава 2, а третьему — 4.

Авторы с глубокой благодарностью примут любые замечания и конструктивную критику.

*В. Дурнев, М. Башкин, О. Якимова*

# Глава 1. Булевы функции

## §1. Булевы функции

В этом разделе рассматриваются некоторые вопросы, относящиеся к одному из, казалось бы, простейших и в то же время одному из интереснейших математических понятий — понятию *булевой функции*. Однако простота этого понятия обманчива. Достаточно напомнить, что открывающий список “*Проблемы III тысячелетия*” вопрос о совпадении классов **NP** и **P** может быть сформулирован как вопрос о булевых функциях, а именно как вопрос о существовании полиномиального алгоритма для проверки выполнимости булевых функций, заданных конъюнктивными нормальными формами.

Булевы функции находят многочисленные применения при описании работы различных дискретных преобразователей информации — компьютеров, шифраторов и т.д.

Обозначим через  $E_2$  множество  $\{0, 1\}$ .

**Определение 1.**  *$n$ -местной булевой функцией называется любое отображение  $f$  множества  $E_2^n$  во множество  $E_2$ .*

Традиционно через  $P_2(n)$  обозначается множество всех  $n$ -местных булевых функций, а через  $P_2$  — множество всех булевых функций.

Каждую  $n$ -местную булеву функцию можно задать таблицей следующего вида, содержащей  $2^n + 1$  строк и  $n + 2$  столбцов

№	$x_1$	$x_2$	...	$x_{n-1}$	$x_n$	$f(x_1, x_2, \dots, x_{n-1}, x_n)$
1	$\varepsilon_{1,1}$	$\varepsilon_{1,2}$	...	$\varepsilon_{1,n-1}$	$\varepsilon_{1,n}$	$\varepsilon_1$
2	$\varepsilon_{2,1}$	$\varepsilon_{2,2}$	...	$\varepsilon_{2,n-1}$	$\varepsilon_{2,n}$	$\varepsilon_2$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	$\vdots$	$\vdots$
$2^n - 1$	$\varepsilon_{2^n-1,1}$	$\varepsilon_{2^n-1,2}$	...	$\varepsilon_{2^n-1,n-1}$	$\varepsilon_{2^n-1,n}$	$\varepsilon_{2^n-1}$
$2^n$	$\varepsilon_{2^n,1}$	$\varepsilon_{2^n,2}$	...	$\varepsilon_{2^n,n-1}$	$\varepsilon_{2^n,n}$	$\varepsilon_{2^n}$

В этой таблице все  $\varepsilon_{i,j}$  и  $\varepsilon_i$  ( $i = 1, \dots, 2^n$ ,  $j = 1, \dots, n$ ) — это 0 или 1. Для единообразия набору  $\varepsilon_{1,1}, \varepsilon_{1,2}, \dots, \varepsilon_{1,n-1}, \varepsilon_{1,n}$  можно сопоставить натуральное число  $2^{n-1}\varepsilon_{1,1} + 2^{n-2}\varepsilon_{1,2} + \dots + 2\varepsilon_{1,n-1} + \varepsilon_{1,n}$ , двоичными цифрами которого являются элементы этого набора, и перечислять наборы значений аргументов в порядке возрастания этих чисел от 0 до  $2^n - 1$ . Таким образом, в первой строке таблицы набор значений состоит из одних нулей, а в последней — из одних единиц.



При фиксации наборов значений аргументов получаем биективное отображение множества всех  $n$ -местных функций на множество таблиц указанного вида. Так как число таких таблиц равно числу различных последних столбцов, а оно равно  $2^{2^n}$ , то получаем следующую теорему.

**Теорема 1.** При любом  $n$  множество  $P_2(n)$  всех  $n$ -местных булевых функций состоит из  $2^{2^n}$  элементов.

Таким образом, существует четыре 1-одноместные булевы функции: две из них равны тождественно нулю и единице и обозначаются 0 и 1 соответственно, одна тождественная функция, равная своему аргументу, которая иногда обозначается через  $U_1^1$ , и отрицание  $\bar{x}$ , определяемое равенствами  $\bar{0} = 1$  и  $\bar{1} = 0$ .

При  $n$  равном двум получаем 16 2-местных функций. В их число входят две функции, тождественно равные нулю и единице, которые также обозначаются как 0 и 1 соответственно, две функции, равные тождественно своему первому и второму аргументу, обозначаемые соответственно  $U_1^2$  и  $U_2^2$  и называемые функциями проектирования, и 12 других функций, играющих разную роль в теории и приложениях.

По ряду причин наиболее важными из них оказались: конъюнкция, обозначаемая через  $\&$ ,  $\wedge$  или  $\cdot$ , дизъюнкция  $\vee$ , импликация  $\rightarrow$ , эквивалентность  $\leftrightarrow$ , сложение по модулю 2  $\oplus$ , штрих Шеффера  $|$  и символ Лукасевича  $\dagger$  или стрелка Пирса  $\downarrow$ . Эти функции задаются следующими таблицами

$x_1$	$x_2$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\oplus$	$ $	$\dagger$
0	0	0	0	1	1	0	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	0	0	1	1	0
1	1	1	1	1	1	0	0	0

В теории булевых функций, как и в любом разделе математики, сложилась своя специфическая терминология.

**Определение 2.**  $n$ -местная булева функция  $f(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n)$  существенно зависит от своей  $i$ -ой переменной  $x_i$ , если найдется такая последовательность  $\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \dots, \varepsilon_n$ , состоящая из 0 и 1, что

$$f(\varepsilon_1, \dots, \varepsilon_{i-1}, 0, \varepsilon_{i+1}, \dots, \varepsilon_n) \neq f(\varepsilon_1, \dots, \varepsilon_{i-1}, 1, \varepsilon_{i+1}, \dots, \varepsilon_n).$$

Переменные, от которых существенно зависит функция, называются ее существенными переменными, а остальные — несущественными.

**Определение 3.** Если одну булеву функцию можно получить из другой конечным числом операций введения и удаления несущественных переменных, то они считаются равными.

Последнее определение позволяет относительно любого конечного набора булевых функций предполагать, без ограничения общности, что все функции этого набора зависят от одних и тех же переменных. Этого же можно было

бы добиться и по-другому, как это делается, например, в теории рекурсивных функций — введением в рассмотрение функций проектирования  $U_m^n(x_1, \dots, x_n) = x_m$ .

Другим распространенным способом задания булевых функций является их задание термами или формулами, что по сути дела равносильно. Мы остановимся на первом варианте.

Пусть  $\Gamma$  — произвольная система булевых функций. Каждой  $n$ -местной булевой функции  $f$  из  $\Gamma$  сопоставим  $n$ -местный функциональный символ  $\tilde{f}$ , который будем называть именем функции  $f$ .

Индуктивно определим понятие *терма над множеством функций  $\Gamma$* . Предварительно зафиксируем счетное множество переменных  $\{x_1, x_2, \dots, x_n, \dots\}$ .

#### Определение 4.

- 1) Каждая переменная  $x_i$  является термом над множеством функций  $\Gamma$ .
- 2) Если  $f$  —  $n$ -местная булева функция из  $\Gamma$ , а  $t_1, \dots, t_n$  — термы над множеством функций  $\Gamma$ , то  $\tilde{f}(t_1, \dots, t_n)$  — терм над множеством функций  $\Gamma$ .
- 3) Выражение является термом над множеством функций  $\Gamma$  тогда и только тогда, когда это следует из пунктов 1) и 2).

В дальнейшем имя  $\tilde{f}$  булевой функции  $f$  будем обозначать просто через  $f$ , что не приведет к недоразумениям.

Каждый терм  $t$  естественным образом определяет булеву функцию, которую мы обозначим через  $f_t$ .

Индукцией по длине терма  $t$  определим его значение при заданных значениях входящих в него переменных.

Пусть все переменные, входящие в терм  $t$ , содержатся в списке  $x_1, \dots, x_n$ . Возьмем произвольный набор  $\varepsilon_1, \dots, \varepsilon_n$  из 0 и 1 в качестве значений переменных  $x_1, \dots, x_n$ . Определим значение терма  $t$  на этом наборе в соответствии с определением терма.

- 1) Если терм  $t$  — это переменная  $x_i$ , то его значением на указанном наборе будет  $\varepsilon_i$ .
- 2) Пусть терм  $t$  имеет вид  $\tilde{g}(t_1, \dots, t_m)$ , где  $\tilde{g}$  —  $m$ -местный функциональный символ, а значит,  $g$  —  $m$ -местная функция. Обозначим через  $\alpha_1, \dots, \alpha_m$  значения термов  $t_1, \dots, t_m$  при значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$ . Тогда значением терма  $t$  при значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$  будет  $g(\alpha_1, \dots, \alpha_m)$ .

Определим функцию  $f_t$  следующим образом:  $f_t(\varepsilon_1, \dots, \varepsilon_n)$  равно значению терма  $t$  при значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$ .

**Определение 5.**  $n$ -местная функция  $\varphi$  представима термом  $t$ , если все его переменные содержатся среди  $x_1, \dots, x_n$  и  $f_t = \varphi$ , т.е. при любых значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$  значение терма  $t$  равно  $\varphi(\varepsilon_1, \dots, \varepsilon_n)$ .

## §2. Нормальные формы

В этом разделе рассматривается вопрос о представлении булевых функций термами специального вида.

Введем удобное обозначение  $x^\varepsilon = x$ , если  $\varepsilon = 1$  и  $x^\varepsilon = \bar{x}$ , если  $\varepsilon = 0$ .

Непосредственная проверка показывает, что  $\alpha^\beta = 1$  тогда и только тогда, когда  $\alpha = \beta$ .

Примем некоторые общепринятые соглашения: для 2-местной булевой функции  $f$  и термов  $t_1$  и  $t_2$  вместо  $f(t_1, t_2)$  будем писать  $(t_1 f t_2)$ , а часто просто  $t_1 f t_2$ . Например, вместо  $\vee(t_1, t_2) = t_1 \vee t_2$ , а вместо  $\&(t_1, t_2) = t_1 \& t_2$ . Кроме того, запись  $t_1 f t_2 f t_3 f \dots f t_n$  будет служить сокращением для  $((\dots((t_1 f t_2) f t_3) f \dots) f t_n)$ .

Терм вида  $x_{i_1}^{\varepsilon_1} \& \dots \& x_{i_k}^{\varepsilon_k}$ , где  $1 \leq i_1 < \dots < i_k \leq n$ ,  $\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}$ , называется *элементарной конъюнкцией* входящих в него переменных  $x_{i_1}, \dots, x_{i_k}$ .

Терм вида  $\vee x_{i_1}^{\varepsilon_1} \& \dots \& x_{i_k}^{\varepsilon_k}$ , где дизъюнкция берется по некоторым наборам индексов  $(i_1, \dots, i_k)$  и показателей  $(\varepsilon_1, \dots, \varepsilon_k)$ , называется *дизъюнктивной нормальной формой* (ДНФ).

Терм вида  $x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}$ , где  $\varepsilon_1, \dots, \varepsilon_n \in \{0, 1\}$ , называется *совершенной элементарной конъюнкцией* переменных  $x_1, \dots, x_n$ .

Терм вида  $\vee x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}$ , где дизъюнкция берется по некоторым наборам показателей  $(\varepsilon_1, \dots, \varepsilon_n)$ , называется *совершенной дизъюнктивной нормальной формой* (СДНФ).

**Теорема 1.** (Совершенная дизъюнктивная нормальная форма (СДНФ).) Для любой, неравной тождественно 0,  $n$ -местной булевой функции  $f$  выполняется равенство

$$f(x_1, \dots, x_n) = \bigvee_{\substack{(\varepsilon_1, \dots, \varepsilon_n) \in E_2^n \\ f(\varepsilon_1, \dots, \varepsilon_n) = 1}} x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}$$

*Доказательство.* Пусть  $\varepsilon_1, \dots, \varepsilon_n$  — произвольный набор значений переменных  $x_1, \dots, x_n$ . Если на этом наборе функция  $f$  принимает значение 1, то в правую часть доказываемого равенства входит соответствующая элементарная конъюнкция  $x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}$ , которая на наборе  $\varepsilon_1, \dots, \varepsilon_n$  значений переменных  $x_1, \dots, x_n$  принимает значение 1.

Если же на наборе  $\varepsilon_1, \dots, \varepsilon_n$  значений переменных  $x_1, \dots, x_n$  функция  $f$  принимает значение 0, то в правую часть равенства не входит соответствующая элементарная конъюнкция  $x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}$ . Поэтому любая входящая в правую часть этого равенства элементарная конъюнкция на рассматриваемом наборе  $\varepsilon_1, \dots, \varepsilon_n$  значений переменных  $x_1, \dots, x_n$  принимает значение 0. Значит, на этом наборе значений переменных правая часть равенства принимает значение 0.  $\square$

Терм

$$\bigvee_{\substack{(\varepsilon_1, \dots, \varepsilon_n) \in E_2^n \\ f(\varepsilon_1, \dots, \varepsilon_n) = 1}} x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}$$



представляет собой дизъюнкцию совершенных элементарных конъюнкций. Поэтому говорят, что он имеет *совершенную дизъюнктивную нормальную форму*. В совершенную элементарную конъюнкцию переменных  $x_1, \dots, x_n$  каждая из этих переменных или ее отрицание входит ровно один раз. Если отказаться от этого требования, т.е. рассмотреть произвольную конъюнкцию переменных или их отрицаний, то *дизъюнкция* таких конъюнкций называется просто *дизъюнктивной нормальной формой*.

Заметим, что равная тождественно 0 функция представима, например, следующим термом  $x_1 \& \bar{x}_1$ . Поэтому *любая булева функция представима термом над множеством из трех функций  $\{\bar{x}, \vee, \&\}$ , имеющим дизъюнктивную нормальную форму*.

Двойственными понятиями к понятиям совершенной дизъюнктивной нормальной формы и дизъюнктивной нормальной формы служат понятия *совершенной конъюнктивной нормальной формы* и *конъюнктивной нормальной формы*.

Терм вида  $x_{i_1}^{\varepsilon_1} \vee \dots \vee x_{i_k}^{\varepsilon_k}$ , где  $1 \leq i_1 < \dots < i_k \leq n$ ,  $\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}$ , называется *элементарной дизъюнкцией* входящих в него переменных  $x_{i_1}, \dots, x_{i_k}$ .

Терм вида  $\& x_{i_1}^{\varepsilon_1} \vee \dots \vee x_{i_k}^{\varepsilon_k}$ , где конъюнкция берется по некоторым наборам индексов  $(i_1, \dots, i_k)$  и показателей  $(\varepsilon_1, \dots, \varepsilon_k)$ , называется *конъюнктивной нормальной формой* (КНФ).

Терм вида  $x_1^{\varepsilon_1} \vee \dots \vee x_n^{\varepsilon_n}$ , где  $\varepsilon_1, \dots, \varepsilon_n \in \{0, 1\}$ , называется *совершенной элементарной дизъюнкцией* переменных  $x_1, \dots, x_n$ .

Терм вида  $\& x_1^{\varepsilon_1} \vee \dots \vee x_n^{\varepsilon_n}$ , где конъюнкция берется по некоторым наборам показателей  $(\varepsilon_1, \dots, \varepsilon_n)$ , называется *совершенной конъюнктивной нормальной формой* (СКНФ).

**Теорема 2.** (*Совершенная конъюнктивная нормальная форма (СКНФ).*) Для любой, неравной тождественно 1,  $n$ -местной булевой функции  $f$  выполняется равенство

$$f(x_1, \dots, x_n) = \&_{\substack{(\varepsilon_1, \dots, \varepsilon_n) \in E_2^n \\ f(\varepsilon_1, \dots, \varepsilon_n) = 0}} x_1^{\bar{\varepsilon}_1} \vee \dots \vee x_n^{\bar{\varepsilon}_n}$$

*Доказательство.* Пусть  $\varepsilon_1, \dots, \varepsilon_n$  — произвольный набор значений переменных  $x_1, \dots, x_n$ . Если на этом наборе функция  $f$  принимает значение 0, то в правую часть доказываемого равенства входит соответствующая элементарная дизъюнкция  $x_1^{\bar{\varepsilon}_1} \vee \dots \vee x_n^{\bar{\varepsilon}_n}$ , которая на наборе  $\varepsilon_1, \dots, \varepsilon_n$  значений переменных  $x_1, \dots, x_n$  принимает значение 0. А значит, на этом наборе правая часть принимает значение 0.

Если же на наборе  $\varepsilon_1, \dots, \varepsilon_n$  значений переменных  $x_1, \dots, x_n$  функция  $f$  принимает значение 1, то в правую часть равенства не входит соответствующая элементарная дизъюнкция  $x_1^{\bar{\varepsilon}_1} \vee \dots \vee x_n^{\bar{\varepsilon}_n}$ . Поэтому любая входящая в правую часть этого равенства элементарная дизъюнкция на рассматриваемом наборе  $\varepsilon_1, \dots, \varepsilon_n$  значений переменных  $x_1, \dots, x_n$  принимает значение 1. Значит, на

этом наборе значений переменных правая часть равенства принимает значение 1.  $\square$

Терм

$$\bigwedge_{\substack{(\varepsilon_1, \dots, \varepsilon_n) \in E_2^n \\ f(\varepsilon_1, \dots, \varepsilon_n) = 1}} x_1^{\varepsilon_1} \vee \dots \vee x_n^{\varepsilon_n}$$

представляет собой конъюнкцию совершенных элементарных дизъюнкций. Поэтому говорят, что он имеет *совершенную конъюнктивную нормальную форму*. В совершенную элементарную дизъюнкцию переменных  $x_1, \dots, x_n$  каждая из этих переменных или ее отрицание входит ровно один раз. Если отказаться от этого требования, т.е. рассмотреть произвольную дизъюнкцию переменных или их отрицаний, то конъюнкция таких дизъюнкций называется просто *конъюнктивной нормальной формой*.

Заметим, что равная тождественно 1 функция представима, например, следующим термом  $x_1 \vee \bar{x}_1$ . Поэтому *любая булева функция представима термом над множеством из трех функций  $\{\bar{x}, \vee, \&\}$ , имеющим конъюнктивную нормальную форму*.

Обобщением доказанных теорем служит следующая теорема о разложении функции, которая доказывается аналогичным рассуждением.

**Теорема 3.** Для любой  $n$ -местной булевой функции  $f$  при любом  $k$  ( $1 \leq k \leq n$ ) выполняется равенство

$$f(x_1, \dots, x_n) = \bigvee_{(\varepsilon_1, \dots, \varepsilon_k) \in E_2^k} x_1^{\varepsilon_1} \& \dots \& x_k^{\varepsilon_k} \& f(\varepsilon_1, \dots, \varepsilon_k, x_{k+1}, \dots, x_n).$$

При  $k = 1$  получается разложение Шеннона

$$f(x_1, \dots, x_n) = (\bar{x}_1 \& f(0, x_2, \dots, x_n)) \vee (x_1 \& f(1, x_2, \dots, x_n)).$$

### §3. Замыкание классов функций

**Определение 1.** Для произвольного множества  $\Gamma$  булевых функций через  $[\Gamma]$  обозначается множество всех булевых функций, представимых термами над множеством  $\Gamma$ . Множество  $[\Gamma]$  называется **замыканием** множества булевых функций  $\Gamma$ . Если  $[\Gamma] = \Gamma$ , то множество булевых функций  $\Gamma$  называется **замкнутым**.

Отметим простейшие свойства операции замыкания

- 1)  $\Gamma \subseteq [\Gamma]$ ;
- 2) Если  $U \subseteq W$ , то  $[U] \subseteq [W]$ ;
- 3)  $[[\Gamma]] = [\Gamma]$ .

**Определение 2.** Множество  $\Gamma$  булевых функций называется (функционально) полным, если  $[\Gamma] = P_2$ , т.е. любая булева функция представима термом над множеством  $\Gamma$ .

Так как конъюнкция  $x_1 \& x_2$  представима термом  $\overline{x_1 \vee x_2}$ , а дизъюнкция  $x_1 \vee x_2$  — термом  $\overline{\bar{x}_1 \& \bar{x}_2}$ , то из предыдущих теорем следует полнота каждой из следующих трех систем булевых функций

$$\{\bar{x}, \&, \vee\}, \quad \{\bar{x}, \&\}, \quad \{\bar{x}, \vee\}.$$

Так как функция  $\bar{x}$  представима термом  $x|x$ , где  $|$  — штрих Шеффера, а дизъюнкция  $x_1 \vee x_2$  — термом  $(x_1|x_1)|(x_2|x_2)$ , то полной является система, состоящая из одной функции Шеффера. Аналогичным образом устанавливается полнота системы, состоящей лишь из символа Лукасевича  $\dagger$  (стрелки Пирса  $\downarrow$ ).

Рассмотрим еще одну важную полную систему булевых функций. Вместо  $x_1 \& x_2$  пишем просто  $x_1 x_2$ . Так как функция  $\bar{x}$  представима термом  $x \oplus 1$ , то полной является следующая система из четырех булевых функций:

$$\{0, 1, x_1 x_2, x_1 \oplus x_2\}.$$

Термы вида

$$\sum_{i=1}^n \sum_{1 \leq i_1 < i_2 < \dots < i_t \leq n} a_{i_1, i_2, \dots, i_t} x_{i_1} x_{i_2} \dots x_{i_t} \oplus a,$$

где коэффициенты  $a_{i_1, i_2, \dots, i_t}$  и  $a$  — это 0 или 1, называются полиномами Жегалкина.

Так как для булевых функций выполняются равенства

$$fg = gf, \quad f \oplus g = g \oplus f, \quad f(g \oplus h) = fg \oplus fh, \quad ff = f,$$

то из представимости произвольной булевой функции термом над множеством

$$\{0, 1, x_1 x_2, x_1 \oplus x_2\}$$

следует представимость произвольной булевой функции полиномом Жегалкина.

**Теорема 1.** Произвольная булева функция однозначно представима полиномом Жегалкина.

*Доказательство.* В силу вышесказанного необходимо доказать лишь однозначность представления. Если два различных полинома Жегалкина представляют одну и ту же булеву функцию, то их сумма будет ненулевым полиномом Жегалкина, представляющим тождественно равную 0 функцию. Если этот полином имеет вид

$$\sum_{i=1}^n \sum_{1 \leq i_1 < i_2 < \dots < i_t \leq n} a_{i_1, i_2, \dots, i_t} x_{i_1} x_{i_2} \dots x_{i_t} \oplus a,$$

то легко понять, что  $a = 0$ . Среди ненулевых коэффициентов выберем такое  $a_{i_1, i_2, \dots, i_t}$ , что  $a_{i_1, i_2, \dots, i_t} = 1$  и  $t$  — наименьшее из возможных. Полагая  $x_{i_1} = 1$ ,  $x_{i_2} = 1, \dots, x_{i_t} = 1$ , остальные переменные равными 0, получим, что значение полинома равно 1, что противоречит предположению.  $\square$

Конъюнкция  $x_{i_1} x_{i_2} \dots x_{i_t}$  называется *одночленом* степени  $k$ . *Степенью нелинейности* (порядком) многочлена Жегалкина функции  $f$  называется наибольшая из степеней входящих в него одночленов. Степень функции  $f$  обозначается через  $\deg f$ . Функции степени 1 называются аффинными или линейными.

Конечно, стремясь к максимальной согласованности с аналитической геометрией, линейной алгеброй и функциональным анализом, следовало бы называть линейными функции вида  $a_1 x_1 + \dots + a_n x_n$ , а функции более общего вида  $a_0 + a_1 x_1 + \dots + a_n x_n$  называть аффинными. Однако в дальнейшем функциям вида  $a_1 x_1 + \dots + a_n x_n$  не будет уделено особое внимание, поэтому мы будем называть линейными наряду с ними и функции вида  $a_0 + a_1 x_1 + \dots + a_n x_n$ .

## §4. Теорема Э. Поста о полноте

Важнейшим вопросом теории булевых функций является вопрос об “эффективных” необходимых и достаточных условиях полноты системы функций. Исчерпывающий ответ на него в рассматриваемом случае 2-значных функций даст теорема Э. Поста.

Рассмотрим следующие пять замкнутых классов булевых функций.

Пусть  $\varepsilon$  — это 0 или 1. Класс  $C_\varepsilon$  состоит из всех функций, сохраняющих  $\varepsilon$ , т.е. таких функций  $f$ , для которых выполняется равенство  $f(\varepsilon, \dots, \varepsilon) = \varepsilon$ . Легко проверить, что класс  $C_\varepsilon$  замкнут. Класс  $C_\varepsilon(n)$  всех  $n$ -местных функций, сохраняющих  $\varepsilon$ , состоит из  $2^{2^n-1}$  функций.

**Определение 1.**  $n$ -местная функция  $f$  называется *линейной*, если она удовлетворяет равенству вида

$$f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n,$$

где  $a_0, a_1, \dots, a_n$  — фиксированный для  $f$  набор коэффициентов из 0 и 1.

Класс  $L(n)$   $n$ -местных линейных функций состоит из  $2^{n+1}$  функций.

Еще раз заметим, что иногда в литературе функции из класса  $L(n)$  называются *аффинными* функциями. В таком случае линейные функции — это аффинные функции с  $a_0 = 0$ , т.е. функции вида  $a_1 x_1 \oplus \dots \oplus a_n x_n$ .

Через  $L$  обозначается класс всех линейных функций. Так как  $L = \{1, \oplus\}$ , то легко понять, что  $L$  — замкнутый класс. Впрочем, в этом легко убедиться и непосредственно.

**Определение 2.**  $n$ -местная функция  $f$  называется *самодвойственной*, если она удовлетворяет равенству

$$f(\neg x_1, \dots, \neg x_n) = \neg f(x_1, \dots, x_n).$$

Обозначим через  $S$  класс всех самодвойственных функций.

Так как на наборах  $(\varepsilon_1, \dots, \varepsilon_n)$  и  $(\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n)$   $n$ -местная самодвойственная функция принимает противоположные значения, то для ее задания необходимо лишь  $2^n/2$  строк таблицы, поэтому класс  $S(n)$   $n$ -местных самодвойственных функций состоит из  $2^{2^{n-1}}$  элементов.

**Теорема 1.** Класс  $S$  самодвойственных функций замкнут.

*Доказательство.* Так как каждая переменная  $x_i$  задает самодвойственную функцию, то достаточно доказать, что если  $g(x_1, \dots, x_n)$ ,  $f_1(x_1, \dots, x_n)$ , ...,  $f_m(x_1, \dots, x_n)$  — самодвойственные функции, а функция  $f$  является их суперпозицией, т.е. удовлетворяет равенству

$$f(x_1, \dots, x_n) = g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

то  $f$  — самодвойственная функция. Но это сразу следует из равенств

$$\begin{aligned} f(\neg x_1, \dots, \neg x_n) &= g(f_1(\neg x_1, \dots, \neg x_n), \dots, f_m(\neg x_1, \dots, \neg x_n)) = \\ &= g(\neg f_1(x_1, \dots, x_n), \dots, \neg f_m(x_1, \dots, x_n)) = \\ &= \neg g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) = \\ &= \neg f(x_1, \dots, x_n). \end{aligned}$$

□

В доказательстве мы воспользовались возможностью введения фиктивных переменных, поэтому могли считать, что функции зависят от одного и того же набора переменных. При этом саму переменную  $x_i$  мы можем трактовать как  $n$ -местную функцию проектирования  $U_i^n(x_1, \dots, x_n)$ .

Для определения пятого необходимого нам замкнутого класса функций определим на множестве  $E_2^n$  отношение частичного порядка, полагая для наборов  $\alpha = (\alpha_1, \dots, \alpha_n)$  и  $\beta = (\beta_1, \dots, \beta_n)$

$$\alpha \leq \beta \iff \alpha_1 \leq \beta_1 \& \dots \& \alpha_n \leq \beta_n.$$

Очевидно, что отношение  $\leq$  на множестве  $E_2^n$  является отношением частичного порядка, т.е. оно рефлексивно, транзитивно и антисимметрично.

**Определение 3.**  $n$ -местная функция  $f$  называется монотонной, если для любых двух наборов значений ее аргументов  $\alpha$  и  $\beta$  из неравенства  $\alpha \leq \beta$  следует неравенство  $f(\alpha) \leq f(\beta)$ .

Обозначим через  $M(n)$  класс всех  $n$ -местных монотонных функций, а через  $M$  — класс всех монотонных функций.

Вопрос о функции  $\psi(n) = |M(n)|$ , число элементов множества  $M(n)$ , в отличие от рассмотренных выше функций  $|C_0(n)|$ ,  $|C_1(n)|$ ,  $|L(n)|$  и  $|S(n)|$ , является существенно более сложным. Приведем некоторые сведения исторического характера, заимствованные из книги В.М. Фомичева [47]. Сама постановка вопроса восходит к Р. Дедекинду (1897 г.). Им же были вычислены значения функции



$\psi(n)$  при  $n \leq 4$ . В 1940 г. Р. Черч вычислил  $\psi(5)$ . В 1948 г. М. Уорд вычислил  $|M(6)|$  и получил нижнюю оценку

$$2^{B(n)} \leq \psi(n), \quad \text{где } B(n) = C_n^{\lfloor n/2 \rfloor}, \quad \text{а } [\alpha] \text{ — целая часть } \alpha.$$

В качестве верхней оценки функции  $\psi(n)$  первоначально служила функция  $n^{B(n)}$ . Эта оценка постепенно в ряде работ уточнялась и была доведена до  $3^{B(n)}$ . Таким образом, были установлены неравенства

$$2^{B(n)} \leq |M(n)| \leq 3^{B(n)}.$$

В последующих работах эти неравенства уточнялись и была получена асимптотическая оценка функции  $\psi(n)$ , однако обсуждение этого вопроса увело бы нас слишком далеко от основной темы. Мы лишь хотели продемонстрировать, как близко от основной темы нашего обсуждения находятся очень сложные математические вопросы.

**Теорема 2.** *Класс  $M$  монотонных функций замкнут.*

*Доказательство.* Так как каждая переменная  $x_i$  задает монотонную функцию, то достаточно доказать, что если  $g(x_1, \dots, x_m), f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$  — монотонные функции, а функция  $f$  является их суперпозицией, т.е. удовлетворяет равенству

$$f(x_1, \dots, x_n) = g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

то  $f$  — монотонная функция. Но это сразу следует из неравенств

$$f_1(\alpha) \leq f_1(\beta) \& \dots \& f_m(\alpha) \leq f_m(\beta), \\ g(f_1(\alpha), \dots, f_m(\alpha)) \leq g(f_1(\beta), \dots, f_m(\beta)), \quad f(\alpha) \leq f(\beta).$$

□

В теории булевых функций важную роль играет следующая теорема, доказанная Э. Постом.

**Теорема 3. (Э. Пост)** *Для того, чтобы система функций  $\Gamma$  была полной, необходимо и достаточно, чтобы она не содержалась ни в одном из пяти замкнутых классов функций  $C_0, C_1, L, S$  и  $M$ , т.е. чтобы в ней нашлись такие функции  $f_0, f_1, f_2, f_3$  и  $f_4$ , что*

$$f_0 \notin C_0, \quad f_1 \notin C_1, \quad f_2 \notin L, \quad f_3 \notin S, \quad f_4 \notin M.$$

Необходимость указанного условия очевидна.

Доказательству его достаточности традиционно предшествует доказательство нескольких лемм.

**Лемма 1. (Лемма о несамодвойственной функции.)** Если  $f$  — несамодвойственная функция, то через нее и отрицание выразимы обе константы 0 и 1.

*Доказательство.* Пусть  $f$  — несамодвойственная функция. Тогда найдется такой набор  $(\varepsilon_1, \dots, \varepsilon_n)$ , что

$$f(\varepsilon_1, \dots, \varepsilon_n) = f(\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n).$$

Рассмотрим функцию

$$\varphi(x) = f(x^{\varepsilon_1}, \dots, x^{\varepsilon_n}).$$

Тогда

$$\begin{aligned} \varphi(0) = f(0^{\varepsilon_1}, \dots, 0^{\varepsilon_n}) &= f(\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n) = \\ &= f(\varepsilon_1, \dots, \varepsilon_n) = f(1^{\varepsilon_1}, \dots, 1^{\varepsilon_n}) = \varphi(1). \end{aligned}$$

Значит, функция  $\varphi(x)$  — константа, тогда  $\overline{\varphi(x)}$  — другая константа.  $\square$

**Лемма 2. (Лемма о немонотонной функции.)** Если  $f$  — немонотонная функция, то через нее и константы 0 и 1 выразимо отрицание.

*Доказательство.* Пусть  $f$  — немонотонная функция, тогда найдутся два таких набора  $\alpha$  и  $\beta$ , что  $\alpha < \beta$ , но  $f(\alpha) > f(\beta)$  (напомним, что  $\alpha < \beta \Leftrightarrow \alpha \leq \beta \& \alpha \neq \beta$ ). Так как от набора  $\alpha$  к набору  $\beta$  можно перейти путем конечного числа преобразований типа “один нулевой элемент набора заменяется на 1” и  $f(\alpha) > f(\beta)$ , то найдутся такие два “соседних” набора  $\tilde{\alpha}$  и  $\tilde{\beta}$ , что  $\tilde{\alpha} < \tilde{\beta}$ , но  $f(\tilde{\alpha}) > f(\tilde{\beta})$ . Пусть

$$\begin{aligned} \tilde{\alpha} &= (\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n), \quad \tilde{\beta} = (\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n), \\ f(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1}, \dots, \alpha_n) &= 1, \quad f(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1}, \dots, \alpha_n) = 0 \end{aligned}$$

Рассмотрим функцию

$$\varphi(x) = f(\alpha_1, \dots, \alpha_{i-1}, x, \alpha_{i+1}, \dots, \alpha_n).$$

Тогда  $\varphi(0) = 1$ ,  $\varphi(1) = 0$ , т.е.  $\varphi(x) = \bar{x}$ .  $\square$

**Лемма 3. (Лемма о нелинейной функции.)** Если  $f$  — нелинейная функция, то через нее, отрицание и константы 0 и 1 выразима конъюнкция.

*Доказательство.* Так как  $f$  — нелинейная функция, то соответствующий ей полином Жегалкина содержит слагаемые степени не менее двух. Можно считать, что этот полином имеет вид

$$x_1 x_2 f_1(x_3, \dots, x_n) \oplus x_1 f_2(x_3, \dots, x_n) \oplus x_2 f_3(x_3, \dots, x_n) \oplus f_4(x_3, \dots, x_n),$$

причем полином  $f_1(x_3, \dots, x_n)$  не равен тождественно нулю. Значит, найдутся такие  $\varepsilon_3, \dots, \varepsilon_n$ , что  $f_1(\varepsilon_3, \dots, \varepsilon_n) = 1$ . Рассмотрим функцию

$$\varphi(x_1, x_2) = f(x_1, x_2, \varepsilon_3, \dots, \varepsilon_n).$$



Тогда

$$\varphi(x_1, x_2) = x_1 x_2 \oplus \alpha x_1 \oplus \beta x_2 \oplus \gamma.$$

В силу равенства

$$\varphi(x_1 \oplus \beta, x_2 \oplus \alpha) = x_1 x_2 \oplus \alpha \beta \oplus \gamma$$

получаем, что

$$x_1 x_2 = \varphi(x_1 \oplus \beta, x_2 \oplus \alpha) \oplus \alpha \beta \oplus \gamma.$$

Для завершения доказательства леммы остается заметить, что  $x \oplus 1 = \bar{x}$ .  $\square$

Приступаем к доказательству теоремы Э. Поста. Пусть  $f_0, f_1, f_2, f_3$  и  $f_4$  — такие функции, что

$$f_0 \notin C_0, f_1 \notin C_1, f_2 \notin L, f_3 \notin S, f_4 \notin M.$$

Воспользуемся функциями  $f_0, f_1$  и  $f_3$  для построения констант 0 и 1.

Так как  $f_0 \notin C_0$ , то  $f_0(0, \dots, 0) = 1$ . Рассмотрим два случая.

Если и  $f_0(1, \dots, 1) = 1$ , то одна константа 1 уже есть  $f_0(x, \dots, x) = 1$ , а вторую получаем из равенства

$$0 = f_1(1, \dots, 1) = f_1(f_0(x, \dots, x), \dots, f_0(x, \dots, x)).$$

Если же  $f_0(1, \dots, 1) = 0$ , то

$$\bar{x} = f_0(x, \dots, x).$$

По лемме о несамодвойственной функции из функций  $\bar{x}$  и  $f_3$  получаем обе константы 0 и 1.

Используя константы 0 и 1 и немонотонную функцию  $f_4$ , по лемме о немонотонной функции получаем отрицание  $\bar{x}$ .

Используя константы 0 и 1, отрицание  $\bar{x}$  и нелинейную функцию  $f_2$ , по лемме о нелинейной функции получаем конъюнкцию  $x_1 \& x_2$ .

Таким образом,  $\{\bar{x}, x_1 \& x_2\} \subseteq [\Gamma]$ . Но тогда

$$P_2 = [\{\bar{x}, x_1 \& x_2\}] \subseteq [\Gamma] \subseteq P_2.$$

Значит,  $[\Gamma] = P_2$ .

**Следствие.** Если  $\Gamma$  — полная система функций, то в ней существует полная подсистема, состоящая из четырех функций.

Пусть  $f_0, f_1, f_2, f_3$  и  $f_4$  — такие функции из системы  $\Gamma$ , что

$$f_0 \notin C_0, f_1 \notin C_1, f_2 \notin L, f_3 \notin S, f_4 \notin M.$$

Покажем, что одну из этих функций можно удалить, не нарушая полноты системы.

Если  $f_0(1, \dots, 1) = 0$ , то  $f_0 \notin C_1$  и функцию  $f_1$  можно удалить.

Если же  $f_0(1, \dots, 1) = 1$ , то  $f_0 \notin S$  и можно удалить функцию  $f_3$ .

Покажем, что дальнейшее сокращение числа функций в полной системе не всегда возможно. Рассмотрим систему из четырех функций  $f_1 = x_1x_2$ ,  $f_2 = 0$ ,  $f_3 = 1$  и  $f_4 = x_1 \oplus x_2 \oplus x_3$ . Тогда  $f_3 \notin C_0$ ,  $f_2 \notin C_1$ ,  $f_1 \notin S$  и  $f_4 \notin M$ ,  $f_1 \notin L$ , т.е. система из четырех функций  $f_1 = x_1x_2$ ,  $f_2 = 0$ ,  $f_3 = 1$  и  $f_4 = x_1 \oplus x_2 \oplus x_3$  полна, но

$$\{f_2, f_3, f_4\} \subseteq L, \quad \{f_1, f_3, f_4\} \subseteq C_1, \quad \{f_1, f_2, f_4\} \subseteq C_0, \quad \{f_1, f_2, f_3\} \subseteq M.$$

**Следствие.** Любой замкнутый класс булевых функций, отличный от класса  $P_2$  всех функций, содержится в одном из пяти замкнутых классов функций  $C_0$ ,  $C_1$ ,  $L$ ,  $S$  и  $M$ .

В 1921 г. Э. Пост дал полное описание всех замкнутых классов булевых функций. Сообщение об этом выдающемся результате было опубликовано в заметке [55], а подробные доказательства изложены в монографии [56]. Их изложению посвящена и монография [52].

Э. Пост установил, что множество всех замкнутых классов булевых функций счетно и в каждом замкнутом классе  $K$  существует конечная система функций  $F \subseteq K$  такая, что  $K = [F]$ . Если при этом ни для какого собственного подмножества  $F_1$  множества  $F$  не выполняется равенство  $K = [F_1]$ , то множество  $F$  называется базисом класса  $K$ .

Например, базисами класса  $S$  самодвойственных функций являются следующие три системы функций

$$\{(x \& y) \vee (x \& \bar{z}) \vee (\bar{y} \& \bar{z})\}, \quad \overline{\{(x \& y) \vee (x \& z) \vee (y \& z)\}}, \\ \{\bar{x}, (x \& y) \vee (x \& z) \vee (y \& z)\}.$$

Базисом класса  $M$  монотонных функций является система из четырех функций

$$\{(x \vee y), (x \& y), 0, 1\}.$$

Функция  $(x \& y) \vee (x \& z) \vee (y \& z)$  образует базис подкласса класса  $M$ , состоящего из самодвойственных монотонных функций.

Базисом класса  $L$  линейных функций является система из двух функций  $\{0, (x \oplus y \oplus 1)\}$ .

Исчерпывающие сведения о замкнутых классах булевых функций можно найти в монографии [52].

**Определение 4.** Замкнутый класс булевых функций, отличный от класса  $P_2$  всех функций, называется максимальным, если он не содержится ни в каком замкнутом классе, отличном от него самого и класса  $P_2$  всех функций.

**Следствие.** Любой максимальный класс булевых функций совпадает с одним из пяти замкнутых классов функций  $C_0$ ,  $C_1$ ,  $L$ ,  $S$  и  $M$ .

Максимальные классы функций носят название *предполных* классов. Это связано с тем, что если  $K$  — максимальный класс, то  $[K] = K \neq P_2$ , но для любой функции  $f$ , не входящей в  $K$ ,  $[K \cup \{f\}] = P_2$ .

Покажем, что *каждый из пяти замкнутых классов функций  $C_0, C_1, L, S$  и  $M$  является максимальным.*

Конечно, это можно было бы доказать, используя лемму Цорна, однако такое доказательство было бы “слишком далеко от дискретной математики”. Поэтому рассмотрим в некотором смысле “более конструктивное” доказательство.

Для доказательства достаточно воспользоваться следующей таблицей Поста.

	$C_0$	$C_1$	$L$	$S$	$M$
0	+	—	+	—	+
1	—	+	+	—	+
$\neg x$	—	—	+	+	—
$x_1 x_2$	+	+	—	—	+
$x_1 \oplus x_2 \oplus x_3$	+	+	+	+	—
$x_1 x_2 \oplus x_2 x_3 \oplus x_1 x_3$	+	+	—	+	+

Наличие + (—) на пересечении некоторой строки и некоторого столбца свидетельствует, что соответствующая функция входит (не входит) в соответствующий класс. И остается воспользоваться теоремой Э. Поста. Например, для установления максимальной класса  $L$  заметим, что плюсам из этого столбца в каждом из оставшихся столбцов соответствует хотя бы один минус, поэтому для получения полной системы функций достаточно к системе  $L$  присоединить любую, не входящую в нее функцию.

В заключение параграфа рассмотрим вопрос о нахождении всех полных систем в классе  $P_2(n)$  всех  $n$ -местных функций.

Для этого занумеруем все  $n$ -местные функции, например, следующим образом. Зафиксируем нумерацию всех наборов  $(\varepsilon_{i,1}, \dots, \varepsilon_{i,n})$  значений аргументов, например, в порядке возрастания двоичных чисел

$$\overline{\varepsilon_{i,1} \dots \varepsilon_{i,n}} = 2^{n-1} \varepsilon_{i,1} + \dots + \varepsilon_{i,n}.$$

Функции  $f$  присвоим номер

$$\overline{f(\varepsilon_{1,1}, \dots, \varepsilon_{1,n}) f(\varepsilon_{2,1}, \dots, \varepsilon_{2,n}) \dots f(\varepsilon_{2^n,1}, \dots, \varepsilon_{2^n,n})}.$$

Заметим, что при такой нумерации номер 0 будет у нулевой функции, а максимальный номер  $2^{2^n} - 1$  — у единичной функции.

Пусть  $m = 2^{2^n} - 1$ . Рассмотрим таблицу

	$C_0$	$C_1$	$L$	$S$	$M$
0	$\alpha_{0,1}$	$\alpha_{0,2}$	$\alpha_{0,3}$	$\alpha_{0,4}$	$\alpha_{0,5}$
1	$\alpha_{1,1}$	$\alpha_{1,2}$	$\alpha_{1,3}$	$\alpha_{1,4}$	$\alpha_{1,5}$
...	...	...	...	...	...
$m$	$\alpha_{m,1}$	$\alpha_{m,2}$	$\alpha_{m,3}$	$\alpha_{m,4}$	$\alpha_{m,5}$

где  $\alpha_{i,j} = 1$ , если функция  $f_i$  не принадлежит  $j$ -ому классу, и  $\alpha_{i,j} = 0$  в противном случае.

Записываем условие “Быть полной системой функций” в виде “формулы”

$$\bigwedge_{i=1}^5 \bigvee_{a_i, j=1} f_i.$$

Преобразуем эту “формулу” в эквивалентную “формулу” вида

$$\bigvee_{i \in A} \bigwedge_{j \in B_i} f_j.$$

Тогда все полные системы функций даются семейством множеств

$$(\{f_j \mid j \in B_i\})_{i \in A}.$$

## §5. Сложность некоторых задач

*Проблема выполнимости для булевых функций состоит в определении по произвольной булевой функции, существует ли такой набор значений ее аргументов, на котором она принимает значение 1.*

Для решения проблемы выполнимости существует простой алгоритм полного перебора всех наборов значений аргументов  $n$ -местной функции  $f$  с вычислением ее значения на каждом наборе. Однако подобный алгоритм не может рассматриваться как “реально выполнимый”, так как в процессе его выполнения в общем случае придется перебрать  $2^n$  наборов значений аргументов. Но если булева функция задана термом длины  $L$ , например, конъюнктивной нормальной формой, является выполнимой и нам “оракул” сообщил соответствующий выполняющий набор, называемый в данном случае *сертификатом выполнимости*, то мы можем за полиномиальное время от  $L$  убедиться в правильности (достоверности) этого сертификата. Поэтому говорят, что *проблема выполнимости для булевых функций принадлежит классу NP*. Она является в этом классе “самой сложной” задачей в том смысле, что любая задача из этого класса за полиномиальное время сводится к ней. Любая проблема, к которой за полиномиальное время сводится проблема выполнимости для булевых функций, называется *NP-трудной проблемой*.

**Теорема 1.** *Проблема полноты для конечных систем булевых функций является NP-трудной.*

*Доказательство.* Для произвольной  $n$ -местной булевой функции  $f(x_1, \dots, x_n)$  рассмотрим функцию

$$\varphi(x_1, \dots, x_n, y_1, y_2) = (f(x_1, \dots, x_n) \& \neg y_1) \vee (\neg y_2).$$

Покажем, что

“функция  $f(x_1, \dots, x_n)$  выполнима тогда и только тогда, когда система  $\{\varphi(x_1, \dots, x_n, y_1, y_2)\}$  полна.”

Если функция  $f(x_1, \dots, x_n)$  невыполнима, т.е. она тождественно равна 0, то  $\varphi(x_1, \dots, x_n, y_1, y_2) \equiv (\neg y_2)$ . Значит,  $[\varphi(x_1, \dots, x_n, y_1, y_2)] \subseteq L \neq P_2$ .

Пусть функция  $f(x_1, \dots, x_n)$  выполнима и  $(\varepsilon_1, \dots, \varepsilon_n)$  — такой набор ее аргументов, что  $f(\varepsilon_1, \dots, \varepsilon_n) = 1$ .

Для доказательства полноты системы  $\{\varphi(x_1, \dots, x_n, y_1, y_2)\}$  воспользуемся теоремой Э. Поста.

Так как  $\varphi(0, \dots, 0, 0, 0) = 1$  и  $\varphi(1, \dots, 1, 1, 1) = 0$ , то  $\varphi(x_1, \dots, x_n, y_1, y_2) \notin C_0$  и  $\varphi(x_1, \dots, x_n, y_1, y_2) \notin C_1$ .

Допустим, что  $\varphi(x_1, \dots, x_n, y_1, y_2) \in L$ .

Тогда выполняется равенство вида

$$\varphi(x_1, \dots, x_n, y_1, y_2) = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n \oplus b_1 y_1 \oplus b_2 y_2.$$

Из которого получаем

$$\begin{aligned} \varphi(\varepsilon_1, \dots, \varepsilon_n, y_1, y_2) &= a_0 \oplus a_1 \varepsilon_1 \oplus \dots \oplus a_n \varepsilon_n \oplus b_1 y_1 \oplus b_2 y_2, \\ y_1 | y_2 &= b_0 \oplus b_1 y_1 \oplus b_2 y_2. \end{aligned}$$

Что противоречит нелинейности функции Шеффера  $|$ .

Значит,  $\varphi(x_1, \dots, x_n, y_1, y_2) \notin L$ .

Так как

$$\varphi(\varepsilon_1, \dots, \varepsilon_n, 0, 0) = 1, \quad \varphi(\varepsilon_1, \dots, \varepsilon_n, 1, 1) = 0,$$

то  $\varphi(x_1, \dots, x_n, y_1, y_2) \notin M$ .

Допустим, что  $\varphi(x_1, \dots, x_n, y_1, y_2) \in S$ . Тогда

$$\varphi(\neg x_1, \dots, \neg x_n, \neg y_1, \neg y_2) = \neg \varphi(x_1, \dots, x_n, y_1, y_2),$$

т.е.

$$\begin{aligned} (f(\neg x_1, \dots, \neg x_n) \& y_1) \vee y_2 &= \overline{(f(x_1, \dots, x_n) \& \neg y_1) \vee (\neg y_2)} = \\ &= \overline{(f(x_1, \dots, x_n) \vee y_1) \& y_2}. \end{aligned}$$

Пологая  $(x_1, \dots, x_n) := (\neg \varepsilon_1, \dots, \neg \varepsilon_n)$ ,  $\varepsilon := \overline{f(\neg \varepsilon_1, \dots, \neg \varepsilon_n)}$ , получим

$$(y_1 \vee y_2) = (\varepsilon \vee y_1) \& y_2.$$

Замена  $y_1$  на  $\varepsilon$ , а  $y_2$  — на  $\neg \varepsilon$  дает равенство  $1 = 0$ .

Полученное противоречие показывает, что  $\varphi(x_1, \dots, x_n, y_1, y_2) \notin S$ .

Поэтому по теореме Э. Поста  $[\varphi(x_1, \dots, x_n, y_1, y_2)] = P_2$ . □

Так как  $[\varphi(x_1, \dots, x_n, y_1, y_2)] = P_2$  тогда и только тогда, когда  $| \in [\varphi(x_1, \dots, x_n, y_1, y_2)]$ , где  $|$  — штрих Шеффера, то получаем

**Следствие 1.** Проблема вхождения в  $[\varphi(x_1, \dots, x_n, y_1, y_2)]$  NP-трудна.

Рассмотрим трудность проблем вхождения в классы  $L$ ,  $M$  и  $S$ .

Так как функция  $f(x_1, \dots, x_n)$  выполнима тогда и только тогда, когда

$$f(x_1, \dots, x_n) \& (y_1 \& y_2) \notin L,$$

то получаем

**Следствие 2.** Проблема вхождения в класс  $L$  является  $NP$ -трудной.

Аналогично, так как функция  $f(x_1, \dots, x_n)$  выполнима тогда и только тогда, когда

$$f(x_1, \dots, x_n) \& (\bar{y}_1) \notin M,$$

то получаем

**Следствие 3.** Проблема вхождения в класс  $M$  является  $NP$ -трудной.

Покажем, что функция  $f(x_1, \dots, x_n)$  невыполнима тогда и только тогда, когда

$$f(x_1, \dots, x_n) \vee y_1 \in S.$$

Если функция  $f(x_1, \dots, x_n)$  невыполнима,

$$f(x_1, \dots, x_n) \vee y_1 = y_1 \in S.$$

Допустим, что

$$f(x_1, \dots, x_n) \vee y_1 \in S.$$

Тогда при любых значениях  $x_1, \dots, x_n$  и  $y_1$  выполняется равенство

$$f(\neg x_1, \dots, \neg x_n) \vee \neg y_1 = \neg(f(x_1, \dots, x_n) \vee y_1).$$

Значит,

$$f(\neg x_1, \dots, \neg x_n) \vee \neg y_1 = \neg f(x_1, \dots, x_n) \& \neg y_1.$$

Полагая  $y_1 = 0$ , получаем, что  $f(x_1, \dots, x_n)$  равно тождественно 0.

Т.е.  $f(x_1, \dots, x_n)$  невыполнима.

Поэтому получаем

**Следствие 4.** Проблема вхождения в класс  $S$  является  $NP$ -трудной.

## §6. Спектральное разложение булевых функций

Булевы функции играют важную роль в криптографии как важное средство проектирования электронных шифраторов, впрочем как и компьютеров, и исследования их свойств.

Одной из самых знаменитых шифрмашин второй мировой войны была “Энигма” (“Enigma”), в устройстве которой важную роль играли шифрующие диски. Ее конструкция была несколько усложнена по сравнению с предшествующими дисковыми шифрмашинами — после дисков располагалась неподвижная обратимая розетка, которая обеспечивала дополнительное прохождение импульса



тока через систему дисков в обратном направлении, что давало двойное шифрование каждой буквы. Одной из особенностей “Энигмы” было неравномерное движение дисков. В 1923 г. “Энигма” выставлялась на конгрессе международного почтового союза. Однако 10 лет этот проект не имел коммерческого успеха. Лишь после прихода к власти в Германии Гитлера в период перевооружения немецкой армии и во время второй мировой войны “Энигма” стала широко использоваться в армии, ВМС и ВВС Германии. Этому, в частности, способствовала портативность “Энигмы”, работа от батареи и прочный, нетяжелый деревянный футляр. В рамках операции “Ультра” английским спецслужбам удалось найти способ читать переписку, зашифрованную на “Энигме”. Эта возможность ценилась настолько высоко, что У. Черчилль фактически пожертвовал городом Ковентри и его жителями, когда английским спецслужбам удалось перехватить и расшифровать сообщение, содержащее информацию о плане бомбардировки этого города немецкой авиацией — не были эвакуированы жители, не предприняты серьезные дополнительные меры безопасности, ибо это могло натолкнуть немецкое командование на догадку, что их зашифрованная переписка читается противником. Мы воздержимся от моральной оценки подобных действий британского руководства, ибо моральные оценки в подобных ситуациях весьма затруднительны — они даются выжившими, а не погибшими, принесенными в жертву.

Для перебора ключевых элементов “Энигмы” с целью решения задачи ее дешифрования в 1942 году группой британских специалистов под руководством А. Тьюринга была сконструирована первая вычислительная машина “Colossus”. Этот первый британский компьютер стал мощнейшим орудием для анализа алгоритмов шифрования.

Множество  $I(f)$  всех наборов аргументов, на которых  $n$ -местная функция  $f$  принимает значение 1, называется *областью истинности* функции  $f$ , а число элементов в нем — *весом* функции  $f$  и обозначается через  $||f||$ .

Ясно, что  $0 \leq ||f|| \leq 2^n$ . Равенство достигается на функциях константах 0 и 1.

Если  $||f|| = 2^{n-1}$ , то функция  $f$  называется *равновероятной* или *сбалансированной*.

На векторном пространстве  $V_n = E_2^n$  всех  $n$ -мерных булевых векторов над полем  $\mathbb{Z}_2$  рассмотрим билинейную функцию, полагая для векторов  $a = (a_1, \dots, a_n)$  и  $b = (b_1, \dots, b_n)$

$$(a, b) = a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_n b_n.$$

Для произвольного фиксированного вектора  $a = (a_1, \dots, a_n)$  функция

$$(a, x) = a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n, \text{ где } x = (x_1, \dots, x_n),$$

является линейной.

Рассмотрим на векторном пространстве  $E_2^n$  функцию

$$e^{i\pi(a,x)} = (-1)^{(a,x)},$$



принимая рациональные значения. Подобные функции называются *псевдобулевыми*. Тогда  $e^{i\pi(a,x)} = 1$ , если  $(a, x) = 0$ , и  $e^{i\pi(a,x)} = -1$ , если  $(a, x) = 1$ .

Существует  $2^n$  функций вида  $(-1)^{(a,x)}$ .

На множестве всех  $n$ -местных функций, определенных на  $E_2^n$ , определим скалярное произведение равенством

$$\langle f, g \rangle = \sum_{x \in E_2^n} f(x)g(x).$$

Билинейность и симметричность этого произведения очевидны. Кроме того,

$$\langle f, f \rangle = \|f\|^2.$$

Следующая теорема утверждает, что функции  $(-1)^{(a,x)}$  попарно ортогональны.

**Теорема 1.** При  $a \neq b$

$$\langle (-1)^{(a,x)}, (-1)^{(b,x)} \rangle = \sum_{x \in E_2^n} (-1)^{(a,x)}(-1)^{(b,x)} = 0$$

и

$$\langle (-1)^{(a,x)}, (-1)^{(a,x)} \rangle = \sum_{x \in E_2^n} (-1)^{(a,x)}(-1)^{(a,x)} = 2^n.$$

*Доказательство.* Если  $a \neq 0$ , то функция  $(a, x)$  принимает значение 0, ровно в половине точек множества  $E_2^n$ , а значение 1 — в другой половине точек множества  $E_2^n$ . Поэтому

$$\sum_{x \in E_2^n} (-1)^{(a,x)} = 0$$

при  $a \neq 0$ . Очевидно, что при  $a = 0$

$$\sum_{x \in E_2^n} (-1)^{(a,x)} = 2^n.$$

Для завершения доказательства теоремы остается воспользоваться равенством

$$\begin{aligned} \langle (-1)^{(a,x)}, (-1)^{(b,x)} \rangle &= \sum_{x \in E_2^n} (-1)^{(a,x)}(-1)^{(b,x)} = \\ &= \sum_{x \in E_2^n} (-1)^{(a,x) \oplus (b,x)} = \sum_{x \in E_2^n} (-1)^{(a \oplus b, x)} \end{aligned}$$

и эквивалентностью  $a = b$  тогда и только тогда, когда  $a \oplus b = 0$ .  $\square$

**Теорема 2. (Разложение в ряд Фурье.)** Любая булева функция  $f$  однозначно представима в виде

$$f(x) = \sum_{a \in E_2^n} C_a(f) (-1)^{(a,x)}.$$

При этом коэффициенты разложения — это коэффициенты Фурье, определяемые равенствами

$$C_a(f) = 1/2^n \langle f(x), (-1)^{(a,x)} \rangle = 1/2^n \sum_{x \in E_2^n} f(x) (-1)^{(a,x)}.$$

*Доказательство.* Если

$$f(x) = \sum_{a \in E_2^n} C_a(f) (-1)^{(a,x)},$$

то, используя скалярное произведение функций  $\langle f, g \rangle$ , получаем

$$\begin{aligned} \langle f(x), (-1)^{(b,x)} \rangle &= \left\langle \sum_{a \in E_2^n} C_a(f) (-1)^{(a,x)}, (-1)^{(b,x)} \right\rangle = \\ &= \sum_{a \in E_2^n} C_a(f) \langle (-1)^{(a,x)}, (-1)^{(b,x)} \rangle = 2^n C_b(f). \end{aligned}$$

Существование указанного разложения можно установить двумя способами.

Для функции  $f$  вычислим ее коэффициенты Фурье, определяемые равенствами

$$C_a(f) = 1/2^n \langle f(x), (-1)^{(a,x)} \rangle = 1/2^n \sum_{y \in E_2^n} f(y) (-1)^{(a,y)}. \quad (1)$$

Подставим их в сумму

$$\sum_{a \in E_2^n} C_a(f) (-1)^{(a,x)}$$

и убедимся, что получим  $f(x)$ .

$$\begin{aligned} \sum_{a \in E_2^n} C_a(f) (-1)^{(a,x)} &= \sum_{a \in E_2^n} (-1)^{(a,x)} (1/2^n \sum_{y \in E_2^n} f(y) (-1)^{(a,y)}) = \\ &= 1/2^n \sum_{y \in E_2^n} f(y) \left( \sum_{a \in E_2^n} (-1)^{(a,x)} (-1)^{(a,y)} \right) = f(x). \end{aligned}$$

Второе доказательство основано на “мощностных соображениях”.

Так как существует  $2^n$  функций вида  $(-1)^{(a,x)}$ , то  $2^{2^n}$  сумм вида

$$\sum_{a \in E_2^n} C_a(f) (-1)^{(a,x)}$$

дают  $2^{2^n}$  различных функций, т.е. все  $n$ -местные функции. Поэтому любая булева функция допускает единственное разложение указанного вида.  $\square$

Набор коэффициентов Фурье  $C(f) = (C_a(f))_{a \in E_2^n}$  функции  $f$  называется ее *спектром Фурье*. Предыдущее равенство (1) можно записать в матричном виде

$$(C_a(f))_{a \in E_2^n} = \frac{1}{2^n} (f(y))_{y \in E_2^n} \cdot ((-1)^{(y,a)})_{\substack{y \in E_2^n \\ a \in E_2^n}}.$$

Переход от вектора  $(f(a))_{a \in E_2^n}$  табличного задания функции  $f(x)$  к ее спектру Фурье  $(C_a(f))_{a \in E_2^n}$  является линейным преобразованием и задается матрицей  $1/2^n H_{2^n}$ , где

$$H_{2^n} = ((-1)^{(y,a)})_{\substack{y \in E_2^n \\ a \in E_2^n}}.$$

Матрица  $H_{2^n}$  — это *матрица Адамара*. Ее элементы равны  $\pm 1$ , и непосредственная проверка показывает, что выполняется равенство

$$H_{2^n} \cdot H_{2^n}^T = 2^n E.$$

Матрицы Адамара играют важную роль в различных разделах комбинаторики. Важные примеры применения матриц Адамара будут рассмотрены в разделе "Комбинаторика".

Рассмотрим еще один способ представления булевых функций. Для произвольной булевой функции  $f$  рассмотрим псевдобулеву функцию

$$\exp f(x) = e^{i\pi f(x)} = (-1)^{f(x)}.$$

Преобразование вектора  $(\exp f(a))_{a \in E_2^n}$  табличного задания функции  $\exp f(x)$  матрицей Адамара  $H_{2^n}$  называется *преобразованием Адамара-Уолша* булевой функции  $f$ . Получаемый при этом набор коэффициентов  $Z(f) = (Z_a(f))_{a \in E_2^n}$  называется *спектром Уолша* функции  $f$ , а сами коэффициенты — *коэффициентами Уолша* булевой функции  $f$ . Коэффициенты Уолша вычисляются по формулам

$$Z_a(f) = \sum_{x \in E_2^n} (-1)^{f(x) \oplus (a, x)} = \sum_{x \in E_2^n} (-1)^{f(x) \odot (a, x)}.$$

Следующая теорема устанавливает связь между спектрами Фурье  $C(f) = (C_a(f))_{a \in V_n}$  и Уолша  $Z(f) = (Z_a(f))_{a \in V_n}$ .

**Теорема 3.** Для любой булевой функции  $f$  и любого  $a \in E_2^n$  выполняется равенство

$$Z_a(f) = \begin{cases} -2 \cdot 2^n C_a(f), & \text{при } a \neq 0; \\ 2^n - 2 \cdot 2^n C_a(f), & \text{при } a = 0. \end{cases}$$

*Доказательство.* При  $a = 0$  получаем

$$C_0(f) = 1/2^n \cdot \|f\|, \quad Z_0(f) = (2^n - \|f\|) - \|f\| = 2^n - 2\|f\|.$$

Для произвольных булевых функций  $f$  и  $g$  и любых  $\alpha$  и  $\beta$  из  $E_2$  пусть  $N_{\alpha, \beta}(f, g)$  — это число элементов множества

$$\{x \mid f(x) = \alpha \& g(x) = \beta\}.$$

Тогда при  $a \neq 0$  получаем

$$\begin{aligned} 2^n \cdot C_a(f) &= N_{1,0}(f, (a, x)) - N_{1,1}(f, (a, x)), \\ Z_a(f) &= N_{0,0}(f, (a, x)) - N_{1,1}(f, (a, x)) - N_{0,1}(f, (a, x)) - N_{1,0}(f, (a, x)). \end{aligned}$$

Для завершения доказательства теоремы остается воспользоваться равенствами

$$\begin{aligned} N_{0,0}(f, (a, x)) + N_{1,0}(f, (a, x)) &= 2^{n-1}, \\ N_{1,0}(f, (a, x)) + N_{1,1}(f, (a, x)) &= \|f\|, \\ N_{0,1}(f, (a, x)) + N_{1,1}(f, (a, x)) &= 2^{n-1}, \\ N_{0,1}(f, (a, x)) &= 2^{n-1} - \|f\| + N_{1,0}(f, (a, x)). \end{aligned}$$

□

Приведем некоторые замечания относительно коэффициентов Фурье. Так как  $C_0(f) = 1/2^n \cdot \|f\|$ , то  $0 \leq C_0(f) \leq 1$ .

При  $a \neq 0$  выполняются неравенства

$$-1/2 \leq C_a(f) \leq 1/2.$$

Для коэффициентов Фурье выполняются некоторые дополнительные равенства и неравенства, например,

$$\sum_{a \in F_2^n} C_a(f) = f(0).$$

Коэффициенты Уолша произвольной булевой функции удовлетворяют следующему условию ортогональности: при любом отличном от нуля  $b \in E_2^n$  выполняется равенство

$$\sum_{a \in E_2^n} Z_a(f) \cdot Z_{a \oplus b}(f) = 0.$$

А при  $b = 0$  выполняется равенство Парсеваля

$$\sum_{a \in E_2^n} (Z_a(f))^2 = 2^{2n}.$$

Справедливость этих равенств следует из следующих соотношений

$$\begin{aligned} \sum_{a \in E_2^n} Z_a(f) \cdot Z_{a \oplus b}(f) &= \sum_{a \in E_2^n} \sum_{x \in E_2^n} (-1)^{f(x)} (-1)^{(a,x)} \sum_{y \in E_2^n} (-1)^{f(y)} (-1)^{(a \oplus b, y)} = \\ &= \sum_{y \in E_2^n} (-1)^{f(y)} (-1)^{(b, y)} \sum_{x \in E_2^n} (-1)^{f(x)} \sum_{a \in E_2^n} (-1)^{(a, x)} (-1)^{(a, y)} = \\ &= 2^n \sum_{y \in E_2^n} (-1)^{2f(y)} (-1)^{(b, y)} = 2^n \sum_{y \in E_2^n} (-1)^{(b, y)} = 2^{2n} \delta_{b, 0}. \end{aligned}$$

Для произвольного поля  $F$  функции, определенные на векторном пространстве  $E_2^n$  со значениями в поле  $F$ , называются  $F$ -булевыми. Если  $F$  — поле действительных или рациональных чисел, то соответствующие функции называются псевдобулевыми. Векторное пространство  $E_2^n$  для краткости будем обозначать через  $V_n$ . Множество  $F(n)$  всех  $F$ -булевых функций, определенных на векторном пространстве  $V_n$  со значениями в  $F$ , является векторным пространством над полем  $F$ . Для произвольного вектора  $a$  из  $V_n$  через  $e_a(x)$  обозначим функцию

$$e_a(x) = \begin{cases} 0, & \text{при } x \neq a; \\ 1, & \text{при } x = a. \end{cases}$$

Нетрудно понять, что система функций  $(e_a(x))_{a \in V_n}$  образует базис векторного пространства  $F(n)$ . Поэтому  $\dim_F F(n) = 2^n$ .

Любая функция из  $F(n)$  однозначно представима в виде линейной комбинации

$$f(x) = \sum_{a \in V_n} f(a) e_a(x).$$

Пусть  $f^\uparrow = (f(a))_{a \in V_n}$  — вектор-столбец табличного задания функции  $f$ . Для любой обратимой матрицы  $A$  порядка  $2^n$  справедливо равенство

$$f^\uparrow = A(A^{-1}f^\uparrow).$$

Поэтому вектор  $h^\uparrow = A^{-1}f^\uparrow = (h(a))_{a \in V_n}$  естественно рассматривать в качестве задания функции  $f$ . Выбирая различные обратимые матрицы  $A$ , получим различные задания функции  $f$ .

Если столбцы матрицы  $A$  занумеровать элементами множества  $E_2^n$ , расположенными в том же порядке, что и строки табличного задания функции  $f$ , и для  $a \in E_2^n$  через  $g_a^\uparrow$  обозначить функцию, заданную столбцом с номером  $a$ , то равенство

$$f^\uparrow = \sum_{a \in V_n} h(a) g_a^\uparrow$$

можно трактовать как разложение функции  $f$  по базису  $(g_a^\uparrow)_{a \in V_n}$ .

## §7. Некоторые приложения булевых функций

Одним из важнейших приложений булевых функций является их использование в качестве средства описания работы цифровых устройств, выполняющих те или иные логические функции (операции). Основу любого современного компьютера составляют различные *дискретные преобразователи* входных сигналов в выходные без запоминания. Такие преобразователи сигналов (без внутренней памяти) называются *функциональными элементами* или *комбинационными логическими схемами*. Функциональные элементы удобно условно обозначать схемой вида

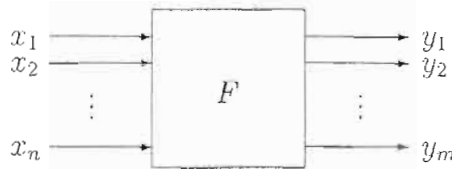


Рис. 1.

$x_1, x_2, \dots, x_n$  — входы функционального элемента  $F$ , а  $y_1, y_2, \dots, y_m$  — его выходы.

Наличие (отсутствие) сигнала на входе  $x_i$  (на выходе  $y_j$ ) можно трактовать следующим образом: переменная  $x_i$  ( $y_j$ ) принимает значение 1 (соответственно 0).

При такой трактовке выходы  $y_1, y_2, \dots, y_m$  задаются булевыми функциями от входных переменных  $x_1, x_2, \dots, x_n$ .

Таким образом работа функционального элемента  $F$  полностью описывается системой из  $m$  булевых функций

$$y_1 = f_1(x_1, \dots, x_n), \dots, y_m = f_m(x_1, \dots, x_n).$$

Присоединяя выходы одних функциональных элементов к входам других, мы можем получать схемы из функциональных элементов, задающие дискретные преобразователи информации (без памяти), при условии, что в этой схеме не возникает циклов. Схемы с циклами играют важную роль при проектировании элементов памяти компьютера.

Особую роль играют функциональные элементы с одним выходом, реализующие булевы функции.

Пусть функциональные элементы  $F_1, F_2, \dots, F_m$  с  $n$  входами, помеченными переменными  $x_1, x_2, \dots, x_n$ , и одним выходом реализуют  $n$ -местные булевы функции  $f_1, f_2, \dots, f_m$ , а функциональный элемент  $G$  с  $m$  входами и одним выходом реализует  $m$ -местную булеву функцию  $g$ .

Если  $n$ -местная функция  $f$  является суперпозицией функций  $g, f_1, f_2, \dots, f_m$ , то следующая схема из функциональных элементов реализует функцию  $f$ :

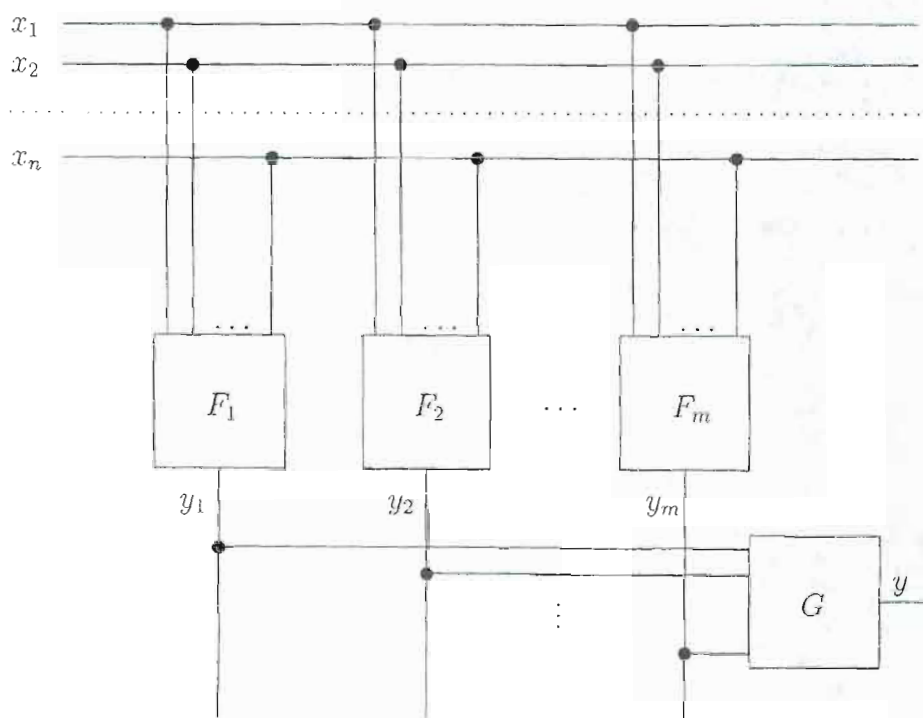


Рис. 2.

Поэтому, если  $f_1, f_2, \dots, f_m$  — полная система булевых функций, а  $F_1, F_2, \dots, F_m$  — соответствующие функциональные элементы, то любую булеву функцию можно реализовать схемой из функциональных элементов  $F_1, F_2, \dots, F_m$ . Выбор той или иной системы базовых функций обусловлен рядом требований, например, “простоты” схемы, понимаемой как минимальность числа входящих в нее базовых элементов, удобства ее физической реализации, надежности работы и т.д.

Удобно функциональный элемент, реализующий  $n$ -местную булеву функцию  $f$ , обозначать через

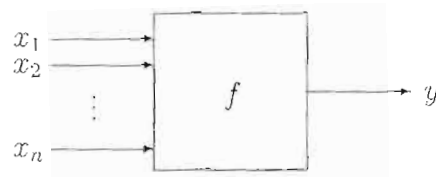


Рис. 3.

Важным примером полной системы булевых функций является набор из трех функций: отрицания  $\neg$ , дизъюнкции  $\vee$  и конъюнкции  $\&$ . Соответствующие функциональные элементы обозначаются через

Элемент “НЕ” (инверсия)



Элемент “И” (конъюнкция)



Элемент “ИЛИ” (дизъюнкция)

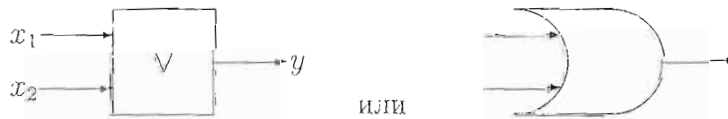
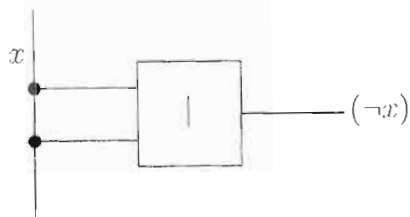


Рис. 4.

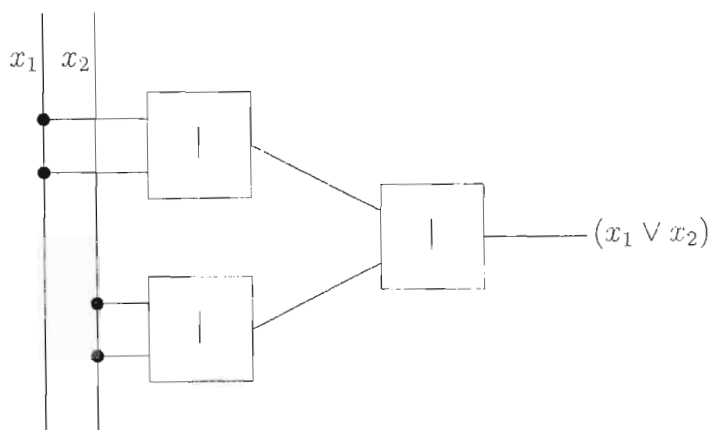
На практике наиболее часто используется в качестве базового логического элемента элемент “И-НЕ”, реализующий функцию Шеффера. Напомним, система, состоящая лишь из функции Шеффера, является полной. Поэтому любую булеву функцию можно реализовать схемой, содержащей лишь этот базовый логический элемент. Приведем схемы, реализующие функции отрицание  $\neg$ ,  $\vee$  и  $\&$ .



Реализация функции  $(\neg x)$



Реализация функции  $(x_1 \vee x_2)$



Реализация функции  $(x_1 \& x_2)$

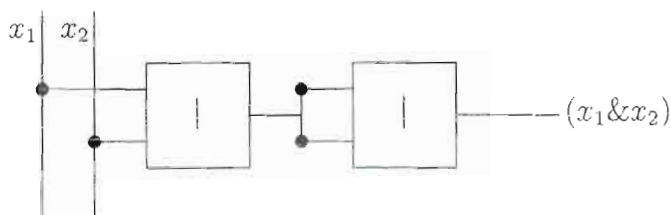


Рис. 5.

Следующий материал заимствован из книги [23]. Важную роль в компьютерах играют следующие два типа функциональных элементов — *дешифраторы* и *шифраторы*.

*Дешифратор* — это функциональный элемент с  $n$  входами  $x_1, x_2, \dots, x_n$  и  $m$  выходами  $y_1, y_2, \dots, y_m$ , в котором каждой комбинации входных сигналов соответствует 1 на одном выходе и 0 на остальных выходах. Булева функция, описывающая  $i$ -ый выход  $y_i$ , является некоторой элементарной конъюнкцией вида

$$x_1^{e_{1,i}} \& \dots \& x_n^{e_{n,i}},$$

причем при  $i \neq j$  соответствующие элементарные конъюнкции различны. Поэтому  $m \leq 2^n$ . Дешифраторы используются, например, для создания управляющего сигнала при получении на вход определенной комбинации логических сигналов. В качестве примера рассмотрим полный дешифратор с двумя входами и с  $2^2$  выходами

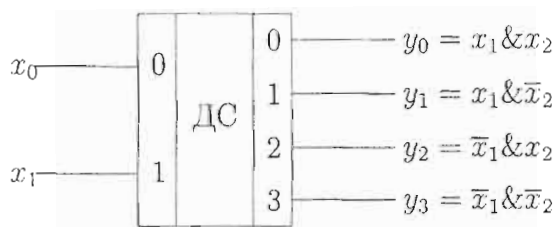


Рис. 6.

Этот дешифратор может быть реализован, например, следующей схемой из базовых функциональных элементов

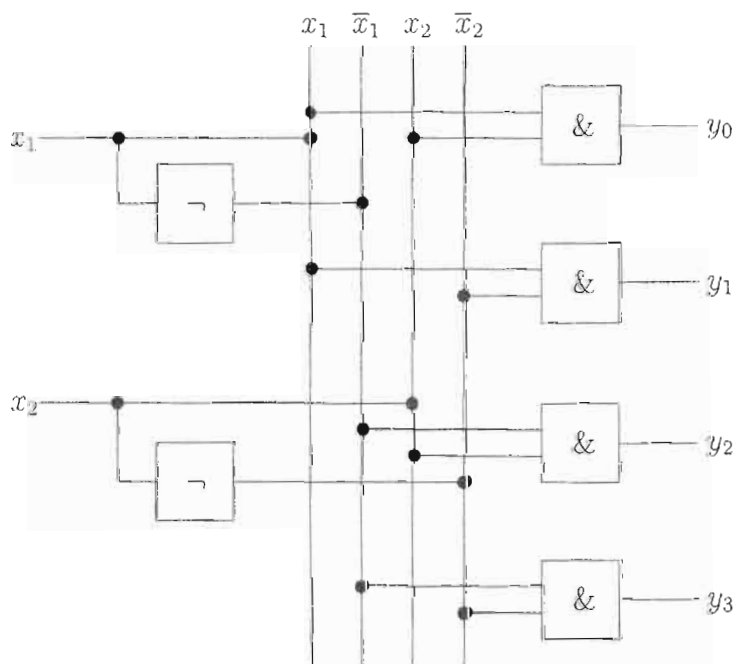


Рис. 7.

Шифраторы выполняют операции, обратные операциям дешифраторов — преобразуют логические единицы, поступающие на входные каналы, в двоичный код на выходе.

Об областях применения шифраторов и дешифраторов будут даны подробные сведения при изучении дисциплины “Электроника и схемотехника”. Шифраторы и дешифраторы относятся к преобразователям кодов. Они используются, в частности, для преобразования десятичных чисел в двоичный код и двоичного представления в десятичное.

Другую серию примеров функциональных элементов дают *мультиплексоры* и *демультиплексоры*, которые предназначены для преобразования нескольких информационных каналов в один. Переключение каналов обеспечивается управляющими сигналами. В качестве примера рассмотрим мультиплексор с четырьмя входными информационными каналами  $D_0$ ,  $D_1$ ,  $D_2$  и  $D_3$  и двумя двоичными управляющими сигналами  $X_0$  и  $X_1$

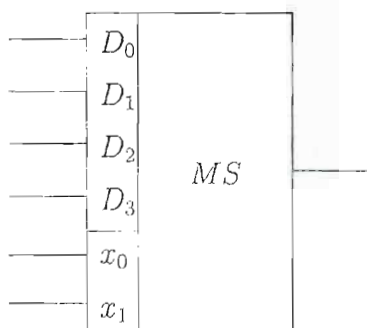


Рис. 8.

Этот мультиплексор может быть реализован, например, следующей схемой из базовых функциональных элементов

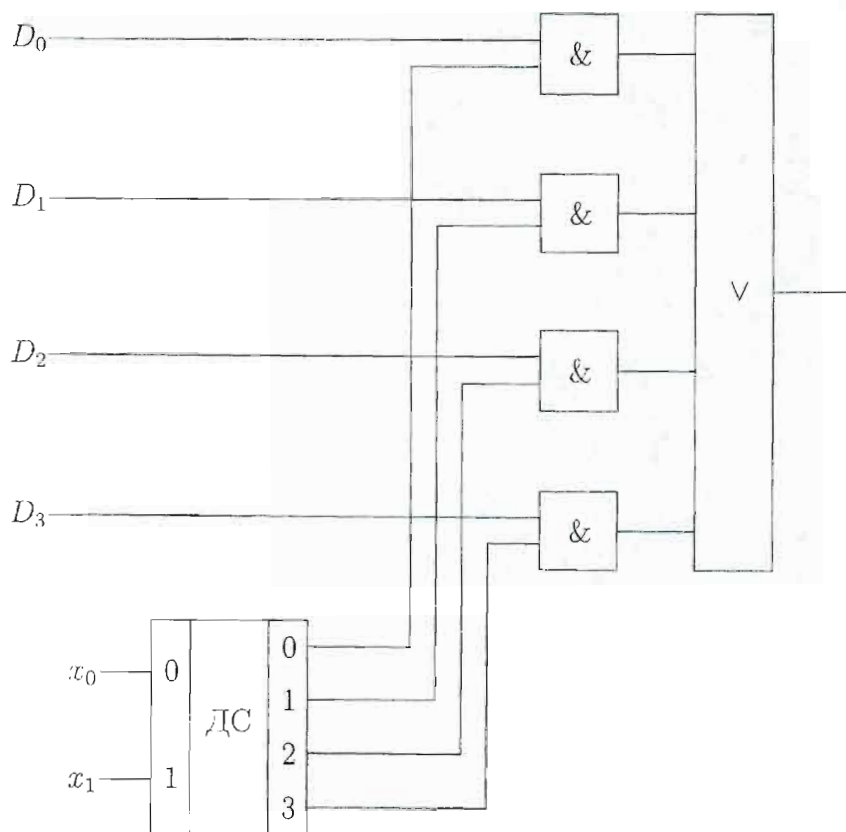


Рис. 9.

Разделение полученного с помощью мультиплексора сложного информационного сигнала на составляющие выполняется с помощью демультиплексора.

Завершим мы рассмотрение примеров схем из функциональных элементов построением схемы двоичного *сумматора* — важнейшего элемента арифметического блока микропроцессора, выполняющего арифметическое сложение двух двоичных чисел.

Сумматоры выполняют сложение чисел с фиксированным числом разрядов. Они называются *многоразрядными* и строятся из *одноразрядных*. В свою очередь одноразрядные сумматоры делятся на *полусумматоры* и *полные сумматоры*.

У полусумматора два входа, на которые подаются двоичные единицы  $a$  и  $b$ , и два выхода —  $s$  — сумма и  $p$  — сигнал переноса.

Полный сумматор имеет дополнительный вход, на который подается сигнал переноса от предыдущего суммирования.

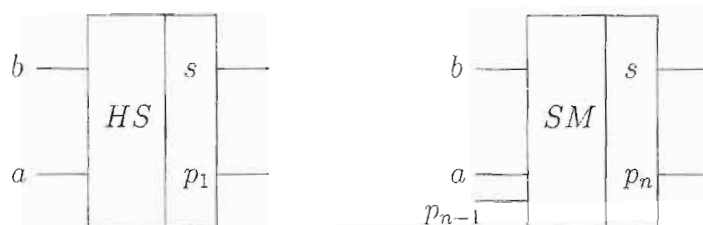


Рис. 10.

Приведем таблицу истинности для одноразрядного полусумматора

Входы		Выходы	
$a$	$b$	$s$	$p$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Рис. 11.

С помощью совершенной дизъюнктивной нормальной формы находим, что выход  $s$  описывается булевой функцией  $(\bar{a} \& b) \vee (a \& \bar{b})$ , а сигнал переноса — функцией  $a \& b$ .

Одноразрядный полусумматор может быть реализован, например, следующей схемой из базовых функциональных элементов:

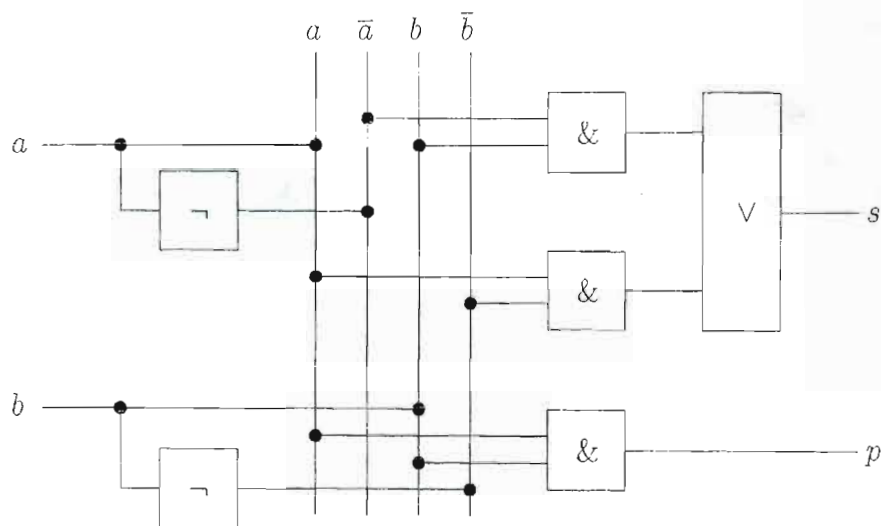


Рис. 12.

Полный одноразрядный сумматор можно построить из двух полусумматоров, например, по следующей схеме:

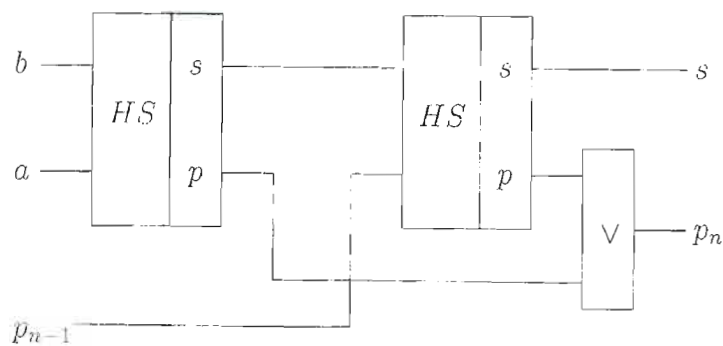


Рис. 13.



Принципиальная схема  $n$ -разрядного двоичного сумматора может иметь следующий вид:

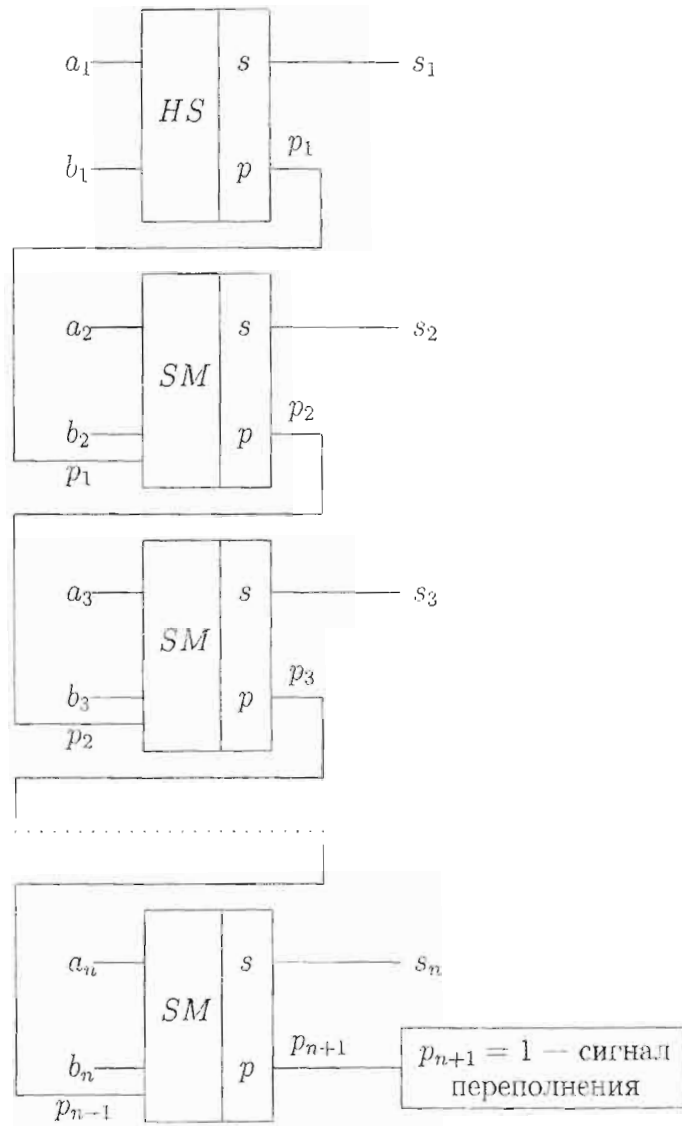


Рис. 14.

## Глава 2. Комбинаторика

### §1. Выборки, перестановки, сочетания и размещения

В этой главе рассматриваются некоторые вопросы, относящиеся к одному из древнейших разделов математики — комбинаторике. При подготовке использована следующая литература: [2, 4–6, 8, 9, 11, 13, 14, 26, 30, 34–36, 38, 39, 41, 44, 46, 49, 51]. Еще в глубокой древности люди сталкивались с задачами, возникающими из игр, где требовалось умение рассчитывать, составлять планы и опровергать планы противника. Разумеется, в этот период еще не было речи об особой науке, занимающейся решением подобных задач, каждая задача рассматривалась особо. Время шло, появлялись новые игры, которые порождали новые задачи. И вот в XVII в. французские математики Блэз Паскаль и Пьер Ферма, разбираясь в ряде игровых задач, сформулировали и доказали первые теоремы комбинаторики. В 1666 году Готтфрид Вильгельм Лейбниц опубликовал “Диссертацию о комбинаторном искусстве”, где впервые появился сам термин “комбинаторный”. Лейбниц считал, что комбинаторика должна заниматься “одинаковым и различным, похожим и непохожим, абсолютным и относительным расположением”.

Однако не только азартные игры давали пищу для комбинаторных размышлений математиков. Еще с давних пор дипломаты и заговорщики, монархи и ученые, стремясь к тайне переписки, изобретали все более и более сложные шифры, а их противники пытались эти шифры разгадать (взломать). И в основу опять были положены комбинаторные принципы. Так, в Англии в XVII в. монархистские заговорщики поражались скорости, с которой Кромвель проникал в их замыслы. Лишь после падения республики и воцарения Карла II они узнали, что все их шифры, которые они считали неразгадываемыми, разгадывал один из лучших английских математиков того времени, профессор Оксфордского университета Уоллис.

Таким образом, принято считать, что XVII век связан с возникновением комбинаторики — ветви математики, изучающей комбинации и перестановки предметов.

Сегодняшний интерес к комбинаторике связан прежде всего с появлением быстродействующих вычислительных машин и расцветом конечной математики. С появлением компьютеров стало возможным проведение вычислений, на

которые ранее ушли бы сотни лет человеческой жизни. Особенно успешно методы комбинаторики применяются при анализе вычислительных задач и алгоритмов. При анализе вычислительных задач их обычно оценивают с точки зрения *размера*, т.е. общего количества различных вариантов, среди которых нужно найти решение, а алгоритмы, используемые для их решения, — с точки зрения *сложности*. При этом различают *сложность по времени*, т.е. количество необходимых шагов алгоритма, и *сложность по памяти*, т.е. объем памяти, необходимый для работы алгоритма.

Еще раз подчеркнем, что во всех случаях основным инструментом такого анализа оказываются формулы и методы комбинаторики, которые мы рассмотрим в этой главе.

Пусть дано некоторое конечное непустое множество  $X$ , состоящее из  $n$  элементов. Возьмем множество натуральных чисел  $\mathbb{N}_k = \{1, 2, \dots, k\}$  и зададим некоторое отображение множества  $\mathbb{N}_k$  во множество  $X$ . Это значит, что числу 1 ставится в соответствие элемент  $x_1 \in X$ , числу 2 — элемент  $x_2 \in X$ , ..., числу  $k$  — элемент  $x_k \in X$ . В результате мы получаем набор  $x_1, x_2, \dots, x_k$  элементов множества  $X$ , в который некоторые элементы могут входить несколько раз. Действительно, при отображении  $\mathbb{N}_k$  в  $X$  может случиться, что разным числам отвечает один и тот же элемент множества  $X$ . Располагая элементы этого набора по порядку номеров, получаем *слово*  $\langle x_1, x_2, \dots, x_k \rangle$  длины  $k$ , составленное из элементов множества  $X$ . Элемент  $x_i$ ,  $1 \leq i \leq k$ , называется  *$i$ -ой компонентой* слова  $\langle x_1, x_2, \dots, x_k \rangle$ . Компонентами слова могут быть множества, слова и т.д. Слово, не содержащее ни одной компоненты (т.е. имеющее длину ноль), называется *пустым* и обозначается  $\Lambda$ . Два слова  $\langle x_1, \dots, x_k \rangle$  и  $\langle y_1, \dots, y_k \rangle$  считаются *равными*, если они имеют одинаковую длину, причем их компоненты, имеющие одинаковые номера, равны.

Пусть  $\alpha$  — слово длины  $k$ , составленное из  $n$ -элементного множества  $X$ . Перенумеруем элементы множества  $X$ :  $X = \{x_1, \dots, x_n\}$ . Тогда каждому числу  $i$ ,  $1 \leq i \leq n$ , соответствует число  $m_i$ , показывающее, сколько раз элемент  $x_i$  встречается среди компонент слова  $\alpha$ . Выписывая по порядку эти числа, получаем  $n$ -мерный вектор  $\langle m_1, \dots, m_n \rangle$ , который называется *составом* слова  $\alpha$ .

Подчеркнем еще раз отличия понятия слова от понятия множества:

- а) в множестве *порядок* элементов не играет роли, а слова, отличающиеся порядком компонент, *различны* даже в том случае, когда они имеют один и тот же состав;
- б) в множестве все элементы *различны* (ни один элемент не может входить во множество дважды), а в слове компоненты могут повторяться.

Пусть  $\alpha$  и  $\beta$  — два слова длины  $k_1$  и  $k_2$ , составленные из  $n_1$  и  $n_2$ -элементных множеств  $X_1$  и  $X_2$  соответственно. Нам понадобятся следующие два правила:

**Правило суммы.** Если слово  $\alpha$  можно выбрать  $m$  способами, а слово  $\beta$  —  $n$  способами, причем любой способ выбора  $\alpha$  отличается от любого способа выбора  $\beta$ , то выбор " $\alpha$  или  $\beta$ " можно сделать  $m + n$  способами.

Дадим другую формулировку этого утверждения: пусть  $M$  и  $N$  — два множества из  $m$  и  $n$  элементов соответственно, причем  $M \cap N = \emptyset$ . Тогда в объединении  $M \cup N$  содержится  $m + n$  элементов.

**Правило произведения.** Если слово  $\alpha$  можно выбрать  $m$  способами, а слова  $\beta$  —  $n$  способами, то слово  $\langle \alpha, \beta \rangle$  можно выбрать  $mn$  способами.

Дадим другую формулировку этого утверждения: пусть  $M$  и  $N$  — два множества из  $m$  и  $n$  элементов соответственно. Число элементов в декартовом произведении конечных множеств  $M$  и  $N$  равно  $mn$ .

По своей природе эти правила являются определениями, и поэтому их нужно понимать, а не доказывать. Заметим также, что в правиле суммы выборы  $\alpha$  и  $\beta$  являются взаимно исключающими, т.е. нет возможности выбрать оба слова одновременно (одинаковыми). Правило произведения наиболее часто используется тогда, когда выборы  $\alpha$  и  $\beta$  независимы. Однако возможность наличия такой зависимости игнорировать нельзя.

**Определение 1.** Размещением с повторениями из  $n$  элементов по  $k$  называется слово длины  $k$ , составленное из  $n$ -элементного множества  $X$ . Число таких слов обозначается  $U(n, k)$ .

**Теорема 1.**  $U(n, k) = n^k$ .

*Доказательство.* Из правила произведения по индукции вытекает, что число размещений с повторениями из  $n$  элементов по  $k$  равно произведению  $k$  сомножителей, каждый из которых равен  $n$ , т.е.  $n^k$ .  $\square$

**Пример 1.** Для запирания сейфов и автоматических камер хранения багажа применяют секретные замки, которые открываются лишь тогда, когда набрано «тайное слово» (или тайный набор цифр). Это слово набирают с помощью одного или нескольких дисков, на которых изображены буквы (или цифры). Пусть число букв на каждом диске равно 12, а число дисков равно 5. Сколько неудачных попыток может быть сделано человеком, не знающим секретного слова и подбирающим его наугад?

Из условия задачи видно, что порядок выбираемых букв существенен и буквы могут повторяться. Поэтому мы имеем здесь дело с размещениями с повторениями. Так как по условию каждая буква может быть выбрана 12 способами, а каждая выборка состоит из 5 букв, то получаем, что число всевозможных комбинаций равно  $U(12, 5) = 12^5 = 248\,832$ . Значит, неудачных попыток может быть 248 831. Считая по 10 секунд на одну попытку, получаем, что для открытия сейфа понадобится более 340 часов непрерывной работы. Впрочем, обычно сейфы делают так, чтобы после первой же неудачной попытки раздавался сигнал тревоги.

**Пример 2.** При передаче сообщений по телеграфу используется код Морзе. В этом коде буквы, цифры и знаки препинания обозначаются точками и тире. При этом для одних букв используется один знак, например Е ·, а для некоторых приходится использовать пять знаков, например Э · · — · ·.

Откуда же взялось число 5? Нельзя ли обойтись меньшим числом знаков, скажем, передавать все сообщения с помощью комбинаций, содержащих не более четырех знаков? Оказывается, что нельзя, и ответ этот дает именно формула для числа размещений с повторениями. Действительно, с помощью одного знака можно передать только  $U(2, 1) = 2$  буквы (Е · и Т —), с помощью двух знаков —  $U(2, 2) = 2^2 = 4$  буквы, с помощью трех знаков —  $U(2, 3) = 2^3 = 8$  букв, с помощью четырех знаков —  $U(2, 4) = 2^4 = 16$  букв. Поэтому общее число букв, которые можно передать не более чем четырьмя знаками, согласно правилу сложения, равно

$$2 + 4 + 8 + 16 = 30.$$

А в русском алфавите 32 буквы, да еще надо передавать цифры и знаки препинания. Ясно, что символов из четырех знаков не хватает. А если брать символы и из 5 знаков, то к полученным 30 прибавится еще 32 символа. Полученных 62 символов вполне достаточно для телеграфирования.

Рассмотрим непустое подмножество  $A$  множества  $X$ , состоящее из  $k$  элементов. Упорядочим элементы множества  $A$ . Проще всего это сделать, занумеровав элементы данного множества. Элемент, получивший номер  $i$ , обозначим  $x_i$ . Получившееся упорядоченное множество обозначим  $\langle x_1, \dots, x_k \rangle$ . Одно и то же множество можно упорядочить различными способами.

**Определение 2.** *Размещение без повторений из  $n$  элементов по  $k$  это упорядоченное  $k$ -элементное подмножество  $n$ -элементного множества. Число таких подмножеств обозначается  $A(n, k)$ .*

**Теорема 2.**  $A(n, k) = \frac{n!}{(n-k)!}$ .

*Доказательство.* Чтобы сосчитать  $A(n, k)$ , будем рассуждать так: составим упорядоченное  $k$ -элементное подмножество  $\langle x_1, \dots, x_k \rangle$   $n$ -элементного множества  $X$ . На первое место  $x_1$  имеем  $n$  кандидатов. После того как оно заполнено, на второе место  $x_2$  остаются  $n - 1$  кандидатов, на третье  $x_3$  остаются  $n - 2$  кандидатов, и т.д. На  $k$ -е место  $x_k$  имеется  $n - k + 1$  кандидатов (после того как мы выбрали  $k - 1$  элемент, остается  $n - (k - 1) = n - k + 1$  элементов). Применяя правило произведения, находим

$$A(n, k) = n \cdot (n - 1) \cdot \dots \cdot (n - k + 1).$$

Эту формулу можно записать иначе, умножив числитель и знаменатель на  $(n - k) \cdot \dots \cdot 1$ . В числителе получится произведение всех чисел от 1 до  $n$ . Хорошо известно, что такие произведения называют *факториалами* и обозначают  $n!$ . Таким образом,

$$A(n, k) = \frac{n!}{(n-k)!}.$$

□



*Пример 3.* Научное общество состоит из 25 человек. Надо выбрать президента общества, вице-президента, ученого секретаря и казначея. Сколькими способами может быть сделан этот выбор, если каждый член общества может занимать лишь один пост?

Так как результат выборов существенно зависит от того, кто какой пост займет, то мы имеем дело с размещениями без повторений из 25 элементов по 4. Поэтому ответ дается формулой  $A(25, 4) = 25 \cdot 24 \cdot 23 \cdot 22 = 303\,600$ .

**Определение 3.** *Перестановкой (или перестановкой без повторений) из  $n$  элементов множества  $X$  называется произвольное упорядочивание элементов множества  $X$ . Число всех перестановок множества  $X$  обозначают  $P(n)$ .*

Перестановки — это предельный случай размещений без повторений при  $k = n$ . Из теоремы 2 получаем

$$P(n) = A(n, n) = n \cdot (n - 1) \cdot \dots \cdot 1 = n!.$$

*Пример 4.* Сколькими способами можно расположить на шахматной доске 8 ладей так, чтобы они не били друг друга?

Из условия ясно, что при таком расположении на каждой горизонтали и каждой вертикали стоит по одной ладье. Возьмем одно из этих расположений и обозначим через  $x_1$  номер занятого поля на первой горизонтали, через  $x_2$  — на второй горизонтали, ..., через  $x_8$  — на восьмой горизонтали. Тогда  $(x_1, x_2, \dots, x_8)$  будет некоторой перестановкой из чисел  $1, 2, \dots, 8$  (ясно, что среди чисел  $x_1, x_2, \dots, x_8$  нет ни одной пары одинаковых, так как иначе две ладьи попали бы на одну и ту же вертикаль). Обратно, если  $x_1, x_2, \dots, x_8$  — некоторая перестановка чисел  $1, 2, \dots, 8$ , то ей соответствует некоторое расположение ладей, при котором они не могут бить друг друга. Таким образом, число искомых расположений ладей равно числу перестановок чисел  $1, 2, \dots, 8$ , то есть  $P(8)$ . Но

$$P(8) = 8! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 40\,320.$$

Точно так же доказывается, что на доске из  $n$  горизонталей и  $n$  вертикалей можно  $n!$  способами расположить  $n$  ладей так, чтобы они не могли бить друг друга.

**Определение 4.** *Сочетанием без повторений из  $n$  элементов по  $k$  называется любое  $k$ -элементное подмножество множества  $X$ . Число таких подмножеств обозначается  $C(n, k)$ .*

**Теорема 3.**  $C(n, k) = \frac{n!}{k!(n-k)!}$ .

*Доказательство.* Составим все  $C(n, k)$  сочетаний из  $n$  элементов по  $k$ . Затем переставим в каждом сочетании элементы всеми возможными способами. Мы

получили, и притом лишь по одному разу, все упорядоченные  $k$ -элементные подмножества  $n$ -элементного множества  $X$ . Их число равно  $A(n, k)$ . Но число  $k$ -элементных подмножеств в  $X$  равно  $C(n, k)$ , а каждое из них можно упорядочить  $P(k) = k!$  способами. Имеем  $C(n, k) \cdot k! = A(n, k)$ . Откуда

$$C(n, k) = \frac{A(n, k)}{k!} = \frac{n!}{k!(n-k)!}.$$

□

**Замечание 1.** Справедлива формула  $C(n, k) = C(n, n-k)$ . Действительно, если выбрать из  $n$  различных элементов некоторое сочетание по  $k$  элементов, то останется дополнительное сочетание по  $n-k$  элементов, а дополнительным к полученному сочетанию по  $n-k$  элементов является исходное сочетание по  $k$  элементов. Таким образом, сочетания по  $k$  и по  $n-k$  элементов образуют взаимно дополнительные пары, потому число этих сочетаний одно и то же.

Рассмотрим другое доказательство формулы  $C(n, k) = C(n, n-k)$ . Для этого дадим геометрическую интерпретацию числам  $C(n, k)$ . Пусть имеется прямоугольная сетка размера  $k \times (n-k)$  (см. рис. 1). Вычислим число различных кратчайших путей на этой сетке, ведущих из левого нижнего угла (точки  $(0, 0)$ ) в правый верхний угол (точку  $(k, n-k)$ ).

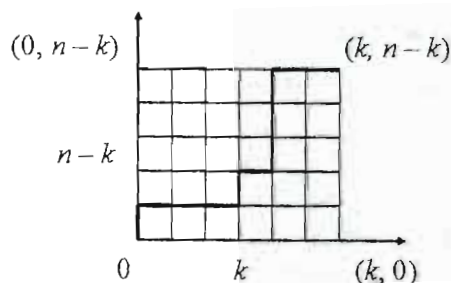


Рис. 1.

Каждый кратчайший путь из точки  $(0, 0)$  в точку  $(k, n-k)$  состоит из  $k + (n-k) = n$  отрезков, причем среди них есть  $k$  горизонтальных и  $n-k$  вертикальных отрезков. Разные пути отличаются лишь порядком чередования горизонтальных и вертикальных отрезков. Поэтому общее число путей равно числу способов, которыми из множества  $n$  отрезков можно выбрать  $k$  горизонтальных отрезков, т.е.  $C(n, k)$ .

Можно было бы рассматривать число способов выбора на  $k$  горизонтальных, а  $n-k$  вертикальных отрезков. Тогда мы получили бы ответ  $C(n, n-k)$ . Таким образом, мы установили геометрически равенство  $C(n, k) = C(n, n-k)$ .

**Замечание 2.** Зафиксируем какой-нибудь из  $n$  элементов множества  $X$ , например  $a$ , и разобьем все сочетания из  $n$  элементов по  $k$  на два класса — содержащие элемент  $a$  и не содержащие этого элемента. Число сочетаний первого

класса равно  $C(n-1, k-1)$  — надо из оставшихся  $n-1$  элементов выбрать еще  $k-1$  элементов. А число сочетаний второго класса равно  $C(n-1, k)$  — надо выбрать  $k$  из всех элементов, исключая  $a$ . Но любое сочетание относится или к первому, или ко второму классу, но не к двум классам одновременно. Поэтому

$$C(n, k) = C(n-1, k-1) + C(n-1, k).$$

Получим теперь это тождество из геометрических соображений.

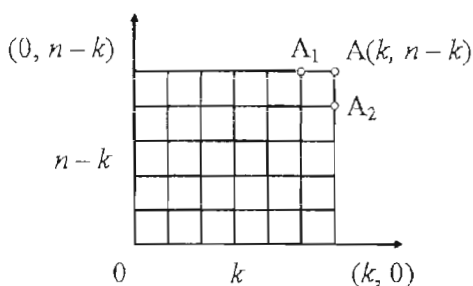


Рис. 2.

Число кратчайших путей из точки  $O(0, 0)$  в точку  $A(k, n-k)$  равно  $C(k + (n-k), k) = C(n, k)$ . Все такие пути можно разделить на 2 группы: пути, проходящие через точку  $A_1(k-1, n-k)$  (число их равно  $C((k-1) + (n-k), k-1) = C(n-1, k-1)$ ), и пути, проходящие через точку  $A_2(k, n-k-1)$  (число их равно  $C(k + (n-k-1), k) = C(n-1, k)$ ). Любой кратчайший путь из точки  $O(0, 0)$  в точку  $A(k, n-k)$  принадлежит либо первой, либо второй группе, но не двум группам одновременно. Следовательно,  $C(n, k) = C(n-1, k-1) + C(n-1, k)$ .

**Замечание 3.** Докажем тождество

$$C(n, k) = \sum_{s=1}^{n-k+1} C(n-s, k-1).$$

Рассмотрим все  $k$ -элементные подмножества множества  $X = \{x_1, x_2, \dots, x_n\}$ . Число их равно  $C(n, k)$ . Разобьем эти подмножества на классы  $T_1, T_2, \dots, T_{n-k+1}$ , отнеся к классу  $T_s$  все те  $k$ -элементные подмножества множества  $X$ , в которых элемент с наименьшим индексом равен  $x_s$ . Очевидно, что эти классы не пересекаются и ими исчерпываются все  $k$ -элементные подмножества множества  $X$ .

Так как каждое подмножество из класса  $T_s$  может быть получено присоединением к  $x_s$  некоторого  $(k-1)$ -элементного подмножества множества  $\{x_{s+1}, x_{s+2}, \dots, x_n\}$ , то класс  $T_s$  состоит из  $C(n-s, k-1)$  подмножеств. Следовательно, доказываемое тождество верно.

Получим теперь это тождество из геометрических соображений.

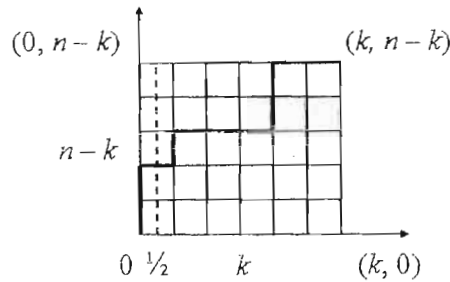


Рис. 3.

Рассмотрим все кратчайшие пути, соединяющие точку  $(0,0)$  с точкой  $(k, n-k)$ . Число таких путей равно  $C(n, k)$ . Отнесем к классу  $B_s$  те пути, которые пересекают прямую  $x = \frac{1}{2}$  в точке  $(\frac{1}{2}, s)$ ,  $s = 0, 1, \dots, n-1$ . Очевидно, что классы  $B_s$  не пересекаются и ими исчерпываются все пути из точки  $(0,0)$  в точку  $(k, n-k)$ . Кроме того, каждый класс  $B_s$  состоит из  $C(n-s-1, k-1)$  путей. Поэтому  $C(n, k) = \sum_{s=0}^{n-k} C(n-s-1, k-1) =$  (выполним замену  $s' = s+1$ )  
 $= \sum_{s'=1}^{n-k+1} C(n-s', k-1).$

**Замечание 4.** Докажем еще одно тождество, которое называется *тождеством Коши*:

$$C(m+n, k) = \sum_{s=0}^k C(m, s)C(n, k-s).$$

Представим, что из группы, состоящей из  $m$  мужчин и  $n$  женщин, мы хотим выбрать  $k$  человек. С одной стороны, это можно сделать  $C(m+n, k)$  способами, если осуществлять выборки из объединенного множества мужчин и женщин. С другой стороны, все  $k$ -элементные подмножества нашего множества можно классифицировать по числу мужчин в подмножестве,  $k$ -элементное подмножество, содержащее  $s$  мужчин, можно получить, выбирая сначала  $s$  мужчин одним из  $C(m, s)$  способов, а затем  $(k-s)$  женщин одним из  $C(n, k-s)$  способов. Таким образом, по правилу произведения число всех возможных подмножеств из  $k$  человек, включающих  $s$  мужчин, равно  $C(m, s)C(n, k-s)$ . Отсюда по правилу суммы непосредственно следует искомое тождество.

**Пример 5.** Сколько прямоугольников можно вырезать из клеток доски, размер которой  $m \times n$ ? (Вырезается один прямоугольник.)

Прямоугольник однозначно определяется положением его сторон. Горизонтальные стороны могут занимать любое из  $m+1$  положения. Тогда число способов их выбора равно  $C(m+1, 2)$ . Аналогично вертикальные стороны можно выбрать  $C(n+1, 2)$  способами. По правилу произведения получаем, что число прямоугольников равно  $C(m+1, 2) \cdot C(n+1, 2)$ .

**Определение 5.** Сочетанием с повторениями из  $n$  элементов по  $k$  называется состав слова длины  $k$ , компоненты которого принадлежат данному  $n$ -элементному множеству  $X$ . Число таких составов обозначается  $V(n, k)$ .

**Теорема 4.**  $V(n, k) = C(n + k - 1, k)$ .

*Доказательство.* Пусть  $x_1, x_2, \dots, x_n$  — элементы множества  $X$ . Рассмотрим произвольное сочетание с повторениями из  $n$  элементов множества  $X$  по  $k$ , т.е. состав  $\langle m_1, m_2, \dots, m_n \rangle$ ,  $m_1 + m_2 + \dots + m_n = k$ . Выпишем по порядку нумерации элементов во множестве  $X$  все компоненты слов, соответствующих этому составу:

$$\underbrace{x_1 x_1 \dots x_1}_{m_1} \mid \underbrace{x_2 x_2 \dots x_2}_{m_2} \mid \underbrace{x_3 x_3 \dots x_3}_{m_3} \mid \dots \mid \underbrace{x_n x_n \dots x_n}_{m_n}.$$

Заметим, что каждому составу такая расстановка соответствует взаимно однозначно. Длина расстановки с учетом вертикальных линий составляет  $k + (n - 1) = n + k - 1$ , где  $k$  — количество элементов в расстановке;  $n - 1$  — число вертикальных линий. Далее, любая такая расстановка однозначно задается выбором из  $n + k - 1$  места  $n - 1$  места для положений вертикальных линий. Согласно теореме 3 это можно сделать  $C(n + k - 1, n - 1)$  способами. Промежуточные места между линиями заполняются соответствующими элементами. Согласно замечанию 1 теоремы 3 имеем  $C(n + k - 1, n - 1) = C(n + k - 1, k)$ .  $\square$

Пример 6. В кондитерском магазине продаются пирожные 4 сортов: наполеоны, эклеры, песочные и слоеные. Сколькими способами можно купить 7 пирожных?

По условию задачи множество  $X$  сортов пирожных состоит из элементов  $x_1, x_2, x_3$  и  $x_4$ , которые обозначают соответственно наполеоны, эклеры, песочные и слоеные пирожные. Тогда покупку из 7 пирожных можно задать составом слова длины 7, компоненты которого принадлежат 4-элементному множеству  $X$ . Поэтому мы имеем дело с сочетаниями с повторениями из 4 элементов по 7. Таким образом, 7 пирожных можно купить  $C(4 + 7 - 1, 7) = \frac{10!}{7!3!} = 120$  способами.

Пример 7. Найти количество целочисленных решений уравнения

$$x_1 + x_2 + \dots + x_n = k, \quad k \geq 0, \quad x_i \geq 0, \quad i = 1, 2, \dots, n; \quad n \geq 1.$$

Рассмотрим следующую интерпретацию решения уравнения. Каждое значение  $x_i = 1_i + 1_i + \dots + 1_i$  представим как сумму единиц, количество которых равно  $x_i$ . Индекс у  $1_i$  указывает на ее принадлежность к разложению числа  $x_i$ . Таким образом, мы ввели  $n$  различных элементов  $\{1_1, 1_2, \dots, 1_n\}$ . Тогда любое решение исходного уравнения можно представить как сумму, составленную из  $k$  произвольных единиц множества  $\{1_1, 1_2, \dots, 1_n\}$ , т.е. как состав слова длины  $k$ , компоненты которого принадлежат множеству  $\{1_1, 1_2, \dots, 1_n\}$ . Данное соответствие является взаимно однозначным, откуда следует, что количество решений уравнения равно числу сочетаний с повторениями  $C(n + k - 1, k)$ .



Можно рассмотреть более общую задачу. Найти количество целочисленных решений уравнения

$$y_1 + y_2 + \dots + y_n = k, \quad y_i \geq a_i, \quad i = 1, 2, \dots, n; \quad n \geq 1.$$

Сделав замену  $y_i = x_i + a_i$ ,  $i = 1, 2, \dots, n$ , получаем уравнение  $x_1 + x_2 + \dots + x_n = k - \sum_{i=1}^n a_i$ , где  $x_i \geq 0$  — целые числа. Мы уже знаем, что число решений этого уравнения при  $k - \sum_{i=1}^n a_i \geq 0$  равно  $C(n + (k - \sum_{i=1}^n a_i) - 1, k - \sum_{i=1}^n a_i)$ . Столько же решений и у исходной системы.

**Определение 6.** Пусть задан состав слов  $\langle m_1, \dots, m_n \rangle$ . Перестановкой с повторениями из  $m_1$  элементов  $x_1$ ,  $m_2$  элементов  $x_2$ , ...,  $m_n$  элементов  $x_n$  называется слово соответствующее данному составу. Число таких слов, соответствующих составу  $\langle m_1, \dots, m_n \rangle$ , обозначается  $P(m_1, m_2, \dots, m_n)$ .

**Теорема 5.**  $P(m_1, m_2, \dots, m_n) = \frac{m!}{m_1! m_2! \dots m_n!}$ , где  $m = m_1 + m_2 + \dots + m_n$ .

*Доказательство.* Перестановки с повторениями имеют тесную связь с сочетаниями. Определим количество этих перестановок следующим образом. Из всех  $m$  мест перестановки  $m_1$  мест занимают элементы  $x_1$ . Выбор мест для них можно сделать  $C(m, m_1)$  способами. Из оставшихся  $m - m_1$  мест элементы  $x_2$  занимают  $m_2$  мест, которые можно выбрать  $C(m - m_1, m_2)$  способами. И так далее. Наконец, те же рассуждения показывают, что элементы  $x_n$  можно расположить в перестановке  $C(m - m_1 - m_2 - \dots - m_{n-1}, m_n)$  способами. Согласно правилу произведения, число перестановок с повторениями равно

$$P(m_1, m_2, \dots, m_n) = C(m, m_1) \cdot C(m - m_1, m_2) \cdot \dots \cdot C(m - m_1 - m_2 - \dots - m_{n-1}, m_n) = \frac{m!}{m_1! m_2! \dots m_n!}.$$

□

**Следствие.** Замечательно, что формула для числа перестановок из  $m_1$  элементов  $x_1$  и  $m - m_1$  элементов  $x_2$  совпадает с формулой сочетаний без повторений из  $m$  элементов по  $m_1$ :

$$P(m_1, m - m_1) = C(m, m_1).$$

**Пример 8.** Когда Христиан Гюйгенс (1629–1695) открыл кольцо Сатурна, он составил анаграмму<sup>1</sup>

<sup>1</sup> Анаграмма — это перестановка букв, посредством которой из одного слова составляется другое, например, слова «лунка» и «кулан» — анаграммы.

аааааа, ссссс, d, ееее, g, h, ііііі, ІІІ, mm,  
nnnnnnnnn, oooo, pp, q, rr, s, tttt, uuuu.

Если поставить в ней буквы в нужном порядке, то получится текст

*«Annulo cingitur tenui, plano, nusquam cohaerente,  
ad eclipticam inclinato».*

(«Окружен кольцом тонким, плоским, нигде не подвешенным, наклонным к эклиптике».)

*Сколько надо сделать перестановок, чтобы дойти до истинного смысла анаграммы Гюйгенса?*

В эту анаграмму входит 7 букв а, 5 букв с, 1 буква d, 5 букв е, 1 буква g, 1 буква h, 7 букв і, 3 буквы l, 2 буквы m, 9 букв n, 4 буквы o, 2 буквы p, 1 буква q, 2 буквы r, 1 буква s, 5 букв t и 5 букв u, а всего 61 буква. По теореме 5 получаем

$$\frac{61!}{7!5!1!5!1!1!7!3!2!9!4!2!1!2!1!5!5!}$$

перестановок. Это громадное число примерно равно  $10^{60}$ .

С задачей перебора всех этих перестановок электронная вычислительная машина, делающая миллион операций в секунду, не справилась бы и за все время существования Солнечной системы.

Однако один из коллег Гюйгенса, Валлис, большой мастер по расшифровке тайнописи, разгадал эту анаграмму и составил по этому поводу свою анаграмму, которую послал Гюйгенсу. Когда ученые обменялись разгадками анаграмм, то получилось так, что будто бы Валлис еще до Гюйгенса сделал то же самое открытие. Потом Валлис признался, что он пошутил, чтобы доказать бесполезность анаграмм в деле тайнописи. Гюйгенс, однако, не оценил этой шутки и рассердился...

Дело в том, что человеку в каком-то смысле легче решить подобную задачу, чем машине. Ведь человек будет брать не все перестановки, а только те, в которых получаются осмысленные слова, будет учитывать морфологические правила и т.д. Это сильно сократит число необходимых попыток. А самое главное — он примерно знает, над какими вопросами думал его корреспондент. Но все равно получается очень громоздкая работа.

## §2. Полиномиальная теорема

Теорема 1. (Полиномиальная теорема.)

$$(x_1 + x_2 + \dots + x_n)^m = \sum_{m_1 + m_2 + \dots + m_n = m} P(m_1, m_2, \dots, m_n) x_1^{m_1} x_2^{m_2} \dots x_n^{m_n},$$

где суммирование выполняется по всем решениям уравнения  $m_1 + m_2 + \dots + m_n = m$  в целых неотрицательных числах,  $m_i \geq 0$ ,  $i = 1, 2, \dots, n$ .

*Доказательство.* Выполним умножение  $(x_1 + x_2 + \dots + x_n)^m =$

$$= \underbrace{(x_1 + x_2 + \dots + x_n)(x_1 + x_2 + \dots + x_n) \dots (x_1 + x_2 + \dots + x_n)}_m.$$

Чтобы привести подобные слагаемые в полученном выражении, необходимо подсчитать количество одночленов вида  $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$  (или перестановок с повторениями из  $m_1$  элементов  $x_1$ ,  $m_2$  элементов  $x_2$ , ...,  $m_n$  элементов  $x_n$ ) для каждого состава  $\langle m_1, m_2, \dots, m_n \rangle$ , где  $m_1 + m_2 + \dots + m_n = m$ . По теореме 5 из §1 это можно сделать  $P(m_1, m_2, \dots, m_n)$  способами.  $\square$

Выражение  $(x_1 + x_2 + \dots + x_n)^m$  называется *перечисляющей производящей функцией перестановок с повторениями* из  $m_1$  элементов  $x_1$ ,  $m_2$  элементов  $x_2$ , ...,  $m_n$  элементов  $x_n$  по всем составам  $\langle m_1, m_2, \dots, m_n \rangle$  таким, что  $m_1 + m_2 + \dots + m_n = m$ .

Полиномиальная теорема позволяет доказать некоторые свойства чисел  $P(m_1, m_2, \dots, m_n)$ .

**Следствие 1.**

$$n^m = \sum_{m_1 + m_2 + \dots + m_n = m} P(m_1, m_2, \dots, m_n).$$

*Доказательство.* В формуле теоремы 1 положим  $x_1 = x_2 = \dots = x_n = 1$ .  $\square$

**Следствие 2.**  $P(m_1, m_2, \dots, m_n) =$

$$= P(m_1 - 1, m_2, \dots, m_n) + P(m_1, m_2 - 1, \dots, m_n) + \dots + P(m_1, m_2, \dots, m_n - 1).$$

*Доказательство.* Чтобы получить эту формулу, надо в формуле

$$(x_1 + x_2 + \dots + x_n)^{m-1} (x_1 + x_2 + \dots + x_n) = (x_1 + x_2 + \dots + x_n)^m$$

$(x_1 + x_2 + \dots + x_n)^{m-1}$  и  $(x_1 + x_2 + \dots + x_n)^m$  разложить по формуле полиномиальной теоремы, выполнить слева умножение на  $(x_1 + x_2 + \dots + x_n)$  и приравнять коэффициенты при одинаковых степенях  $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$ .  $\square$

**Следствие 3.**

$$P(m_1, m_2, \dots, m_n) = \sum_{k_i + l_i = m_i} P(k_1, k_2, \dots, k_n) P(l_1, l_2, \dots, l_n),$$

где суммирование распространено на все целые неотрицательные числа  $k_1, k_2, \dots, k_n$ ;  $l_1, l_2, \dots, l_n$  такие, что  $k_1 + k_2 + \dots + k_n = s$ ,  $l_1 + l_2 + \dots + l_n = t$  и  $k_1 + l_1 = m_1$ ,  $k_2 + l_2 = m_2$ , ...,  $k_n + l_n = m_n$ .

*Доказательство.* Чтобы доказать это следствие, надо перемножить обе части разложений

$$(x_1 + x_2 + \dots + x_n)^s = \sum_{k_1 + k_2 + \dots + k_n = s} P(k_1, k_2, \dots, k_n) x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$$

и

$$(x_1 + x_2 + \dots + x_n)^t = \sum_{l_1 + l_2 + \dots + l_n = t} P(l_1, l_2, \dots, l_n) x_1^{l_1} x_2^{l_2} \dots x_n^{l_n}$$

и сравнить коэффициенты в обеих частях при  $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$ .  $\square$

### §3. Биномиальная теорема. Биномиальные коэффициенты и их свойства

Частным случаем полиномиальной теоремы является

**Теорема 1.** (Биномиальная теорема.)

$$(a + x)^n = \sum_{k=0}^n C(n, k) a^{n-k} x^k.$$

*Доказательство.* Эта формула является частным случаем формулы теоремы 1 из §2 с учетом равенства следствия теоремы 5 из §1.  $\square$

Какой комбинаторный смысл имеют коэффициенты  $C(n, k)$  в формуле биномиальной теоремы? Как мы видели, правая часть этой формулы получается после возведения  $a + x$  в  $n$ -ю степень, т.е. перемножения скобок  $(a + x)$ , приведения подобных членов и расположения слагаемых по убывающим степеням  $a$ . Коэффициент  $C(n, k)$  стоит при выражении  $a^{n-k} x^k$ . Слагаемые такого вида получаются при раскрытии скобок в тех случаях, когда из  $k$  скобок берется  $x$ , а из оставшихся  $n - k$  скобок —  $a$ . Т.е.  $C(n, k)$  — это число способов выбора  $k$  скобок из имеющихся  $n$  скобок (здесь полезно вспомнить замечание 1 после теоремы 3 §1). Выбирая  $k$  скобок из имеющихся  $n$  скобок, мы выделяем  $k$ -элементное подмножество из  $n$ -элементного множества. Следовательно, коэффициенты  $C(n, k)$  в формуле биномиальной теоремы суть не что иное, как числа сочетаний из  $n$  элементов по  $k$  без повторений.

Формулу биномиальной теоремы называют биномом Ньютона. Бином Ньютона называется также *перечисляющей производящей функцией сочетаний без повторений*.

Биномиальная теорема позволяет доказать несколько интересных формул.

**Следствие 1.**  $\sum_{k=0}^n C(n, k) = 2^n$ .

*Доказательство.* Надо в тождестве биномиальной теоремы положить  $a = x = 1$ .  $\square$

**Следствие 2.**  $\sum_{k=0}^n C(n, k)(m-1)^{n-k} = m^n.$

*Доказательство.* Надо в тождестве биномиальной теоремы положить  $a = m-1$  и  $x = 1$ .  $\square$

**Следствие 3.**  $\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} C(n, 2k) = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} C(n, 2k-1) = 2^{n-1}.$

*Доказательство.* Надо в биномиальной теореме положить  $a = 1$  и  $x = -1$ , тогда  $(1-1)^n = \sum_{k=0}^n C(n, k) = 0$ . Группируя положительные и отрицательные члены равенства, установим  $\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} C(n, 2k) = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} C(n, 2k-1)$ . Так как  $\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} C(n, 2k) + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} C(n, 2k-1) = \sum_{k=0}^n C(n, k) = 2^n$ , то каждая из сумм составляет половину числа  $2^n$ .  $\square$

**Следствие 4.**  $\sum_{k=0}^n k \cdot C(n, k) = n2^{n-1}.$

*Доказательство.* Надо в биномиальной теореме положить  $a = 1$ , тогда  $(1+x)^n = \sum_{k=0}^n C(n, k)x^k$ . Дифференцирование последнего равенства по  $x$  дает  $n(1+x)^{n-1} = \sum_{k=0}^n k \cdot C(n, k)x^{k-1}$ . Положив  $x = 1$ , получаем искомое тождество.  $\square$

**Следствие 5.**  $\sum_{k=r}^n (-1)^k C(k, r) C(n, k) = 0, \quad n \geq r.$

*Доказательство.* Надо в биномиальной теореме положить  $a = 1$ , тогда  $(1+x)^n = \sum_{k=0}^n C(n, k)x^k$ . Дифференцирование последнего равенства  $r$  раз по  $x$  дает  $n \cdot (n-1) \cdot \dots \cdot (n-r+1)(1+x)^{n-r} = \sum_{k=r}^n k \cdot (k-1) \cdot \dots \cdot (k-r+1) C(n, k)x^{k-r}$ . Разделив на  $r!$  и положив  $x = -1$ , получаем искомое тождество.  $\square$

**Следствие 6. (Малая теорема Ферма.)** Если  $p$  — простое число, то  $n^p - n$  делится на  $p$ .

*Доказательство.* При  $n = 1$  это утверждение верно, так как  $1^p - 1 = 0$  делится на  $p$ . Пусть доказано, что  $k^p - k$  делится на  $p$ . Чтобы доказать делимость на  $p$  числа  $(k+1)^p - (k+1)$ , рассмотрим разность

$$(k+1)^p - (k+1) - (k^p - k).$$

Раскрывая  $(k+1)^p$  по формуле бинома Ньютона, получим:

$$\begin{aligned} (k+1)^p - (k+1) - (k^p - k) &= (k+1)^p - k^p - 1 = \\ &= C(p, 1)k^{p-1} + C(p, 2)k^{p-2} + \dots + C(p, p-1)k. \end{aligned} \quad (1)$$



Но при  $1 \leq j < p$  имеем:

$$C(p, j) = \frac{p \cdot (p-1) \cdot \dots \cdot (p-j+1)}{1 \cdot 2 \cdot \dots \cdot j}.$$

Поскольку число  $p$  простое, оно не делится ни на одно из чисел  $1, 2, \dots, j$ , стоящих в знаменателе. Поэтому  $C(p, j)$  делится на  $p$  при  $1 \leq j < p$ . Но тогда все слагаемые в правой части равенства (1) делятся на  $p$ , а значит, и левая часть делится на  $p$ . Поскольку в силу предположения  $k^p - k$  делится на  $p$ , то и  $(k+1)^p - (k+1)$  делится на  $p$ .

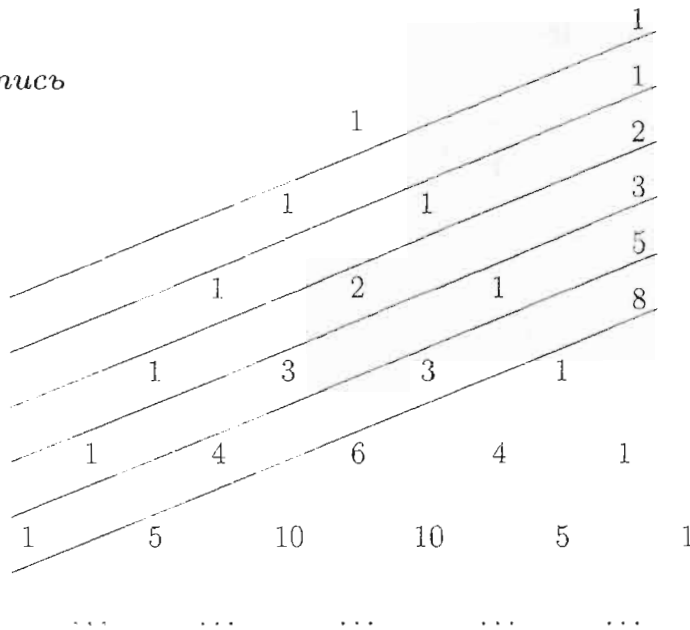
Итак, делимость  $n^p - n$  на  $p$  доказана при  $n = 1$ , а из делимости  $k^p - k$  на  $p$  следует, что и  $(k+1)^p - (k+1)$  делится на  $p$ . Значит,  $n^p - n$  делится на  $p$  при всех натуральных значениях  $n$ .  $\square$

Числа сочетаний  $C(n, k)$  называют **биномиальными коэффициентами**. Замечание 2 теоремы 3 из §1 дает простой способ последовательного вычисления значений  $C(n, k)$ . Сначала надо написать значение  $C(0, 0) = 1$ . В следующей строке напишем значения  $C(1, 0) = 1$  и  $C(1, 1) = 1$  так, чтобы значение  $C(0, 0)$  оказалось над промежутком между этими двумя числами. Далее, мы знаем, что  $C(2, 0) = C(2, 2) = 1$ . Эти числа запишем в следующей строке. А между ними запишем число  $C(2, 1)$  равное, согласно замечанию 2 теоремы 3 из §1, сумме чисел предыдущей строки, стоящих слева и справа от него,  $C(2, 1) = 1 + 1 = 2$ . По тому же правилу заполняем остальные строки: сначала пишем по бокам значения  $C(n, 0) = C(n, n) = 1$ , а все промежуточные значения вычисляем как суммы чисел предыдущей строки, стоящих слева и справа от вычисляемого значения. В результате получаем числовой треугольник, который называют *треугольником Паскаля* или *арифметическим треугольником*:

*символическая запись*

$$\begin{array}{ccccccc}
 & & C(0, 0) & & & & \\
 & & & & & & \\
 & & C(1, 0) & & C(1, 1) & & \\
 & & & & & & \\
 & & C(2, 0) & & C(2, 1) & & C(2, 2) \\
 & & & & & & \\
 & & C(3, 0) & & C(3, 1) & & C(3, 2) & & C(3, 3) \\
 & & & & & & & & \\
 & & C(4, 0) & & C(4, 1) & & C(4, 2) & & C(4, 3) & & C(4, 4) \\
 & & & & & & & & \\
 & & C(5, 0) & & C(5, 1) & & C(5, 2) & & C(5, 3) & & C(5, 4) & & C(5, 5) \\
 & & \dots & & \dots & & \dots & & \dots & & \dots & & \dots
 \end{array}$$

числовая запись



Треугольник Паскаля обладает многими интересными свойствами. Например, суммы чисел, стоящих в горизонтальных рядах, равны  $2^n$  (см. следствие 1 из биномиальной теоремы), а суммы чисел, стоящих на наклонных линиях, равны числам Фибоначчи.

**Замечание.** Формулу теоремы 1 принято называть «биномом Ньютона». Однако она была известна задолго до Ньютона. Ее хорошо знали среднеазиатские математики Омар Хайям, Гиясэддин и др. Известно, что в Западной Европе ее знал Блэз Паскаль. Заслуга же Ньютона была в ином — ему удалось обобщить формулу для  $(a + x)^n$  на случай нецелых показателей. Именно он доказал, что если  $a$  — положительное число и  $|x| < a$ , то для любого действительного значения  $\alpha$  имеет место равенство

$$(a + x)^\alpha = a^\alpha + \alpha a^{\alpha-1}x + \frac{\alpha(\alpha-1)}{1 \cdot 2} a^{\alpha-2}x^2 + \dots + \frac{\alpha(\alpha-1) \dots (\alpha-k+1)}{1 \cdot 2 \dots k} a^{\alpha-k}x^k + \dots \tag{2}$$

Только теперь получилось не конечное число слагаемых, а бесконечный ряд, который называется биномиальным рядом. В случае, когда  $n$  — натуральное число, скобка  $(n - n)$  обращается в нуль. Но эта скобка входит в коэффициенты всех членов, начиная с  $(n + 2)$ -ого, и поэтому все эти члены разложения равны нулю. Поэтому при натуральном  $n$  биномиальный ряд превращается в конечную сумму (бином Ньютона).

Коэффициенты, входящие в сумму (2), принято называть **обобщенными биномиальными коэффициентами** и обозначать  $C(\alpha, k)$ . По определению при  $\alpha \in \mathbb{R}, k \in \mathbb{Z}$

$$C(\alpha, k) = \begin{cases} \frac{\alpha \cdot (\alpha - 1) \cdot \dots \cdot (\alpha - k + 1)}{1 \cdot 2 \cdot \dots \cdot k}, & \text{если } k > 0, \\ 1, & \text{если } k = 0, \\ 0, & \text{если } k < 0. \end{cases}$$

Чтобы доказать формулу Ньютона, обозначим

$$f(x) = (a + x)^\alpha$$

и

$$S(x) = a^\alpha + \alpha a^{\alpha-1}x + \frac{\alpha(\alpha-1)}{1 \cdot 2} a^{\alpha-2}x^2 + \dots + \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{1 \cdot 2 \dots k} a^{\alpha-k}x^k + \dots$$

Тогда справедливо  $\alpha f(x) = (a + x)f'(x)$  и  $\alpha S(x) = (a + x)S'(x)$ . Значит,  $\frac{f'(x)}{f(x)} = \frac{S'(x)}{S(x)}$ , т.е.  $(\ln f(x))' = (\ln S(x))'$ . Так как  $\ln f(x)$  и  $\ln S(x)$  имеют одинаковые производные и равные значения при  $x = 0$ , то они равны. Значит,  $f(x) = S(x)$ , что и требовалось доказать.

## §4. Формула включений и исключений

Пусть имеется  $N$  предметов, некоторые из которых обладают свойствами  $\alpha_1, \alpha_2, \dots, \alpha_n$ . При этом каждый предмет может не обладать ни одним из этих свойств, либо обладать одним или несколькими свойствами. Обозначим через  $N(\alpha_i \alpha_j \dots \alpha_k)$  количество предметов, обладающих свойствами  $\alpha_i, \alpha_j, \dots, \alpha_k$  (и, быть может, еще некоторыми из других свойств). Если нам надо будет подчеркнуть, что берутся лишь предметы, не обладающие некоторым свойством, то это свойство пишем с черточкой. Например, через  $N(\alpha_1 \alpha_2 \bar{\alpha}_4)$  обозначено количество предметов, обладающих свойствами  $\alpha_1$  и  $\alpha_2$ , но не обладающих свойством  $\alpha_4$  (вопрос об остальных свойствах остается открытым).

**Теорема 1. (Формула включений и исключений.)** Число предметов, не обладающих ни одним из указанных свойств, может быть вычислено по формуле

$$N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_n) = \sum_{k=0}^n (-1)^k S_k,$$

где  $S_0 = N$ ,  $S_k = \sum_{i_1 < i_2 < \dots < i_k} N(\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k})$ ,  $k = 1, 2, \dots, n$ .

*Доказательство.* Доказательство проведем индукцией по числу свойств. При одном свойстве формула очевидна. Каждый предмет либо обладает этим свойством, либо не обладает им. Поэтому

$$N(\bar{\alpha}) = N - N(\alpha).$$

Предположим, что формула включений и исключений доказана для случая, когда число свойств равно  $n - 1$ :

$$\begin{aligned} N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1}) &= N - \sum_{i=1}^n N(\alpha_i) + \sum_{i_1 < i_2} N(\alpha_{i_1} \alpha_{i_2}) + \dots + \\ &+ (-1)^k \sum_{i_1 < i_2 < \dots < i_k} N(\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k}) + \dots + (-1)^{n-1} N(\alpha_1 \alpha_2 \dots \alpha_{n-1}). \end{aligned} \quad (1)$$

Эта формула, по предположению, справедлива для любой совокупности. В частности, она верна для совокупности  $N(\alpha_n)$  элементов, обладающих свойством  $\alpha_n$ , т.е.

$$N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1} \alpha_n) = N(\alpha_n) - \sum_{i=1}^n N(\alpha_i \alpha_n) + \sum_{i_1 < i_2} N(\alpha_{i_1} \alpha_{i_2} \alpha_n) + \dots + (-1)^k \sum_{i_1 < i_2 < \dots < i_k} N(\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k} \alpha_n) + \dots + (-1)^{n-1} N(\alpha_1 \alpha_2 \dots \alpha_{n-1} \alpha_n) \quad (2)$$

(добавляется указание, что в каждом случае берутся лишь предметы, обладающие свойством  $\alpha_n$ ).

Вычтем равенство (2) из равенства (1). В правой части получим то, что нам нужно — правую часть формулы включений и исключений. А в левой части получим разность

$$N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1}) - N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1} \alpha_n). \quad (3)$$

Но  $N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1})$  — это число предметов, не обладающих свойствами  $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$  и, может быть, обладающих свойством  $\alpha_n$ . А  $N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1} \alpha_n)$  — это число предметов, которые не обладают свойствами  $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ , но наверняка обладают свойством  $\alpha_n$ . Значит, разность (3) как раз равна числу предметов, не обладающих ни одним из свойств  $\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n$ . Иными словами,

$$N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1}) - N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1} \alpha_n) = N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_{n-1} \bar{\alpha}_n).$$

Таким образом, после вычитания и в левой части получается левая часть формулы включений и исключений. Тем самым эта формула доказана для случая, когда число свойств равно  $n$ .  $\square$

Пример 1. Как применение метода включений и исключений рассмотрим задачу о беспорядках. Сколько существует перестановок  $a_1, a_2, \dots, a_n$  чисел  $1, 2, \dots, n$ ,

$$\begin{array}{ccccccc} 1, & 2, & \dots, & i, & \dots, & n, \\ a_1, & a_2, & \dots, & a_i, & \dots, & a_n, \end{array}$$

таких, что  $a_i \neq i$  при любом  $i = 1, 2, \dots, n$ ?

Здесь  $N$  элементов — это  $n!$  перестановок  $a_1, a_2, \dots, a_n$ , а свойство  $\alpha_i$  выражается равенством  $a_i = i$ ,  $i = 1, 2, \dots, n$ . Тогда  $N(\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_r}) = (n-r)!$  — число перестановок оставляющих на месте  $r$  символов  $i_1, i_2, \dots, i_r$ . Далее, в  $\sum_{i_1 < i_2 < \dots < i_r} N(\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_r})$  имеется  $C(n, r)$  слагаемых — по числу способов выбора  $i_1, i_2, \dots, i_r$  из  $1, 2, \dots, n$ . Применяя формулу включений и исключений, находим

$$\begin{aligned} N(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) &= n! - n(n-1)! + C(n, 2)(n-2)! + \dots + \\ &\quad + (-1)^r C(n, r)(n-r)! + \dots + (-1)^n \cdot 1 = \\ &= n!(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^r \cdot \frac{1}{r!} + \dots + (-1)^n \cdot \frac{1}{n!}). \end{aligned}$$

Заметим, что

$$1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \dots$$

— это начальные слагаемые бесконечного ряда для  $e^{-1}$ . Этот бесконечный ряд знакочередующийся и первый отброшенный член есть  $(-1)^{n+1}/(n+1)!$ . Отсюда видно, что  $N(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)$  отличается от  $n!/e$  меньше, чем на  $1/(n+1)$ , и потому  $n!/e$  является весьма хорошим приближением для числа беспорядков из  $n$  символов.

*Пример 2.* Одной из самых больших загадок математики является расположение простых чисел в ряду всех натуральных чисел. Иногда два простых числа идут через одно число (например, 17 и 19, 29 и 31), а иногда подряд идет миллион составных чисел. Спрашивается, сколько простых чисел содержится среди  $N$  первых натуральных чисел? В этих подсчетах весьма полезным оказался метод, восходящий еще к древнегреческому ученому Эратосфену (он жил в III веке до новой эры в Александрии). Он придумал для этого следующий способ. Сначала вычеркивают каждое второе число после 2 (исключая само число 2). Потом берут первое из оставшихся чисел (а именно 3). Ясно, что это число простое. Вычеркивают каждое третье число, идущее после 3. Первым оставшимся числом будет 5. Вычеркиваем каждое пятое идущее после него число, и т.д. Числа, которые уцелеют после всех вычеркиваний, и являются простыми. Так как во времена Эратосфена писали на восковых табличках и не вычеркивали, а выкалывали цифры, то табличка после описанного процесса напоминала решето. Поэтому метод Эратосфена для нахождения простых чисел получил название «решето Эратосфена».

Подсчитаем, сколько останется чисел в первой сотне, если мы вычеркнем по методу Эратосфена числа, делящиеся на 2, 3 и 5. Иными словами, поставим такой вопрос: сколько чисел в первой сотне не делится ни на одно из чисел 2, 3, 5? Эта задача решается с использованием формулы включений и исключений.

Обозначим через  $\alpha_1$  свойство числа делиться на 2, через  $\alpha_2$  — свойство делимости на 3 и через  $\alpha_3$  — свойство делимости на 5. Тогда  $\alpha_1\alpha_2$  означает, что число делится на 6,  $\alpha_1\alpha_3$  означает, что оно делится на 10, и  $\alpha_2\alpha_3$ , — что оно делится на 15. Наконец,  $\alpha_1\alpha_2\alpha_3$  означает, что число делится на 30. Нам надо найти, сколько чисел от 1 до 100 не делится ни на 2, ни на 3, ни на 5, то есть не обладает ни одним из свойств  $\alpha_1, \alpha_2, \alpha_3$ . По формуле включений и исключений имеем

$$\begin{aligned} N(\bar{\alpha}_1\bar{\alpha}_2\bar{\alpha}_3) &= \\ &= 100 - N(\alpha_1) - N(\alpha_2) - N(\alpha_3) + N(\alpha_1\alpha_2) + N(\alpha_1\alpha_3) + N(\alpha_2\alpha_3) - N(\alpha_1\alpha_2\alpha_3). \end{aligned}$$

Но чтобы найти, сколько чисел от 1 до  $N$  делится на  $n$ , надо разделить  $N$  на  $n$  и взять целую часть получившегося частного. Поэтому

$$\begin{aligned} N(\alpha_1) &= 50, & N(\alpha_2) &= 33, & N(\alpha_3) &= 20, \\ N(\alpha_1\alpha_2) &= 16, & N(\alpha_1\alpha_3) &= 10, & N(\alpha_2\alpha_3) &= 6, & N(\alpha_1\alpha_2\alpha_3) &= 3, \end{aligned}$$

и, значит,

$$N(\bar{\alpha}_1\bar{\alpha}_2\bar{\alpha}_3) = 32.$$

Таким образом, 32 числа от 1 до 100 не делятся ни на 2, ни на 3, ни на 5. Эти числа уцелеют после первых трех шагов процесса Эратосфена. Кроме них, останутся сами числа 2, 3 и 5. Всего останется 35 чисел.

Аналогично можно посчитать, что из первой тысячи после первых трех шагов процесса Эратосфена останется 335 чисел.

**Теорема 2.** Число предметов, обладающих в точности  $m$  свойствами из  $n$  может быть найдено по формуле

$$\hat{N}_m = \sum_{k=0}^{n-m} (-1)^k C(m+k, m) S_{m+k}.$$

*Доказательство.* Перепишем доказываемую формулу в следующем виде:

$$\hat{N}_m = \sum_{k=0}^{n-m} (-1)^k C(m+k, m) S_{m+k} = (-1)^m \sum_{k=m}^n (-1)^k C(k, m) S_k.$$

В правой части этой формулы элемент с точно  $m$  свойствами учитывается один раз в первом слагаемом и не учитывается в остальных слагаемых. Элемент с точно  $t$  свойствами, где  $t > m$ , дает  $(-1)^k C(k, m) C(t, k)$  в слагаемом

$$\sum_{k=m}^n (-1)^k C(k, m) \sum_{i_1 < i_2 < \dots < i_k} N(\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k}).$$

Но из следствия 5 теоремы 1 §3

$$\sum_{k=m}^t (-1)^k C(k, m) C(t, k) = 0,$$

что и доказывает формулу теоремы.  $\square$

**Теорема 3.** Число предметов, обладающих не менее чем  $m$  свойствами из  $n$  может быть найдено по формуле

$$\check{N}_m = \sum_{k=0}^{n-m} (-1)^k C(m-1+k, m-1) S_{m+k}.$$

*Доказательство.* Доказательство проведем индукцией по числу  $m$ . При  $m = 1$  формула очевидна:

$$\check{N}_1 = \sum_{k=0}^{n-1} (-1)^k S_{1+k} = - \sum_{k=1}^n (-1)^k S_k = N - N(\bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_n).$$



Предположим, что формула доказана для случая, когда вычисляется число предметов, обладающих не менее чем  $m - 1$  свойством из  $n$ :

$$\check{N}_{m-1} = \sum_{k=0}^{n-m+1} (-1)^k C(m-2+k, m-2) S_{m-1+k}.$$

Тогда

$$\begin{aligned} \check{N}_m &= \check{N}_{m-1} - \hat{N}_{m-1} = \sum_{k=0}^{n-m+1} (-1)^k C(m-2+k, m-2) S_{m-1+k} - \\ &\quad - \sum_{k=0}^{n-m+1} (-1)^k C(m-1+k, m-1) S_{m-1+k} = \\ &= \sum_{k=1}^{n-m+1} (-1)^k (C(m-2+k, m-2) - C(m-1+k, m-1)) S_{m-1+k} = \\ &= \sum_{k=1}^{n-m+1} (-1)^{k+1} C(m-2+k, m-1) S_{m-1+k} = \\ &= \sum_{k=0}^{n-m} (-1)^{k+2} C(m-1+k, m-1) S_{m+k} = \sum_{k=0}^{n-m} (-1)^k C(m-1+k, m-1) S_{m+k}. \end{aligned}$$

□

## §5. Производящие функции

### 5.1. Основные определения

Пусть  $a_0, a_1, \dots, a_n, \dots$  — последовательность элементов из ассоциативного, коммутативного кольца  $K$  с единицей. Единицу аддитивной группы кольца  $K$  будем обозначать 0, а единицу мультипликативной группы — 1.

**Определение 1.** *Производящей функцией (производящим рядом) последовательности  $\{a_n\}_{n=0,1,\dots}$  называется формальный степенной ряд*

$$A(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots \quad (1)$$

Будем использовать более короткую форму записи для ряда (1):

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

«Формальность» построенной функции означает, что  $A(x)$  мы трактуем только как удобную запись последовательности  $\{a_n\}_{n=0,1,\dots}$ , и несущественно, для каких значений переменной  $x$  соответствующий ряд сходится. Поэтому мы никогда не будем вычислять значение такого ряда для конкретных значений переменной  $x$ , а будем только выполнять некоторые операции на таких рядах, определяя коэффициенты при отдельных степенях переменной  $x$ .

Аналогично можно рассмотреть производящие функции от нескольких переменных. Например,

$$\sum_{l=0}^{\infty} \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} a_{lmn} x^l y^m z^n.$$

Мы ограничимся формальными степенными рядами от одной переменной.

Если  $a_k = 0$  для  $k > n$ , то ряд (1) будем отождествлять с многочленом  $a_0 + \dots + a_n x^n$ .

Введем алгебраические действия над производящими функциями. Рассмотрим производящие функции  $A(x) = \sum_{n=0}^{\infty} a_n x^n$  и  $B(x) = \sum_{n=0}^{\infty} b_n x^n$ . Тогда

*сумма* производящих функций  $A(x)$  и  $B(x)$  есть производящая функция, которая обозначается  $A(x) + B(x)$  и определяется формальным степенным рядом

$$A(x) + B(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n;$$

*умножение производящей функции  $A(x)$  на число  $p \in K$*  есть производящая функция, которая обозначается  $pA(x)$  и определяется формальным рядом

$$pA(x) = \sum_{n=0}^{\infty} p a_n x^n;$$

и *произведение Коши* (коротко: *произведение*) производящих функций  $A(x)$  и  $B(x)$  есть производящая функция, которая обозначается  $A(x) \cdot B(x)$  и определяется формальным степенным рядом

$$A(x) \cdot B(x) = \sum_{n=0}^{\infty} c_n x^n,$$

где  $c_n = a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0 = \sum_{i=0}^n a_i b_{n-i}$ . Последовательность  $\{c_n\}_{n=0,1,\dots}$  называется *сверткой* последовательностей  $\{a_n\}_{n=0,1,\dots}$  и  $\{b_n\}_{n=0,1,\dots}$ .

Легко проверить, что так определенные сложение, умножение на число и произведение рядов удовлетворяют законам ассоциативности, коммутативности и дистрибутивности. Таким образом, множество  $K[[x]]$  формальных степенных рядов с коэффициентами из кольца  $K$  само является кольцом. Причем ассоциативным и коммутативным, если таковым является кольцо  $K$ . Единицей кольца  $K[[x]]$  служит единица кольца  $K$ .

Мы можем определить обратную производящую функцию к производящей функции  $A(x)$ , как обратный элемент в  $K[[x]]$ .

**Определение 2.** *Обратной к производящей функции  $A(x)$  называется производящая функция  $R(x)$  такая, что  $A(x) \cdot R(x) = 1$ .*

**Теорема 1.** *Обратная функция к  $A(x)$  существует тогда и только тогда, когда элемент  $a_0$  обратим в кольце  $K$ .*

*Доказательство.* Обозначим через  $\{r_n\}_{n=0,1,\dots}$  последовательность функции  $R(x)$ . Запишем условия обращения функции  $A(x)$

$$\begin{aligned} a_0 r_0 &= 1 \\ a_0 r_1 + a_1 r_0 &= 0 \\ \dots \\ a_0 r_n + a_1 r_{n-1} + \dots + a_n r_0 &= 0 \\ \dots \end{aligned}$$

Эта система разрешима относительно  $\{r_n\}_{n=0,1,\dots}$  тогда и только тогда, когда  $a_0$  обратим в кольце  $K$ . Элементы  $r_n$  находятся последовательным решением уравнений системы.  $\square$

**Определение 3.** Для производящей функции  $A(x)$  определим производную  $A'(x)$  равенством  $A'(x) = \sum_{n=0}^{\infty} (n+1)a_{n+1}x^n$ .

**Теорема 2.** Дифференцирование обладает следующими свойствами

1.  $(A(x) + B(x))' = A'(x) + B'(x)$ ;
2.  $(A(x) \cdot B(x))' = A'(x) \cdot B(x) + A(x) \cdot B'(x)$ .

*Доказательство.* Свойство 1 очевидно. Чтобы доказать свойство 2, сравним коэффициенты при  $x^n$  в обеих частях равенства. В результате получим  $(n+1) \sum_{k=0}^{n+1} a_k b_{n-k+1}$  в левой части и  $\sum_{k=0}^n (k+1)a_{k+1}b_{n-k} + \sum_{k=0}^n a_k(n-k+1)b_{n-k+1}$  — в правой. Сделаем в сумме  $\sum_{k=0}^n (k+1)a_{k+1}b_{n-k}$  замену индекса суммирования, введя  $j = k+1$ . Это дает  $\sum_{j=1}^{n+1} j a_j b_{n-j+1}$ , что при сложении с  $\sum_{j=0}^n a_j(n-j+1)b_{n-j+1}$  приводит к  $\left(\sum_{k=0}^{n+1} a_k b_{n-k+1}\right)(n+1)$ , что доказывает свойство 2.  $\square$

**Определение 4.** Обратной к операции дифференцирования является операция интегрирования:

$$\int_0^x A(t)dt = a_0 x + \frac{1}{2}a_1 x^2 + \frac{1}{3}a_2 x^3 + \dots = \sum_{n=1}^{\infty} \frac{1}{n} a_{n-1} x^n.$$

Отметим, что свободный член у  $\int_0^x A(t)dt$  равен 0.

**Теорема 3.** Интегрирование обладает следующими свойствами

1.  $\int_0^x A'(t)dt = \left(\int_0^x A(t)dt\right)' = A(x)$ , если  $a_0 = 0$ ;

$$2. \int_0^x (A(t) + B(t))dt = \int_0^x A(t)dt + \int_0^x B(t)dt;$$

$$3. \int_0^x A(t) \cdot B'(t)dt = A(x) \cdot B(x) - \int_0^x B(t) \cdot A'(t)dt, \text{ если } a_0 = b_0 = 0.$$

*Доказательство.* Вытекает из определения формального интеграла.  $\square$

Из математического анализа известно, что если ряд (1) сходится в некоторой окрестности нуля, то его сумма  $A(x)$  является аналитической функцией в этой окрестности и  $a_n = A^{(n)}(0)/n!$ ,  $n = 0, 1, \dots$  ( $A^{(n)}(0)$  обозначает значение  $n$ -ой производной функции  $A(x)$  для  $x = 0$ ; ряд (1) — это не что иное, как ряд Маклорена функции  $A(x)$ ). Это взаимно однозначное соответствие между рядами, сходящимися в окрестности нуля, и функциями, аналитическими в окрестности нуля, позволяет отождествить формальный ряд с определенной через него аналитической функцией в случае рядов, сходящихся в окрестности нуля. Таким образом, будем писать, например,

$$\sum_{n=0}^{\infty} x^n = (1 - x)^{-1}, \quad (2)$$

или

$$\sum_{n=0}^{\infty} \frac{1}{n!} x^n = e^x.$$

Тождества со степенными рядами, если они выступают как средство задания аналитических функций, верны и как соотношения для формальных степенных рядов. Например, тождество  $\left(\sum_{n=0}^{\infty} \frac{x^n}{n!}\right) \left(\sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!}\right) = 1$  справедливо как тождество между аналитическими функциями, а выражение  $e^x e^{-x} = 1$  верно и как утверждение о формальных степенных рядах.

Найдем теперь производящие функции для некоторых последовательностей. В соответствии с биномиальной теоремой имеем

$$\sum_{k=0}^{\infty} C(n, k) x^k = \sum_{k=0}^n C(n, k) x^k = (1 + x)^n. \quad (3)$$

Следовательно, при заданном  $n$  производящей функцией последовательности  $C(n, 0), C(n, 1), C(n, 2), \dots$  является  $(1 + x)^n$ .

Используя (2), получаем

$$\sum_{k=0}^{\infty} 2^k x^k = \sum_{k=0}^{\infty} (2x)^k = (1 - 2x)^{-1},$$

и, следовательно, производящей функцией последовательности  $1, 2, 4, 8, \dots$  является  $(1 - 2x)^{-1}$ . Пользуясь тем, что аналитическую функцию можно дифференцировать почленно, можно написать

$$\sum_{k=0}^{\infty} kx^k = x \sum_{k=0}^{\infty} kx^{k-1} = x \left( \sum_{k=0}^{\infty} x^k \right)' = x \frac{d}{dx} (1 - x)^{-1} = x(1 - x)^{-2},$$

и, следовательно, производящей функцией для последовательности 0, 1, 2, 3, ... является  $x(1-x)^{-2}$ .

Можно рассматривать и обратную задачу поиска последовательности, соответствующей заданной аналитической производящей функции. Например, функции  $(1-4x)^{-\frac{1}{2}}$ .

Используя обобщенную биномиальную теорему, имеем

$$\begin{aligned}
 (1-4x)^{-\frac{1}{2}} &= 1 + \sum_{n=1}^{\infty} \frac{(-\frac{1}{2})(-\frac{1}{2}-1)\dots(-\frac{1}{2}-n+1)}{n!} (-4x)^n = \\
 &= 1 + \sum_{n=1}^{\infty} \frac{4^n (\frac{1}{2})(\frac{3}{2})\dots(\frac{2n-1}{2})}{n!} x^n = 1 + \sum_{n=1}^{\infty} \frac{2^n \cdot 1 \cdot 3 \cdot \dots \cdot (2n-1)}{n!} x^n = \\
 &= 1 + \sum_{n=1}^{\infty} \frac{2^n \cdot n! \cdot 1 \cdot 3 \cdot \dots \cdot (2n-1)}{n! \cdot n!} x^n = 1 + \sum_{n=1}^{\infty} \frac{2 \cdot 4 \cdot \dots \cdot 2n}{n!} \frac{1 \cdot 3 \cdot \dots \cdot (2n-1)}{n!} x^n = \\
 &= 1 + \sum_{n=1}^{\infty} C(2n, n) x^n = \sum_{n=0}^{\infty} C(2n, n) x^n.
 \end{aligned} \tag{4}$$

Значит, данная функция является производящей для последовательности  $a_n = C(2n, n)$ ,  $n = 0, 1, \dots$ .

Производящие функции — это удобный инструмент для доказательства тождеств, связанных с биномиальными коэффициентами.

Пример 1. Приведем еще одно доказательство тождества Коши (см. §1):

$$C(m+n, k) = \sum_{s=0}^k C(m, s) C(n, k-s).$$

Действительно,

$$\begin{aligned}
 \sum_{k=0}^{m+n} C(m+n, k) x^k &= (1+x)^{m+n} = (1+x)^m (1+x)^n = \\
 \sum_{i=0}^m C(m, i) x^i \cdot \sum_{j=0}^n C(n, j) x^j &= \sum_{i=0}^{m+n} \sum_{s=0}^k C(m, s) C(n, k-s) x^k
 \end{aligned}$$

(на последнем шаге мы воспользовались формулой произведения Коши двух рядов). Сравнивая коэффициенты в обеих частях равенства, получаем искомое тождество.

## 5.2. Применение аппарата производящих функций к задаче о составах слов

Рассмотрим следующую задачу:

Обозначим через  $\alpha$  — слово длины  $k$ , составленное из элементов множества  $X = \{x_1, \dots, x_n\}$ ,  $\langle m_1, \dots, m_n \rangle$  — состав слова  $\alpha$ ,  $m_1 + \dots + m_n = k$ . Введем ограничения на количество вхождений каждого элемента  $x_i$  в слово  $\alpha$ , определив соответствующее числовое множество  $M_i$  как множество, состоящее



из всех возможных количеств вхождений  $x_i$  в  $\alpha$ . Сколько составов слов  $\alpha$ , компоненты которого удовлетворяют рассмотренному ограничению, можно составить из элементов множества  $X$ ?

Обозначим искомое число через  $a_k$ . Пусть  $A(x)$  — производящая функция последовательности  $\{a_k\}_{k=0,1,\dots}$ . Тогда справедливо следующее соотношение

$$A(x) = \prod_{i=1}^n \sum_{m_i \in M_i} x^{m_i}. \quad (5)$$

Действительно,

$$\prod_{i=1}^n \sum_{m_i \in M_i} x^{m_i} = \sum_{m_1, \dots, m_n} x^{m_1} \dots x^{m_n} = \sum_{k=1}^{\infty} a_k x^k,$$

где  $a_k = \sum_{m_1 + \dots + m_n = k} 1$ . Здесь суммирование ведется по всем составам  $\langle m_1, \dots, m_n \rangle$  таким, что  $m_i \in M_i$ ,  $i = 1, \dots, n$ , и  $m_1 + \dots + m_n = k$ , в результате получается искомое число составов слов  $\alpha$  длины  $k$ .

**Пример 2.** Сколько разных наборов из  $k$  шаров можно получить, имея 1 синий, 2 одинаковых белых и 4 одинаковых красных шара?

Здесь множество  $X$  состоит из трех элементов  $x_1, x_2$  и  $x_3$ , обозначающих соответственно синий, белый и красный цвета шаров. Возможное число вхождений шара каждого цвета в набор определяется множествами  $M_1 = \{0, 1\}$ ,  $M_2 = \{0, 1, 2\}$ ,  $M_3 = \{0, 1, 2, 3, 4\}$ . Используя формулу (5), запишем производящую функцию

$$A(x) = (1+x)(1+x+x^2)(1+x+x^2+x^3+x^4) = 1+3x+5x^2+6x^3+6x^4+5x^5+3x^6+x^7.$$

Коэффициент при  $x^k$  есть число  $k$ -элементных наборов шаров. Таким образом, можно составить 3 одноэлементных набора, 5 — двухэлементных, 6 — трехэлементных и т.д.

**Пример 3.** В условии предыдущего примера введем дополнительное ограничение: число красных шаров в наборе должно быть нечетно.

Изменение коснется множества, определяющего допустимое число вхождений красного шара:  $M_3 = \{1, 3\}$ . Используя формулу (5), запишем производящую функцию

$$A(x) = (1+x)(1+x+x^2)(x+x^3) = x+2x^2+3x^3+3x^4+2x^5+x^6.$$

Теперь одноэлементный набор может быть только один, существует 2 двухэлементных набора и т.д.

Применим аппарат производящих функций к выводу формул для числа сочетаний без повторов и с повторениями.



**Сочетания без повторений.**  $k$ -элементное подмножество множества  $X$  определяется составом слова, в которое каждый элемент множества  $X$  входит как компонента не более одного раза, т.е.  $M_i = \{0, 1\}$ ,  $i = 1, \dots, n$ . Согласно (5), производящая функция имеет вид

$$A(x) = (1+x)^n = \sum_{k=0}^n C(n, k)x^k,$$

где  $C(n, k)$  — биномиальные коэффициенты.

**Сочетания с повторениями.** Каждый элемент множества  $X$  может появиться в слове любое количество раз, т.е.  $M_i = \{0, 1, 2, \dots\}$ ,  $i = 1, \dots, n$ . Согласно (5), производящая функция имеет вид

$$\begin{aligned} A(x) &= (1+x+x^2+\dots)^n = \\ &[\text{по формуле (2)}] = ((1-x)^{-1})^n = (1-x)^{-n} = \\ &[\text{по формуле биномиального ряда}] = \sum_{k=0}^{\infty} \frac{-n(-n-1)\dots(-n-k+1)}{k!} (-x)^k = \\ &= \sum_{k=0}^{\infty} \frac{n(n+1)\dots(n+k-1)}{k!} (-1)^k (-x)^k = \sum_{k=0}^{\infty} C(n+k-1, k)x^k, \end{aligned}$$

где  $C(n+k-1, k)$  — обобщенные биномиальные коэффициенты.

### 5.3. Свойства производящих функций

Рассмотрим теперь некоторые свойства производящих функций, используемые при их нахождении. Будем обозначать производящие функции последовательностей  $\{a_n\}_{n=0,1,\dots}$ ,  $\{b_n\}_{n=0,1,\dots}$ ,  $\{y_n\}_{n=0,1,\dots}$ ,  $\{z_n\}_{n=0,1,\dots}$  как  $A(x)$ ,  $B(x)$ ,  $Y(x)$ ,  $Z(x)$  соответственно, буквами  $p$  и  $q$  — произвольные постоянные из кольца  $K$ , а буквой  $k$  — фиксированное натуральное число. Приведенные ниже леммы доказываются прямой подстановкой вместо производящих функций соответствующих рядов.

**Лемма 1. (Лемма о линейной комбинации.)** Производящей функцией для последовательности  $y_n = pa_n + qb_n$ ,  $n = 0, 1, \dots$ , является функция  $Y(x) = pA(x) + qB(x)$ .

**Лемма 2. (Лемма о сдвиге начала.)** Производящей функцией для последовательностей

$$y_n = \begin{cases} 0, & \text{для } n = 0, \dots, k-1, \\ a_{n-k}, & \text{для } n = k, k+1, \dots \end{cases} \quad \text{и} \quad z_n = a_{n+k}$$

являются функции  $Y(x) = A(x) \cdot x^k$  и  $Z(x) = \left( A(x) - \sum_{m=0}^{k-1} a_m x^m \right) \cdot x^{-k}$ .

Пример 4. В качестве примера использования обеих лемм рассмотрим оценку суммы

$$\sum_{i=1}^t C(n-i, j).$$

Положим  $a_{ij} = C(n-i, j)$ , и для каждого фиксированного значения  $i$  рассмотрим  $a_{ij}$  как последовательность, задаваемую индексом  $j$ , с производящей функцией

$$A_i(x) = (1+x)^{n-i}.$$

Определим последовательность  $b_j$  следующим образом:

$$b_j = \sum_{i=1}^t a_{ij}.$$

Производящая функция этой последовательности получается путем применения леммы 1

$$B(x) = \sum_{i=1}^t A_i(x) = \sum_{i=1}^t (1+x)^{n-i} = (1+x)^n \sum_{i=1}^t \left( \frac{1}{1+x} \right)^i.$$

Последнее выражение оценим как сумму членов геометрической прогрессии. Таким образом,

$$B(x) = \frac{(1+x)^n}{x} - \frac{(1+x)^{n-t}}{x}.$$

Производящие функции  $(1+x)^n/x$  и  $(1+x)^{n-t}/x$  могут быть получены по лемме 2 с помощью сдвига начала из функций  $(1+x)^n$  и  $(1+x)^{n-t}$  соответственно. Откуда

$$b_j = \sum_{i=1}^t C(n-i, j) = C(n, j+1) - C(n-t, j+1).$$

Замечание. Полезно заметить, что переход от последовательности  $\{a_n\}_{n=0,1,\dots}$  к  $\{na_n\}_{n=0,1,\dots}$  в терминах производящих функций выглядит как сдвиг  $A(x) \cdot x$  и дифференцирование:

$$(A(x) \cdot x)' = \sum_{n=0}^{\infty} na_n x^n.$$

Повторное дифференцирование позволяет умножить  $a_n$ ,  $n = 0, 1, \dots$ , на любой многочлен от  $n$ .

Переход от  $\{a_n\}_{n=0,1,\dots}$  к  $\{a_n/n\}_{n=1,2,\dots}$  в терминах производящих функций выглядит как сдвиг  $(A(t) - a_0)/t$  и интегрирование:

$$\int_0^x \frac{A(t) - a_0}{t} dt = \sum_{n=1}^{\infty} \frac{a_n}{n} x^n.$$

**Лемма 3. (Лемма об изменении масштаба.)** Производящими функциями для последовательностей  $y_n = n \cdot a_n$  и  $z_n = \frac{a_n}{n+1}$ ,  $n = 0, 1, \dots$ , являются функции  $Y(x) = x \cdot A'(x)$  и  $Z(x) = \frac{1}{x} \int_0^x A(t) dt$  соответственно.

Изменение масштаба также полезно при оценке сумм.

**Пример 5.** Найдём сумму  $\sum_{k=2}^{n-1} (n-k)(n-k)C(n-1, n-k)$ .

$$\text{Имеем, } \sum_{k=2}^{n-1} (n-k)(n-k)C(n-1, n-k) = \sum_{k=1}^{n-2} k^2 C(n-1, k).$$

Обозначив  $a_k = k^2 C(n-1, k)$ ,  $b_k = k C(n-1, k)$  и  $d_k = C(n-1, k)$ , получаем  $b_k = k d_k$  и, таким образом,

$$B(x) = x \cdot D'(x).$$

Из  $a_k = k b_k$  следует

$$A(x) = x \cdot B'(x) = x \cdot D'(x) + x^2 \cdot D''(x).$$

Используя замечание после биномиальной теоремы, заключаем, что  $D(x) = (1+x)^{n-1}$ , и производящая функция  $A(x)$  является многочленом степени  $n-1$ . Тогда

$$A(x) = x(n-1)(1+x)^{n-2} + x^2(n-1)(n-2)(1+x)^{n-3}$$

и можно вычислить значение многочлена  $A(x)$  при  $x = 1$ , т.е.

$$A(1) = \sum_{k=1}^{n-1} k^2 C(n-1, k).$$

Откуда

$$\begin{aligned} \sum_{k=2}^{n-1} (n-k)(n-k)C(n-1, n-k) &= (n-1)2^{n-2} + (n-1)(n-2)2^{n-3} - (n-1) = \\ &= n(n-1)2^{n-3} - (n-1). \end{aligned}$$

**Лемма 4. (Лемма о свертке.)** Производящей функцией для последовательности  $y_n = \sum_{m=0}^n a_m b_{n-m}$ ,  $n = 0, 1, \dots$ , является функция  $Y(x) = A(x) \cdot B(x)$ .

**Пример 6.** Покажем, что для любого  $t$  справедливо тождество

$$\sum_{n=0}^t C(2n, n)C(2t-2n, t-n) = 4^t.$$

Согласно (4) имеем  $C(2n, n)$  — коэффициент при  $x^n$  в разложении  $(1-4x)^{-\frac{1}{2}}$ , а  $C(2t-2n, t-n)$  — коэффициент при  $x^{t-n}$  в  $(1-4x)^{-\frac{1}{2}}$ . По лемме о свертке левая

часть доказываемого тождества является коэффициентом при  $x^t$  в произведении  $(1-4x)^{-\frac{1}{2}} \cdot (1-4x)^{-\frac{1}{2}}$ . Но  $(1-4x)^{-\frac{1}{2}} \cdot (1-4x)^{-\frac{1}{2}} = (1-4x)^{-1} =$   
[используя (2)]  $= 1 + 4x + (4x)^2 + \dots + (4x)^t + \dots$

Отсюда получаем искомое тождество.

**Лемма 5. (Лемма о частичных суммах.)** Производящей для последовательности  $y_n = \sum_{m=0}^n a_m$  является функция  $Y(x) = \frac{A(x)}{1-x}$ .

*Доказательство.* Действительно,

$$\begin{aligned} Y(x) &= a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + \dots = \\ &= a_0 + a_0x + a_0x^2 + \dots + \\ &\quad + a_1x + a_1x^2 + \dots + \\ &\quad + a_2x^2 + \dots + \\ &\quad \dots = \\ &= a_0(1 + x + x^2 + \dots) + \\ &\quad + a_1x(1 + x + x^2 + \dots) + \\ &\quad + a_2x^2(1 + x + x^2 + \dots) + \\ &\quad \dots = \\ &= (a_0 + a_1x + a_2x^2 + \dots) \cdot (1 + x + x^2 + \dots). \end{aligned}$$

Используя (2) и определение  $A(x)$ , получаем требуемый результат.  $\square$

## §6. Рекуррентные уравнения

В качестве основного поля в этом параграфе будем рассматривать поле комплексных чисел.

**Определение 1.** Рекуррентным (от латинского *recurrere* — возвращаться) уравнением или рекуррентным соотношением порядка  $k$  называется равенство

$$a_{n+k} = F(a_{n+k-1}, a_{n+k-2}, \dots, a_n), \quad (1)$$

позволяющее вычислить значение  $a_{n+k}$ , если известны  $k$  предыдущих значений этой последовательности.

**Определение 2.** Последовательность  $\{a_n\}_{n=0,1,\dots}$  называется решением рекуррентного уравнения (1), если она удовлетворяет равенству (1) при всех значениях  $n$ .

Рекуррентное уравнение (1) имеет бесконечное множество решений, так как  $k$  первых членов последовательности могут быть заданы произвольно. Задание их значений

$$a_1 = x_1, \quad a_2 = x_2, \quad \dots, \quad a_k = x_k \quad (2)$$

называется заданием начальных условий.

Решение (1), удовлетворяющее начальным условиям (2), называется частным.

Решение рекуррентного уравнения (1)  $a_n = f(n, C_1, \dots, C_k)$  называется *общим*, если:

- 1) оно содержит  $k$  произвольных постоянных  $C_i, i = 1, \dots, k$ ;
- 2) при любых значениях этих постоянных оно удовлетворяет формуле (1);
- 3) выбором значений постоянных  $C_i, i = 1, \dots, k$ , из него можно выделить частное решение, удовлетворяющее любым начальным условиям (2).

Пример 1. Рассмотрим рекуррентное уравнение порядка 2

$$a_{n+2} = 3a_{n+1} - 2a_n. \quad (3)$$

Оно имеет частное решение  $a_n = 1, n = 0, 1, \dots$ , удовлетворяющее начальным условиям  $a_0 = a_1 = 1$  и частное решение  $a_n = 2^n, n = 0, 1, \dots$ , удовлетворяющее начальным условиям  $a_0 = 1, a_1 = 2$ . Общим решением является последовательность

$$a_n = C_1 \cdot 1^n + C_2 \cdot 2^n. \quad (4)$$

В самом деле, подставив (4) в (3), легко убедиться, что последовательность (4) обращает уравнение (3) в тождество. Поэтому остается только показать, что любое решение нашего уравнения можно представить в виде (4). Но любое решение (3) однозначно определяется значениями  $a_1 = a$  и  $a_2 = b$ . Рассмотрим систему

$$\begin{cases} C_1 + 2C_2 = a \\ C_1 + 4C_2 = b \end{cases}$$

Эта система имеет решения относительно  $C_1$  и  $C_2$  при любых значениях  $a$  и  $b$ . Поэтому (4) действительно является общим решением уравнения (3).

**Замечание.** Если последовательность  $\{a_n\}_{n=0,1,\dots}$  есть решение рекуррентного уравнения (1), то последовательность  $b_n = a_{n+k_0}$  ( $k_0$  — любое натуральное число), являющаяся частью исходной последовательности, тоже будет решением уравнения (1).

Читатель, наверное, уже обратил внимание, что использованная терминология аналогична терминологии теории дифференциальных уравнений. Эта аналогия будет продолжаться и дальше.

### 6.1. Линейные однородные рекуррентные уравнения с постоянными коэффициентами

**Определение 3.** *Линейным однородным рекуррентным уравнением (соотношением) с постоянными коэффициентами порядка  $k$  называется уравнение вида*

$$a_{n+k} = p_1 a_{n+k-1} + p_2 a_{n+k-2} + \dots + p_k a_n, \quad n \geq 0, \quad (5)$$

где  $p_i$ ,  $i = 1, \dots, k$ , константы и  $p_k \neq 0$  (это условие на  $p_k$  необходимо, так как при  $p_k = 0$  уравнение (5) имело бы порядок ниже  $k$ ).

Назовем  $F(x) = x^k - p_1 x^{k-1} - \dots - p_k$  **характеристическим полиномом** этого рекуррентного уравнения, и пусть

$$F(x) = (x - \alpha_1)^{l_1} \dots (x - \alpha_s)^{l_s}, \quad l_1 + \dots + l_s = r$$

— разложение  $F(x)$  на линейные множители.

**Теорема 1.** Пусть последовательность  $\{a_n\}_{n=0,1,\dots}$  удовлетворяет линейному рекуррентному соотношению (5) с постоянными коэффициентами. Тогда

$$a_n = \sum_{i=1}^s P_i(n) \alpha_i^n$$

для всех  $n$ , где  $P_i(n)$  — полином степени не выше  $l_i - 1$  относительно  $n$ . Коэффициенты полинома  $P_i(n)$  определяются начальными значениями  $a_0, a_1, \dots, a_{k-1}$  последовательности  $\{a_n\}_{n=0,1,\dots}$ .

**Доказательство.** Пусть  $A(x)$  — производящая функция для последовательности  $\{a_n\}_{n=0,1,\dots}$ . Обозначим через  $K(x)$  полином

$$K(x) = 1 - p_1 x - p_2 x^2 - \dots - p_k x^k. \quad (6)$$

Тогда очевидно, что

$$A(x)K(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{k-1} x^{k-1} = C(x),$$

где  $C(x)$  — полином степени не выше  $k - 1$ . Действительно, если  $c_{n+k}$  есть коэффициент при  $x^{n+k}$ ,  $n \geq 0$ , в произведении  $A(x)K(x)$ , то в силу (5)

$$c_{n+k} = a_{n+k} - p_1 a_{n+k-1} - \dots - p_k a_n = 0.$$

Таким образом, для последовательности  $\{a_n\}_{n=0,1,\dots}$ , удовлетворяющей линейному рекуррентному уравнению (5), производящая функция  $A(x)$  есть формальная рациональная функция

$$A(x) = \frac{C(x)}{K(x)}.$$

Рассмотрим **характеристический полином**

$$F(x) = x^k - p_1 x^{k-1} - \dots - p_k \quad (7)$$

(напомним, что  $p_k \neq 0$ ) и его разложение на линейные множители

$$F(x) = (x - \alpha_1)^{l_1} \dots (x - \alpha_s)^{l_s}, \quad l_1 + \dots + l_s = r, \quad (8)$$



где  $\alpha_1, \dots, \alpha_s$  — корни (возможно комплексные) полинома  $F(x)$ . Сравнивая  $F(x)$  из формулы (7) и  $K(x)$  из формулы (6) видим, что

$$K(x) = x^k F\left(\frac{1}{x}\right),$$

и в соответствии с разложением (8) для  $F(x)$  получаем разложение на множители для  $K(x)$ :

$$K(x) = (1 - \alpha_1 x)^{l_1} \dots (1 - \alpha_s x)^{l_s}, \quad l_1 + \dots + l_s = k.$$

Выразим рациональную функцию  $A(x) = C(x)/K(x)$  в виде суммы простых дробей

$$A(x) = \frac{C(x)}{K(x)} = \sum_{i=1}^s \sum_{j=1}^{l_i} \frac{\beta_{ij}}{(1 - \alpha_i x)^j}, \quad (9)$$

где  $\beta_{ij}$  — подходящие постоянные, что дает выражение производящей функции как суммы функций вида

$$\frac{\beta}{(1 - \alpha x)^j} = \beta(1 - \alpha x)^{-j}.$$

По формуле биномиального ряда получаем

$$\beta(1 - \alpha x)^{-j} = \beta \left( 1 + (-j)(-\alpha x) + \dots + \frac{(-j) \dots (-j - n + 1)(-\alpha x)^n}{n!} + \dots \right).$$

В этом выражении коэффициент при  $x^n$  равен

$$\frac{\beta(n + j - 1) \dots j}{n!} \alpha^n = \beta C(n + j - 1, n) \alpha^n = \beta C(n + j - 1, j - 1) \alpha^n.$$

Заметим, что

$$\sum_{j=1}^{l_i} C(n + j - 1, j - 1) \alpha_i^n = P_i(n) \alpha_i^n,$$

где  $P_i(n)$  — полином от  $n$  степени не выше  $l_i - 1$ , и что любой полином  $P_i(n)$  может быть получен соответствующим выбором постоянных  $\beta_{ij}$ . Таким образом, (9) можно записать в виде

$$A(x) = \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \sum_{i=1}^s P_i(n) \alpha_i^n x^n,$$

и, сравнивая коэффициенты при  $x^n$ , получаем, что

$$a_n = \sum_{i=1}^s P_i(n) \alpha_i^n,$$

где степень  $P_i(n)$  не выше  $l_i - 1$ . □

Пример 2. Рассмотрим последовательность Фибоначчи

$$0, 1, 1, 2, 3, 5, 8, 13, \dots,$$

где каждое следующее число является суммой двух предыдущих чисел.

Таким образом, числа последовательности Фибоначчи задаются рекуррентным уравнением

$$a_{n+2} - a_{n+1} - a_n = 0$$

и начальными условиями

$$a_0 = 0, \quad a_1 = 1.$$

Найдем общую формулу для чисел Фибоначчи. Характеристическое уравнение

$$x^2 - x - 1 = 0$$

имеет два действительных не равных корня  $\alpha_1 = \frac{1-\sqrt{5}}{2}$  и  $\alpha_2 = \frac{1+\sqrt{5}}{2}$ . Следовательно, общим решением рекуррентного уравнения будет последовательность

$$a_n = C_1 \alpha_1^n + C_2 \alpha_2^n.$$

Система для нахождения  $C_1$  и  $C_2$  имеет вид

$$\begin{cases} C_1 + C_2 = 0, \\ C_1 \alpha_1 + C_2 \alpha_2 = 1. \end{cases}$$

Тогда  $\Delta = \begin{vmatrix} 1 & 1 \\ \alpha_1 & \alpha_2 \end{vmatrix} = \alpha_2 - \alpha_1 = \sqrt{5},$

$$\Delta_1 = \begin{vmatrix} 0 & 1 \\ 1 & \alpha_2 \end{vmatrix} = -1, \quad \Delta_2 = \begin{vmatrix} 1 & 0 \\ \alpha_1 & 1 \end{vmatrix} = 1,$$

$$C_1 = \frac{\Delta_1}{\Delta} = -\frac{1}{\sqrt{5}}, \quad C_2 = \frac{\Delta_2}{\Delta} = \frac{1}{\sqrt{5}}.$$

Окончательно получаем

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

## 6.2. Линейные неоднородные рекуррентные уравнения с постоянными коэффициентами

**Определение 4.** *Линейным неоднородным рекуррентным уравнением (соотношением) с постоянными коэффициентами порядка  $k$  называется равенство вида (или уравнение вида)*

$$a_{n+k} = p_1 a_{n+k-1} + p_2 a_{n+k-2} + \dots + p_k a_n + \varphi(n), \quad n \geq 0, \quad (10)$$

где  $p_i, i = 1, \dots, k$ , константы,  $p_k \neq 0$  (при  $p_k = 0$  уравнение имело бы порядок ниже  $k$ ),  $\varphi(n)$  — некоторая функция, не равная тождественно нулю.

Каждому неоднородному рекуррентному уравнению соответствует однородное рекуррентное уравнение (5).

Обозначим  $\{a_n^{\text{част. неодн.}}\}_{n=0,1,\dots}$  частное решение неоднородного рекуррентного уравнения и  $\{a_n^{\text{общ. одн.}}\}_{n=0,1,\dots}$  общее решение соответствующего ему однородного уравнения.

**Теорема 2.** Общее решение  $\{a_n\}_{n=0,1,\dots}$  неоднородного рекуррентного уравнения может быть найдено в виде суммы частного решения  $\{a_n^{\text{част. неодн.}}\}_{n=0,1,\dots}$  неоднородного рекуррентного уравнения и общего решения  $\{a_n^{\text{общ. одн.}}\}_{n=0,1,\dots}$  соответствующего ему однородного рекуррентного уравнения

$$a_n = a_n^{\text{част. неодн.}} + a_n^{\text{общ. одн.}}.$$

*Доказательство.* Так как при подстановке  $a_n^{\text{част. неодн.}} + a_n^{\text{общ. одн.}}$  в (10) получается верное тождество, то  $a_n^{\text{част. неодн.}} + a_n^{\text{общ. одн.}}$  действительно является решением (10).

Пусть  $\{a'_n\}_{n=0,1,\dots}$  — произвольное частное решение (10). По условию теоремы имеем заданное частное решение  $\{a_n^{\text{част. неодн.}}\}_{n=0,1,\dots}$ . По тогда разность  $a''_n = a'_n - a_n^{\text{част. неодн.}}$  является частным решением соответствующего однородного рекуррентного уравнения, и оно может быть определено заданием неопределенных коэффициентов в выражении  $a_n^{\text{общ. одн.}}$ .  $\square$

Рассмотрим некоторые методы нахождения частных решений неоднородных рекуррентных уравнений для частных случаев функции  $\varphi(n)$ . Следующие две теоремы легко доказываются подстановкой частного решения  $\{a_n^{\text{част. неодн.}}\}_{n=0,1,\dots}$  в (10).

**Теорема 3.** (О правой части вида  $A \cdot b^n$ ) Если в (10)  $\varphi(x) = A \cdot b^n$ , то частное решение (10) может быть найдено в виде

$$a_n^{\text{част. неодн.}} = D n^k b^n,$$

где  $k$  — кратность, с которой константа  $b$  входит в число корней характеристического уравнения, а  $D$  — некоторая постоянная.

Обозначим  $P_s(n)$  многочлен степени  $s$ :  $P_s(n) = \sum_{m=0}^s l_m n^m$ .

**Теорема 4.** (О правой части вида  $P_s(n)$ ) Если правая часть неоднородного рекуррентного уравнения имеет вид  $\varphi(n) = P_s(n)$ , то его частное решение может быть найдено в виде

$$a_n^{\text{част. неодн.}} = n^k Q_s(n),$$

где  $k$  — кратность, с которой константа 1 входит в число корней характеристического уравнения, а  $Q_s(n)$  — некоторый многочлен степени  $s$  (той же степени, что и многочлен  $P_s(n)$ ).

При практическом применении этой теоремы многочлен  $Q_s(n)$  записывается с неопределенными коэффициентами, которые находятся подстановкой частного решения  $\{a_n^{\text{част. неодн.}}\}_{n=0,1,\dots}$  в неоднородное рекуррентное уравнение. Аналогичным образом определяется константа  $D$  в частном решении, найденном по теореме 3.

Пример 3. Решим рекуррентное уравнение  $a_{n+2} - 4a_{n+1} + 4a_n = 3 \cdot 2^n$  при  $a_0 = 1$ ,  $a_1 = 4$ .

Рассмотрим характеристическое уравнение

$$x^2 - 4x + 4 = 0.$$

Имеем  $(x - 2)^2 = 0$ ,  $\alpha_1 = \alpha_2 = 2$ .

Правая часть уравнения имеет вид, рассматриваемый в теореме 3

$$\varphi(n) = A \cdot b^n, \quad A = 3, \quad b = 2.$$

Константа  $b$  входит в число корней характеристического уравнения с кратностью  $k = 2$ . Частное решение неоднородного уравнения ищем в виде

$$a_n^{\text{част. неодн.}} = D \cdot n^2 \cdot 2^n.$$

Подставляем его в левую часть неоднородного уравнения

$$\begin{aligned} D(n+2)^2 \cdot 2^{n+2} - 4D(n+1)^2 \cdot 2^{n+1} + 4Dn^2 \cdot 2^n &= \\ = D \cdot 2^n \cdot [(4n^2 + 16n + 16) - (8n^2 + 16n + 8) + 4n^2] &= D \cdot 2^n \cdot 8. \end{aligned}$$

Приравниваем результат к правой части  $8 \cdot D \cdot 2^n = 3 \cdot 2^n$ , откуда  $D = \frac{3}{8}$ .

Тогда  $a_n^{\text{част. неодн.}} = \frac{3n^2 \cdot 2^n}{8}$ .

Общее решение однородного уравнения имеет вид

$$a_n^{\text{общ. одн.}} = C_1 2^n + C_2 n 2^n.$$

Общее решение неоднородного уравнения имеет вид

$$a_n = a_n^{\text{общ. одн.}} + a_n^{\text{част. неодн.}} = C_1 2^n + C_2 n 2^n + \frac{3n^2}{8} \cdot 2^n = \left(\frac{3}{8}n^2 + C_2 n + C_1\right) \cdot 2^n.$$

Найдем константы  $C_1$  и  $C_2$  из начальных условий

$$\begin{cases} a_0 = 1 \\ a_1 = 4 \end{cases}, \quad \begin{cases} C_1 = 1 \\ (\frac{3}{8} + C_2 + C_1) \cdot 2 = 4 \end{cases}, \quad \begin{cases} C_1 = 1 \\ C_2 = \frac{5}{8} \end{cases}.$$

Следовательно,  $a_n = (3n^2 + 5n + 8) \cdot 2^{n-3}$ .

Пример 4. Решим рекуррентное уравнение  $a_{n+2} - 3a_{n+1} + 2a_n = 6n^2 - 4n - 13$  при  $a_0 = 5$ ,  $a_1 = 6$ .

Рассмотрим характеристическое уравнение

$$x^2 - 3x + 2 = 0, \quad \alpha_1 = 1, \quad \alpha_2 = 2.$$

Правая часть уравнения имеет вид, рассматриваемый в теореме 4

$$\varphi(n) = P_s(n), \quad P_s(n) = 6n^2 - 4n - 13, \quad s = 2.$$

Константа 1 входит в число корней характеристического уравнения с кратностью  $k = 1$ . Частное решение неоднородного уравнения ищем в виде

$$a_n^{\text{част. неодн.}} = n^k \cdot Q_s(n) = n \cdot (b_2 n^2 + b_1 n + b_0) = b_2 n^3 + b_1 n^2 + b_0 n.$$

Подставляем его в левую часть неоднородного уравнения

$$[b_2(n+2)^3 + b_1(n+2) + b_0(n+2)] + [-3b_2(n+1)^3 - 3b_1(n+1)^2 - 3b_0(n+1)] + \\ + [2b_2 n^3 + 2b_1 n^2 + 2b_0 n] = -3b_2 n^2 + (3b_2 - 2b_1)n + (5b_2 + b_1 - b_0).$$

Приравниваем результат к правой части

$$-3b_2 n^2 + (3b_2 - 2b_1)n + (5b_2 + b_1 - b_0) = 6n^2 - 4n - 13.$$

Если равны два многочлена, то равны все их коэффициенты

$$\begin{cases} -3b_2 & = 6, \\ 3b_2 - 2b_1 & = -4, \\ 5b_2 + b_1 - b_0 & = -13. \end{cases}$$

Решаем систему

$$\begin{cases} b_2 = \frac{6}{-3} = -2, \\ b_1 = -\frac{1}{2}(-4 - 3b_2) = -1, \\ b_0 = -(-13 - 5b_2 - b_1) = 2. \end{cases}$$

Тогда  $a_n^{\text{част. неодн.}} = -2n^3 - n^2 + 2n$ .

Общее решение однородного уравнения имеет вид

$$a_n^{\text{общ. одн.}} = C_1 \cdot 1^n + C_2 \cdot 2^n = C_1 + C_2 \cdot 2^n.$$

Общее решение неоднородного уравнения имеет вид

$$a_n = a_n^{\text{общ. одн.}} + a_n^{\text{част. неодн.}} = C_1 + C_2 \cdot 2^n - 2n^3 - n^2 + 2n.$$

Находим константы  $C_1$  и  $C_2$  из начальных условий

$$\begin{cases} a_0 = 5, \\ a_1 = 6, \end{cases} \quad \begin{cases} C_1 + C_2 & = 5, \\ C_1 + 2C_2 - 2 - 1 + 2 & = 6. \end{cases}$$

Решая систему, получаем  $C_1 = 3$ ,  $C_2 = 2$ .

Следовательно, искомым частным решением неоднородного рекуррентного уравнения будет последовательность

$$a_n = 3 + 2 \cdot 2^n - 2n^3 - n^2 + 2n = 2^{n+1} - 2n^3 - n^2 + 2n + 3.$$

### 6.3. Применение линейных рекуррентных последовательностей в радиолокации и криптографии

Пусть  $GF(q)$  — конечное поле из  $q$  элементов.

*Линейной рекуррентной последовательностью*  $\{a_n\}_{n=0,1,\dots}$ , где все  $a_n \in GF(q)$ , будем называть последовательность, определяемую линейным однородным рекуррентным уравнением степени  $k$  с заданными начальными условиями. *Периодичность* последовательности  $\{a_n\}_{n=0,1,\dots}$  означает, что существует такое натуральное число  $T$ , что  $a_n = a_{n+T}$  для всех  $n = 0, 1, \dots$ . Наименьшее такое  $T$  называется *периодом* последовательности  $\{a_n\}_{n=0,1,\dots}$ .

Пример 5. Как мы уже знаем, рекуррентное уравнение

$$a_{n+2} - a_{n+1} - a_n = 0$$

над  $\mathbb{Z}$  с начальными значениями  $a_0 = 0$ ,  $a_1 = 1$  задает последовательность Фибоначчи

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots$$

Рассмотрим ее в  $GF(11)$ :

$$0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, 2, 3, 5, 8, \dots$$

Эта последовательность периодична с периодом  $T = 10$ .

Пример 6. Рассмотрим над  $GF(2)$  рекуррентное уравнение  $a_{n+5} - a_{n+3} - a_n = 0$  с начальными значениями  $a_0 = 1$ ,  $a_1 = 0$ ,  $a_2 = 0$ ,  $a_3 = 0$ ,  $a_4 = 0$ .

Тогда получаем периодическую последовательность

$$1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, \dots$$

с периодом  $T = 31$ .

Линейные рекуррентные последовательности, причем, как правило, большого периода, нашли применение в радиолокации и криптографии.

Для определения положения движущегося объекта в атмосфере и пространстве используется радиолокатор. Антенна радиолокатора излучает электромагнитную энергию узким пучком. Направление этого пучка меняется при перемещении антенны. Частота  $f$  излучения находится в пределах  $2 \cdot 10^8 - 10^{10}$  Гц, длина волны  $\lambda = c/f$  — соответственно в пределах 3 см–1,5 м (так как скорость





Схема радиолокационной системы

света около 300 000 км/с). Когда пучок облучает некоторый объект, то часть его энергии отражается назад к антенне. Сама регистрация отраженной энергии служит указанием наличия объекта в заданном направлении. Но точное положение объекта в пространстве можно узнать, только определив расстояние до него. Расстояние до объекта можно определить в результате измерения времени между моментом излучения импульса энергии и моментом прихода его отражения. Возникают трудности в связи с тем, что объект перемещается в пространстве, а также в связи с тем, что в атмосфере могут возникать разные помехи. Поэтому

ни посылка единичного импульса, ни посылка серии одинаковых импульсов не могут полностью решить эту задачу. Задача успешно решается посылкой длинной серии импульсов, закодированной таким образом, что эта серия воспроизводит периодическую последовательность с очень большим периодом. В результате, получив любой отраженный импульс, можно точно определить и момент его отправления, и момент его получения.

Приемная антенна, которая может совпадать с излучающей, также обладает резко выраженной направленностью действия, что увеличивает точность локации направления. Все это вместе позволяет установить точное местонахождение непрерывно перемещающегося объекта. Как пишут в доступных источниках, период порядка  $10^6$  достаточен для локации Луны, порядка  $10^9$  — для локации Венеры. Системы связи со спутниками используют периоды порядка  $10^{15}$ . При передаче  $10^6$  импульсов в секунду этот период будет порядка года. Заметим, что прямой анализ таких последовательностей для определения их характеристик совершенно невыносим. Ими можно пользоваться лишь благодаря хорошей теории используемых линейных рекуррентных последовательностей.

Рассмотрим теперь применение линейных рекуррентных последовательностей в криптографии.

**Пример 7.** Зашифруем сообщение на английском языке, которое может быть записано в алфавите, состоящем из 26 букв a–z, пробела и 4 знаков препинания: ",", "!", "?". Пронумеруем символы алфавита соответственно от 1 до 31.

Рассмотрим решение предыдущего примера:

1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0.



Так как

$$\sum_{n=0}^{\infty} a_{n+2}x^{n+2} = A(x) - (a_0 + a_1x),$$

$$\sum_{n=0}^{\infty} a_{n+1}x^{n+1} = A(x) - a_0,$$

то  $A(x) - (a_0 + a_1x) - p_1x(A(x) - a_0) - p_2x^2A(x) = 0$ .

Отсюда

$$A(x)(1 - p_1x - p_2x^2) = a_0 + a_1x - p_1a_0x$$

и

$$A(x) = \frac{a_0 + (a_1 - p_1a_0)x}{1 - p_1x - p_2x^2}.$$

Пример 8. Найдем производящую функцию последовательности Фибоначчи.

Так как для этой последовательности

$$a_{n+2} - a_{n+1} - a_n = 0, \quad a_0 = 0, \quad a_1 = 1,$$

то

$$A(x) = \frac{0 + (1 - 1 \cdot 0)x}{1 - x - x^2} = \frac{x}{1 - x - x^2}.$$

Разлагая эту дробь на простейшие, получаем

$$A(x) = \frac{\alpha_1}{\alpha_1 - \alpha_2} \cdot \frac{1}{1 - \alpha_1x} - \frac{\alpha_2}{\alpha_1 - \alpha_2} \cdot \frac{1}{1 - \alpha_2x},$$

где  $\alpha_1 = \frac{1 + \sqrt{5}}{2}$ ,  $\alpha_2 = \frac{1 - \sqrt{5}}{2}$ .

Разлагая в степенной ряд, получаем

$$A(x) = \sum_{n=0}^{\infty} \frac{\alpha_1^{n+1} - \alpha_2^{n+1}}{\alpha_1 - \alpha_2} x^n = \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left( \frac{1 - \sqrt{5}}{2} \right)^{n+1} \right] x^n.$$

Откуда следует уже известная нам формула для общего члена последовательности Фибоначчи.

*Другой способ нахождения производящей функции для чисел Фибоначчи использует элементарные понятия линейной алгебры. Рассмотрим пару последовательных чисел Фибоначчи  $a_n, a_{n+1}$  как координаты вектора в двумерном вещественном пространстве  $\mathbb{R}^2$ :*

$$\begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} \in \mathbb{R}^2.$$

Тогда переход от вектора  $\begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}$  к вектору  $\begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix}$  осуществляется по правилу:

$$\Phi : \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} \mapsto \begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ a_n + a_{n+1} \end{pmatrix}.$$

Последнее преобразование линейно, и его можно записать в матричном виде:

$$\Phi: \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} = \Phi \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}.$$

Переход от вектора  $\begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix}$  к вектору  $\begin{pmatrix} a_{n+2} \\ a_{n+3} \end{pmatrix}$  осуществляется путем повторного применения преобразования  $\Phi$ , и т.д. Таким образом, производящая функция для векторной последовательности Фибоначчи принимает вид:

$$\begin{aligned} A(x) &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} x + \begin{pmatrix} 2 \\ 3 \end{pmatrix} x^2 + \dots = \\ &= \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} + \Phi \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \cdot x + \Phi^2 \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \cdot x^2 + \dots = \\ &= (I + \Phi x + \Phi^2 x^2 + \dots) \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = (I - x\Phi)^{-1} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}. \end{aligned}$$

Здесь через  $I$  обозначена единичная матрица,  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , и выражение  $(I - x\Phi)^{-1}$  понимается как обратная матрица к матрице  $I - x\Phi$ .

Явное выражение для чисел Фибоначчи можно получить, вычислив явно матрицу  $\Phi^n$  для произвольного  $n$ . Для этого матрицу  $\Phi$  нужно диагонализировать, представив ее в виде

$$\Phi = T^{-1} \tilde{\Phi} T,$$

где  $\tilde{\Phi}$  — диагональная матрица, а матрица  $T$  невырождена. Имеем,

$$\Phi = \frac{1}{\alpha_2^{-1} - \alpha_1^{-1}} \begin{pmatrix} 1 & 1 \\ \alpha_1^{-1} & \alpha_2^{-1} \end{pmatrix} \begin{pmatrix} \alpha_1^{-1} & 0 \\ 0 & \alpha_2^{-1} \end{pmatrix} \begin{pmatrix} \alpha_2^{-1} & -1 \\ -\alpha_1^{-1} & 1 \end{pmatrix}.$$

Отсюда, воспользовавшись уравнением

$$\Phi^n = T^{-1} \tilde{\Phi}^n T,$$

и выражениями для чисел  $\alpha_1, \alpha_2$ , получаем формулу для общего члена последовательности Фибоначчи.

Заметим, что производящая функция для последовательности Фибоначчи оказалась рациональной — отношением двух многочленов. На самом деле в нашем выводе мы нигде не использовали специальный вид этого рекуррентного уравнения. Действуя точно таким же образом, мы можем доказать аналогичную теорему о производящей функции для произвольной последовательности, задаваемой линейным рекуррентным уравнением.

**Теорема 5.** Пусть последовательность  $a_n$  задается линейным однородным рекуррентным уравнением (5) порядка  $k$  с постоянными коэффициентами и начальными значениями  $a_0, \dots, a_{k-1}$ . Тогда производящая функция  $A(x) = a_0 + a_1 x + a_2 x^2 + \dots$  рациональна,  $A(x) = \frac{P(x)}{Q(x)}$ , причем степень многочлена  $Q(x)$  равна  $k$ , а степень многочлена  $P(x)$  не превосходит  $k - 1$ .

*Доказательство.* Умножим производящую функцию  $A(x)$  на  $p_1x + p_2x^2 + \dots + p_kx^k$ :

$$\begin{aligned}(p_1x + p_2x^2 + \dots + p_kx^k)A(x) &= \\ &= p_1a_0x + p_1a_1x^2 + p_1a_2x^3 + \dots + p_1a_{k-1}x^k + \dots + \\ &\quad + p_2a_0x^2 + p_2a_1x^3 + \dots + p_2a_{k-2}x^k + \dots + \\ &\quad + p_3a_0x^3 + \dots + p_3a_{k-3}x^k + \dots + \\ &\quad \dots + p_k a_0 x^k + \dots = \\ &= P(x) + A(x),\end{aligned}$$

где степень многочлена  $P(x)$  не превосходит  $k - 1$ . Действительно, коэффициент при  $x^{n+k}$  в правой части первого равенства совпадает с правой частью уравнения (5). Отсюда получаем утверждение теоремы.  $\square$

**Замечание.** Доказательство этой теоремы дало нам более сильное утверждение: мы доказали, что многочлен  $Q(x)$  имеет вид

$$Q(x) = 1 - p_1x - p_2x^2 - \dots - p_kx^k.$$

Оказывается, что рациональные производящие функции в точности совпадают с производящими функциями для последовательностей, задаваемых линейными рекуррентными уравнениями. Точнее, справедлива следующая обратная теорема.

**Теорема 6.** Если производящая функция  $A(x) = \sum_{n=0}^{\infty} a_n x^n$  рациональна, т.е.

$A(x) = \frac{P(x)}{Q(x)}$ , где многочлены  $P(x)$  и  $Q(x)$  взаимно просты, то начиная с некоторого номера  $n$  последовательность  $a_0, a_1, a_2, \dots$  задается линейным однородным рекуррентным уравнением степени  $k$  с постоянными коэффициентами, где  $k$  — степень многочлена  $Q(x)$ .

## 6.5. Асимптотика

Производящие функции могут быть полезны для исследования асимптотического поведения  $a_n$  при  $n \rightarrow \infty$ .

Напомним, что функции  $\varphi(n)$  и  $\psi(n)$  асимптотически равны (пишем  $\varphi(n) \sim \psi(n)$ ) при  $n \rightarrow \infty$ , если  $\lim_{n \rightarrow \infty} \frac{\varphi(n)}{\psi(n)} = 1$ .

**Теорема 7.** Пусть производящая функция  $A(x)$  последовательности  $\{a_n\}_{n=0,1,\dots}$  имеет вид  $A(x) = \frac{Q(x)}{P(x)}$ , где  $Q(x)$  и  $P(x)$  — многочлены с действительными коэффициентами. Пусть  $\alpha_1$  — наименьший по абсолютной величине корень многочлена  $P(x)$ . Тогда

- 1) если  $\alpha_1$  — простой (не являющийся кратным) действительный корень, то при  $n \rightarrow \infty$

$$a_n \sim -\frac{Q(\alpha_1)}{P'(\alpha_1)}\alpha_1^{-n-1}, \text{ где } P'(\alpha_1) = \left. \frac{d}{dx}P(x) \right|_{x=\alpha_1};$$

- 2) если  $\alpha_1$  — действительный корень кратности  $k$ , то при  $n \rightarrow \infty$

$$a_n \sim \frac{(-1)^k k! Q(\alpha_1)}{P^{(k)}(\alpha_1)} C(n+k-1, k-1) \left( \frac{1}{\alpha_1} \right)^{n+k},$$

где  $P^{(k)}(\alpha_1)$  есть производная порядка  $k$  от  $P(t)$  в точке  $x = \alpha_1$ .

*Доказательство.* 1) Разложим  $A(x)$  на простые дроби:

$$A(x) = \frac{C_1}{\alpha_1 - x} + \frac{C_2}{\alpha_2 - x} + \dots + \frac{C_s}{\alpha_s - x} + B(x),$$

где  $B(x)$  — многочлен. Для нахождения коэффициента  $C_1$  умножим  $A(x)$  на  $\alpha_1 - x$ . Тогда

$$(\alpha_1 - x)A(x) = \frac{-Q(x)}{(x - \alpha_2) \dots (x - \alpha_s)}.$$

При  $x = \alpha_1$  левая часть равна  $C_1$ , а правая —  $\frac{-Q(\alpha_1)}{P'(\alpha_1)}$ . Таким образом,  $C_1 = \frac{-Q(\alpha_1)}{P'(\alpha_1)}$ . Аналогично можно вычислить и коэффициенты  $C_i$  ( $i = 2, \dots, s$ ).

Дробь  $\frac{1}{1 - t/\alpha_j}$  можно разложить в геометрическую прогрессию

$$\left( 1 - \frac{x}{\alpha_j} \right)^{-1} = \sum_{n=0}^{\infty} \left( \frac{x}{\alpha_j} \right)^n.$$

Получаем

$$A(x) = \sum_{j=1}^s \frac{C_j}{\alpha_j} \sum_{n=0}^{\infty} \left( \frac{x}{\alpha_j} \right)^n + B(x).$$

Отсюда для больших  $n$

$$a_n \sim \frac{C_1}{\alpha_1^{n+1}} + \frac{C_2}{\alpha_2^{n+1}} + \dots + \frac{C_s}{\alpha_s^{n+1}} \sim C_1 \alpha_1^{-n-1}.$$

2) Доказательство этого утверждения теоремы может быть проведено похожим образом.  $\square$

**Пример 9.** Найдём асимптотическое поведение  $a_n$  при  $n \rightarrow \infty$  для последовательности Фибоначчи.



В этом случае

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

$\alpha_1 = \frac{1 - \sqrt{5}}{2}$  — наименьший по абсолютной величине корень многочлена  $P(x) = 1 - x - x^2$ . Тогда по первой части теоремы 7

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

## §7. Разбиения. Числа Стирлинга и их свойства

**Определение 1.** *Разбиением  $n$ -элементного множества  $X$  на  $k$  подмножеств называется произвольное семейство его подмножеств  $\pi = \{B_1, \dots, B_k\}$ , такое что  $B_1 \cup B_2 \cup \dots \cup B_k = X$ ,  $B_i \cap B_j = \emptyset$  для  $1 \leq i < j \leq k$  и  $B_i \neq \emptyset$  для  $1 \leq i \leq k$ .*

Подмножества  $B_i$ ,  $i = 1, \dots, k$ , называются **блоками** разбиения.

Множество всех разбиений множества  $X$  на  $k$  блоков будем обозначать  $\Pi_k(X)$ , а множество всех разбиений множества  $X$  через  $\Pi(X)$ . Очевидно, что  $\Pi(X) = \Pi_1(X) \cup \dots \cup \Pi_n(X)$  (более того, множество  $\{\Pi_1(X), \dots, \Pi_n(X)\}$  является разбиением множества  $\Pi(X)$ ).

С разбиением тесно связано понятие отношения эквивалентности. Каждому разбиению  $\pi$  можно сопоставить отношение эквивалентности

$$E(\pi) = \bigcup_{B \in \pi} (B \times B) \quad (1)$$

(элементы  $x, y \in X$  находятся в отношении  $E(\pi)$  тогда и только тогда, когда они принадлежат одному блоку разбиения  $\pi$ ). И наоборот, каждому отношению эквивалентности  $E$  на множестве  $X$  можно сопоставить разбиение

$$X/E = \{[x]_E \mid x \in X\}, \quad (2)$$

где  $[x]_E$  обозначает класс эквивалентности элемента  $x$ , т.е. множество всех элементов, находящихся в отношении  $E$  к элементу  $x$ :

$$[x]_E = \{y \in X \mid xEy\}.$$

Нетрудно заметить, что формулы (1) и (2) определяют взаимно однозначное соответствие между разбиениями и отношениями эквивалентности на множестве  $X$ .

Если  $\pi, \sigma \in \Pi(X)$  и каждый блок разбиения  $\sigma$  есть объединение блоков разбиения  $\pi$ , то  $\pi$  называется **измельчением** разбиения  $\sigma$ , пишут  $\pi \leq \sigma$ .

Пример 1.

$$\{\{1\}, \{2, 5\}, \{4, 6\}, \{3\}\} \leq \{\{1, 2, 3, 5\}, \{4, 6\}\}.$$

Можно доказать, что  $\pi \leq \sigma$  тогда и только тогда, когда для отношений эквивалентности, соответствующих данным разбиениям, выполняется соотношение  $E(\pi) \subseteq E(\sigma)$ . Определенное таким образом отношение  $\leq$  является частичным упорядочением на множестве  $\Pi(X)$ . Некоторые свойства множества  $\Pi(X)$ , упорядоченного с помощью отношения измельчения, напоминают аналогичные свойства множества  $\Pi(X)$ , упорядоченного на основе включения.

**Определение 2.** Числом Стирлинга второго рода  $S(n, k)$  называется число разбиений  $n$ -элементного множества на  $k$  блоков:

$$S(n, k) = |\Pi_k(X)|, \text{ где } |X| = n. \quad (3)$$

Пример 2.  $S(4, 2) = 7$ , так как существуют в точности 7 разбиений множества  $\{1, \dots, 4\}$  на два блока:

$$\begin{aligned} &\{\{1, 2, 3\}, \{4\}\}, \{\{1, 2, 4\}, \{3\}\}, \{\{1, 3, 4\}, \{2\}\}, \{\{1, 2\}, \{3, 4\}\}, \\ &\{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}, \{\{1\}, \{2, 3, 4\}\}. \end{aligned}$$

По определению положим  $S(n, k) = 0$  при  $k > n$ ,  $S(0, 0) = 1$ .

С числами Стирлинга второго рода связано, как и с биномиальными коэффициентами, много любопытных тождеств. Докажем одно из таких тождеств, напоминающее тождество, связанное с треугольником Паскаля.

**Теорема 1.**

$$\begin{aligned} S(n, k) &= S(n-1, k-1) + kS(n-1, k) && \text{для } 0 < k < n, \\ S(n, n) &= 1 && \text{для } n \geq 0, \\ S(n, 0) &= 0 && \text{для } n > 0. \end{aligned}$$

*Доказательство.* Последние две формулы теоремы очевидны. Докажем первую. Рассмотрим множество всех разбиений множества  $\{1, \dots, n\}$  на  $k$  блоков. Это множество распадается на два различных класса: тех разбиений, которые содержат одноэлементный блок  $\{n\}$ , и тех разбиений, для которых  $n$  является элементом большего (по крайней мере двухэлементного) блока. Мощность первого класса равна  $S(n-1, k-1)$ , т.е. такова, каково число разбиений множества  $\{1, \dots, n-1\}$  на  $k-1$  блоков. Мощность другого класса составляет  $kS(n-1, k)$ , так как каждому разбиению множества  $\{1, \dots, n-1\}$  на  $k$  блоков соответствует в этом классе в точности  $k$  разбиений, образованных добавлением элемента  $n$  поочередно к каждому блоку.  $\square$

Формулы теоремы позволяют легко вычислять значения  $S(n, k)$  даже для больших значений  $n$  и  $k$ . В следующей таблице представлены числа  $S(n, k)$  для  $0 \leq n, k \leq 10$ .

$n \backslash k$	0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0	0
3	0	1	3	1	0	0	0	0	0	0	0
4	0	1	7	6	1	0	0	0	0	0	0
5	0	1	15	25	10	1	0	0	0	0	0
6	0	1	31	90	65	15	1	0	0	0	0
7	0	1	63	301	350	140	21	1	0	0	0
8	0	1	127	966	1701	1050	266	28	1	0	0
9	0	1	255	3025	7770	6951	2646	462	36	1	0
10	0	1	511	9330	34105	42525	22827	5880	750	45	1

Эту таблицу можно трактовать как “треугольник Стирлинга,” в котором каждое значение, кроме крайних, равных единице, можно получить как сумму чисел, находящихся над ним, а именно числа, расположенного в точности над ним и умноженного на  $k$ , и числа под ним с левой стороны.

Теорема 2.

$$S(n, k) = \sum_{i=k-1}^{n-1} C(n-1, i) S(i, k-1) \text{ для } k \geq 2.$$

*Доказательство.* Рассмотрим множество всех разбиений  $S(n, k)$  множества  $X = \{1, \dots, n\}$ . Это множество распадается на различные классы, соответствующие разным подмножествам множества  $X$ , которые являются блоками, содержащими элемент  $n$ . Отметим, что для каждого  $b$ -элементного подмножества  $B \subseteq X$ , содержащего элемент  $n$ , существует в точности  $S(n-b, k-1)$  разбиений множества  $X$  на  $k$  блоков, содержащих  $B$  в качестве блока. Действительно, каждое такое разбиение однозначно соответствует разбиению множества  $X \setminus B$  на  $k-1$  блоков. Далее,  $b$ -элементное множество  $B \subseteq X$ , содержащее элемент  $n$ , можно выбрать  $C(n-1, b-1)$  способами. Таким образом,

$$\begin{aligned} S(n, k) &= \sum_{b=1}^{n-(k-1)} C(n-1, b-1) S(n-b, k-1) = \\ &= \sum_{b=1}^{n-(k-1)} C(n-1, n-b) S(n-b, k-1) = \sum_{i=k-1}^{n-1} C(n-1, i) S(i, k-1). \end{aligned}$$

□

Число всех разбиений  $n$ -элементного множества называется *числом Белла* и обозначается  $B_n$ , т.е.

$$B_n = |\Pi(X)|, \text{ где } |X| = n.$$

Другими словами,

$$B_n = \sum_{k=0}^n S(n, k), \quad B_0 = 1.$$

**Теорема 3.**

$$B_{n+1} = \sum_{i=0}^n C(n, i) B_i.$$

*Доказательство.* Доказательство этой теоремы проводится аналогично доказательству предыдущей теоремы. Множество всех разбиений множества  $X = \{1, \dots, n+1\}$  можно разбить на различные классы в зависимости от блока  $B$ , содержащего элемент  $n+1$ , или — что равнозначно — в зависимости от множества  $X \setminus B$ . Для каждого множества  $X \setminus B \subseteq \{1, \dots, n\}$  существует в точности  $|\Pi(X \setminus B)| = B_{|X \setminus B|}$  разбиений множества  $X$ , содержащих  $B$  в качестве блока. Группируя классы в зависимости от мощности множества  $X \setminus B$ , получаем искомую формулу.  $\square$

$n$	$B_n$
0	1
1	1
2	2
3	5
4	15
5	52
6	203
7	877
8	4 140
9	21 147
10	115 975
11	678 570
12	4 213 597
13	27 644 437
14	190 899 322
15	1 382 958 545
16	10 480 142 147
17	82 864 869 804
18	682 076 806 159
19	5 832 742 205 057
20	51 724 158 235 372

Таблица чисел  $B_n$   
для  $0 \leq n \leq 20$ .

Существует зависимость между числами  $S(n, k)$  и числом всех функций из  $n$ -элементного множества на  $k$ -элементное множество, т.е. функций  $f : X \rightarrow Y$ ,  $f(X) = Y$  для  $|X| = n$ ,  $|Y| = k$ . Каждой такой функции  $f$  можно поставить в соответствие следующее разбиение множества  $X$  на  $k$  блоков:

$$N(f) = \{f^{-1}(y) : y \in Y\},$$

называемое *ядром* функции  $f$  (условие  $f(X) = Y$  дает гарантию того, что подмножества  $f^{-1}(y)$  непустые). С другой стороны, каждому разбиению  $\pi \in \Pi_k(X)$  соответствует в точности  $k!$  функций из  $X$  на  $Y$  таких, что  $N(f) = \pi$ . Каждая такая функция взаимно однозначно соответствует соотнесению блоков разбиения  $\pi$  элементам множества  $Y$ . Обозначая через  $s_{n,k}$  число функций из  $X$  на  $Y$ , получаем

$$s_{n,k} = k! S(n, k). \quad (4)$$

Пользуясь этой формулой, можно доказать еще одно свойство чисел Стирлинга второго

рода, которое касается связи между многочленами  $x^k$  и многочленами

$$[x]_k = x(x-1)\dots(x-k+1). \quad (5)$$

Произвольный многочлен  $P(x)$  от неизвестного  $x$  степени  $n$  мы можем однозначно представить как  $P(x) = \sum_{k=0}^n a_k [x]_k$ . Это частный случай того очевидного

факта, что существует однозначное разложение  $P(x) = \sum_{k=0}^n a_k p_k(x)$  для произвольной последовательности многочленов  $p_0(x), p_1(x), \dots$  такой, что  $p_k(x)$  есть многочлен степени  $k$  для каждого  $k \geq 0$ . Другими словами, каждая такая последовательность образует базис в линейном пространстве многочленов. Оказывается, что числа Стирлинга второго рода в точности равны коэффициентам перехода от базиса  $1, x, x^2, \dots$  к базису  $1, [x]_1, [x]_2, \dots$ .

**Теорема 4.** Для каждого  $n \geq 0$

$$x^n = \sum_{k=0}^n S(n, k) [x]_k. \quad (6)$$

*Доказательство.* Предположим сначала, что  $x$  — неотрицательное целое число. Подсчитаем двумя способами число всех функций  $f: A \rightarrow B$ , где  $|A| = n$ ,  $|B| = x$ . С одной стороны, оно равно  $x^n$ . С другой стороны, множество таких функций  $f$  мы можем классифицировать относительно множества  $f(A)$ . Очевидно, что каждая функция  $f$  является отображением множества  $A$  на множество  $f(A)$ , таким образом, для произвольного подмножества  $Y \subseteq B$ , где  $|Y| = k$ , число всех функций  $f: A \rightarrow B$  таких, что  $f(A) = Y$ , равно  $s_{n,k}$ , т.е. в соответствии с формулой (4)  $k!S(n, k)$ . Учитывая тот факт, что подмножество  $Y$  мощности  $k$  можно выбрать  $C(n, k)$  способами, получаем

$$x^n = \sum_{k=0}^x C(x, k) k! S(n, k) = \sum_{k=0}^n [x]_k S(n, k) \quad (7)$$

(верхний индекс суммирования можно заменить с  $x$  на  $n$ , так как  $S(n, k) = 0$  для  $k > n$  и  $[x]_k = 0$  для  $k < x$ ). Поскольку равенство многочленов выполняется для произвольного целого числа  $x \geq 0$ , эти многочлены тождественно равны (так как их разность либо является тождественно равной нулю, либо имеет бесконечное число нулей).  $\square$

**Определение 3.** Числа Стирлинга первого рода  $s(n, k)$  суть коэффициенты при последовательных степенях переменной  $x$  в многочлене  $[x]_k$ :

$$[x]_n = \sum_{k=0}^n s(n, k) x^k. \quad (8)$$



Другими словами, числа  $s(n, k)$  играют обратную роль в отношении к числам  $S(n, k)$  — позволяют перейти от базиса  $1, [x]_1, [x]_2, \dots$  к базису  $1, x, x^2, \dots$ . Очевидно, что  $s(n, k) = 0$  для  $k > n$ . Числа  $s(n, k)$  удобно вычислять, пользуясь следующей

**Теорема 5.**  $s(n, k) = s(n-1, k-1) - (n-1)s(n-1, k)$  для  $0 < k < n$ ,  
 $s(n, n) = 1$  для  $n \geq 0$ ,  
 $s(n, n) = 0$  для  $n > 0$ .

*Доказательство.* Последние две формулы очевидны. Первую формулу теоремы получаем, сравнивая коэффициенты при  $x^k$  с обеих частей равенства  $[x]_n = [x]_{n-1}(x - n + 1)$ .

$$\begin{aligned} \text{То есть имеем } \sum_{k=0}^n s(n, k)x^k &= \\ &= (x - n + 1) \sum_{k=0}^{n-1} s(n-1, k)x^k = \\ &= \sum_{k=0}^{n-1} s(n-1, k)x^{k+1} - \\ &\quad - (n-1) \sum_{k=0}^{n-1} s(n-1, k)x^k = \\ &= \sum_{k=1}^n \left( s(n-1, k-1) - \right. \\ &\quad \left. - (n-1)s(n-1, k) \right) x^k + \\ &\quad + s(n-1, n-1)x^n - \\ &\quad - (n-1)s(n-1, 0). \quad \square \end{aligned}$$

$n \backslash k$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	0	1									
2	0	0	1								
3	0	0	1	0							
4	0	0	0	1	0						
5	0	0	0	0	1	0					
6	0	0	0	0	0	1	0				
7	0	0	0	0	0	0	1	0			
8	0	0	0	0	0	0	0	1	0		
9	0	0	0	0	0	0	0	0	1	0	
10	0	0	0	0	0	0	0	0	0	1	0

Таблица чисел  $s(n, k)$  для  $0 \leq n, k \leq 10$ .



## §8. Системы представителей

Рассмотрим слово  $\langle A_1, \dots, A_n \rangle$ , которое состоит из конечных (не обязательно непересекающихся и не обязательно различных) множеств  $A_i$ ,  $i = 1, \dots, n$ .

**Определение 1.** *Системой различных представителей для  $\langle A_1, \dots, A_n \rangle$  (или трансверсалью  $\langle A_1, \dots, A_n \rangle$ ) называется слово  $\langle a_1, \dots, a_n \rangle$ , где  $a_i \in A_i$ ,  $1 \leq i \leq n$ , и  $a_i \neq a_j$  для  $i \neq j$ . Говорят, что в этом случае элемент  $a_i$  представляет множество  $A_i$ .*

Рассмотрим два примера.

Пример 1. Пусть даны пять множеств:

$$\begin{aligned} A_1 &= \{1, 2, 3\}, \\ A_2 &= \{1, 2, 4\}, \\ A_3 &= \{1, 2, 5\}, \\ A_4 &= \{3, 4, 5, 6\}, \\ A_5 &= \{3, 4, 5, 6\}. \end{aligned}$$

Тогда слово  $\langle 1, 2, 5, 3, 4 \rangle$  очевидно является трансверсалью для  $\langle A_1, A_2, A_3, A_4, A_5 \rangle$ .

Пример 2. Рассмотрим другие пять множеств:

$$\begin{aligned} B_1 &= \{1, 2\}, \\ B_2 &= \{1, 2\}, \\ B_3 &= \{1, 2\}, \\ B_4 &= \{3, 4, 5, 6\}, \\ B_5 &= \{3, 4, 5, 6\}. \end{aligned}$$

Оказывается, что в данной ситуации трансверсали не существует.

Отсюда возникает вопрос:

в каком случае существует трансверсаль?

Как видно из последнего примера, очевидное необходимое условие для существования трансверсали состоит в том, чтобы в совокупности всех элементов произвольных  $n$  множеств  $A_i$  содержалось не менее  $n$  различных элементов. Примечателен тот факт (доказанный впервые Филиппом Холлом в 1935 г.), что это очевидное необходимое условие для существования трансверсали является также достаточным.

**Теорема 1. (Теорема Ф.Холла.)** Трансверсаль  $\langle a_1, \dots, a_n \rangle$  для  $\langle A_1, \dots, A_n \rangle$  существует тогда и только тогда, когда для каждого  $J \subseteq \{1, \dots, n\}$

$$\left| \bigcup_{j \in J} A_j \right| \geq |J|. \quad (1)$$

*Доказательство.* Необходимость. Если трансверсаль  $\langle a_1, \dots, a_n \rangle$  для  $\langle A_1, \dots, A_n \rangle$  существует, то для каждого  $J$  имеем

$$\left| \bigcup_{j \in J} A_j \right| \geq \left| \bigcup_{j \in J} \{a_j\} \right| = |J|.$$

Достаточность. Заметим, что если каждое  $A_i$  содержит единственный элемент  $a_i$ , то выполнение (1) означает, что  $a_1, \dots, a_n$  различны и, значит, образуют трансверсаль. Нашей основной операцией будет такое вычеркивание некоторых элементов из некоторых подмножеств  $A_i$ , что для получающихся в результате подмножеств  $\bar{A}_i \subseteq A_i$ ,  $i = 1, \dots, n$ , условие (1) все еще выполняется. Если после ряда вычеркиваний, каждое из которых сохраняет условие (1), остаются множества  $\bar{A}_i$ , содержащие каждое по единственному элементу  $a_i$ , то  $a_1, \dots, a_n$  будут образовывать трансверсаль, и теорема Холла будет доказана.

В качестве первого тривиального вычеркивания, которое не нарушает условия (1), мы можем удалить из каждого множества  $A_i$ , содержащего более  $n$  элементов, все, кроме  $n$  элементов. Назовем множество  $r$  подмножеств  $A_{i_1}, \dots, A_{i_r}$  блоком и обозначим его через  $B_{r,s}$ , где  $s$  — число различных элементов в подмножествах  $A_{i_1}, \dots, A_{i_r}$ . Тогда условие (1) эквивалентно утверждению, что  $s \geq r$  для любого блока  $B_{r,s}$ . Если  $s = r$ , то такой блок  $B_{r,r}$  назовем критическим блоком. Условимся рассматривать пустой блок как критический блок  $B_{0,0}$ . Также можно определить объединение и пересечение блоков. Предположим, что  $X_1, \dots, X_m, Y_{m+1}, \dots, Y_r$  — подмножества  $A_i$  в блоке  $B_{r,s}$  и что  $X_1, \dots, X_m, Z_{m+1}, \dots, Z_t$  — подмножества  $A_j$  в блоке  $B_{t,v}$ , где  $X_1, \dots, X_m$  — все подмножества, общие для обоих блоков (напомним, что подмножества  $A_i, A_j$  различаются своими индексами, а не элементами, которые они содержат). Тогда определим пересечение  $B_{r,s} \cap B_{t,v}$  как блок  $B_{u,w}$ , подмножествами которого являются  $X_1, \dots, X_m$ , а объединение  $B_{r,s} \cup B_{t,v}$  — как блок, подмножествами которого являются  $X_1, \dots, X_m, Y_{m+1}, \dots, Y_r, Z_{m+1}, \dots, Z_t$ ; это будет блок  $B_{y,z}$  с  $y = r + t - u$ .

**Лемма 1.** Если условие (1) выполнено, то объединение  $B_{r,r} \cup B_{t,t}$  и пересечение  $B_{r,r} \cap B_{t,t}$  критических блоков — снова критические блоки.

*Доказательство.* Пусть  $B_{r,r} \cap B_{t,t} = B_{u,v}$  и  $B_{r,r} \cup B_{t,t} = B_{y,z}$ ; число  $z$  элементов объединения равно числу  $r + t$  элементов в  $B_{r,r}$  и  $B_{t,t}$ , уменьшенному на число элементов, содержащихся в обоих блоках, которое не меньше числа  $v$  элементов пересечения. Таким образом,  $z \leq r + t - v$ . По условию (1) имеем также, что  $v \geq u$  и  $z \geq y$ . Так как  $y + u = r + t$ , то

$$r + t - v \geq z \geq y = r + t - u \geq r + t - v.$$

Следовательно, всюду имеем равенство, и  $z = y$ ,  $u = v$ . □

**Лемма 2.** Если  $B_{k,k}$  — критический блок, то вычеркивание элементов  $B_{k,k}$  из множеств, не принадлежащих  $B_{k,k}$ , не нарушает условия (1).

*Доказательство.* Пусть  $B_{r,s}$  — произвольный блок. Нужно показать, что если  $(B_{r,s})' = B_{r,s'}$  — блок, полученный после вычеркивания, то  $s' \geq r$ . Пусть  $B_{r,s} \cap B_{k,k} = B_{u,v}$ ,  $B_{r,s} \cup B_{k,k} = B_{y,z}$  и  $B_{r,s}$  состоит из множеств  $X_1, \dots, X_m, Y_{m+1}, \dots, Y_r$ , а  $B_{k,k}$  — из множеств  $X_1, \dots, X_m, Z_{m+1}, \dots, Z_k$ , где  $X_1, \dots, X_m$  — все множества, общие для обоих блоков. Тогда  $B_{u,v}$  состоит из  $X_1, \dots, X_m$ , а  $B_{y,z}$  — из

$$X_1, \dots, X_m, Y_{m+1}, \dots, Y_r, Z_{m+1}, \dots, Z_k.$$

После вычеркивания получим блок  $(B_{r,s})' = B_{r,s'}$ , состоящий из

$$X_1, \dots, X_m, Y'_{m+1}, \dots, Y'_r.$$

Но так как  $Y_{m+1}, \dots, Y_r$  входят в  $B_{y,z}$ , то они в совокупности содержат  $z - k$  элементов, не содержащихся в  $B_{k,k}$ . Таким образом,  $s' = v + z - k$ , так как в  $B'_{r,s'}$  входят элементы пересечения  $B_{u,v}$  вместе с  $z - k$  элементами из  $Y'_{m+1}, \dots, Y'_r$ . Поскольку  $y = r + k - u$  и  $z \geq y$ ,  $v \geq u$ , то

$$s' = v + z - k \geq u + y - k = r.$$

Таким образом,  $s' \geq r$ , то есть и после вычеркивания условие (1) все еще выполняется.  $\square$

Докажем теперь теорему Ф.Холла, используя индукцию по числу  $n$  множеств, поскольку теорема тривиальна при  $n = 1$ . Предположим, что в системе подмножеств  $A$  множеств  $A_1, \dots, A_n$ , имеется критический блок  $B_{k,k}$ , не совпадающий со всей системой, то есть  $1 \leq k < n$ . Вычеркнув, если необходимо, элементы  $B_{k,k}$  из остальных множеств, можем считать, что  $A$  состоит из  $B_{k,k}$  и блока  $B_{n-k,v}$ , которые не имеют общих элементов. По лемме 2 условие (1) не нарушается и по индукции  $B_{k,k}$  и  $B'_{n-k,v}$  оба имеют трансверсали, а так как они не пересекаются, то в совокупности дают трансверсаль для  $A$ . Предположим далее, что в системе  $A$  множеств  $A_1, \dots, A_n$  нет критического блока, кроме, быть может, всей системы. Выберем тогда произвольный элемент какого-нибудь множества в качестве его представителя и вычеркнем этот элемент из всех остальных множеств. При этом блок  $B_{r,s}$  с  $r < n$  становится блоком  $B'_{r,s'}$ , где  $s' = s$  или  $s - 1$ . Но по предположению блок  $B_{r,s}$  не был критическим и, значит,  $s \geq r + 1$ , следовательно,  $s' \geq r$ , и условие (1) выполняется для системы из  $n - 1$  остальных множеств. По предположению индукции они имеют трансверсаль, которая вместе с выбранным выше представителем одного множества образует трансверсаль для всей системы.  $\square$

**Следствие.** Если  $n$  множеств  $A_1, \dots, A_n$  имеют трансверсаль и если наименьшее из этих множеств содержит  $t$  элементов, то при  $t \geq n$  существует не меньше, чем  $t(t-1) \dots (t-n+1)$  различных трансверсалей, а при  $t < n$  существует не меньше, чем  $t!$  различных трансверсалей.

*Доказательство.* Это следствие получается при более тщательном рассмотрении доказательства теоремы. Должно существовать хотя бы одно множество, в



котором в качестве представителя можно выбрать любой элемент, так как если нет критических блоков, это справедливо для любого множества, но если критические блоки имеются, то это верно для некоторого множества в минимальном критическом блоке. Множество, которое может иметь в качестве представителя любой свой элемент, обозначим через  $A_1$ . Выбор представителя в  $A_1$  можно осуществить не менее чем  $t$  способами. Вычеркнем теперь элемент, выбранный в качестве представителя для  $A_1$ , из  $A_2, \dots, A_n$  и получим множества  $A'_2, \dots, A'_n$ , которые обладают трансверсалью и в которых наименьшее множество содержит не меньше, чем  $t - 1$  элементов. Продолжая дальше таким же образом, мы можем получить не менее, чем  $t(t - 1) \dots (t - n + 1)$  трансверсаль, если  $t \geq n$ , и не менее чем  $t!$  трансверсаль, если  $t < n$ .  $\square$

Рассмотренное доказательство не является первоначальным доказательством Ф.Холла, а принадлежит М.Холлу (Marshall Hall). Его можно использовать, чтобы распространить теорему на случай системы  $A$ , состоящей из бесконечного числа конечных множеств. Например, если мы имеем систему из множеств  $A_0 = \{1, 2, 3, \dots\}$  и  $A_i = \{i\}$ ,  $i = 1, 2, \dots$ , то эта система не имеет трансверсали, так как представители для  $A_i$ ,  $i = 1, 2, \dots$ , выбираются однозначно и не остается ни одного элемента, который представлял бы только  $A_0$ . Однако для любого  $k$ , конечного или бесконечного, любые  $k$  из данных выше множеств содержат среди своих элементов не менее  $k$  различных.

Теорема Ф.Холла по существу эквивалентна следующей теореме о 0-1-матрицах. Под *линией* такой матрицы мы будем понимать ее строку или столбец.

**Теорема 2. (Теорема Кенига–Эгевари)** *Если прямоугольная матрица составлена из нулей и единиц, то минимальное число линий, которые содержат все единицы, равно максимальному числу единиц, которые могут быть выбраны так, чтобы никакие две из них не лежали на одной и той же линии.*

*Доказательство.* Пусть  $A = (a_{ij})$  есть  $(n \times t)$ -матрица из нулей и единиц. Пусть  $m$  — минимальное число линий, содержащих все единицы, а  $M$  — максимальное число единиц, из которых никакие две не лежат на одной и той же линии. Тогда, очевидно,  $m \geq M$ . Воспользуемся теоремой Ф.Холла, чтобы доказать обратное неравенство  $M \geq m$ . Предположим, что минимальное покрытие  $m$  линиями состоит из  $r$  строк и  $s$  столбцов, где  $r + s = m$ . Переставим строки и столбцы так, чтобы указанные линии были первыми  $r$  строками и первыми  $s$  столбцами соответственно. При перестановке строк и столбцов значения  $M$  и  $m$  очевидно не изменятся. Первым строкам  $R_1, \dots, R_r$  сопоставим множества  $S_1, S_2, \dots, S_r$ , где множество  $S_i$ ,  $i = 1, \dots, r$ , состоит из тех значений  $j$ , для которых  $a_{ij} = 1$ , а  $j > s$ . Другими словами,  $S_i$  есть множество индексов столбцов (исключая первые  $s$  столбцов), на пересечении которых с  $i$ -ой строкой находятся единицы.

Покажем, что множества  $S_i$  удовлетворяют условию (1), так как если какие-либо  $k$  из этих множеств содержат не более  $k - 1$  элементов, то соответствующие  $k$  строк можно заменить не более чем  $k - 1$  столбцами так, чтобы все

единицы содержались в этом новом наборе строк и столбцов. Но ввиду минимальности  $m$  это невозможно. Следовательно, множества  $S_i$  удовлетворяют условию (1), и по теореме Ф.Холла они имеют  $r$  различных представителей, то есть таких единиц в первых  $r$  строках, что никакие две из них не лежат на одной и той же линии и ни одна не лежит в первых  $s$  столбцах. Рассуждая аналогично, мы можем выбрать  $s$  единиц в первых  $s$  столбцах, из которых никакие две не лежат на одной и той же линии и ни одна не находится в первых  $r$  строках. Тем самым мы нашли  $m = r + s$  единиц с тем свойством, что никакие две из них не лежат на одной линии. Следовательно,  $M \geq m$ . Учитывая ранее полученное неравенство  $m \geq M$ , заключаем, что  $m = M$ .  $\square$

**Замечание.** Обратно, легко вывести теорему Ф.Холла из теоремы Кенига–Эгевари. Если даны множества  $A_1, \dots, A_n$  с элементами  $a_1, \dots, a_m$ , то образуем матрицу  $A = (a_{ij})$ , где  $a_{ij} = 1$ , если  $a_j$  находится в  $A_i$ , и  $a_{ij} = 0$  в противном случае. Если единицы в  $A$  содержатся в каких-либо  $r$  строках и  $s$  столбцах и  $r + s < n$ , то в  $k = n - r$  строках, не входящих в число покрывающих строк, единицы имеются только в  $s < n - r = k$  столбцах, и для этих  $k$  множеств условие (1) нарушается. Но если минимальное покрытие линиями содержит  $r + s = n$  линий, то по теореме Кенига–Эгевари имеется  $n$  единиц, из которых никакие две не лежат на одной линии, и соответствующие этим единицам элементы образуют трансверсаль для  $A_1, \dots, A_n$ .

Теорию различных представителей можно успешно применить к изучению латинских прямоугольников и латинских квадратов.

## §9. Латинские прямоугольники и квадраты

Латинские квадраты и прямоугольники стали известны благодаря одной знаменитой задаче Леонарда Эйлера. В 1782 г. Эйлер предложил следующую проблему:

*Среди 36 офицеров находится по шесть офицеров шести различных званий из шести полков. Можно ли построить этих офицеров в каре так, чтобы в каждой колонне и каждой шеренге встречались офицеры всех званий и всех полков?*

Лишь в 1901 г. удалось доказать, что это невозможно. Однако связанные с задачей Эйлера латинские квадраты и прямоугольники не перестали вызывать интерес, так как вскоре обнаружилось, что они имеют многообразные практические применения. А в конце 60-х годов прошлого века они были применены и в кодировании. Получающиеся на их основе коды хотя и далеки по своим параметрам от оптимальных, но зато допускают простые алгоритмы декодирования.

**Определение 1.** Назовем матрицу

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \quad (1)$$

элементы которой  $a_{ij} \in \{1, 2, \dots, n\}$ , латинским  $(m \times n)$ -прямоугольником, если каждая строка есть некоторая перестановка чисел  $1, 2, \dots, n$  и в каждом столбце ни одно число не повторяется.

Очевидно, что для существования таких матриц необходимо, чтобы выполнялось неравенство  $m \leq n$ .

**Определение 2.** Если  $m = n$ , то латинский прямоугольник называется латинским квадратом и каждое число  $1, 2, \dots, n$  появляется точно один раз в каждой строке и каждом столбце.

Понятие латинского квадрата было введено Леонардом Эйлером, который впервые их исследовал, беря за основу латинский алфавит. Обратим внимание на то, что для произвольного порядка  $n$  число латинских квадратов до сих пор неизвестно. Если  $l_n$  — число латинских квадратов, в которых элементы первой строки и первого столбца упорядочены по возрастанию, то число  $L_n$  латинских квадратов порядка  $n$  определяется по формуле

$$L_n = n! \cdot (n-1)! \cdot l_n.$$

Ряд известных значений  $l_n$  сведем в таблицу

$n$	2	3	4	5	6	7	8	9
$l_n$	1	1	4	56	9 408	16 942 080	535 281 401 856	377 597 570 964 258 816

Вот, например, все латинские квадраты  $4 \times 4$  (с упорядоченной по возрастанию первой строкой и первым столбцом):

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

В связи с задачей построения латинских квадратов порядка  $n$ , возникает естественный вопрос:

можно ли к  $(m \times n)$ -прямоугольнику, где  $m < n$ , добавить еще одну строку, чтобы получился латинский  $((m+1) \times n)$ -прямоугольник, и если можно, то сколькими способами?

Если имеется только одна строка, то проблема о числе способов добавления второй строки есть задача о беспорядках, и как мы знаем, это число есть целое, приближенно равное  $n!/e$ . Более того, Ямамото (Yamamoto K.) в 1951



году было показано, что если  $m$  мало в сравнении с  $n$  ( $m < \sqrt[3]{n}$ ), то число способов добавления строки приближенно равно  $n!/e^m$ . Следующая теорема дает нижнюю границу для всех значений  $m$ , которая почти наверняка занижена при  $m \leq n - 3$ .

**Теорема 1.** Число способов добавления строки к латинскому  $(m \times n)$ -прямоугольнику, дающих в результате латинский  $((m + 1) \times n)$ -прямоугольник, не меньше  $(n - k)!$ .

*Доказательство.* Пусть  $A_i$ ,  $i = 1, \dots, n$ , — множество чисел, которые не появляются в  $i$ -ом столбце данного латинского  $(m \times n)$ -прямоугольника  $A$ . Тогда трансверсаль множеств  $A_i$  можно добавить к  $A$  в качестве строки, чтобы получить латинский  $((m + 1) \times n)$ -прямоугольник, так как она будет содержать числа от 1 до  $n$  и ни одно из них не будет повторением какого-либо числа в соответствующем столбце. Обратно, строка, которая может быть добавлена к  $A$  для получения латинского  $((m + 1) \times n)$ -прямоугольника, будет трансверсалью для множеств  $A_i$ .

Задача состоит теперь в том, чтобы показать, что множества  $A_i$  имеют трансверсаль, и найти число возможных трансверсалей. Множество  $A_i$  состоит из  $n - m$  чисел, не содержащихся в  $i$ -ом столбце  $A$ . Каждое число  $1, 2, \dots, n$  появляется  $m$  раз в  $A$  и, следовательно,  $n - m$  раз в множествах  $A_1, \dots, A_n$ , взятых вместе. Набор  $k$  из этих множеств  $A_1, \dots, A_m$  будет содержать  $k(n - m)$  чисел с учетом кратностей. Но так как ни одно из этих чисел не появляется более чем  $n - m$  раз, то среди элементов этих  $k$  множеств должно быть не менее  $k$  различных чисел. Следовательно, условие (1) теоремы Ф.Холла удовлетворяется. Так как каждое из множеств  $A_i$  содержит  $n - m$  элементов, то по следствию теоремы Ф.Холла существует не менее  $(n - m)!$  трансверсалей.  $\square$

Рассмотрим теперь применение латинских квадратов в кодировании. Основной задачей кодирования является экономная, удобная и практически безошибочная передача сообщений. Напомним, что кодом называют конечное или счетное множество слов в некотором алфавите. Мы будем понимать под кодом конечное множество двоичных векторов  $x$  фиксированной длины  $l$  (рассматриваемые здесь коды называются *групповыми*), определяемое системой

$$Hx = 0, \quad (2)$$

где  $H$  — заданная двоичная  $s \times l$ -матрица, называемая *проверочной матрицей кода*. Проверочная матрица в основном используется при декодировании полученных сообщений и для исправления ошибок. Из линейной алгебры известно, что множество таким образом заданных векторов  $x$  образует линейное подпространство в пространстве  $\mathbb{Z}_2^l$ . Заметим, что у нас нет необходимости указывать полный список кодовых слов, так как код полностью определен системой линейных уравнений (2) или матрицей  $H$ .

Имеется и другой способ матричного задания группового кода. Так как множество векторов кода образует подпространство в линейном пространстве  $\mathbb{Z}_2^l$ , то

в нем можно выбрать базис. Пусть  $\mathbf{g}_1, \dots, \mathbf{g}_t$  — базисные векторы рассматриваемого кода. Тогда всевозможные кодовые векторы исчерпываются линейными комбинациями

$$\alpha_1 \mathbf{g}_1 + \dots + \alpha_t \mathbf{g}_t,$$

где  $\alpha_i \in \mathbb{Z}_2$ .

Матрица

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1t} \\ g_{21} & g_{22} & \dots & g_{2t} \\ \dots & \dots & \dots & \dots \\ g_{t1} & g_{t2} & \dots & g_{tt} \end{pmatrix},$$

составленная из векторов

$$\begin{aligned} \mathbf{g}_1 &= (g_{11}, g_{12}, \dots, g_{1t}), \\ \mathbf{g}_2 &= (g_{21}, g_{22}, \dots, g_{2t}), \\ &\dots \\ \mathbf{g}_t &= (g_{t1}, g_{t2}, \dots, g_{tt}), \end{aligned}$$

называется *порождающей матрицей кода*.

Заметим, что базис можно выбрать не единственным образом, поэтому порождающая матрица  $G$  определена неоднозначно. Последнее, впрочем, верно и в отношении проверочной матрицы  $H$ .

Пусть необходимо закодировать сообщение  $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_t)$ , где  $\alpha_i \in \mathbb{Z}_2$ ,  $i = 1, 2, \dots, t$ . Сопоставим ему кодовый вектор  $\mathbf{a}$

$$\mathbf{a} = \alpha G = (\alpha_1, \alpha_2, \dots, \alpha_t) \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1t} \\ g_{21} & g_{22} & \dots & g_{2t} \\ \dots & \dots & \dots & \dots \\ g_{t1} & g_{t2} & \dots & g_{tt} \end{pmatrix},$$

совпадающий с линейной комбинацией строк порождающей матрицы.

Выясним, как связаны порождающая и проверочная матрицы. Из (2) следует, что каждая строка порождающей матрицы, являясь кодовым вектором, удовлетворяет соотношению

$$h_{i1}g_{j1} + h_{i2}g_{j2} + \dots + h_{it}g_{jt} = 0.$$

Другими словами, любая строка порождающей и любая строка проверочной матриц ортогональны друг другу. Таким образом, в матричной записи получаем

$$GH^T = 0, \tag{3}$$

где  $H^T$  — транспонированная матрица  $H$ .

Рассмотрим теперь вопрос построения групповых кодов с помощью латинских квадратов. Существенным здесь является свойство ортогональности латинских квадратов, которое определяется следующим образом.

**Определение 3.** Два латинских квадрата порядка  $n$  называются *ортогональными*, если при наложении любого из них на другой мы получим множество всех упорядоченных пар  $(i, j)$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq n$ .

Ортогональными латинскими квадратами порядка 3 являются, например, следующие две матрицы

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}.$$

А это пример ортогональных латинских квадратов порядка  $n$

$$A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 2 & 2 & 2 & \dots & 2 \\ 3 & 3 & 3 & \dots & 3 \\ \dots & \dots & \dots & \dots & \dots \\ n & n & n & \dots & n \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 2 & 3 & \dots & n \end{pmatrix}. \quad (4)$$

Легко видеть, что матрица порядка  $n$  является латинским квадратом тогда и только тогда, когда она ортогональна обоим матрицам  $A$  и  $B$ .

Пусть  $C$  — латинский квадрат ортогональный матрицам  $A$  и  $B$ . Определим для любого его элемента  $k$  двоичную матрицу  $C_k$ , которая получается из  $C$  заменой всех элементов, равных  $k$ , единицами, а всех остальных — нулями. Таким образом, для матрицы  $C$  получаем матрицы порядка  $n$   $C_1, C_2, \dots, C_n$ . Каждой матрице  $C_k$  поставим в соответствие вектор  $v_k$ , первые  $n$  координат которого являются последовательными элементами первой строки матрицы  $C_k$ , следующие  $n$  координат — элементами второй строки и т.д. Иными словами,  $n^2$  координат вектора  $v_k$  — это все элементы матрицы  $C_k$ , “вытянутой” в одну общую строку. Образует, наконец, матрицу  $\tilde{C}$  порядка  $n \times n^2$ , строками которой являются векторы  $v_k$ :

$$\tilde{C} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Например, для матрицы

$$C = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

имеем:

$$C_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad C_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$v_1 = (100001010), \quad v_2 = (010100001), \quad v_3 = (001010100),$$

$$\tilde{C} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Пусть теперь  $D_1, D_2, \dots, D_r$  — попарно ортогональные латинские квадраты.  $A$  и  $B$  — матрицы (4). Образует из всех этих матриц указанным выше способом матрицы  $\tilde{A}, \tilde{B}, \tilde{D}_1, \tilde{D}_2, \dots, \tilde{D}_r$ , а затем построим матрицу  $H$ , которую можно условно представить в виде:

$$H = \begin{pmatrix} \tilde{A} : \\ \tilde{B} : \\ \tilde{D}_1 : & I_m \\ \tilde{D}_2 : \\ \vdots : \\ \tilde{D}_r : \end{pmatrix}$$

(матрицы  $\tilde{A}, \tilde{B}, \tilde{D}_1, \tilde{D}_2, \dots, \tilde{D}_r$  подписываются одна под другой и к получившейся матрице приписывается справа единичная матрица  $I_m$  соответствующего порядка  $m$ ).

Матрицу  $H$  будем считать проверочной матрицей кода, построенного с помощью латинских квадратов. Число строк этой матрицы, как вытекает из построения, равно  $s = (r + 2)n$ , а число столбцов составляет  $l = n^2 + (r + 2)n$ .

Напомним, что множество кодовых векторов  $x = (x_1, x_2, \dots, x_l)$  в этом случае определяется системой (2). А любое сообщение  $a = (a_1, a_2, \dots, a_s)$  может быть закодировано по правилу  $a = \alpha G$ , где  $G$  — порождающая матрица кода, найденная из (3).

Чтобы оценить способности кода исправлять и обнаруживать ошибки, введем понятие **кодového расстояния** как минимального расстояния между различными кодовыми векторами. Расстояние между двумя векторами — это число несовпадающих координат этих векторов (*расстояние Хемминга*).

Известно, что код способен исправлять любые комбинации из  $t$  (и меньшего числа) ошибок тогда и только тогда, когда его кодовое расстояние больше  $2t$ .

Для каждого  $x_i$ , используя (2), выпишем систему проверок. Очевидно, что для каждого символа  $x_i$  она будет состоять из  $r + 2$  соотношений (по числу матриц, используемых для построения), и эти соотношения будут попарно ортогональны (что объясняется свойством ортогональности исходных матриц). А значит, кодовое расстояние не может быть меньше, чем  $r + 3$ .

Пример 1. В качестве примера рассмотрим код, построенный с помощью двух ортогональных латинских квадратов порядка 3:

$$D_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}.$$

В этом случае

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

$$\tilde{A} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad \tilde{B} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

$$\tilde{D}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad \tilde{D}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Наконец, проверочная матрица искомого кода такова:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Легко видеть, что для каждого из 9 информационных символов может быть составлено четыре ортогональных проверки. Рассмотрим для примера символ  $x_1$  и решим, верно он был передан или нет (для остальных символов данный вопрос решается аналогично). Из первой, четвертой, седьмой и десятой строк матрицы  $H$  имеем следующие проверки для первого символа  $x_1$ :

$$\begin{aligned} x_1 &= x_2 + x_3 + x_{10}, \\ x_1 &= x_4 + x_7 + x_{13}, \\ x_1 &= x_6 + x_8 + x_{16}, \\ x_1 &= x_5 + x_9 + x_{19}. \end{aligned} \tag{5}$$

Если ошибки при передаче отсутствовали, то в принятом слове будет выполняться каждое из соотношений (4). Соотношения для символа  $x_1$  имеют по построению матрицы  $H$  вид, когда всякий другой символ входит в правую часть (4) ровно одной проверки. Поэтому если среди значений  $x_1, x_2 + x_3 + x_{10}, x_4 + x_7 + x_{13}, x_6 + x_8 + x_{16}, x_5 + x_9 + x_{19}$  большинство составляют нули, то полагаем, что нуль и есть верное значение для  $x_1$ , если же большинство из них единицы, то верным значением для  $x_1$  считаем единицу.



Аналогичные проверки могут быть составлены и для других символов. Очевидно, что мы получим верное значение  $x$ , если при передаче произошло не более 2 ошибок (кодовое расстояние здесь не меньше пяти).

## §10. Матрицы Адамара

Матрицы Адамара были названы в честь одного из крупнейших французских математиков конца XIX и первой половины XX века Жака Адамара. В начале второй половины прошлого века было замечено, что эти матрицы могут быть использованы для построения кодов с большим кодовым расстоянием.

**Определение 1.** Квадратная матрица  $H$  порядка  $n$  с элементами  $\pm 1$  называется **матрицей Адамара**, если выполняется условие

$$HH^T = nI_n, \quad (1)$$

где  $I_n$  — единичная матрица  $n \times n$  и  $H^T$  — транспонированная матрица  $H$ .

Из (1) следует, что если  $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n$  — строки матрицы  $H$ , то эти строки как векторы удовлетворяют условию ортогональности:

$$(\mathbf{h}_i, \mathbf{h}_j) = \begin{cases} n, & \text{если } i = j, \\ 0, & \text{если } i \neq j, \end{cases} \quad (2)$$

где  $(\mathbf{h}_i, \mathbf{h}_j) = \sum_{k=1}^n h_{ik}h_{jk}$  — евклидово скалярное произведение векторов  $\mathbf{h}_i$  и  $\mathbf{h}_j$ .

Из равенств  $HH^T = nI_n$  сразу следует, что  $\frac{1}{n}H^T = H^{-1}$ , поэтому  $\frac{1}{n}H^TH = I_n$ , значит,  $H^TH = nI_n = HH^T$ , т.е. матрица  $H$  удовлетворяет условию нормальности:

$$H^TH = HH^T.$$

**Лемма 1.** Перестановка строк или столбцов матрицы Адамара  $H_1$ , а также умножение строк или столбцов на  $-1$  переводят матрицу  $H_1$  в матрицу Адамара  $H_2$ .

*Доказательство.* Действительно, перестановка строк матрицы  $H_1$  в соответствии с формулой (2) сохраняет все скалярные произведения строк, а перестановка столбцов связана лишь с изменением порядка слагаемых в формуле скалярного произведения строк матрицы  $H_1$ . Аналогичным образом не изменяются скалярные произведения строк и при умножении строк или столбцов на  $-1$ .  $\square$

Будем считать матрицы Адамара  $H_1$  и  $H_2$  **эквивалентными**, если

$$H_2 = PH_1Q,$$

где  $P$  и  $Q$  — мономиальные матрицы перестановки с элементами  $+1$  и  $-1$ , т.е.  $P$  и  $Q$  имеют по одному ненулевому элементу в каждой строке и в каждом столбце,



и этот ненулевой элемент равен  $+1$  или  $-1$ . Матрица  $P$  осуществляет перестановку и меняет знаки у строк, а  $Q$  — у столбцов. Для любой данной матрицы Адамара мы всегда можем найти эквивалентную ей матрицу Адамара, первая строка и первый столбец которой состоят целиком из  $+1$ . Такая матрица Адамара называется **нормализованной**. Перестановка строк, кроме первой, или столбцов, кроме первого, не нарушает нормальности матрицы, но, вообще говоря, могут существовать эквивалентные нормализованные матрицы, которые не получаются одна из другой простой перестановкой строк и столбцов.

Далее под матрицей Адамара будем понимать нормализованную матрицу Адамара.

Приведем несколько примеров матриц Адамара:

$$(1), \quad \begin{matrix} n=1 & n=2 & n=4 \end{matrix} \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}, \quad n=8$$

Рассмотрим вопрос построения матриц Адамара порядка  $n$ . Надо сказать, что такое построение является совсем нелегким делом, и этому вопросу посвящен внушительный раздел современной комбинаторики. Ниже мы рассмотрим два метода построения матриц Адамара.

Начнем с **наиболее простого способа** построения матриц Адамара сколь угодно больших порядков. Пусть  $H_n$  — матрица Адамара порядка  $n$  и  $-H_n$  — матрица с противоположными элементами. Составим из них матрицу порядка  $2n$  следующим образом:

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}.$$

Матрица  $H_{2n}$  является матрицей Адамара, так как

$$H_{2n} \cdot H_{2n}^T = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix} \cdot \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix} = \begin{pmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{pmatrix} = 2nI_{2n}.$$

Пример 1. Именно таким способом были получены матрицы Адамара порядков 1, 2, 4 и 8, приведенные выше.

Следующий метод построения матриц Адамара — **метод Пэли**. Пусть  $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$  — поле вычетов по модулю  $p$ , где  $p$  — простое число вида  $p = 4q + 3$ ,  $q \in \mathbb{N}$ . Определим на  $\mathbb{Z}_p$  характер  $\chi(\bar{i})$  следующим образом:

$$\chi(\bar{i}) = \begin{cases} 0, & \text{если } \bar{i} = \bar{0}; \\ 1, & \text{если } (\exists \bar{j} \in \mathbb{Z}_p)(\bar{j}^2 = \bar{i} \text{ \& } \bar{i} \neq \bar{0}); \\ -1, & \text{если } \neg(\exists \bar{j} \in \mathbb{Z}_p)(\bar{j}^2 = \bar{i} \text{ \& } \bar{i} \neq \bar{0}). \end{cases}$$

**Лемма 2.** Функция  $\chi(\bar{i})$  обладает следующими свойствами:

- 1)  $\chi(\bar{i}) \equiv i^{\frac{p-1}{2}} \pmod{p}$ ;
- 2)  $\chi(\bar{i}\bar{j}) = \chi(\bar{i})\chi(\bar{j})$ ;
- 3)  $\sum_{i=0}^{p-1} \chi(\bar{i}) = \sum_{i=1}^{p-1} \chi(\bar{i}) = 0$ ;
- 4)  $\chi(\overline{-1}) = \chi(\overline{p-1}) = -1$ ;
- 5) для всякого  $\bar{c} \neq \bar{0}$  выполняется равенство

$$\chi(\bar{1})\chi(\bar{1} + \bar{c}) + \chi(\bar{2})\chi(\bar{2} + \bar{c}) + \dots + \chi(\overline{p-1})\chi(\overline{p-1} + \bar{c}) = -1. \quad (3)$$

*Доказательство.*

1) При  $i \equiv 0 \pmod{p}$  тождество очевидно.

Пусть  $i \not\equiv 0 \pmod{p}$ . Согласно малой теореме Ферма  $i^{p-1} \equiv 1 \pmod{p}$ , откуда  $(i^{\frac{p-1}{2}} - 1)(i^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$ . Один и только один из сомножителей левой части последнего сравнения делится на  $p$  (оба сомножителя не могут одновременно делиться на  $p$ , так как в противном случае их разность 2 должна была бы делиться на  $p$ ). Поэтому  $i$  удовлетворяет только одному из тождеств

$$i^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ или } i^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Каждое из тождеств имеет  $\frac{p-1}{2}$  решений в  $\mathbb{Z}_p$ . Если  $\exists j$ , что  $i \equiv j^2 \pmod{p}$ , то  $i$  удовлетворяет первому сравнению. Действительно,  $i^{\frac{p-1}{2}} \equiv (j^2)^{\frac{p-1}{2}} = j^{p-1} \equiv 1 \pmod{p}$ . Таким образом, все  $\bar{i}$  для которых  $\exists j$ , что  $i \equiv j^2 \pmod{p}$ , удовлетворяют сравнению  $i^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . Так как число таких  $\bar{i}$  равно  $\frac{p-1}{2}$ , то  $\chi(\bar{i}) = 1 \equiv i^{\frac{p-1}{2}} \pmod{p}$  выполняется тогда и только тогда, когда  $\exists j$ , что  $\bar{i} = \bar{j}^2$ . Следовательно,  $\chi(\bar{i}) = -1 \equiv i^{\frac{p-1}{2}} \pmod{p}$  тогда и только тогда, когда  $\nexists j$ , что  $\bar{i} = \bar{j}^2$ .

2) Используя первое свойство, получаем  $i^{\frac{p-1}{2}} j^{\frac{p-1}{2}} = (ij)^{\frac{p-1}{2}} \equiv \chi(\bar{i}\bar{j}) \pmod{p}$  и  $i^{\frac{p-1}{2}} j^{\frac{p-1}{2}} \equiv \chi(\bar{i})\chi(\bar{j}) \pmod{p}$ , поэтому второе свойство верно.

3) Так как каждое из тождеств  $i^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$  имеет  $\frac{p-1}{2}$  решений, то  $\chi(\bar{i}) = 1$  для  $\frac{p-1}{2}$  элементов поля  $\mathbb{Z}_p$ , и  $\chi(\bar{i}) = -1$  также для  $\frac{p-1}{2}$  элементов поля  $\mathbb{Z}_p$ . Откуда и получаем искомое.

4) Для доказательства этого свойства заметим, что  $\chi(\overline{-1}) = (-1)^{\frac{p-1}{2}} = -1$ , так как  $p = 4q + 3$ .

5) В поле  $\mathbb{Z}_p$  для любого  $\bar{u} \neq \bar{0}$  существует единственный  $\bar{v}_u \neq \bar{0}$  такой, что  $\bar{u} + \bar{c} = \bar{u} \bar{v}_u$ . Если  $\bar{u}$  пробегает все ненулевые элементы  $\mathbb{Z}_p$ , то  $\bar{v}_u$  пробегает все элементы  $\mathbb{Z}_p$ , исключая  $\bar{1}$ , так как при  $\bar{u} + \bar{c} = \bar{0}$  имеем  $\bar{v}_u = \bar{0}$ . Следовательно,

$$\begin{aligned} & \chi(\bar{1})\chi(\bar{1} + \bar{c}) + \chi(\bar{2})\chi(\bar{2} + \bar{c}) + \dots + \chi(\overline{p-1})\chi(\overline{p-1} + \bar{c}) = \\ & = \chi(\bar{1})^2\chi(\bar{v}_1) + \chi(\bar{2})^2\chi(\bar{v}_2) + \dots + \chi(\overline{p-1})^2\chi(\bar{v}_{p-1}) = \\ & = \chi(\bar{v}_1) + \chi(\bar{v}_2) + \dots + \chi(\bar{v}_{p-1}) = (\chi(\bar{1}) + \chi(\bar{2}) + \dots + \chi(\overline{p-1})) - \chi(\bar{1}) = \\ & = 0 - 1 = -1. \end{aligned}$$

□

Рассмотрим теперь квадратную матрицу  $Q$  порядка  $p$ , элементы которой  $q_{ij}$ ,  $i, j = 1, 2, \dots, p$ , определяются следующим образом:

$$q_{ij} = \chi(\bar{j} - \bar{i}).$$

Так как  $q_{ij} = \chi(\bar{j} - \bar{i}) = \chi(\overline{-1})\chi(\bar{i} - \bar{j}) = -q_{ji}$ , то

$$Q = -Q^T. \quad (4)$$

Если  $QQ^T = B = (b_{ij})$ , то

$$\begin{aligned} \text{при } i = j \text{ имеем } b_{ii} &= \sum_{t=1}^p \chi(\bar{t} - \bar{i})\chi(\bar{t} - \bar{i}) = \chi(\bar{0})^2 + \sum_{t \neq i} \chi(\bar{t} - \bar{i})^2 = \\ &= \sum_{t=1}^{p-1} 1 = p-1; \end{aligned}$$

при  $i \neq j$  имеем  $b_{ij} = \sum_{t=1}^p \chi(\bar{t} - \bar{i})\chi(\bar{t} - \bar{j}) = \sum_{t=1}^p \chi(\bar{t} - \bar{i})\chi((\bar{t} - \bar{i}) + (\bar{i} - \bar{j})) =$   
 $= \sum_{u=1}^p \chi(\bar{u})\chi(\bar{u} + \bar{c}) = -1$ , где предпоследнее равенство получается из предыдущего упорядочиванием слагаемых по  $\bar{u} = \bar{t} - \bar{i}$  при  $\bar{c} = \bar{i} - \bar{j}$ , а последнее следует из (3).

Пусть  $I$  — единичная матрица порядка  $p$ , а  $J$  — квадратная матрица того же порядка, все элементы которой равны 1. Тогда мы доказали, что  $QQ^T = pI - J$ . Кроме того, так как  $\sum_{t=1}^p q_{it} = \sum_{t=1}^p \chi(\bar{t} - \bar{i}) = \sum_{u=0}^{p-1} \chi(\bar{u}) = 0$  и  $\sum_{t=1}^p q_{tj} = \sum_{t=1}^p \chi(\bar{j} - \bar{t}) = \sum_{u=0}^{p-1} \chi(\bar{u}) = 0$ , где в обоих случаях предпоследний переход осуществлялся с помощью упорядочивания слагаемых, то  $QJ = JQ = 0$ .

Итак, мы доказали равенства

$$QQ^T = pI - J, \quad QJ = JQ = 0. \quad (5)$$

Покажем, что матрица

$$H = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \dots & \dots & \dots & \dots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \vdots & Q - I & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \dots & \dots & \dots & \dots \end{pmatrix}$$

является матрицей Адамара порядка  $p + 1$ . Действительно, вычисляя произведение  $HH^T$ , получаем:

$$HH^T = \begin{pmatrix} p+1 & 0 & \dots & 0 \\ 0 & \dots & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \vdots & J + (Q - I)(Q^T - I) & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots \end{pmatrix}.$$

Отсюда, с учетом (4) и (5), имеем:

$$J + (Q - I)(Q^T - I) = J + QQ^T - Q - Q^T + I = J + pI - J - Q + Q + I = (p + 1)I.$$

Таким образом,  $HH^T = (p + 1)I$ .

Пример 2. Построим матрицу Адамара порядка 8. При этом  $p = 7$ . Функция  $\chi(i)$  задается следующей таблицей:

$\bar{i}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\chi(\bar{i})$	0	1	1	-1	1	-1	-1

Тогда матрицы  $Q$  и  $H$  имеют вид:

$$Q = \begin{pmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{pmatrix},$$

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{pmatrix}.$$

С матрицами Адамара связан ряд нерешенных проблем. Например, для любого ли  $n$  существует матрица Адамара порядка  $n$ ? Следующая теорема дает необходимое условие существования.

**Теорема 1.** Для существования матрицы Адамара порядка  $n$  необходимо, чтобы либо  $n = 1, 2$ , либо было кратно 4.

*Доказательство.* Матрицы Адамара порядков 1 и 2 были рассмотрены выше. Случай  $n = 3$  исключается, так как два вектора размерности 3 с координатами  $\pm 1$  не могут быть ортогональными.

При  $n \geq 4$  приведем матрицу  $H$  к нормализованному виду  $\hat{H}$ . Рассмотрим матрицу  $\hat{H}$ , образованную первыми тремя строками матрицы  $\hat{H}$ . Столбцы матрицы  $\hat{H}$  могут принадлежать одному из 4 видов:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}.$$

Обозначим через  $x, y, z, w$  число столбцов матрицы  $\hat{H}$  каждого вида. Тогда из условий ортогональности строк матрицы  $\hat{H}$  получаем систему уравнений

$$\begin{cases} x + y + z + w = n, \\ x - y + z - w = 0, \\ x + y - z - w = 0, \\ x - y - z + w = 0. \end{cases}$$

Эта система имеет единственное решение  $x = y = z = w = n/4$ . Таким образом, при  $n \geq 4$  имеем  $n = 4\mu$ , где  $\mu$  — натуральное число.  $\square$

До настоящего времени остается открытым вопрос: для любого ли  $n$ , кратного 4, существует матрица Адамара порядка  $n$ ? Неизвестно, в частности, существует ли матрица Адамара порядка 268 (это наименьший порядок, кратный 4, для которого матрица Адамара еще не построена).

Рассмотрим применение матриц Адамара в кодировании.

Пусть

$$H = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{n1} & h_{n2} & \dots & h_{nn} \end{pmatrix}, \quad h_{ij} = \pm 1,$$

— матрица Адамара. Из (2) следует, что для любой пары строк с номерами  $i$  и  $j$  ( $i \neq j$ ) верно равенство:

$$h_{i1}h_{j1} + h_{i2}h_{j2} + \dots + h_{in}h_{jn} = 0. \quad (6)$$

Таким образом, число слагаемых в (6), равных  $+1$ , должно совпадать с числом слагаемых, равных  $-1$ . Следовательно,  $n$  четно и любые две строки совпадают ровно в  $n/2$  позициях и различаются в остальных.



Пусть теперь  $A$  — двоичная матрица, получающаяся из матрицы  $H$ , построенной в последнем примере, заменой элемента  $+1$  на  $0$ ,  $-1$  на  $1$ . Множество векторов-строк матрицы  $A$  образует тогда код с расстоянием Хемминга между любыми кодовыми словами, равным  $n/2$ . Так, из матрицы Адамара порядка 8 получаем матрицу  $A$ , задающую код длины 8 с кодовым расстоянием 4:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \quad (7)$$

Не меняя кодового расстояния, можно уменьшить длину кода, если отбросить первый (нулевой) символ каждого слова.

Указанным образом из всякой матрицы Адамара порядка  $n$  можно получить двоичный код Адамара типа  $(n-1, n, n/2)$  ( $n-1$  — длина кодового вектора,  $n$  — число векторов кода,  $n/2$  — кодовое расстояние). Это, как правило, код, не являющийся групповым (например, код, задаваемый матрицей (7), не является групповым).

С матрицей  $A$  связаны еще два кода, которые тоже называют кодами Адамара.

Первый из них получается так. Перейдем от матрицы  $A$  к матрице  $\bar{A}$ , заменив все элементы матрицы  $A$  их дополнениями (т.е. заменив единицы нулями, а нули — единицами). Тогда строки матрицы  $\bar{A}$  образуют код типа  $(n, 2n, n/2)$ .

Другой код Адамара получается из предыдущего отбрасыванием первого символа в каждом кодовом слове. Это будет код типа  $(n-1, 2n, \frac{n}{2}-1)$ .

Например, из матрицы (7) можно получить таким способом коды Адамара типов  $(8, 16, 4)$  и  $(7, 16, 3)$ .

Коды Адамара, как видно из их определения, обладают интересной особенностью: расстояние между любыми двумя кодовыми векторами одинаково и совпадает поэтому с кодовым расстоянием. Подобные коды называют *эквивалентными*, и в некоторых случаях их использование дает особые преимущества.

Коды Адамара, обладая большим кодовым расстоянием, позволяют соответственно исправить и большое количество ошибок (первые два из них исправляют ошибки примерно в четверти позиций кодового слова). Достигается это, конечно, ценой высокой избыточности.

## §11. Блок-схемы

Блок-схема является одной из наиболее интересных комбинаторных конфигураций. Это не только чисто математический объект, но и средство для решения ряда практических задач. Рассмотрим такой пример.



*Пример 1.* Пусть нам необходимо сравнить урожайность  $v$  сортов пшеницы, если в нашем распоряжении имеется  $b$  опытных полей. Так как урожайность зависит не только от сорта, но и от разницы в условиях развития растения (в первую очередь от плодородия почвы), то эксперимент по проверке урожайности будет правильно поставлен, если удастся устранить влияние этих различий. Поэтому желательно соблюдение следующих условий:

- а) на каждом поле выделяется одинаковое число  $k$  участков, в которые высевается какой-либо один сорт пшеницы;
- б) каждый сорт высевается на одинаковом числе  $t$  опытных полей;
- в) каждая пара различных сортов встречается вместе на одном и том же числе  $\lambda$  опытных полей.

В связи с этим, возникает вопрос: а возможно ли соблюдение всех этих условий?

Уточним условие задачи. Пусть нужно испытать  $v = 6$  сортов пшеницы на  $k = 10$  опытных полей. Обозначим сорта буквами  $v_1, v_2, \dots, v_6$ , а поля —  $b_1, b_2, \dots, b_{10}$ . Разделим каждое поле на 3 участка и засеем поля по следующей схеме:

$$\begin{aligned} b_1 &= \{v_1, v_2, v_3\}, & b_5 &= \{v_1, v_5, v_6\}, & b_8 &= \{v_2, v_4, v_6\}, \\ b_2 &= \{v_1, v_2, v_5\}, & b_6 &= \{v_2, v_3, v_6\}, & b_9 &= \{v_3, v_4, v_5\}, \\ b_3 &= \{v_1, v_3, v_4\}, & b_7 &= \{v_2, v_4, v_5\}, & b_{10} &= \{v_3, v_5, v_6\}, \\ b_4 &= \{v_1, v_4, v_6\}, \end{aligned} \quad (1)$$

(в скобках записаны сорта пшеницы, посеянные на участках соответствующего поля). Все условия соблюдены:

- а) каждое поле разделено на 3 участка;
- б) каждый сорт посеян на 5 полях (например,  $v_3$  на полях  $b_1, b_3, b_6, b_9, b_{10}$ ;  $v_5$  на полях  $b_2, b_5, b_7, b_9, b_{10}$ , и т.д.);
- в) каждые два различных сорта посажены вместе на каких-либо двух полях (например,  $v_1$  и  $v_6$  на полях  $b_4$  и  $b_5$ ;  $v_3$  и  $v_4$  на полях  $b_3$  и  $b_9$ , и т.д.).

Схема (1) называется **блок-схемой** эксперимента. Ее можно рассматривать как конфигурацию, состоящую из 10 подмножеств на множестве из 6 элементов.

Конфигурации, удовлетворяющие условиям типа а)–в), имеют большое прикладное значение, в частности при планировании экспериментов, где позволяют не только получать достоверные опытные данные, но также обеспечивают правильную организацию опытов, что приводит к экономии, достигающей многих миллионов рублей.

**Определение 1.** *Уравновешенной неполной блок-схемой (далее просто блок-схема) называется такое размещение  $v$  различных элементов по  $b$  подмножествам (блокам), что каждый блок содержит точно  $k$  элементов, каждый элемент появляется точно в  $t$  различных блоках и каждая пара различных элементов  $y$  и  $z$  появляется точно в  $\lambda$  блоках.*

Поясним смысл понятий, встретившихся в этом определении.

Пусть  $S$  — множество из  $v$  элементов. Рассмотрим условие о парах элементов. Пусть  $y$  и  $z$  — пара элементов множества  $S$ . Тогда каждое  $k$ -элементное подмножество (или блок), содержащие  $y$  и  $z$ , имеет вид  $\{y, z, x_3, \dots, x_k\}$ , где  $x_3, x_4, \dots, x_k$  — любые  $k - 2$  элемента из  $S$ , отличные от  $y$  и  $z$ . Общее число таких блоков равно числу сочетаний без повторения из  $v - 2$  элементов по  $k - 2$ , т.е.  $C(v - 2, k - 2)$ . А общее число  $k$ -элементных подмножеств в  $S$  равно числу сочетаний без повторения из  $v$  элементов по  $k$ , т.е.  $C(v, k)$ . Таким образом, мы получили выражения параметров  $\lambda$  и  $b$  через  $v$  и  $k$ , т.е.

$$\lambda = C(v - 2, k - 2) \text{ и } b = C(v, k).$$

Такая блок-схема называется *полной блок-схемой*, так как никакая уравновешенная блок-схема на множестве из  $v$  элементов, у которой блоки имеют величину  $k$  и все различны между собой, не может иметь большее число блоков. Но можно рассматривать блок-схемы с меньшим числом блоков. Такие блок-схемы называются *неполными*. Неполные блок-схемы представляют больший интерес.

Блок-схемы называются *уравновешенными*, поскольку в них любая пара различных элементов встречается с одинаковой вероятностью (в этом случае говорят также об «одинаковой встречаемости»). Иногда о блок-схемах говорят как о конфигурациях, уравновешенных (или сбалансированных) относительно пар элементов, так как изучаются также конфигурации, уравновешенные относительно троек, четверок элементов и т.д.

Рассмотрим вопрос о встречаемости элементов блок-схемы в блоках. Очевидно, что все элементы должны появляться в блоках одинаковое число раз. Действительно, пусть некоторый элемент  $a \in S$  входит точно в  $r_a$  блоков. Подсчитаем число пар, которые он образует во всех блоках с каждым из остальных элементов  $v$ -множества  $S$ . С элементами всякого блока, в который он входит, образуется  $k - 1$  пара. Так как всего таких блоков  $r_a$ , то искомое число равно  $r_a(k - 1)$ . С другой стороны, по определению блок-схемы число появлений любой пары  $\{a, x\}$ , где  $x \neq a, x \in S$ , равно  $\lambda$ . Следовательно, всего таких появлений  $\lambda(v - 1)$ . Итак,  $r_a(k - 1) = \lambda(v - 1)$ , откуда следует, что  $r_a$  фактически не зависит от  $a$ .

Напомним, что  $r$  — число появлений элемента в блоках,  $b$  — число блоков в схеме. Тогда справедливо соотношение  $r(k - 1) = \lambda(v - 1)$ . Кроме того, так как каждый блок состоит из  $k$  элементов, а каждый из  $v$  элементов принадлежит в точности  $r$  блокам, то получаем, что  $bk = vr$ . Целые числа  $b, v, r, k, \lambda$  называются *параметрами блок-схемы*. Уравновешенную неполную блок-схему с параметрами  $b, v, r, k, \lambda$  называют  $(b, v, r, k, \lambda)$ -*конфигурацией*.

Таким образом, параметры блок-схемы удовлетворяют следующим соотношениям

$$bk = vr, \tag{2}$$

$$r(k - 1) = \lambda(v - 1). \tag{3}$$

Существование этих соотношений показывает, что пять параметров блок-схемы не независимы: задавая любые три из них, мы получаем из (2) и (3) значения остальных.

Целочисленность параметров накладывает ограничения на существование блок-схем.

*Пример 2.* Не существует блок-схемы с  $\lambda = 1$ ,  $k = 3$ ,  $v = 5$  или 6. Действительно, из (3) при  $v = 6$  следует, что  $2r = 5$ . При  $v = 5$  из (3) получается, что  $r = 2$ , но тогда (2) означает, что  $3b = 10$ , что невозможно.

Очевидно, что блок-схемы с  $\lambda = 1$ ,  $k = 3$  в силу (3) не существует ни при каком четном  $v$ .

*Пример 3.* Рассмотрим  $(b, v, r, k, \lambda)$ -конфигурацию на 7-множестве с  $b = v = 7$ ,  $r = k = 3$ ,  $\lambda = 1$ :

$$\begin{aligned} b_1 &= \{v_1, v_2, v_4\}, & b_4 &= \{v_4, v_5, v_7\}, & b_6 &= \{v_2, v_6, v_7\}, \\ b_2 &= \{v_2, v_3, v_5\}, & b_5 &= \{v_1, v_5, v_6\}, & b_7 &= \{v_1, v_3, v_7\}, \\ b_3 &= \{v_3, v_4, v_6\}, \end{aligned}$$

В ней проявляется общая закономерность, вытекающая из (2): если в уравновешенной неполной блок-схеме число блоков равно числу элементов, т.е.  $b = v$ , то число появлений каждого элемента в блоках схемы равно величине блока, т.е.  $r = k$  (и наоборот).

Блок-схемы, для которых  $b = v$  (и, значит,  $r = k$ ), называются *симметричными*.

## §12. Конечные проективные плоскости

В евклидовой геометрии на плоскости через любые две точки проходит только одна прямая, а любые две (непараллельные) прямые пересекаются только в одной точке. Оговорка относительно непараллельных прямых устраняется в проективной геометрии введением еще одной (несобственной, бесконечно удаленной) прямой, на которой располагаются точки пересечения параллельных прямых. Такая дополненная плоскость называется *проективной*. В комбинаторной математике рассматриваются конечные проективные плоскости.

Пусть  $S$  — конечное множество точек, для подмножеств которого, называемых *прямыми*, выполняются следующие условия:

- 1) две различные точки принадлежат одной и только одной прямой;
- 2) две различные прямые имеют одну и только одну общую точку;
- 3) существуют четыре точки, из которых никакие три не лежат на одной прямой.

**Определение 1.** Конфигурация  $\mathcal{P}$  на конечном множестве точек  $S$  называется **конечной проективной плоскостью**, если для ее подмножеств (прямых) выполняются условия 1–3.

**Теорема 1.** Пусть  $n \geq 2$  — целое число. Для проективной плоскости  $\mathcal{P}$ , заданной на конечном множестве точек  $S$ , равносильны следующие свойства:

- а) некоторая прямая содержит точно  $n + 1$  точек;
- б) некоторая точка принадлежит точно  $n + 1$  прямым;
- в) каждая прямая содержит точно  $n + 1$  точек;
- г) каждая точка принадлежит точно  $n + 1$  прямым;
- д)  $S$  состоит из  $n^2 + n + 1$  точек;
- е)  $\mathcal{P}$  состоит из  $n^2 + n + 1$  прямых.

*Доказательство.* Пусть  $A, B, C, D$  — четыре точки, из которых никакие три не лежат на одной прямой. Существование таких точек обеспечено условием 3. Тогда мы имеем прямые  $L_1, \dots, L_6$ , содержащие  $A, B, C, D$  и еще три точки  $X, Y, Z$ :

$$\begin{aligned} L_1 &: A, B, X, \dots, \\ L_2 &: A, C, Y, \dots, \\ L_3 &: A, D, Z, \dots, \\ L_4 &: B, C, Z, \dots, \\ L_5 &: B, D, Y, \dots, \\ L_6 &: C, D, X, \dots, \end{aligned} \tag{1}$$

где  $X, Y, Z$  — точки пересечения пар прямых  $L_1, L_6$ ;  $L_2, L_5$  и  $L_3, L_4$ . Из условий 1–3 нетрудно заключить, что шесть прямых  $L_1, \dots, L_6$  различны и точки  $A, \dots, Z$  также различны.

Кроме того, не существует, очевидно, никаких других отношений принадлежности между этими семью точками и шестью прямыми. Например, не может быть  $A \in L_4$ , так как тогда через две различные точки  $A, B$  проходили бы две различные прямые  $L_1$  и  $L_4$ .

Допустим теперь, что выполняется свойство а). Пусть  $L$  — прямая точно с  $n + 1$  точками на ней, скажем  $Q_1, Q_2, \dots, Q_{n+1}$ . Если  $P$  — точка, не лежащая на  $L$ , то прямые  $PQ_i, i = 1, \dots, n + 1$ , различны, так как если  $PQ_i = PQ_j$ , то  $P \in Q_i Q_j = L$  — противоречие. Далее, каждая прямая, проходящая через  $P$ , пересекает  $L$  и, значит, должна быть одной из  $n + 1$  прямых  $PQ_i, i = 1, \dots, n + 1$ . По крайней мере две из точек  $A, B, C, D$ , из (1) не лежат на  $L$ , и потому такая точка  $P$  существует. Пусть теперь  $P$  — точка, лежащая точно на  $n + 1$  прямых  $K_1, \dots, K_{n+1}$ . Если  $M$  — некоторая прямая, не проходящая через  $P$ , то  $M$  пересекает  $K_1, \dots, K_{n+1}$  в точках  $Q_1, \dots, Q_{n+1}$ , которые все различны, поскольку  $P$  есть единственная точка, лежащая более чем на одной из прямых



$K_1, \dots, K_{n+1}$ . Если бы на  $M$  существовала еще одна точка  $Q_{n+2}$ , то существовала бы прямая  $PQ_{n+2}$ , не совпадающая ни с какой  $K_j$ , так как в противном случае  $PQ_{n+2}$  содержала бы и некоторое  $Q_j$  и тогда

$$PQ_{n+2} = pQ_{n+2}Q_j = Q_{n+2}Q_j = M,$$

что противоречит предположению  $P \notin M$ .

Наша исходная прямая  $L$  содержала точно  $n+1$  точку, следовательно, каждая точка, не лежащая на  $L$ , лежит точно на  $n+1$  прямых. К таким точкам относятся по крайней мере две из точек  $A, B, C, D$ , например,  $A$  и  $B$ . Поэтому каждая прямая, не проходящая через  $A$  или через  $B$ , содержит точно  $n+1$  точку, т.е. каждая прямая, исключая, быть может,  $L_1 = ABX$ , содержит точно  $n+1$  точку. Тогда  $L_2 = ACY$  содержит точно  $n+1$  точку, и точка  $Z$ , не лежащая на  $L_2$ , лежит точно на  $n+1$  прямой. Следовательно,  $L_1$ , которая не содержит  $Z$ , также должна содержать  $n+1$  точку. Таким образом, свойство а) влечет за собой свойство в).

Но для любой точки  $P$  мы можем найти прямую, не проходящую через нее, и потому, так же, как и выше, существует точно  $n+1$  прямая, проходящая через  $P$ , чем доказаны свойства б) и г). Пусть теперь  $P_0$  — некоторая точка, и пусть  $n+1$  прямая  $L_1, \dots, L_{n+1}$  проходит через  $P_0$ . Каждая из них содержит точно  $n$  точек, отличных от  $P_0$ , и поскольку  $P_0$  соединяется одной из этих прямых с любой точкой плоскости  $\mathcal{P}$ , общее число точек в  $S$  равно  $1 + (n+1) = n^2 + n + 1$ , тем самым доказано свойство д). Аналогично, если  $L_0$  — прямая, содержащая точки  $P_1, \dots, P_{n+1}$ , каждая из которых лежит точно на  $n$  других прямых, то в  $\mathcal{P}$  будет  $1 + (n+1)n = n^2 + n + 1$  прямых и свойство е) также доказано.

Мы показали, что свойство а) влечет за собой остальные пять свойств, поэтому свойство в) также влечет за собой все остальные. Аналогично в силу двойственности, поменяв ролями “точки” и “прямые”, мы видим, что свойство б) и свойство г) влекут за собой остальные. Если выполняется свойство д), то прямая  $L_1$  из (1) содержит  $m+1$  точек при некотором целом  $m \geq 2$ , и поэтому, как показано выше,  $S$  содержит  $m^2 + m + 1$  точек. Но из равенства  $m^2 + m + 1 = n^2 + n + 1$  для целых положительных  $m$  и  $n$  следует, что  $m = n$ , и свойство д) влечет за собой свойство а), а потому и все остальные свойства. Аналогичным образом из свойства е) вытекает свойство б), а значит, и все другие.  $\square$

Конечная проективная плоскость, каждая прямая которой состоит из  $n+1$  точек, называется *проективной плоскостью порядка  $n$* . Так как по теореме 1 число точек проективной плоскости равно числу прямых, каждая прямая содержит одинаковое число точек, равное  $n+1$ , и через любые две точки проходит в точности одна прямая, то любая конечная проективная плоскость порядка  $n$  есть симметричная уравновешенная неполная блок-схема с параметрами  $b = v = n^2 + n + 1$ ,  $r = k = n + 1$ ,  $\lambda = 1$ .

Обратно, пусть на множестве  $S$  задана симметричная блок-схема  $\mathcal{P}$  с параметрами  $b = v = n^2 + n + 1$ ,  $r = k = n + 1$ ,  $\lambda = 1$ , где  $n \geq 2$ . Если мы назовем элементы  $S$  *точками*, а блоки — *прямыми*, то  $\mathcal{P}$  можно рассматривать как



конечную проективную плоскость на множестве точек  $S$ . Таким образом, блок-схема примера 3 §11 дает пример конечной проективной плоскости порядка 2.

**Пример 1.** Рассмотрим проективную плоскость порядка 3 на множестве из 13 элементов  $\{1, 2, \dots, 13\}$ :

$$\begin{aligned} b_1 &= \{1, 2, 4, 10\}, & b_6 &= \{2, 6, 7, 9\}, & b_{10} &= \{6, 10, 11, 13\}, \\ b_2 &= \{2, 3, 5, 11\}, & b_7 &= \{3, 7, 8, 10\}, & b_{11} &= \{1, 7, 11, 12\}, \\ b_3 &= \{3, 4, 6, 12\}, & b_8 &= \{4, 8, 9, 11\}, & b_{12} &= \{2, 8, 12, 13\}, \\ b_4 &= \{4, 5, 7, 13\}, & b_9 &= \{5, 9, 10, 12\}, & b_{13} &= \{1, 3, 9, 13\}, \\ b_5 &= \{1, 5, 6, 8\}, \end{aligned}$$

Построим по этой плоскости двоичный код. Для этого введем матрицу инцидентного отношения  $M = (m_{ij})$ :

$$m_{ij} = \begin{cases} 1, & \text{если элемент } i \text{ принадлежит прямой } b_j; \\ 0, & \text{если элемент } i \text{ не принадлежит прямой } b_j. \end{cases}$$

Тогда

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

где кодовые векторы записаны в строках матрицы  $M$ . Данный код способен обнаруживать 11 ошибок и исправлять 5.

В комбинаторной математике рассматриваются не только конечные плоскости, но также конечные пространства больших размерностей. С помощью конечных проективных плоскостей (а также конечных проективных пространств) устанавливается связь между теорией блок-схем и геометрией, которая позволяет использовать в комбинаторике различные соображения геометрического характера.

## §13. Генерация комбинаторных объектов

### 13.1. Порождение перестановок

Проблема порождения всех  $n!$  перестановок  $n$ -элементного множества имеет давнюю историю. Ис возникновение можно отнести к началу XVII века, когда



получая каждую перестановку из предшествующей ей и небольшого количества добавочной информации. Это делается с помощью трех векторов: текущей перестановки  $\pi = (\pi_1, \pi_2, \dots, \pi_n)$ , обратной к ней перестановки  $p = (p_1, p_2, \dots, p_n)$  и записи направления  $d_i$ , в котором сдвигается каждый элемент  $i$  ( $-1$ , если он сдвигается влево;  $+1$ , если вправо; и  $0$ , если не сдвигается). Элемент сдвигается до тех пор, пока не достигнет элемента, большего, чем он сам; в этом случае сдвиг прекращается. В этот момент направление сдвига данного элемента изменяется на противоположное и передвигается следующий меньший его элемент, который можно сдвинуть. Поскольку хранится перестановка, обратная к  $\pi$ , то в  $\pi$  легко найти место следующего меньшего элемента. Следующий алгоритм представляет собой реализацию рассмотренного метода.

```

for i = 1 to n do {  $\pi_i = p_i = i$ ;
                    $d_i = -1$ ;
 $d_1 = 0$ ;
 $\pi_0 = \pi_{n+1} = m = n + 1$ ; {Метки границы}
while m  $\neq$  1 do { print  $\pi = (\pi_1, \pi_2, \dots, \pi_n)$ ;
                   m = n;
                   while  $\pi_{p_m+d_m} > m$  do {  $d_m = -d_m$ ;
                                                m = m - 1;
 $\pi_{p_m} \leftrightarrow \pi_{p_m+d_m}$ ; {Изменить  $\pi$ }
 $p_{\pi_{p_m}} \leftrightarrow p_m$ . {Изменить  $p = \pi^{-1}$ ,  $\pi_{p_m+d_m} = m$ }

```

Рассмотрим механизм работы этого алгоритма на примере порождения перестановок из 4 элементов. Последовательность итераций алгоритма приведена в следующей таблице (метки границы  $\pi_0$  и  $\pi_5$  мы опускаем, вместо значений  $d_i = \pm 1$  пишем соответственно  $+$  или  $-$ ).

$i$	$d$				$p$				$\pi$				$m$	Комментарий
	$d_1$	$d_2$	$d_3$	$d_4$	$p_1$	$p_2$	$p_3$	$p_4$	$\pi_1$	$\pi_2$	$\pi_3$	$\pi_4$		
1	0	-	-	-	1	2	3	4	1	2	3	4	4	Элемент 4 сдвигается влево
2	0	-	-	-	1	2	4	3	1	2	4	3	4	
3	0	-	-	-	1	3	4	2	1	4	2	3	4	
4	0	-	-	-	2	3	4	1	4	1	2	3	4	
5	0	-	-	+	2	4	3	1	4	1	3	2	3	Элемент 3 сдвигается на 1 позицию влево, 4 начинает движение вправо
6	0	-	-	+	1	4	3	2	1	4	3	2	4	
7	0	-	-	+	1	4	2	3	1	3	4	2	4	
8	0	-	-	+	1	3	2	4	1	3	2	4	4	

9	0	-	-	-	2	3	1	4	3	1	2	4	3	Элемент 3 сдвигается еще на 1 позицию влево
10	0	-	-	-	2	4	1	3	3	1	4	2	4	
11	0	-	-	-	3	4	1	2	3	4	1	2	4	
12	0	-	-	-	3	4	2	1	4	3	1	2	4	
13	0	-	+	+	4	3	2	1	4	3	2	1	2	Элемент 2 сдвигается на 1 позицию влево, 3 и 4 меняют направления движения
14	0	-	+	+	4	3	1	2	3	4	2	1	4	
15	0	-	+	+	4	2	1	3	3	2	4	1	4	
16	0	-	+	+	3	2	1	4	3	2	1	4	4	
17	0	-	+	-	3	1	2	4	2	3	1	4	3	
18	0	-	+	-	4	1	2	3	2	3	4	1	4	
19	0	-	+	-	4	1	3	2	2	4	3	1	4	
20	0	-	+	-	4	2	3	1	4	2	3	1	4	
21	0	-	+	+	3	2	4	1	4	2	1	3	3	
22	0	-	+	+	3	1	2	4	2	4	1	3	4	
23	0	-	+	+	2	1	4	3	2	1	4	3	4	
24	0	-	+	+	2	1	3	4	2	1	3	4	4	
25	0	+	-	-	—	—	—	—	—	—	—	—	1	Остановка
$i$	$d_1$	$d_2$	$d_3$	$d_4$	$p_1$	$p_2$	$p_3$	$p_4$	$\pi_1$	$\pi_2$	$\pi_3$	$\pi_4$	$m$	Комментарий
	$d$				$p$				$\pi$					

Корректность алгоритма доказывается индукцией по  $n$ . Случай  $n = 1$  тривиален. Пусть алгоритм правильно работает для  $n$ . Покажем, что он будет правильно работать и для  $n + 1$ . Алгоритм начинает работу с перестановки  $12 \dots n(n + 1)$ , где  $n + 1$  первый сдвигаемый элемент. Он сдвигается до тех пор, пока не будет получена перестановка  $(n + 1)12 \dots n$ . При этом будут порождены  $n + 1$  перестановок, в которых число  $n + 1$  занимает места  $n + 1, n, \dots, 1$ . Теперь начинает движение число  $n$ , сдвигаясь на 1 позицию. Число  $n + 1$  меняет направление и начинает сдвигаться вправо. Когда будет получена перестановка  $1 \dots n(n - 1)(n + 1)$ , будут получены еще  $n + 1$  перестановка. Далее происходит перестановка элементов  $n$  и  $n - 2$ , а  $n + 1$  начинает двигаться влево. Таким образом, алгоритм порождает  $n + 1$  перестановку элемента  $n + 1$  в перестановке  $12 \dots n$ . Когда будет достигнута последняя перестановка чисел  $1, 2, \dots, n$ , то число  $n + 1$ , выполнив  $n + 1$  сдвигов, перестанет быть подвижным, и алгоритм останавливается. Общее число сдвигов, выполненных алгоритмом, равно  $(n + 1) \cdot n! = (n + 1)!$ .

Рассмотренный алгоритм — один из наиболее эффективных алгоритмов порождения перестановок.



### 13.2. Порождение подмножеств множества

Задача порождения подмножеств множества  $A = \{a_1, a_2, \dots, a_n\}$  эквивалентна задаче порождения  $n$ -разрядных двоичных векторов. Действительно, любое подмножество  $B$  множества  $A$  однозначно задается  $n$ -мерным двоичным вектором  $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ , определяемым следующим образом:

$$\alpha_i = \begin{cases} 1, & \text{если } a_i \in B \\ 0, & \text{если } a_i \notin B \end{cases}.$$

Очевидно, что наиболее прямым способом порождения всех двоичных наборов длины  $n$  является счет в системе счисления с основанием 2, что реализовано следующим алгоритмом:

```
for i = 0 to n do b_i = 0;
while b_n ≠ 1 do {
  print(b_{n-1}, b_{n-2}, ..., b_0);
  i = 0;
  while b_i = 1 do {
    b_i = 0;
    i = i + 1;
  }
  b_i = 1.
```

Перевод этого алгоритма на язык подмножеств множества  $\{a_1, a_2, \dots, a_n\}$  приводит к приведенному ниже алгоритму, где добавлен фиктивный элемент  $a_{n+1}$ :

```
S = ∅;
while a_{n+1} ∉ S do {
  print(S);
  i = 1;
  while a_i ∈ S do {
    S = S - {a_i};
    i = i + 1;
  }
  S = S ∪ {a_i}.
```

### 13.3. Порождение размещений с повторениями

Воспользуемся тем, что задача порождения множества всех размещений с повторениями длины  $k$  из  $n$  элементов  $\{a_0, a_1, \dots, a_{n-1}\}$  эквивалентна задаче порождения множества  $k$ -разрядных чисел в системе счисления с основанием  $n$ . На  $k$ -ом месте в размещении располагается элемент  $a_i$  тогда и только тогда, когда цифра в  $k$ -ом разряде соответствующего числа равна  $i$ . Напомним, что всего размещений с повторениями  $n^k$ .

Пусть, например,  $k = 2$  и  $n = 3$ . Тогда выпишем все 2-разрядные числа в системе счисления с основанием 3:

00,      01,      02,      10,      11,      12,      20,      21,      22.

Им соответствуют размещения:

$\langle a_0 a_0 \rangle$ ,  $\langle a_0 a_1 \rangle$ ,  $\langle a_0 a_2 \rangle$ ,  $\langle a_1 a_0 \rangle$ ,  $\langle a_1 a_1 \rangle$ ,  $\langle a_1 a_2 \rangle$ ,  $\langle a_2 a_0 \rangle$ ,  $\langle a_2 a_1 \rangle$ ,  $\langle a_2 a_2 \rangle$ .



Следующий алгоритм использует фиктивный элемент  $b_k$  при порождении наборов длины  $k$  в системе счисления с основанием  $n$ , где  $b_i \in \{0, 1, \dots, n-1\}$ ,  $i = 0, 1, \dots, k$ , т.е.  $b_i$  — это цифры генерируемого числа в системе счисления с основанием  $n$ :

```
for i = 0 to k do bi = 0;

while bk ≠ 1 do {
  print(bk-1, bk-2, ..., b0);
  i = 0;
  while bi = n - 1 do {
    bi = 0;
    i = i + 1;
  }
  bi = bi + 1.
}
```

### 13.4. Порождение сочетаний

В качестве основного множества будем рассматривать множество натуральных чисел  $\mathbb{N}_n = \{1, 2, \dots, n\}$ . Будем порождать все сочетания длины  $k$  из этого множества.

Рассмотрим, например,  $C(6, 3) = 20$ , сочетания из шести элементов по три (т.е. трехэлементные подмножества множества  $\mathbb{N}_6 = \{1, 2, 3, 4, 5, 6\}$ ). Эти подмножества будем записывать в виде  $a_1 < a_2 < a_3$ , где  $a_i \in \mathbb{N}_6$ ,  $i = 1, 2, 3$ , т.е. упорядочив элементы по возрастанию:

123	135	234	256
124	136	235	345
125	145	236	346
126	146	245	356
134	156	246	456

Сочетания, представленные в виде упорядоченных по возрастанию элементов, можно порождать последовательно простым способом. А именно, рассмотрим сочетание  $a_1 = 1, a_2 = 2, \dots, a_k = k$ . Следующее сочетание находится просмотром текущего сочетания  $a_1, a_2, \dots, a_k$  справа налево с тем, чтобы определить место самого правого элемента, который еще не достиг своего максимального значения, т.е. ищем наибольшее  $a_j$ , такое, что  $a_j + 1$  не входит в данное сочетание. Если таких  $a_j$  нет (это происходит только в случае  $a_1 = n - k + 1, \dots, a_k = n$ ), то стоп. А если такое  $a_j$  есть, то образуем новое сочетание  $a'_1, \dots, a'_k$ , полагая

$$a'_1 = a_1, \dots, a'_{j-1} = a_{j-1}, a'_j = a_j + 1, a'_{j+1} = a'_j + 1, \dots, a'_k = a'_{k-1} + 1.$$

Данный алгоритм реализуем следующим образом:

```

 $a_0 = -1;$ 
for  $i = 0$  to  $k$  do  $a_i = i;$ 
 $j = 1;$ 

while  $j \neq 0$  do {
    print( $a_1, a_2, \dots, a_k$ );
     $j = k;$ 
    while  $a_j = n - k + j$  do  $j = j - 1;$ 
     $a_j = a_j + 1;$ 
    for  $i = j + 1$  to  $k$  do  $a_i = a_{i-1} + 1.$ 
}
```

Рассмотрим механизм работы этого алгоритма на примере порождения сочетаний из 4 элементов по 2. Последовательность итераций алгоритма приведена в следующей таблице:

$i$	Сочетания $a_1, a_2$	$a_j$
1	1, 2	2
2	1, 3	3
3	1, 4	1
4	2, 3	3
5	2, 4	2
6	3, 4	СТОП

# Глава 3. Функции $k$ -значной логики. Схемы из функциональных элементов

## §1. $k$ -значные функции

В этом разделе будут достаточно кратко рассмотрены некоторые вопросы, относящиеся к  $k$ -значным логикам. При этом будет установлена как имеющаяся определенная аналогия с классической 2-значной логикой, так и отдельные принципиальные различия.

Многие определения для  $k$ -значных логик совершенно аналогичны соответствующим определениям для 2-значной логики.

Обозначим через  $E_k$  множество  $\{0, 1, \dots, k-1\}$ .

**Определение 1.**  $n$ -местной  $k$ -значной функцией называется любое отображение  $f$  множества  $E_k^n$  во множество  $E_k$ .

Через  $P_k(n)$  будем обозначать множество всех  $n$ -местных  $k$ -значных функций, а через  $P_k$  — множество всех  $k$ -значных функций.

Каждую  $n$ -местную  $k$ -значную функцию, так же как и любую булеву функцию, можно задать таблицей следующего вида, содержащей  $k^n + 1$  строк и  $n + 2$  столбцов:

№	$x_1$	$x_2$	$\dots$	$x_{n-1}$	$x_n$	$f(x_1, x_2, \dots, x_{n-1}, x_n)$
1	$\varepsilon_{1,1}$	$\varepsilon_{1,2}$	$\dots$	$\varepsilon_{1,n-1}$	$\varepsilon_{1,n}$	$\varepsilon_1$
2	$\varepsilon_{2,1}$	$\varepsilon_{2,2}$	$\dots$	$\varepsilon_{2,n-1}$	$\varepsilon_{2,n}$	$\varepsilon_2$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$	$\vdots$
$k^n - 1$	$\varepsilon_{k^n-1,1}$	$\varepsilon_{k^n-1,2}$	$\dots$	$\varepsilon_{k^n-1,n-1}$	$\varepsilon_{k^n-1,n}$	$\varepsilon_{k^n-1}$
$k^n$	$\varepsilon_{k^n,1}$	$\varepsilon_{k^n,2}$	$\dots$	$\varepsilon_{k^n,n-1}$	$\varepsilon_{k^n,n}$	$\varepsilon_{k^n}$

В этой таблице все  $\varepsilon_{i,j}$  и  $\varepsilon_i$  ( $i = 1, \dots, k^n$ ,  $j = 1, \dots, n$ ) — это элементы множества  $\{0, 1, \dots, k-1\}$ .

Для единообразия набору  $\varepsilon_{i,1}, \varepsilon_{i,2}, \dots, \varepsilon_{i,n-1}, \varepsilon_{i,n}$  можно сопоставить натуральное число  $k^{n-1}\varepsilon_{i,1} + k^{n-2}\varepsilon_{i,2} + \dots + k\varepsilon_{i,n-1} + \varepsilon_{i,n}$ ,  $k$ -ичными цифрами которого являются элементы этого набора, и перечислять наборы значений аргументов

в порядке возрастания этих чисел от 0 до  $k^n - 1$ . Таким образом, в первой строке таблицы набор значений состоит из одних нулей, а в последней — из одних лишь чисел  $k - 1$ .

При фиксации наборов значений аргументов получаем биективное отображение множества всех  $n$ -местных  $k$ -значных функций на множество таблиц указанного вида. Так как число таких таблиц равно числу различных последних столбцов, а оно равно  $k^{k^n}$ , то получаем следующую теорему.

**Теорема 1.** При любом  $n$  множество  $P_k(n)$  всех  $n$ -местных  $k$ -значных функций состоит из  $k^{k^n}$  элементов.

**Определение 2.**  $n$ -местная  $k$ -значная функция  $f(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n)$  существенно зависит от своей  $i$ -ой переменной  $x_i$ , если найдется такая последовательность  $\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \dots, \varepsilon_n$ , состоящая из чисел множества  $E_k$ , и такие два различных элемента  $\alpha$  и  $\beta$  этого множества, что

$$f(\varepsilon_1, \dots, \varepsilon_{i-1}, \alpha, \varepsilon_{i+1}, \dots, \varepsilon_n) \neq f(\varepsilon_1, \dots, \varepsilon_{i-1}, \beta, \varepsilon_{i+1}, \dots, \varepsilon_n).$$

Переменные, от которых существенно зависит функция, называются ее существенными переменными, а остальные — несущественными.

**Определение 3.** Если одну  $k$ -значную функцию можно получить из другой конечным числом операций введения и удаления несущественных переменных, то они считаются равными.

Последнее определение позволяет относительно любого конечного набора  $k$ -значных функций предполагать, без ограничения общности, что все функции этого набора зависят от одних и тех же переменных. Этого можно было бы добиться и по-другому, как это делается, например, в теории рекурсивных функций — введением в рассмотрение функций проектирования  $U_m^n(x_1, \dots, x_n) = x_m$ .

Другим способом задания  $k$ -значных функций является их задание термами или формулами, так же как и булевых функций, что по сути дела равносильно. Так же как и в булевом случае, мы остановимся на первом варианте.

Пусть  $\Gamma$  — произвольная система  $k$ -значных функций. Каждой  $n$ -местной  $k$ -значной функции  $f$  из  $\Gamma$  сопоставим  $n$ -местный функциональный символ  $\tilde{f}$ , который будем называть именем функции  $f$ .

Индуктивно определим понятие термина над множеством функций  $\Gamma$ . Предварительно зафиксируем счетное множество переменных  $\{x_1, x_2, \dots, x_n, \dots\}$ .

**Определение 4.** 1) Каждая переменная  $x_i$  является термом над множеством функций  $\Gamma$ .

2) Если  $f$  —  $n$ -местная  $k$ -значная функция из  $\Gamma$ , а  $t_1, \dots, t_n$  — термы над множеством функций  $\Gamma$ , то  $\tilde{f}(t_1, \dots, t_n)$  — терм над множеством функций  $\Gamma$ .

3) Выражение является термом тогда и только тогда, когда это следует из пунктов 1) и 2).

В дальнейшем имя  $\tilde{f}$   $k$ -значной функции  $f$  будем обозначать просто через  $f$ , что не приведет к недоразумениям.

Каждый терм  $t$  естественным образом определяет  $k$ -значную функцию, которую мы обозначим через  $f_t$ .

Индукцией по длине терма  $t$  определим его значение при заданных значениях входящих в него переменных.

Пусть все переменные, входящие в терм  $t$ , содержатся в списке  $x_1, \dots, x_n$ . Возьмем произвольный набор  $\varepsilon_1, \dots, \varepsilon_n$  из  $E_k$  в качестве значений переменных  $x_1, \dots, x_n$ . Определим значение терма  $t$  на этом наборе в соответствии с определением терма.

1) Если терм  $t$  — это переменная  $x_i$ , то его значением на указанном наборе будет  $\varepsilon_i$ .

2) Пусть терм  $t$  имеет вид  $\tilde{g}(t_1, \dots, t_m)$ , где  $\tilde{g}$  —  $m$ -местный функциональный символ, а значит,  $g$  —  $m$ -местная функция. Обозначим через  $\alpha_1, \dots, \alpha_m$  значения термов  $t_1, \dots, t_m$  при значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$ . Тогда значением терма  $t$  при значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$  будет  $g(\alpha_1, \dots, \alpha_m)$ .

Определим функцию  $f_t$  следующим образом:  $f_t(\varepsilon_1, \dots, \varepsilon_n)$  равно значению терма  $t$  при значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$ .

**Определение 5.**  $n$ -местная функция  $\varphi$  представима термом  $t$ , если все его переменные содержатся среди  $x_1, \dots, x_n$  и  $f_t = g$ , т.е. при любых значениях  $\varepsilon_1, \dots, \varepsilon_n$  переменных  $x_1, \dots, x_n$  значение терма  $t$  равно  $\varphi(\varepsilon_1, \dots, \varepsilon_n)$ .

## §2. Замыкание классов $k$ -значных функций

**Определение 1.** Для произвольного множества  $\Gamma$   $k$ -значных функций через  $[\Gamma]$  обозначается множество всех  $k$ -значных функций, представимых термами над множеством  $\Gamma$ . Множество  $[\Gamma]$  называется замыканием множества  $k$ -значных функций  $\Gamma$ . Если выполняется равенство  $[\Gamma] = \Gamma$ , то множество  $\Gamma$  называется замкнутым.

Отметим простейшие свойства операции замыкания

- 1)  $\Gamma \subseteq [\Gamma]$ ;
- 2) Если  $U \subseteq W$ , то  $[U] \subseteq [W]$ ;
- 3)  $[[\Gamma]] = [\Gamma]$ .

**Определение 2.** Множество  $\Gamma$   $k$ -значных функций называется (функционально) полным, если  $[\Gamma] = P_k$ , т.е. любая  $k$ -значная функция представима термом над множеством  $\Gamma$ , т.е.  $[\Gamma] = P_k$ .

Приведем несколько примеров полных систем функций и рассмотрим вопрос о некоторых критериях полноты. Прежде всего рассмотрим ряд  $k$ -значных функций, которые в некотором смысле можно считать элементарными.

1)  $\bar{x} = x + 1 \pmod{k}$ . Функция  $\bar{x}$  “циклический сдвиг” рассматривается в качестве одного из обобщений булева отрицания.

2) Другим обобщением булева отрицания служит функция отрицание Лукасевича  $N(x) = k - 1 - x$ . Эта функция часто обозначается через  $\sim x$ .



3) Целую серию обобщений булева отрицания дают функции  $I_t(x)$  ( $0 \leq t \leq k-1$ ), определяемые равенством

$$I_t(x) = \begin{cases} k-1 & \text{при } x = t, \\ 0 & \text{при } x \neq t. \end{cases}$$

Функции  $I_t(x)$  также называются *характеристическими функциями числа  $t$* .

4) Другую серию обобщений булева отрицания дают функции  $J_t(x)$  ( $0 \leq t \leq k-1$ ), определяемые равенством

$$J_t(x) = \begin{cases} 1 & \text{при } x = t, \\ 0 & \text{при } x \neq t. \end{cases}$$

Функции  $J_t(x)$  также называются *характеристическими функциями числа  $t$* .

5) Обобщением булевой конъюнкции служит функция  $\min(x_1, x_2)$ .

6) В качестве еще одного обобщения булевой конъюнкции выступает функция  $x_1 x_2 \pmod k$ .

7) Обобщением булевой дизъюнкции служит функция  $\max(x_1, x_2)$ .

8)  $x_1 + x_2 \pmod k$ .

Если через  $x_1 \circ x_2$  обозначить любую из функций  $\max(x_1, x_2)$ ,  $\min(x_1, x_2)$ ,  $x_1 + x_2 \pmod k$  и  $x_1 x_2 \pmod k$ , то негрудно проверить выполнимость равенств

1) ассоциативность

$$((x_1 \circ x_2) \circ x_2) = (x_1 \circ (x_2 \circ x_2))$$

и 2) коммутативность

$$(x_1 \circ x_2) = (x_2 \circ x_1).$$

В дальнейшем вместо записи  $\min(x_1, x_2)$  мы часто будем использовать запись  $(x_1 \& x_2)$ , а вместо записи  $\max(x_1, x_2)$  — запись  $(x_1 \vee x_2)$ .

В теории  $k$ -значных функций важную роль играет следующая система функций:

$$\{0, 1, \dots, k-1, I_0(x), I_1(x), \dots, I_{k-1}(x), \min(x_1, x_2), \max(x_1, x_2)\}$$

Напомним, что при  $0 \leq s, t \leq k-1$  выполняется равенство

$$I_t(s) = \begin{cases} k-1 & \text{при } s = t, \\ 0 & \text{при } s \neq t. \end{cases}$$

Кроме того, справедливы следующие равенства:

$$I_s(I_t(x)) = \begin{cases} I_0(x) \vee \dots \vee I_{t-1}(x) \vee I_{t+1}(x) \vee \dots \vee I_{k-1}(x) & \text{при } s = 0, \\ 0 & \text{при } 0 < s < k-1, \\ I_t(x) & \text{при } s = k-1; \end{cases}$$

и выполнены дистрибутивные законы

$$\begin{aligned}(x_1 \vee x_2)x_3 &= (x_1x_3) \vee (x_2x_3), \\ (x_1x_2) \vee x_3 &= (x_1 \vee x_3)(x_2 \vee x_3).\end{aligned}$$

Следующее равенство носит название “исключение чистых вхождений переменной”:

$$x = 1 \cdot I_1(x) \vee 2 \cdot I_2(x) \vee \dots \vee (k-1) \cdot I_{k-1}(x).$$

Правило введения переменной

$$x_1 = x_1(I_0(x_2) \vee I_1(x_2) \vee \dots \vee I_{k-1}(x_2)).$$

Непосредственная простая проверка убеждает в справедливости следующей теоремы.

**Теорема 1 (Теорема о разложении).** Для любой  $n$ -местной функции  $f$  из  $P_k$  выполняется равенство

$$f(x_1, \dots, x_n) = \bigvee_{(\varepsilon_1, \dots, \varepsilon_n) \in E_k^n} I_{\varepsilon_1}(x_1) \& \dots \& I_{\varepsilon_n}(x_n) \& f(\varepsilon_1, \dots, \varepsilon_n).$$

В качестве непосредственного следствия этой теоремы получаем следующее утверждение:

система функций

$$\{0, 1, \dots, k-1, I_0(x), I_1(x), \dots, I_{k-1}(x), \min(x_1, x_2), \max(x_1, x_2)\}$$

полна.

Менее тривиальной, а значит и более содержательной, является следующая теорема.

**Теорема 2.** Система из двух функций  $\bar{x}$  и  $\max(x_1, x_2)$  является полной.

*Доказательство.* Для доказательства теоремы достаточно показать, что функции константы  $0, 1, \dots, k-1$  и функции  $I_0(x), I_1(x), \dots, I_{k-1}(x)$  и  $\min(x_1, x_2)$  выразимы через функции  $\bar{x}$  и  $\max(x_1, x_2)$ .

Для получения констант воспользуемся следующими равенствами:

$$\begin{aligned}x+1 &= \bar{x}, \quad x+2 = \overline{x+1}, \dots, x = (x+(k-1))+1 = \overline{x+(k-1)}, \\ \max(x, x+1, x+2, \dots, x+(k-1)) &= k-1, \\ 0 &= (k-1)+1 = \overline{(k-1)}, \quad 1 = 0+1 = \bar{0}, \dots, k-2 = (k-3)+1 = \overline{(k-3)}.\end{aligned}$$

Для получения функций  $I_0(x), I_1(x), \dots, I_{k-1}(x)$  воспользуемся равенством

$$I_t(x) = \max_{s \neq k-1-t} (x+s)+1 = \overline{\max_{s \neq k-1-t} (x+s)},$$

в верности которого убеждаемся простым рассмотрением двух случаев а)  $x = t$  и б)  $x \neq t$ .

Если ввести в рассмотрение функции  $f_{s,t}(x)$ , заданные равенствами

$$f_{s,t}(x) = \begin{cases} s & \text{при } x = t, \\ 0 & \text{при } x \neq t, \end{cases}$$

то нетрудно убедиться в верности равенства  $f_{s,t}(x) = s + 1 + \max(I_t(x), k - 1 - s)$ .

Кроме того, для любой одноместной функции  $f(x)$  выполняется равенство

$$f(x) = \max(f_{f(0),0}(x), f_{f(1),1}(x), \dots, f_{f(k-1),k-1}(x)).$$

Поэтому получаем, в частности, равенство

$$\sim x = \max(f_{k-1,0}(x), f_{k-2,1}(x), \dots, f_{0,k-1}(x)).$$

Для получения функции  $\min(x_1, x_2)$  можно воспользоваться равенством

$$\min(x_1, x_2) = \sim \max(\sim x_1, \sim x_2).$$

□

Среди  $k$ -значных функций имеются аналоги функции Шеффера, таковой является, например, *функция Вебба*  $V_k(x_1, x_2)$ , заданная равенством

$$V_k(x_1, x_2) = \max(x_1, x_2) + 1 \pmod{k} = \overline{\max(x_1, x_2)} = \overline{(x_1 \vee x_2)}.$$

Полнота системы, состоящей лишь из функции Вебба  $V_k(x_1, x_2)$ , следует из предыдущей теоремы и следующих равенств:

$$\bar{x} = V_k(x, x),$$

$$\max(x_1, x_2) + 1 = V_k(x_1, x_2), \max(x_1, x_2) + 2 = \overline{\max(x_1, x_2) + 1}, \dots$$

$$\max(x_1, x_2) = \max(x_1, x_2) + k = \overline{\max(x_1, x_2) + (k - 1)}.$$

### §3. Полнота систем $k$ -значных функций

Важным вопросом теории  $k$ -значных функций, как и теории булевых функций, является вопрос об “эффективных” необходимых и достаточных условиях полноты системы функций. В случае 2-значных функций исчерпывающий ответ на него, как мы уже знаем, дает теорема Э. Поста.

Прежде всего заметим, что любая бесконечная полная система  $k$ -значных функций содержит *конечную полную подсистему*. В самом деле, пусть  $K$  — бесконечная полная система функций. Тогда функция Вебба  $V(x_1, x_2)$  выражается через некоторую *конечную* подсистему  $K^*$  системы  $K$ . Поэтому

$$P_k = [V(x_1, x_2)] \subseteq [K^*] \subseteq [K] \subseteq P_k.$$

Значит,  $[K^*] = P_k$ , т.е.  $K^*$  — конечная полная подсистема системы  $K$ .

Существуют различные уточнения постановки проблемы полноты. Остановимся прежде всего на алгоритмической формулировке.

*Существует ли алгоритм, позволяющий по произвольной конечной системе  $k$ -значных функций определить, является ли она полной.*

По чисто техническим причинам удобно ввести в рассмотрение функции проектирования, т.е. функции  $I_t^m(x_1, \dots, x_m)$  ( $1 \leq t \leq m$ ), заданные равенством

$$I_t^m(x_1, \dots, x_m) = x_t.$$

Функции проектирования позволяют функцию  $f$ , переменные которой содержатся среди  $x_1, \dots, x_n$ , рассматривать как  $n$ -местную функцию от этих переменных. Следующая теорема устанавливает алгоритмическую разрешимость проблемы полноты для класса  $k$ -значных функций.

**Теорема 1.** *Существует алгоритм, позволяющий по произвольной конечной системе  $k$ -значных функций определить, является ли она полной.*

*Доказательство.* Рассмотрим произвольную конечную систему  $K$   $k$ -значных функций  $f_1, \dots, f_m$ . Без ограничения общности можно считать, что все они зависят от одних и тех же переменных  $x_1, \dots, x_n$ . Напомним, что через  $[K]$  мы обозначаем замыкание системы функций  $K$ .

Через  $[K]_{x_1, \dots, x_n}$  обозначается множество всех функций из  $[K]$ , зависящих лишь от переменных  $x_1, \dots, x_n$ .

Первым шагом будет построение множества  $[K]_{x_1, x_2}$ .

Для этого по индукции построим возрастающую последовательность

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_s \subseteq \dots$$

$k$ -значных функций от переменных  $x_1$  и  $x_2$ .

Полагаем  $K_0 = \emptyset$ .

Предположим, что уже построены множества

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_s.$$

Пусть

$$K_s = \{g_1(x_1, x_2), \dots, g_{s_t}(x_1, x_2)\}.$$

Через  $K'_s$  обозначим множество функций вида

$$f_j(G_1(x_1, x_2), \dots, G_n(x_1, x_2)),$$

где  $1 \leq j \leq m$  и каждая функция  $G_i(x_1, x_2)$  — это либо функция из класса  $K_s$ , либо функция  $I_1^2$ , либо функция  $I_2^2$  (2-местные функции проектирования соответственно на первую или вторую переменную).



Полагаем

$$K_{s+1} = K_s \cup K'_s.$$

Получаем цепочку множеств

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_s \subseteq K_{s+1}.$$

Нетрудно понять, что если  $K_{s+1} = K_s$ , то  $K_{s+2} = K_{s+1}$ ,  $K_{s+3} = K_{s+2}$  и т.д., т.е. цепочка множеств

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_s \subseteq \dots$$

стабилизируется. Можно найти такое  $s^* \leq k^{k^2}$ , что

$$K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{s^*} = K_{s^*+1} = K_{s^*+2} = \dots$$

Нетрудно понять, что

$$K_{s^*} = [f_1, \dots, f_m]_{x_1, x_2},$$

где для произвольного класса  $K$  через  $K_{x_1, x_2}$  обозначено множество всех функций из класса  $K$ , зависящих от двух переменных  $x_1$  и  $x_2$ .

Возможны два случая.

1) Функция Вебба  $V_{x_1, x_2}$  не входит в  $K_{s^*}$ . Так как  $K_{s^*} = [f_1, \dots, f_m]_{x_1, x_2}$ , то функция Вебба  $V_{x_1, x_2}$  не входит и в  $[f_1, \dots, f_m]$ . Поэтому  $[f_1, \dots, f_m] \neq P_k$ , значит, система  $f_1, \dots, f_m$  не является полной.

2) Функция Вебба  $V_{x_1, x_2}$  входит в  $K_{s^*} = [f_1, \dots, f_m]_{x_1, x_2}$ .

Тогда

$$P_k = [V_{x_1, x_2}] \subseteq K_{s^*} \subseteq [f_1, \dots, f_m] \subseteq P_k.$$

Значит,  $[f_1, \dots, f_m] = P_k$ , т.е. система  $k$ -значных функций  $f_1, \dots, f_m$  является полной.  $\square$

Другой подход к вопросу о полноте систем функций можно назвать *описательным*. Он состоит в указании некоторых необходимых и достаточных свойств системы функций  $K$ , обеспечивающих ее полноту.

Пусть  $K$  — произвольный класс функций.

**Определение 1.**  $m$ -местная функция  $g(x_1, \dots, x_m)$  *сохраняет класс функций*  $K$ , если для любых  $m$  функций  $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$  из класса  $K$

$$g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \in K.$$

Для произвольного класса  $K$  обозначим через  $\langle K \rangle$  *множество всех функций, сохраняющих класс*  $K$ . Нетрудно понять, что в  $\langle K \rangle$  входят все функции проектирования  $I_t^m(x_1, \dots, x_m)$  и  $\langle K \rangle$  — *замкнутый класс*, т.е. выполняется равенство  $[\langle K \rangle] = \langle K \rangle$ .

Следующая теорема А.В. Кузнецова о функциональной полноте может рассматриваться как обобщение теоремы Э. Поста на  $k$ -значные функции.



**Теорема 2 (А.В. Кузнецов).** *Можно построить такую конечную систему замкнутых классов в  $P_k$*

$$K_1, K_2, \dots, K_m,$$

*что для любой системы  $K$  функций из  $P_k$  имеет место эквивалентность*

$$K - \text{полная система функций} \iff K \not\subseteq K_1 \& K \not\subseteq K_2 \& \dots \& K \not\subseteq K_m.$$

При построении классов функций  $K_1, \dots, K_m$  особую роль будут играть функции, зависящие лишь от двух переменных  $x_1$  и  $x_2$ .

Это приводит к следующему понятию:

**Определение 2.** *Класс функций  $K$  называется  $n$ -замкнутым, если  $[K]_{x_1, \dots, x_n} \subseteq K$ .*

Если все функции из  $n$ -замкнутого класса  $K$  являются  $n$ -местными, то  $[K]_{x_1, \dots, x_n} = K$ .

В дальнейшем будет полезна следующая простая лемма.

**Лемма 1.** *Если класс  $K$  состоит лишь из 2-местных функций, содержит функции проектирования  $I_1^2$  и  $I_2^2$  и является 2-замкнутым, т.е. выполняется равенство  $[K]_{x_1, x_2} = K$ , то выполнено и равенство*

$$\langle K \rangle_{x_1, x_2} = K.$$

*Доказательство.* Требуется доказать, что при сделанных предположениях 2-местная функция сохраняет класс  $K$  тогда и только тогда, когда она принадлежит этому классу.

Если  $f(x_1, x_2)$ ,  $f_1(x_1, x_2)$  и  $f_2(x_1, x_2)$  — произвольные функции из класса  $K$ , то

$$f(f_1(x_1, x_2), f_2(x_1, x_2)) \in [K]_{x_1, x_2} = K,$$

поэтому  $f(x_1, x_2) \in \langle K \rangle_{x_1, x_2}$ , значит,  $K \subseteq \langle K \rangle_{x_1, x_2}$ .

Для доказательства обратного включения  $\langle K \rangle_{x_1, x_2} \subseteq K$  возьмем функцию  $f(x_1, x_2)$  из класса  $\langle K \rangle_{x_1, x_2}$ . Так как класс  $K$  содержит функции проектирования  $I_1^2$  и  $I_2^2$ , то

$$f(x_1, x_2) = f(I_1^2(x_1, x_2), I_2^2(x_1, x_2)) \in K.$$

□

*Доказательство теоремы А.В. Кузнецова.* Для построения классов функций  $K_1, \dots, K_m$  предварительно построим систему  $S_1, \dots, S_p$  всех различных собственных подмножеств множества  $(P_k)_{x_1, x_2}$  всех 2-местных  $k$ -значных функций, обладающих двумя свойствами:

1) каждое из множеств  $S_j$  ( $1 \leq j \leq p$ ) содержит обе функции проектирования  $I_1^2(x_1, x_2)$  и  $I_2^2(x_1, x_2)$ ;

2) для каждого  $j$  ( $1 \leq j \leq p$ ) выполняется равенство

$$[S_j]_{x_1, x_2} = S_j.$$

Для построения системы  $S_1, \dots, S_p$  среди всех  $2^{k^2} - 2$  различных собственных подмножеств множества  $(P_k)_{x_1, x_2}$  всех 2-местных  $k$ -значных функций выбираем лишь те, которые содержат обе функции проектирования  $I_1^2(x_1, x_2)$  и  $I_2^2(x_1, x_2)$ .

Среди этих подмножеств отбираем те, для которых выполнено свойство 2).

Для этого, как описано выше при доказательстве предыдущей теоремы, для каждого испытываемого класса  $S$  строим множество  $[S]_{x_1, x_2}$  и проверяем выполнимость равенства  $[S]_{x_1, x_2} = S$ .

Для каждого  $j$  ( $1 \leq j \leq p$ ) полагаем

$$S_j^* = \langle S_j \rangle,$$

т.е.  $S_j^*$  состоит из всех функций, сохраняющих класс  $S_j$ .

Из построенных множеств оставляем лишь те, которые не содержатся в других. Получаем систему классов  $K_1, \dots, K_m$ .

Покажем, что для произвольной системы  $K$  функций из  $P_k$  имеет место эквивалентность

$$K \text{ — полная система функций} \iff K \not\subseteq K_1 \text{ \& } K \not\subseteq K_2 \text{ \& } \dots \text{ \& } K \not\subseteq K_m.$$

Пусть  $K$  — полная система функций из  $P_k$ . Предположим, что существует такое  $t$ , что  $K \subseteq K_t$ . Найдется такое  $i$ , что  $K_t = \langle S_i \rangle$ . Как показано выше, из равенства  $K_t = \langle S_i \rangle$  следует, что  $K_t$  — замкнутый класс.

Так как класс  $S_i$  содержит функции проектирования  $I_1^2$  и  $I_2^2$  и является 2-замкнутым, т.е. выполняется равенство  $[S_i]_{x_1, x_2} = S_i$ , то выполнено и равенство

$$(\langle S_i \rangle)_{x_1, x_2} = S_i.$$

Но по построению  $S_i \neq (P_k)_{x_1, x_2}$ , значит,

$$(K_t)_{x_1, x_2} = (\langle S_i \rangle)_{x_1, x_2} \neq (P_k)_{x_1, x_2}.$$

Так как  $K_t$  — замкнутый класс, то

$$[K] \subseteq K_t \neq (P_k).$$

Что противоречит предположению о полноте системы функций  $K$ .

Для доказательства обратного рассмотрим систему функций  $K$ , не содержащуюся ни в одном из классов  $K_1, \dots, K_m$ . Докажем ее полноту.

Предположим противное, т.е. что  $[K] \neq P_k$ . Тогда функция Вебба  $V_k(x_1, x_2)$  не принадлежит  $[K]$ . Полагаем  $S = [K \cup \{I_1^2(x_1, x_2), I_2^2(x_1, x_2)\}]$ . Нетрудно понять, что тогда и  $V_k(x_1, x_2) \notin S$ .

Полагаем  $T = (S)_{x_1, x_2}$ .

Тогда

1) множество  $T$  содержит обе функции проектирования  $I_1^2(x_1, x_2)$  и  $I_2^2(x_1, x_2)$ ;

2) обозначим через  $F$  множество  $K \cup \{I_1^2(x_1, x_2), I_2^2(x_1, x_2)\}$ , тогда  $S = [F]$  и выполняются равенства

$$[T]_{x_1, x_2} = [(S)_{x_1, x_2}]_{x_1, x_2} = [[F]_{x_1, x_2}]_{x_1, x_2} = [F]_{x_1, x_2} = S_{x_1, x_2} = T.$$

Так как  $V_k(x_1, x_2) \notin T$  и  $I_1^2, I_2^2 \in T$ , то найдется такое  $j$  ( $1 \leq j \leq p$ ), что  $T = S_j$ .

Так как  $S = [K \cup \{I_1^2(x_1, x_2), I_2^2(x_1, x_2)\}]$ , то  $S$  — замкнутый класс и он сохраняет класс  $(S)_{x_1, x_2} = T = S_j$ . Поэтому  $S \subseteq S_j^*$ . Класс  $S_j^*$  содержится в одном из классов  $K_1, \dots, K_m$ , кроме того,  $K \subseteq S$ , значит, и класс  $K$  содержится в одном из классов  $K_1, \dots, K_m$ . Полученное противоречие завершает доказательство теоремы.  $\square$

Еще в 30-е годы XX века Д. Слупецкий для  $k \geq 3$  установил критерий полноты системы  $k$ -значных функций. Позже этот критерий был обобщен С.В. Яблонским.

**Теорема 3 (Д. Слупецкий — С.В. Яблонский).** Пусть  $k \geq 3$ . Если система  $K$  функций из  $P_k$  содержит все одноместные функции, то для ее полноты необходимо и достаточно, чтобы в нее входила некоторая функция  $f$ , имеющая не менее двух существенных переменных и принимающая все  $k$  значений.

Традиционно доказательство базируется на ряде лемм.

**Лемма о трех наборах.** Если  $x_1$  — одна из существенных переменных функции  $f(x_1, \dots, x_n)$ , имеющей не менее двух существенных переменных и принимающей не менее трех значений, то найдутся три набора вида

$$\begin{aligned} (a, a_2, \dots, a_n), \\ (b, a_2, \dots, a_n), \\ (a, b_2, \dots, b_n), \end{aligned}$$

на которых функция  $f(x_1, \dots, x_n)$  принимает три различных значения.

*Доказательство.* Пусть функция  $f(x_1, \dots, x_n)$  принимает  $l$  ( $l \geq 3$ ) значений. По предположению  $x_1$  — существенная переменная. Поэтому найдутся такие наборы  $(\alpha, a_2, \dots, a_n)$  и  $(\beta, a_2, \dots, a_n)$ , что

$$f(\alpha, a_2, \dots, a_n) \neq f(\beta, a_2, \dots, a_n).$$

Значит, на наборах

$$(0, a_2, \dots, a_n), (1, a_2, \dots, a_n), \dots, (k-1, a_2, \dots, a_n)$$

функция  $f(x_1, x_2, \dots, x_n)$  принимает не менее двух значений. При этом возможны два случая.

1) Функция  $f(x_1, x_2, \dots, x_n)$  на этих наборах принимает лишь два значения. Тогда третье значение эта функция принимает на некотором наборе вида  $(a, b_2, \dots, b_n)$ . Остается выбрать такие наборы  $(a, a_2, \dots, a_n)$  и  $(b, a_2, \dots, a_n)$ , что

$$f(a, a_2, \dots, a_n) \neq f(b, a_2, \dots, a_n).$$

В этом случае искомые наборы — это  $(a, a_2, \dots, a_n)$ ,  $(b, a_2, \dots, a_n)$  и  $(a, b_2, \dots, b_n)$ .

2) Функция  $f(x_1, x_2, \dots, x_n)$  на этих наборах принимает более двух значений. Воспользуемся тем, что у функции  $f(x_1, x_2, \dots, x_n)$  есть еще одна существенная переменная. Значит, найдется такое  $a$ , что функция  $f(a, x_2, \dots, x_n)$  не является постоянной. Поэтому найдутся такие наборы  $(a, a_2, \dots, a_n)$  и  $(a, b_2, \dots, b_n)$ , что

$$c_1 = f(a, a_2, \dots, a_n) \neq f(a, b_2, \dots, b_n) = c_2.$$

Так как функция  $f(x_1, x_2, \dots, x_n)$  на наборах вида  $(\alpha, a_2, \dots, a_n)$  принимает более двух значений, то найдется такой набор  $(b, a_2, \dots, a_n)$ , что

$$c_3 = f(b, a_2, \dots, a_n) \& c_3 \neq c_1 \& c_3 \neq c_2.$$

И в этом случае  $(a, a_2, \dots, a_n)$ ,  $(b, a_2, \dots, a_n)$  и  $(a, b_2, \dots, b_n)$  — искомые наборы.  $\square$

**Замечание.** Разместим найденные наборы в матрицу

$$\begin{pmatrix} a & a_2 & \dots & a_n \\ b & a_2 & \dots & a_n \\ a & b_2 & \dots & b_n \end{pmatrix}.$$

В каждом столбце полученной матрицы содержится не более двух различных элементов. В первом столбце ровно два различных элемента. Нетрудно понять, что и еще по крайней мере в одном столбце содержатся два различных элемента, так как в противном случае  $(a, a_2, \dots, a_n) = (a, b_2, \dots, b_n)$ , что противоречит неравенству  $f(a, a_2, \dots, a_n) \neq f(a, b_2, \dots, b_n)$ .

**Квадрат** — это система из четырех наборов вида

$$\begin{pmatrix} a_1, & \dots, & a_{i-1}, & a', & a_{i+1}, & \dots, & a_{j-1}, & b', & a_{j+1}, & \dots, & a_n \\ a_1, & \dots, & a_{i-1}, & a', & a_{i+1}, & \dots, & a_{j-1}, & b'', & a_{j+1}, & \dots, & a_n \\ a_1, & \dots, & a_{i-1}, & a'', & a_{i+1}, & \dots, & a_{j-1}, & b', & a_{j+1}, & \dots, & a_n \\ a_1, & \dots, & a_{i-1}, & a'', & a_{i+1}, & \dots, & a_{j-1}, & b'', & a_{j+1}, & \dots, & a_n \end{pmatrix}$$

при условии, что  $a' \neq a''$  и  $b' \neq b''$ . Сами наборы будем называть *вершинами* квадрата.

**Лемма о квадрате.** Если функция  $f$  принимает не менее трех значений и существенно зависит от не менее двух своих переменных, то существует квадрат, в вершинах которого функция принимает не менее двух различных значений, причем одно из этих значений принимается лишь в одной вершине.



*Доказательство.* Для функции  $f$  выполнены условия леммы о трех наборах. Без ограничения общности можно считать, что переменная  $x_1$  является существенной, тогда из доказательства леммы о трех наборах следует, что найдутся три набора вида

$$\begin{aligned}(a, a_2, \dots, a_n), \\ (b, a_2, \dots, a_n), \\ (a, b_2, \dots, b_n),\end{aligned}$$

на которых функция  $f$  принимает три различных значения.

В соответствии с замечанием после леммы о трех наборах разместим эти наборы в матрицу и добавим к ней четвертую строку, чтобы получить матрицу вида

$$\begin{array}{cccccccc} a & a_2 & a_3 & \dots & a_m & a_{m+1} & \dots & a_n \\ b & a_2 & a_3 & \dots & a_m & a_{m+1} & \dots & a_n \\ a & b_2 & b_3 & \dots & b_m & a_{m+1} & \dots & a_n \\ b & b_2 & b_3 & \dots & b_m & a_{m+1} & \dots & a_n \end{array},$$

где выделено наибольшее  $m$  ( $2 \leq m \leq n$ ) такое, что  $a_m \neq b_m$  (такое  $m$  существует).

На этих наборах функция принимает не менее трех различных значений, поэтому одно из значений принимается в точности один раз. Однако указанные наборы могут не составлять квадрат, так как наборы  $(a_2, a_3, \dots, a_{m-1})$  и  $(b_2, b_3, \dots, b_{m-1})$  могут не совпадать.

Вернемся к наборам

$$\begin{aligned}(a, a_2, a_3, \dots, a_n) \\ (b, a_2, a_3, \dots, a_n), \\ (a, b_2, b_3, \dots, b_n)\end{aligned}$$

на которых функция  $f$  принимает три различных значения  $\delta_1, \delta_2$  и  $\delta_3$ .

Рассмотрим последовательность пар наборов вида

$$\begin{array}{cc} (a, a_2, a_3, \dots, a_n) & (a, b_2, a_3, \dots, a_n) \\ (b, a_2, a_3, \dots, a_n) & (b, b_2, a_3, \dots, a_n) \\ (a, b_2, b_3, \dots, a_n) & \dots (a, b_2, b_3, \dots, b_n) \\ (b, b_2, b_3, \dots, a_n) & \dots (b, b_2, b_3, \dots, b_n) \end{array}.$$

Нетрудно заметить, что любые два соседних столбца в полученной матрице размера  $2 \times (n-1)$ , элементами которой являются наборы, либо совпадают, либо образуют квадрат.

Удалив повторяющиеся столбцы, получим последовательность столбцов  $A_1, \dots, A_k$ , каждый из которых состоит из двух наборов.

На элементах столбца  $A_1$  функция  $f$  принимает два различных значения  $\delta_1$  и  $\delta_2$ .



Среди значений, которые функция  $f$  принимает на элементах столбца  $A_k$ , есть  $\delta_3$ . Поэтому на элементах последнего столбца  $A_k$  функция  $f$  не принимает по крайней мере одно из значений  $\delta_1$  и  $\delta_2$ .

Значит, найдутся такие два последовательных столбца  $A_t$  и  $A_{t+1}$ , что на элементах столбца  $A_t$  функция  $f$  принимает два различных значения  $\delta_1$  и  $\delta_2$ , а на элементах столбца  $A_{t+1}$  функция  $f$  хотя бы одно из этих значений не принимает.

Наборы, входящие в столбцы  $A_t$  и  $A_{t+1}$ , образуют искомый квадрат.  $\square$

Если  $K_1, \dots, K_n$  — произвольные непустые подмножества множества  $E_k$ , то их прямое произведение  $K_1 \times \dots \times K_n$  будем называть кубом.

**Лемма 2.** Если функция  $f(x_1, \dots, x_n)$  принимает  $l$  значений, причем  $l \geq 3$ , и существенно зависит от не менее двух своих переменных, то существует такой куб  $K_1 \times \dots \times K_n$ , на элементах которого функция  $f(x_1, \dots, x_n)$  принимает все эти  $l$  значений и при любом  $t$  ( $1 \leq t \leq n$ ) выполняются неравенства  $1 \leq |K_t| \leq l - 1$ .

*Доказательство.* Для функции  $f$  выполнены условия леммы о трех наборах. Без ограничения общности можно считать, что переменная  $x_1$  является существенной, тогда из доказательства леммы о трех наборах следует, что найдутся три набора вида

$$\begin{aligned} &(a, a_2, \dots, a_n), \\ &(b, a_2, \dots, a_n), \\ &(a, b_2, \dots, b_n), \end{aligned}$$

на которых функция  $f$  принимает три различных значения.

Выберем  $l - 3$  набора, на которых функция  $f$  принимает остальные  $l - 3$  значения,

$$(c_1^{(1)}, \dots, c_n^{(1)}), \dots, (c_1^{(l-3)}, \dots, c_n^{(l-3)}).$$

Полагаем

$$\begin{aligned} K_1 &= \{a, b, c_1^{(1)}, \dots, c_1^{(l-3)}\}, \\ K_2 &= \{a_2, b_2, c_2^{(1)}, \dots, c_2^{(l-3)}\}, \\ &\dots \\ K_n &= \{a_n, b_n, c_n^{(1)}, \dots, c_n^{(l-3)}\}. \end{aligned}$$

Нетрудно понять, что в качестве искомого куба можно взять куб  $K_1 \times \dots \times K_n$ .

$\square$

*Доказательство теоремы.* Пусть  $k \geq 3$  и система  $K$  функций из  $P_k$  содержит все одноместные функции.

Покажем, что для ее полноты необходимо, чтобы в нее входила некоторая функция  $f$ , имеющая не менее двух существенных переменных и принимающая все  $k$  значений. Функция  $f$ , имеющая не менее двух существенных переменных и принимающая все  $k$  значений, называется *существенной*.

Предположим, что система  $K$  не содержит существенных функций.

Покажем, что тогда и замыкание  $[K]$  системы  $K$  не содержит существенных функций.

Предположим, что  $f(x_1, \dots, x_n)$  — существенная функция, реализуемая некоторым термом  $t$  над системой  $K$ .

Так как по предположению система  $K$  не содержит существенных функций, то длина терма  $t$  больше единицы. Значит, он имеет вид

$$g(t_1, \dots, t_m),$$

где  $g$  — функция из системы  $K$ , а  $t_1, \dots, t_m$  — подходящие термы. В этом случае функция  $g$  называется *ведущей* или *главной*.

Если функция  $g$  не является одноместной, то она либо не принимает все  $k$  значений и в этом случае терм  $t$  не может реализовать существенную функцию  $f$ , либо функция  $g$  не имеет двух существенных переменных. В последнем случае функцию  $g$  в записи терма  $t$  можно заменить подходящей одноместной функцией из  $K$  (по предположению система  $K$  содержит все одноместные функции) и получить новый терм  $t'$ , реализующий ту же функцию  $f$ , главная функция которого одноместная.

Кроме того, если в терме  $t'$  все функции, не имеющие двух существенных переменных, заменить подходящими одноместными функциями (по предположению все одноместные функции содержатся в системе  $K$ ), то полученный терм, который мы будем продолжать обозначать через  $t$ , реализует ту же функцию  $f$ .

Так как функция  $f$  по предположению существенная, то терм  $t$  имеет вид

$$f_1(f_2(\dots f_p(g(t_1, \dots, t_m)) \dots)),$$

где  $f_1, \dots, f_p$  — одноместные функции,  $t_1, \dots, t_m$  — подходящие термы, а  $g(x_1, \dots, x_m)$  —  $m$ -местная функция из системы  $K$ , имеющая две существенные переменные. Значит, она принимает не более  $k - 1$  значений, поэтому и функция  $f$  принимает не более  $k - 1$  значений, что противоречит предположению о ее существенности.

Для доказательства достаточности предположим, что  $k \geq 3$ , система  $K$  функций из  $P_k$  содержит все одноместные функции и в нее входит некоторая функция  $f$ , имеющая не менее двух существенных переменных и принимающая все  $k$  значений ( $f$  — существенная функция).

Индукцией по  $l$  докажем, что замыкание  $[K]$  системы функций  $K$  содержит все функции из  $P_k$ , принимающие  $l$  значений.

Начнем с  $l = 2$ . Покажем, что замыкание  $[K]$  системы функций  $K$  содержит все функции из  $P_k$ , принимающие 2 значения. В свою очередь для этого достаточно доказать, что замыкание  $[K]$  системы функций  $K$  содержит все функции из  $P_k$ , принимающие два значения 0 и 1.

В самом деле, если нам это удастся сделать, то пусть функция  $g(x_1, \dots, x_n)$  принимает два значения  $\alpha$  и  $\beta$ . Рассмотрим функцию

$$g_0(x_1, \dots, x_n) = \begin{cases} 0, & \text{если } g(x_1, \dots, x_n) = \alpha; \\ 1, & \text{если } g(x_1, \dots, x_n) = \beta. \end{cases}$$

Полагаем

$$\mu_{\alpha, \beta}(x) = \begin{cases} \alpha, & \text{если } x = 0; \\ \beta, & \text{если } x = 1. \end{cases}$$

Так как по условию система  $K$  содержит все одноместные функции, то в ней содержится функция  $\mu_{\alpha, \beta}(x)$ . Поэтому если мы докажем, что функция  $g_0(x_1, \dots, x_n)$  содержится в  $[K]$ , то далее будет достаточно воспользоваться равенством

$$g(x_1, \dots, x_n) = \mu_{\alpha, \beta}(g_0(x_1, \dots, x_n)).$$

Докажем, что в  $[K]$  содержатся две 2-местные функции  $\vee_{0,1}$  и  $\wedge_{0,1}$ , которые на наборах из 0, 1 ведут себя как обычные дизъюнкция и конъюнкция.

По лемме о квадрате найдется такой квадрат

$$\begin{pmatrix} a_1, & \dots, & a_{i-1}, & a', & a_{i+1}, & \dots, & a_{j-1}, & b', & a_{j+1}, & \dots, & a_n \end{pmatrix} \\ \begin{pmatrix} a_1, & \dots, & a_{i-1}, & a', & a_{i+1}, & \dots, & a_{j-1}, & b'', & a_{j+1}, & \dots, & a_n \end{pmatrix} \\ \begin{pmatrix} a_1, & \dots, & a_{i-1}, & a'', & a_{i+1}, & \dots, & a_{j-1}, & b', & a_{j+1}, & \dots, & a_n \end{pmatrix} \\ \begin{pmatrix} a_1, & \dots, & a_{i-1}, & a'', & a_{i+1}, & \dots, & a_{j-1}, & b'', & a_{j+1}, & \dots, & a_n \end{pmatrix},$$

что  $a' \neq a''$ ,  $b' \neq b''$  и на наборах которого функция  $f$  принимает не менее двух значений, причем одно из них, обозначим его через  $\gamma$ , — ровно на одном наборе (в одной вершине).

Рассмотрим функцию  $\varphi(x)$  от одной переменной

$$\varphi(x) = \begin{cases} 0, & \text{если } x = \gamma; \\ 1, & \text{если } x \neq \gamma. \end{cases}$$

По условию теоремы функция  $\varphi(x)$ , как и любая одноместная функция, содержится в  $K$ . Константы 0 и 1, рассматриваемые как одноместные функции, также содержатся в  $K$ , поэтому в замыкание  $[K]$  входит следующая функция  $h(x_1, x_2)$ , определяемая равенством

$$h(x_1, x_2) = \varphi(f(a_1, \dots, a_{i-1}, x_1, a_{i+1}, \dots, a_{j-1}, x_2, a_{j+1}, \dots, a_n)).$$

Функция  $h(x_1, x_2)$  принимает ровно два значения 0 и 1. На квадрате

$$\{(a', b'), (a'', b'), (a', b''), (a'', b'')\}$$

она также принимает ровно два значения 0 и 1, причем значение 0 — только на одном наборе. Обозначим этот набор через  $(a, b)$ .

В системе  $K$  найдутся две одноместные функции  $\psi_1(x)$  и  $\psi_2(x)$  такие, что

$$\begin{aligned}\psi_1(0) &= a, & \psi_1(1) &\in \{a', a''\} \setminus \{a\}, \\ \psi_2(0) &= b, & \psi_2(1) &\in \{b', b''\} \setminus \{b\}.\end{aligned}$$

Полагаясь

$$x_1 \vee_{0,1} x_2 = h(\psi_1(x_1), \psi_2(x_2)).$$

Построенная функция  $\vee_{0,1}$  принадлежит замыканию  $[K]$  и на наборах из 0 и 1 ведет себя как дизъюнкция.

Функция  $J_0(x)$  принадлежит  $K$ , поэтому замыканию  $[K]$  принадлежит и следующая функция:

$$x_1 \wedge_{0,1} x_2 = J_0(J_0(x_1) \vee_{0,1} J_0(x_2)),$$

которая на наборах из 0 и 1 ведет себя как конъюнкция.

Если  $g(x_1, \dots, x_n)$  — произвольная функция, принимающая лишь значения 0 и 1, то ее принадлежность замыканию  $[K]$  следует из следующего равенства:

$$g(x_1, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_n) \in E_k^n} \bigwedge_{0,1} J_{\sigma_1}(x_1) \wedge_{0,1} \dots \wedge_{0,1} J_{\sigma_n}(x_n) \wedge_{0,1} g(\sigma_1, \dots, \sigma_n).$$

Отсюда, как было показано выше, следует, что и произвольная функция  $g(x_1, \dots, x_n)$ , принимающая лишь два значения, принадлежит замыканию  $[K]$ .

Для произвольной функции  $g(x_1, \dots, x_n)$ , принимающей лишь значения  $b_0, \dots, b_{l-1}$  через  $\chi_g(x_1, \dots, x_n)$  обозначим функцию, заданную равенствами

$$\chi_g(x_1, \dots, x_n) = \begin{cases} 0, & \text{если } g(x_1, \dots, x_n) = b_0; \\ 1, & \text{если } g(x_1, \dots, x_n) = b_1; \\ \dots & \\ l-1, & \text{если } g(x_1, \dots, x_n) = b_{l-1}. \end{cases}$$

Ради некоторого сокращения будем весь набор  $(x_1, \dots, x_n)$  обозначать через  $\bar{x}$ . Равенства

$$g(\bar{x}) = (b_0 \wedge J_0(\chi_g(\bar{x}))) \vee (b_1 \wedge J_1(\chi_g(\bar{x}))) \vee \dots \vee (b_{l-1} \wedge J_{l-1}(\chi_g(\bar{x})))$$

и

$$\chi_g(\bar{x}) = (0 \wedge J_0(g(\bar{x}))) \vee (1 \wedge J_1(g(\bar{x}))) \vee \dots \vee ((l-1) \wedge J_{l-1}(g(\bar{x})))$$

показывают, что в дальнейшем говоря о функции  $h$ , принимающей  $l$  значений, без ограничений общности можно считать, что функция  $h$  принимает в качестве значений  $0, 1, \dots, l-1$ .

Предположим, что замыкание  $[K]$  содержит все функции, принимающие не более, чем  $l-1$  значений (при  $l-1 < k$ ).



Пусть функция  $g(x_1, \dots, x_n)$  принимает  $l$  значений  $\gamma_1, \dots, \gamma_l$ . Покажем, что и она принадлежит замыканию  $[K]$ .

Для существенной функции  $f(x_1, \dots, x_n)$ , содержащейся в  $K$ , по лемме о кубе найдется такой куб  $K_1 \times \dots \times K_n$ , что при любом  $t$  ( $1 \leq t \leq n$ )  $1 \leq |K_t| \leq l - 1$  и на наборах этого куба функция  $f(x_1, \dots, x_n)$  принимает эти  $l$  значений  $\gamma_1, \dots, \gamma_l$ .

Для каждого  $t$  ( $1 \leq t \leq n$ ) определим функцию  $\psi_t(x_1, \dots, x_n)$ , принимающую значения в  $K_t$  так, чтобы выполнялось тождество

$$g(x_1, \dots, x_n) = f(\psi_1(x_1, \dots, x_n), \dots, \psi_n(x_1, \dots, x_n)).$$

Так как для каждого  $t$  ( $1 \leq t \leq n$ ) функция  $\psi_t(x_1, \dots, x_n)$  принимает не более  $l - 1$  значений, то по индуктивному предположению все построенные функции  $\psi_1(x_1, \dots, x_n), \dots, \psi_n(x_1, \dots, x_n)$  принадлежат замыканию  $[K]$ . Поэтому и функция  $g(x_1, \dots, x_n)$  принадлежит замыканию  $[K]$ . Это завершает доказательство теоремы.  $\square$

Определенный интерес представляют полные системы функций, состоящие из одной функции. Это приводит к следующему понятию.

**Определение 3.** Если система, состоящая из одной функции  $f$  полна, то функция  $f$  называется функцией Шеффера.

**Теорема 4.** Функция  $f$  является функцией Шеффера тогда и только тогда, когда она порождает все одноместные функции.

*Доказательство.* Если функция  $f$  является функцией Шеффера, то она, конечно, порождает все одноместные функции.

Для доказательства обратного утверждения предположим, что функция  $f$  порождает все одноместные функции.

Покажем, что функция  $f$  является существенной.

Если бы она не принимала некоторое значение  $b$ , то порождаемые ею одноместные функции также не принимали бы это значение. Значит, из этой функции нельзя было бы получить все одноместные функции. Поэтому функция  $f$  принимает все  $k$  значений. Если бы она не содержала двух существенных переменных, то была бы перестановкой, поэтому и все порождаемые ею функции были бы перестановками, а значит, и не включали бы в свой состав всех одноместных функций.  $\square$

В  $P_2$  полиномы Жегалкина образуют полную систему функций. Аналогичный вопрос возникает и для класса  $P_k$  при  $k \geq 3$ . Ответ на него дает следующая теорема, интересная своей связью с теорией чисел и алгеброй. В ней речь идет о представлении функций из  $P_k$  полиномами по  $\text{mod } k$ .

**Теорема 5.** Система  $\{0, 1, 2, \dots, k - 1, \cdot (\text{mod } k), + (\text{mod } k)\}$  полна тогда и только тогда, когда  $k$  — простое число.



*Доказательство.* Если  $k = p$  — простое число, то воспользуемся малой теоремой Ферма: если  $a$  не делится на  $p$ , то  $a^{p-1} \equiv 1 \pmod{p}$ .

Рассмотрим функцию  $\varphi(x) = 1 - x^{p-1} \pmod{p}$ . Тогда  $\varphi(0) = 1$  и  $\varphi(a) = 0$  при  $a \neq 0$ . Значит,  $\varphi(x) = J_0(x)$ .

Далее  $J_t(x) = \varphi(x - t)$ . И остается воспользоваться равенством

$$f(x_1, \dots, x_n) = \sum_{\substack{\text{mod } p \\ (\sigma_1, \dots, \sigma_n) \in E_k^n}} J_{\sigma_1}(x_1) \cdot \dots \cdot J_{\sigma_n}(x_n) \cdot f(\sigma_1, \dots, \sigma_n).$$

Для доказательства обратного предположим, что  $k$  — составное число  $k = k_1 k_2$ ,  $1 < k_1, k_2 < k$ . Покажем, что функция  $J_0(x)$  не представима полиномом. Предположим противное, т.е. что  $J_0(x) = c_0 + c_1 x + \dots + c_t x^t$ . Так как  $J_0(0) = 1$ , то  $c_0 = 1$ . Но  $J_0(k_1) = 0$ , поэтому  $0 = 1 + c_1 k_1 + \dots + c_t (k_1)^t$ . Умножив на  $k_2$ , получим противоречие  $k_2 \equiv 0 \pmod{k}$ . □

Хорошо известно, что если число  $k = p^m$  является степенью простого числа  $p$ , то множество  $E_{p^m}$  может быть наделено структурой конечного поля Галуа  $GF(p^m)$ , т.е. на нем могут быть определены две операции, одну из которых называют сложением и обозначают, например, через  $\oplus$ , а вторую — умножением и обозначают, например, через  $\odot$ , относительно которых множество  $E_{p^m}$  становится полем. Чтобы не усложнять обозначений, будем эти операции обозначать обычным образом через  $+$  и  $\cdot$ , что не приведет к недоразумениям.

Затем для любого натурального числа  $n$  вводится кольцо полиномов  $GF(p^m)[x_1, \dots, x_n]$  от  $n$  переменных  $x_1, \dots, x_n$ , что позволяет поставить вопрос о представимости функций из  $P_k$  полиномами над этим полем. Ответ на этот вопрос положительный, и, хотя он относится уже скорее к алгебре, чем к дискретной математике в понимаемом в пособии не слишком расширительном смысле, представляется уместным по крайней мере коснуться его здесь.

Пусть  $K$  — произвольное поле, а  $p(x)$  — неприводимый полином из  $K[x]$ . Введем в  $K[x]$  отношение эквивалентности  $\equiv_{p(x)}$  — сравнимость полиномов по  $\text{mod } p(x)$ , полагая для произвольных полиномов  $f(x)$  и  $g(x)$  из  $K[x]$ :

$$f(x) \equiv_{p(x)} g(x) \iff \text{найдется такой полином } h(x), \\ \text{что } f(x) - g(x) = p(x)h(x).$$

Нетрудно проверить, что введенное отношение  $\equiv_{p(x)}$  действительно является отношением эквивалентности, т.е. оно рефлексивно, симметрично и транзитивно.

Класс эквивалентности, определяемый полиномом  $f(x)$ , будем обозначать через  $\overline{f(x)}$  или  $\bar{f}$ .

Фактормножество множества  $K[x]$  по отношению эквивалентности  $\equiv_{p(x)}$ , т.е. множество  $\{\overline{f(x)} \mid f(x) \in K[x]\}$  классов эквивалентности, как обычно, обозначаем через  $K[x]/\equiv_{p(x)}$ .

На множестве  $K[x] / \equiv_{p(x)}$  естественным образом определяются операции сложения и умножения

$$\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)}, \quad \overline{f(x)} \cdot \overline{g(x)} = \overline{f(x) \cdot g(x)}$$

и легко проверяется, что относительно этих операций  $K[x] / \equiv_{p(x)}$  является коммутативным кольцом с единицей, причем это справедливо для любого полинома  $p(x)$ .

Заметим, что нулем (нейтральным элементом относительно сложения) в этом кольце является класс  $\bar{0}$ , состоящий из всех полиномов, делящихся на полином  $p(x)$ , а единицей (нейтральным элементом относительно умножения) — класс  $\bar{1}$ .

Если  $p(x)$  — неприводимый полином, то построенное кольцо является полем.

Требуется лишь установить обратимость любого ненулевого элемента этого кольца. Пусть  $\overline{f(x)} \neq \bar{0}$ . Тогда полином  $f(x)$  не делится на полином  $p(x)$ . Так как последний полином неприводим, то единица является наибольшим общим делителем полиномов  $f(x)$  и  $p(x)$ . Поэтому найдутся такие полиномы  $u(x)$  и  $v(x)$ , что

$$1 = f(x)u(x) + p(x)v(x).$$

Переходя к соответствующим классам, получаем

$$\begin{aligned} \bar{1} &= \overline{f(x)u(x) + p(x)v(x)} = \\ &= \overline{f(x)u(x)} + \overline{p(x)v(x)} = \overline{f(x)} \cdot \overline{u(x)} + \overline{p(x)} \cdot \overline{v(x)} = \overline{f(x)} \cdot \overline{u(x)}, \end{aligned}$$

так как  $\overline{p(x)} = \bar{0}$ .

Отображение  $\varphi : a \mapsto \bar{a}$  задает изоморфное вложение исходного поля  $K$  в построенное поле  $K[x] / \equiv_{p(x)}$ . Это позволяет “отождествить” каждый элемент  $a$  поля  $K$  с соответствующим элементом  $\bar{a}$  поля  $K[x] / \equiv_{p(x)}$  — образом элемента  $a$  относительно отображения  $\varphi$  и считать, что

$$K \subseteq K[x] / \equiv_{p(x)}.$$

Для некоторого сокращения обозначим поле  $K[x] / \equiv_{p(x)}$  через  $F$ .

Рассмотрим в поле  $F$  элемент  $\alpha = \bar{x}$ . Пусть исходный полином  $p(x)$  имеет вид

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n.$$

Тогда

$$\begin{aligned} p(\alpha) &= a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = \bar{a}_0 + \bar{a}_1\bar{x} + \bar{a}_2\bar{x}^2 + \dots + \bar{a}_n\bar{x}^n = \\ &= \overline{a_0 + a_1x + a_2x^2 + \dots + a_nx^n} = \overline{p(x)} = \bar{0}. \end{aligned}$$

Т.е. в построенном поле  $F$  элемент  $\alpha = \bar{x}$  является корнем исходного полинома  $p(x)$ .

**Теорема 6.** Для любого поля  $K$  и полинома  $f(x)$  из  $K[x]$  положительной степени существует поле  $F$  такое, что  $K \subseteq F$  и полином  $f(x)$  имеет в поле  $F$  корень.

Для любого поля  $K$  и полинома  $f(x)$  из  $K[x]$  положительной степени существует поле  $\tilde{F}$  такое, что  $K \subseteq \tilde{F}$  и полином  $f(x)$  раскладывается в кольце  $\tilde{F}[x]$  в произведение линейных полиномов.

*Доказательство.* Пусть  $f(x)$  — полином положительной степени из  $K[x]$ . Рассмотрим произвольный неприводимый полином  $p(x)$ , делящий  $f(x)$ , т.е.  $f(x) = p(x)g(x)$ .

По полиному  $p(x)$  построим расширение  $F_1 \supseteq K$ , в котором полином  $p(x)$  имеет корень  $\alpha_1$ . Тогда  $\alpha_1$  — корень полинома  $f(x)$  и в  $F_1[x]$  выполняется равенство

$$f(x) = (x - \alpha_1)f_1(x)$$

для подходящего полинома  $f_1(x)$ . Это завершает доказательство первой части теоремы.

Доказательство второй части теоремы следует из ее первой части.

Пусть  $n$  — степень полинома  $f(x)$ . Если  $n = 1$ , то полагаем  $\tilde{F} = F_1$ .

При  $n > 1$ , отправляясь от поля  $F_1$  и полинома  $f_1(x)$ , строим такое расширение  $F_2 \supseteq F_1 \supseteq K$ , в котором полином  $f_1(x)$  имеет корень  $\alpha_2$ . Тогда в  $F_2[x]$  выполняется равенство

$$f(x) = (x - \alpha_1)(x - \alpha_2)f_2(x)$$

для подходящего полинома  $f_2(x)$ .

Через  $n$  шагов мы построим такое расширение  $F_n \supseteq K$ , что в  $F_n[x]$  выполняется равенство

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

где  $a$  — старший коэффициент полинома  $f(x)$ . □

Покажем, что на любом множестве из  $p^m$  элементов, где  $p$  — простое число, можно ввести структуру поля.

**Теорема 7.** Для произвольного простого числа  $p$  и любого натурального числа  $m$  существует поле из  $p^m$  элементов.

*Доказательство.* Полагаем  $q = p^m$ . Над полем  $Z_p$  вычетов по модулю  $p$  рассмотрим полином  $x^q - x$ . Построим такое расширение  $F \supseteq Z_p$ , что в  $F[x]$  полином  $x^q - x$  раскладывается на линейные множители.

Напомним, что в поле  $F \supseteq Z_p$  для любого элемента  $b$  выполнено равенство  $pb = 0$ , а значит, и равенство  $qb = 0$ .

Обозначим через  $H$  множество всех корней в  $F$  полинома  $x^q - x$ , т.е.

$$H = \{a \mid a \in F \text{ \& } a^q = a\}.$$

Так как производная полинома  $x^q - x$  равна  $-1$ , то все корни этого полинома различны, т.е.  $H$  состоит из  $q = p^m$  элементов.

Покажем, что  $H$  — подполе поля  $F$ .

Для этого установим справедливость в поле  $F$  равенств

$$(a \pm b)^q = a \pm b, \quad (a \cdot b)^q = a \cdot b.$$

Последнее равенство, конечно, сразу следует из равенства  $(a \cdot b)^q = a^q \cdot b^q$ .

Для установления справедливости первого равенства докажем, прежде всего, равенство

$$(a + b)^p = a^p + b^p.$$

Воспользуемся хорошо известным равенством

$$(a + b)^p = \sum_{i=1}^p C_p^i a^i b^{p-i},$$

где  $C_p^i$  — натуральные числа, определяемые равенством

$$\frac{p!}{i!(p-i)!}.$$

Если  $1 \leq i \leq p-1$ , то число  $C_p^i$  делится на  $p$ , так как ни  $i!$ , ни  $(p-i)!$  не делится на  $p$ . Поэтому в сумме только первое и последнее слагаемые могут быть отличны от нуля. Это дает равенство

$$(a + b)^p = a^p + b^p,$$

из которого индукцией по  $t$  получаем равенство

$$(a + b)^{p^t} = a^{p^t} + b^{p^t}.$$

В частности, при  $t = m$  получаем

$$(a + b)^q = a^q + b^q.$$

Если  $p > 2$ , то  $q$  — нечетное число, поэтому получаем

$$(a - b)^q = a^q + (-b)^q = a^q - b^q.$$

При  $p = 2$  достаточно заметить, что  $-a = a$ .

Если  $a$  и  $b$  принадлежат  $H$ , то  $a^q = a$  и  $b^q = b$ . Поэтому

$$(a \pm b)^q = a^q \pm b^q = a \pm b,$$

значит,  $a \pm b \in H$ .

Следовательно,  $H$  — подполе поля  $F$ , состоящее из  $p^m$  элементов.

Так как  $H$  состоит из всех корней полинома  $x^q - x$ , разлагающегося над полем  $F$  в произведение линейных множителей, то справедливо равенство

$$x^q - x = \prod_{a \in H} (x - a).$$

□

Поле из  $q = p^m$  элементов будем обозначать через  $GF(p^m)$  или более кратко —  $F_q$ .

Рассмотрим вопрос о представимости функций, определенных на  $E_k = F_q$ , полиномами.

Покажем, что для произвольной  $n$ -местной функции  $f(x_1, \dots, x_n)$  из  $P_k(n)$  справедлива следующая *интерполяционная формула*

$$f(x_1, \dots, x_n) = \sum_{a_1, \dots, a_n \in F_q} f(a_1, \dots, a_n) \frac{x_1 - x_1^q}{x_1 - a_1} \cdot \frac{x_2 - x_2^q}{x_2 - a_2} \cdot \dots \cdot \frac{x_n - x_n^q}{x_n - a_n}.$$

Для произвольного элемента  $a$  поля  $F_q$  рассмотрим полином

$$\varphi_a(x) = \frac{x - x^q}{x - a} = - \prod_{c \in F_q \setminus \{a\}} (x - c).$$

Очевидно, что при  $b \neq a$   $\varphi_a(b) = 0$ .

Покажем, что  $\varphi_a(a) = 1$ .

Нетрудно понять, что  $\prod_{c \in F_q \setminus \{a\}} (a - c)$  — это *произведение всех ненулевых элементов поля  $F_q$* . Напомним, что для произвольного поля  $F$  через  $F^*$  обозначается множество всех ненулевых элементов этого поля.

Так как

$$x^q - x = \prod_{a \in F_q} (x - a),$$

то

$$x^{q-1} - 1 = \prod_{a \in F_q^*} (x - a),$$

поэтому

$$-1 = \prod_{a \in F_q^*} (-a) = (-1)^{q-1} \prod_{a \in F_q^*} a = \prod_{a \in F_q^*} a.$$

Значит,  $\varphi_a(a) = 1$ .

Поэтому

$$\begin{aligned} \frac{x_1 - x_1^q}{x_1 - a_1} \cdot \frac{x_2 - x_2^q}{x_2 - a_2} \cdot \dots \cdot \frac{x_n - x_n^q}{x_n - a_n} (b_1, b_2, \dots, b_n) &= \\ &= \begin{cases} 1, & \text{если } (b_1, b_2, \dots, b_n) = (a_1, a_2, \dots, a_n); \\ 0, & \text{если } (b_1, b_2, \dots, b_n) \neq (a_1, a_2, \dots, a_n). \end{cases} \end{aligned}$$



Из последнего равенства сразу следует справедливость интерполяционной формулы для произвольной  $n$ -местной функции  $f(x_1, \dots, x_n)$  из  $P_k(n)$ .

Так же как и в случае булевых функций, вводится понятие предполного класса функций.

**Определение 4.** Класс  $K$  функций из  $P_k$  называется **предполным** (максимальным), если он замкнут, отличен от  $P_k$  и для любой функции  $f$  из  $P_k \setminus K$  выполняется равенство  $[K \cup \{f\}] = P_k$ .

В этих терминах доказанная выше теорема А. Кузнецова может быть переформулирована следующим образом:

**Теорема 8.** Для любого  $k$  в  $P_k$  существует лишь конечное число предполных классов  $K_1, \dots, K_{\varphi(k)}$ .

Система функций  $F$  из  $P_k$ , отличная от  $P_k$ , является полной тогда и только тогда, когда она не содержится ни в одном из предполных классов  $K_1, \dots, K_{\varphi(k)}$ .

Как мы уже знаем,  $\varphi(2) = 5$ . Известно, что функция  $\varphi(k)$  растет достаточно быстро, например, как показал С.В. Яблонский,  $\varphi(3) = 18$ ,  $\varphi(4) = 80$ ,  $\varphi(5) = 667$  и  $\varphi(6) = 15237$ .

Установленные выше факты для  $k$ -значных функций в определенной мере свидетельствуют о имеющейся аналогии с булевыми функциями.

В заключение рассмотрим некоторые особенности, присущие  $k$ -значным функциям при  $k \geq 3$ .

Напомним, что для класса  $P_2$  булевых функций Э. Пост установил следующие два фундаментальных результата

- 1) каждый замкнутый класс функций в  $P_2$  имеет конечный базис,
- 2) множество всех замкнутых классов функций в  $P_2$  счетно.

При  $k \geq 3$  в классе  $P_k$  ситуация более сложная.

Во-первых, при  $k \geq 3$  в классе  $P_k$  существуют замкнутые классы, не имеющие базиса.

Во-вторых, при  $k \geq 3$  в классе  $P_k$  существуют замкнутые классы, имеющие счетный базис, но не имеющие конечного базиса.

В-третьих, при  $k \geq 3$  в классе  $P_k$  имеется несчетное множество замкнутых классов.

Для доказательства первого утверждения рассмотрим следующую последовательность функций  $f_0 = 0$ ,

$$f_n(x_1, \dots, x_n) = \begin{cases} 1 & \text{при } x_1 = x_2 = \dots = x_n = 2, \\ 0 & \text{в противном случае.} \end{cases}$$

Обозначим через  $K$  замыкание класса функций  $\{f_0, f_1, f_2, \dots, f_n, \dots\}$ . Из равенства

$$f_i(\dots, f_j(x_1, \dots, x_n), \dots) = 0$$

следует, что класс  $K$  состоит из переменных и всех функций, получаемых из функций системы

$$f_0, f_1, f_2, \dots, f_n, \dots$$

переименованием и отождествлением переменных.

В ходе доказательства нам потребуется равная тождественно нулю функция от произвольного числа переменных. Она может быть получена из функции  $f_0$  введением фиктивных переменных.

Покажем, что класс  $K$  не имеет базиса. Предположим противное. Так как любая функция вида

$$f_n(g_1(x_{i_1}, \dots, x_{i_m}), \dots, g_n(x_{i_1}, \dots, x_{i_s}))$$

равна тождественно нулю, если хотя бы одна из функций  $g_1, \dots, g_n$  отлична от переменной, то в базис могут входить только функции, полученные из функций вида  $f_n(x_1, \dots, x_n)$  переименованием и отождествлением переменных.

Пусть  $n_0$  — наименьшее  $n$  такое, что в базис входят функции, полученные из функций вида  $f_n(x_1, \dots, x_n)$  переименованием переменных; а  $f$  — соответствующая функция из базиса, т.е.  $f(v_1, \dots, v_m) = f_{n_0}(u_1, \dots, u_n)$ . Возможны два случая.

1) Базис класса  $K$ , кроме функции  $f$ , содержит некоторую функцию  $f'$ , получаемую переименованием переменных из некоторой функции  $f_{n_1}$ . По выбору числа  $n_0$  выполняется неравенство  $n_0 \leq n_1$ . Но тогда функция  $f$  может быть получена из функции  $f'$  отождествлением переменных, что противоречит определению базиса.

2) Базис класса  $K$  состоит из единственной функции  $f$ . Так как любая функция вида  $f_{n_0}(\dots, f_{n_0}, \dots)$  равна тождественно нулю, то из единственной функции  $f$  нельзя получить функцию  $f_n$  при  $n > n_0$ .

Полученное противоречие показывает, что в классе  $K$  нет базиса. Несколько сложнее построить пример замкнутого класса со счетным базисом, не имеющего конечного базиса.

Ю.И. Янов и А.А. Мучник ввели в рассмотрение последовательность  $k$ -значных функций

$$f_m(x_1, \dots, x_m) = \begin{cases} 1 & \text{при } x_1 = \dots = x_{n-1} = x_{n+1} = \dots = x_m = 2, x_n = 1, \\ n & n = 1, \dots, m, \\ 0 & \text{в противном случае.} \end{cases}$$

Обозначим через  $K$  замыкание множества функций

$$\{f_2, f_3, \dots, f_n, \dots\}.$$

Покажем, что

$$\{f_2, f_3, \dots, f_n, \dots\}$$

— базис класса  $K$ . Для этого достаточно установить, что ни одна функция  $f_m$  этой системы не может быть выражена через остальные.

Предположим противное. Пусть функция  $f_m(x_1, \dots, x_m)$  задается некоторым термом, ее не содержащим, т.е. выполнено равенство

$$f(x_1, \dots, x_m) = f_s(t_1(f_1, \dots, f_{m-1}, f_{m+1}, \dots, f_p), \dots, t_s(f_1, \dots, f_{m-1}, f_{m+1}, \dots, f_p))$$

Рассмотрим все возможные случаи.

1) Среди термов  $t_1, \dots, t_s$  по крайней мере два отличны от символов переменных. Тогда при любых значениях переменных  $x_1, \dots, x_n$  эти термы принимают значения 0 или 1, поэтому правая часть равенства равна тождественно нулю. Однако функция  $f_m(x_1, \dots, x_m)$  принимает и значение 1. Полученное противоречие показывает, что этот случай невозможен.

2) Среди термов  $t_1, \dots, t_s$  лишь один терм  $t_l$  отличен от символа переменной. Значит, остальные термы — это переменные. Так как общее число термов  $s \geq 2$ , то термы-переменные действительно есть. Пусть терм  $t_k$  — это переменная  $x_r$ .

Рассмотрим следующий набор значений переменных:

$$x_1 = x_2 = \dots = x_{r-1} = x_{r+1} = \dots = x_m = 2, \quad x_r = 1.$$

Так как на этом наборе терм  $t_l$  примет значение 0 или 1, то в правой части два значения отличны от 2, поэтому правая часть равна 0. В то же время на этом наборе левая часть равна 1. Полученное противоречие показывает, что этот случай невозможен.

3) Все термы  $t_1, \dots, t_s$  — это символы переменных. Так как  $m \neq s$  и все переменные функции  $f_m$  являются существенными, то  $s > m$ . Значит, некоторая переменная  $x_p$  входит в правую часть дважды. Тогда на наборе значений переменных

$$x_1 = \dots = x_{p-1} = x_{p+1} = \dots = x_m = 2, \quad x_p = 1$$

левая часть принимает значение 1, а правая — 0.

Тем самым установлено, что

$$\{f_2, f_3, \dots, f_n, \dots\}$$

— базис класса  $K$ . Если бы в классе  $K$  существовал некоторый конечный базис, то некоторая конечная часть множества

$$\{f_2, f_3, \dots, f_n, \dots\}$$

была бы базисом класса  $K$ , что невозможно.

Так как при любом  $k$  множество  $P_k$  счетно, то множество всех его подмножеств, являющихся замкнутыми классами, имеет мощность, не превосходящую мощности континуума.

Остается показать, что при  $k \geq 3$  эта мощность равна мощности континуума.

Рассмотрим построенный выше класс

$$K = \{f_2, f_3, \dots, f_n, \dots\}.$$

Для произвольных двух различных возрастающих последовательностей натуральных чисел  $2 \leq p_1 < p_2 < \dots < p_n < \dots$  и  $2 \leq q_1 < q_2 < \dots < q_n < \dots$

$$[\{f_{p_1}, f_{p_2}, \dots, f_{p_n}, \dots\}] \neq [\{f_{q_1}, f_{q_2}, \dots, f_{q_n}, \dots\}].$$

Поэтому мощность множества всех замкнутых классов в  $P_k$  при  $k \geq 3$  не меньше мощности континуума, а значит, она равна мощности континуума.

## §4. О сложности схем из функциональных элементов

В этом параграфе достаточно кратко рассматриваются некоторые вопросы, связанные со сложностью реализации булевых функций. Базовым понятием будет понятие функционального элемента как некоторого “черного ящика” с набором входных и выходных контактов. Напомним, что схематично функциональный элемент можно представить так:

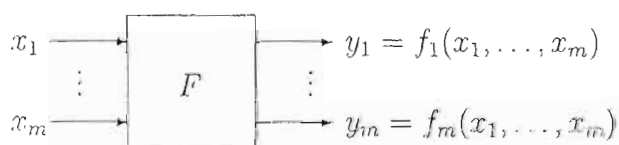


Рис. 1.

Как и ранее, входные контакты этого элемента обозначены через  $x_1, \dots, x_m$ , а выходные — через  $y_1, \dots, y_n$ . Наличие сигнала на входе или выходе интерпретируется как значение 1 соответствующей переменной, а его отсутствие — как значение 0. При подаче сигналов на некоторые входы (при значениях 1 соответствующих входных переменных и значениях 0 остальных входных переменных) на выходах появятся или не появятся сигналы (выходные переменные примут значения 1 или 0). Таким образом, выходные переменные задаются булевыми функциями от входных переменных. Если выходы одних функциональных элементов присоединить к входам некоторых других элементов так, чтобы в описывающем эту схему ориентированном графе не возникло циклов, то полученную схему назовем схемой из функциональных элементов без элементов задержки. Только такие схемы мы и будем рассматривать, называя их просто схемами из функциональных элементов. Так как любой функциональный элемент с  $m$  выходами может быть заменен на  $m$  элементов с одним выходом и теми же входами, что и исходный функциональный элемент, то особый интерес представляют функциональные элементы с одним выходом. Произвольная схема описанного выше типа из таких элементов будет задавать некоторую систему булевых функций — выходы этой схемы описываются булевыми функциями от входных переменных. Если зафиксировать некоторый набор булевых функций  $f_1, \dots, f_m$  и сопоставить им функциональные элементы



$F_1, \dots, F_m$  с соответствующим числом входных переменных, то естественно возникает вопрос, какие булевы функции реализуются схемами из этих элементов и какова для каждой конкретной булевой функции, реализуемой такими схемами, минимальная сложность реализующей ее схемы, понимаемая как общее число функциональных элементов, включенных в схему. Особый интерес представляет случай, когда  $f_1, \dots, f_m$  — полная система булевых функций. В этом случае любую булеву функцию можно реализовать некоторой схемой из функциональных элементов  $F_1, \dots, F_m$ . Мы рассмотрим лишь ставший уже классическим случай схем из функциональных элементов, соответствующих полной системе из трех булевых функций: отрицания  $\neg$ , дизъюнкции  $\vee$  и конъюнкции  $\&$ .

Схема из трех функциональных элементов, соответствующих булевым функциям отрицания  $\neg$ , дизъюнкции  $\vee$  и конъюнкции  $\&$ , описывается ориентированным графом без циклов, в каждую вершину которого входит не более двух ребер, т.е. степень  $d_+(v)$  полузахода каждой его вершины  $v$  не превосходит 2.

Каждой вершине  $v$  степени полузахода 0 ( $d_+(v) = 0$ , ребра не входят в эту вершину), сопоставляется символ некоторой переменной  $x_i$ .

Каждой вершине  $v$  степени полузахода 1 ( $d_+(v) = 1$ , в эту вершину входит лишь одно ребро), сопоставляется отрицание  $\neg$ .

Каждой вершине  $v$  степени полузахода 2 ( $d_+(v) = 2$ , в эту вершину входят два ребра), сопоставляется дизъюнкция  $\vee$  или конъюнкция  $\&$ .

Вершины, из которых не выходят ребра, помечаются для наглядности некоторым символом, например,  $\Diamond$ , им сопоставляются булевы функции от входных переменных, которые называются реализуемыми этой схемой из функциональных элементов. Для задания этих функций нумеруются вершины этого графа таким образом, чтобы для любой дуги номер ее начальной вершины был меньше номера конечной вершины. Затем двигаясь от вершин, помеченных переменными, каждой вершине сопоставляется булева функция, полученная применением расположенной в этой вершине булевой функции (отрицания  $\neg$ , дизъюнкции  $\vee$  или конъюнкции  $\&$ ) к булевым функциям, сопоставленным вершинам, из которых в рассматриваемую вершину ведут ребра.

Вершины схемы  $S$ , помеченные функциями отрицания  $\neg$ , дизъюнкции  $\vee$  или конъюнкции  $\&$ , называются элементами схемы  $S$ .

Число  $L(S)$  элементов схемы  $S$  называется ее сложностью.

Сложностью  $L(f)$  булевой функции  $f$  называется наименьшая сложность  $L(S)$  реализующих эту функцию схем  $S$ .

При изучении схем из функциональных элементов чрезвычайно важную роль играет функция Шеннона  $L(n)$ , определяемая равенством

$$L(n) = \max_{f \in P_2(n)} L(f).$$

Напомним, что через  $P_2(n)$  обозначается множество всех  $n$ -местных булевых функций.



Изучение функции  $L(f)$  для отдельных функций  $f$  представляет собой весьма сложную математическую задачу. Большой прогресс достигнут в исследовании функции Шеннона  $L(n)$ .

Нашей ближайшей целью будет получение некоторых оценок для функции Шеннона  $L(n)$ .

**Теорема 1.** Для любого натурального числа  $n$  выполняется неравенство  $L(n) \leq n2^n$ .

*Доказательство.* Рассмотрим элементарную конъюнкцию

$$x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}.$$

Допустим, что в ней содержится  $k$  вхождений переменных, а значит,  $n - k$  вхождений отрицаний переменных. Заменяя подформулу вида

$$\overline{x_{i_1}} \& \dots \& \overline{x_{i_k}}$$

на равносильную ей

$$\overline{x_{i_1} \vee \dots \vee x_{i_k}},$$

нетрудно построить реализующую эту функцию схему, содержащую один элемент “отрицание”  $\neg$ ,  $k - 1$  элемент “дизъюнкция”  $\vee$  и  $n - k$  элементов “конъюнкция”  $\&$ . Общее число элементов этой схемы  $n$ , поэтому

$$L(x_1^{\varepsilon_1} \& \dots \& x_n^{\varepsilon_n}) \leq n.$$

Аналогичным образом можно доказать, что

$$L(x_1^{\varepsilon_1} \vee \dots \vee x_n^{\varepsilon_n}) \leq n.$$

Рассмотрим произвольную  $n$ -местную булеву функцию  $f$ . Обозначим через  $t$  число наборов, на которых функция  $f$  принимает значение 1. Тогда на  $2^n - t$  наборах она принимает значение 0. Если  $t \leq 2^{n-1}$ , то рассмотрим совершенную дизъюнктивную нормальную форму для  $f$ . В противном случае  $2^n - t \leq 2^{n-1}$  и мы рассмотрим совершенную конъюнктивную нормальную форму для  $f$ .

Для построения реализующей функцию  $f$  схемы, воспользуемся построенными выше  $t$  схемами, реализующими элементарные конъюнкции. Используя дополнительно  $t - 1$  элемент “дизъюнкция”  $\vee$ , построим схему, реализующую функцию  $f$  и содержащую не более  $tn + t - 1$  элементов. Остается заметить, что при сделанных предположениях выполняются неравенства

$$tn + t - 1 \leq (n + 1)2^{n-1} - 1 \leq n2^n.$$

В случае  $t \geq 2^{n-1}$  рассуждение проводится по той же схеме, но с использованием совершенной конъюнктивной нормальной формы для  $f$ .  $\square$

Ставший классическим результат О.Б. Лупанова, полученный с использованием тонких методов синтеза схем, утверждает, что  $L(n) \sim \frac{2^n}{n}$ , т.е.  $\lim_{n \rightarrow \infty} L(n)/\frac{2^n}{n} = 1$ .

Рассмотрим еще одну хорошо известную область применения булевых функций — *контактные схемы* или *схемы из двухпозиционных переключателей*. При одном положении переключателя ток через него проходит, а при другом — нет. Они рассматриваются с середины 30-х годов XX века в качестве математических моделей электрических цепей, составленных из замыкающих и размыкающих контактов. Контакт, “нормальное положение” которого открытое, т.е. при отсутствии сигнала он разомкнут, а при подаче на него сигнала замыкается, естественно назвать “*замыкающим контактом*”, а контакт, “нормальное положение” которого закрытое, т.е. при отсутствии сигнала он замкнут, а при подаче на него сигнала размыкается, естественно назвать “*размыкающим контактом*”. Хотя физическая реализация таких контактов для нас не является важной, заметим, что они могут быть реализованы как электромагнитные реле, на полупроводниковой основе и т.д., в зависимости от области применения, силы используемых токов — в физических установках распространены электромагнитные реле, в компьютерах — полупроводники. Первые работы в этой области относятся к 30-м годам XX века и принадлежат В.И. Шестакову и К. Шеннону.

Математической моделью *контактной схемы* служит граф, ребра которого помечены переменными или их отрицаниями, при этом *переменная соответствует замыкающему контакту, а отрицание переменной — размыкающему*. В графе выделены две вершины  $u$  и  $v$ , называемые *полюсами*. С каждой контактной схемой связана ее *функция проводимости*  $f_{u,v}$ , определяемая естественным образом

- 1) если  $u = v$ , то  $f_{u,v} = 1$ ,
- 2) если  $u \neq v$  и в графе нет цепей, соединяющих  $u$  и  $v$ , то  $f_{u,v} = 0$ ,
- 3) если  $u \neq v$  и в графе есть цепи, соединяющие  $u$  и  $v$ , то для нахождения  $f_{u,v}$  необходимо для каждой цепи, соединяющей  $u$  и  $v$ , взять конъюнкцию меток ее ребер, а затем взять дизъюнкцию по всем таким цепям.

*Сложность* контактной схемы — это число ее ребер. *Две контактные схемы считаются эквивалентными, если их функции проводимости равны*.

*Сложностью* булевой функции называется наименьшая сложность контактных схем, реализующих ее как функцию проводимости.

С контактными схемами связаны две основные задачи

- 1) построение контактной схемы с заданной функцией проводимости,
- 2) построение “наиболее простой” контактной схемы с заданной функцией проводимости.

Решение второй задачи может проходить по следующему плану:

- 1) построение контактной схемы с заданной функцией проводимости,
- 2) упрощение построенной контактной схемы.

Построение контактной схемы по заданию булевой функции, например, по ее дизъюнктивной или конъюнктивной нормальной форме, основано на следую-

щем замечании:

если  $f_{a,b}$  — функция проводимости контактной схемы  $KC_1$  с полюсами  $a$  и  $b$ , а  $f_{c,d}$  — функция проводимости контактной схемы  $KC_2$  с полюсами  $c$  и  $d$ , то  $(f_{a,b} \& f_{c,d})$  — функция проводимости контактной схемы  $KC_{\&}$  с полюсами  $a$  и  $d$ , полученной из схем  $KC_1$  и  $KC_2$  отождествлением полюсов  $b$  и  $c$  (последовательное соединение схем  $KC_1$  и  $KC_2$ , см. рис. 2), а  $(f_{a,b} \vee f_{c,d})$  — функция проводимости контактной схемы  $KC_{\vee}$  с полюсами  $a$  и  $b$ , полученной из схем  $KC_1$  и  $KC_2$  отождествлением полюсов  $a$  с  $c$  и  $b$  с  $d$  (параллельное соединение схем  $KC_1$  и  $KC_2$ , см. рис. 3); построение контактной схемы с функцией проводимости  $\neg f_{a,b}$  очевидно.

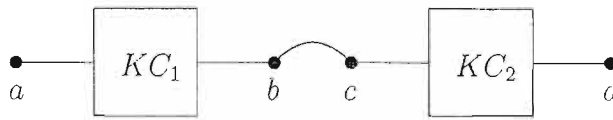


Рис. 2.

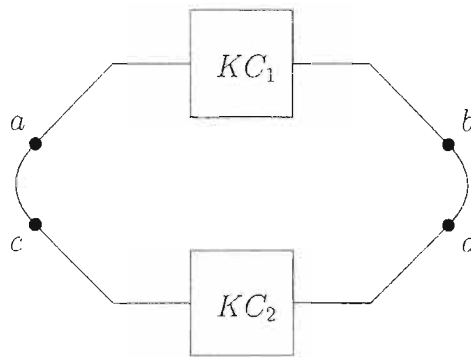


Рис. 3.

Вопрос упрощения контактных схем существенно более сложный. Разработаны методы построения “экономных” схем из функциональных элементов и контактных схем, в основе которых лежит анализ специфики реализуемых функций. Рассмотрим два простых примера.

Первый пример связан с реализацией функции голосования. Рассмотрим лишь случай функции голосования  $f(x, y, z)$  от трех переменных, значение которой равно 1 тогда и только тогда, когда не менее двух переменных принимают значение 1. Совершенная дизъюнктивная нормальная форма этой функции имеет вид

$$(\bar{x} \& y \& z) \vee (x \& \bar{y} \& z) \vee (x \& y \& \bar{z}) \vee (x \& y \& z).$$

Если строить функциональную схему по этой СДНФ, то потребуется 14 элементов. Заметив, что эту СДНФ можно заменить ей эквивалентной формулой (термом) вида

$$(x \& (y \vee z)) \vee (y \& z),$$

получим схему, содержащую лишь 4 функциональных элемента. Соответствующие схема из функциональных элементов и контактная схема изображены на рисунках 4 и 5.

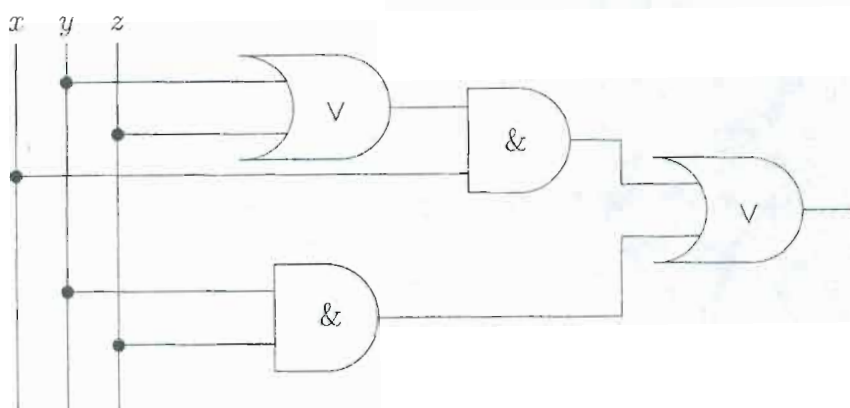


Рис. 4.

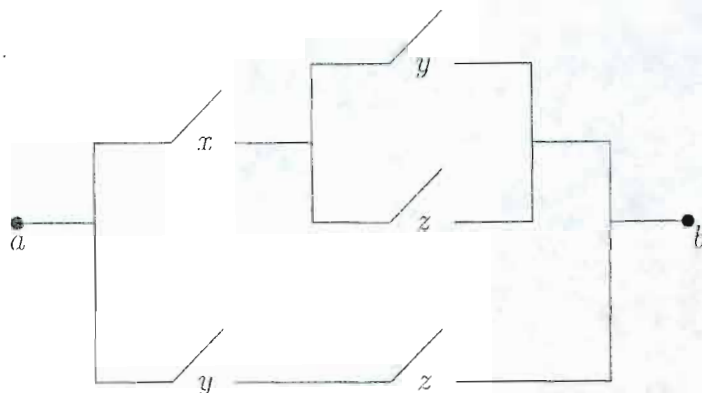


Рис. 5.

Рассмотрим еще один пример, представляющий, на наш взгляд, интерес. На трех выходах из большого помещения требуется расположить выключатели таким образом, чтобы независимо от положения любых двух из них можно было бы третьим выключателем как включать, так и выключать свет в этом помещении. Обозначим выключатели через  $x$ ,  $y$  и  $z$ . Двум возможным положениям выключателя соответствуют два значения соответствующей переменной 0 и 1. Пусть  $f(x, y, z)$  — функция, значение которой на наборе  $(\alpha, \beta, \delta)$  равно 1, если при данном наборе положений выключателей свет горит и 0 в противном случае. Возможная таблица значений функции  $f(x, y, z)$  изображена на рис. 6.

	$x$	$y$	$z$	$f$
1	0	0	0	0
2	0	0	1	1
3	0	1	0	1
4	0	1	1	0
5	1	0	0	1
6	1	0	1	0
7	1	1	0	0
8	1	1	1	1

Рис. 6.

Интересно заметить, что функция  $f(x, y, z)$  является самодвойственной. Совершенная дизъюнктивная нормальная форма функции  $f(x, y, z)$  имеет вид

$$(\bar{x} \& \bar{y} \& z) \vee (\bar{x} \& y \& \bar{z}) \vee (x \& \bar{y} \& \bar{z}) \vee (x \& y \& z). \quad (1)$$

Если строить контактную схему исходя из этой СДНФ, то потребуется 12 переключателей. Соответствующая схема изображена на рис. 7.

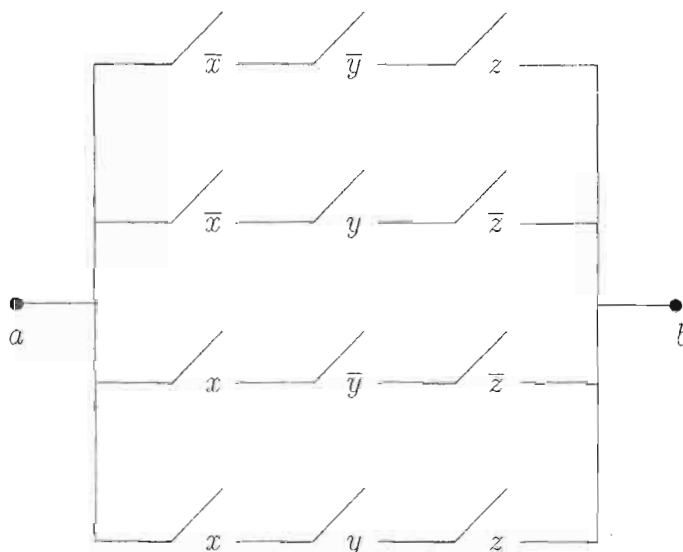


Рис. 7.

Так как формула (1) равносильна формуле  $(\bar{x} \& ((\bar{y} \& z) \vee (y \& \bar{z}))) \vee (x \& ((\bar{y} \& \bar{z}) \vee (y \& z)))$ , то можно построить схему, содержащую 10 переключателей. Пример такой контактной схемы приведен на рис. 8, а на рис. 9 приведена соответствующая схема из функциональных элементов.

Однако можно построить схему, содержащую лишь 8 переключателей. Функция  $f(x, y, z)$  — это частный случай функции четности  $x_1 \oplus x_2 \oplus \dots \oplus x_n$ , для которой Шеннон в работе 1949 г. построил контактную схему, содержащую  $4n-4$  переключателей, а Кардо в 1952 г. доказал, что дальнейшее уменьшение числа переключателей невозможно — схема Шеннона минимальна. Контактная схема Шеннона для 3-местной функции с 8 переключателями изображена на рис. 10.



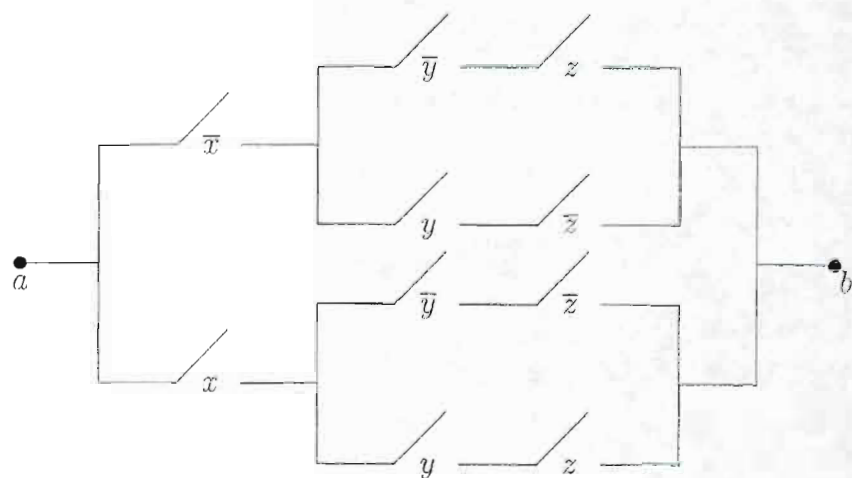


Рис. 8.

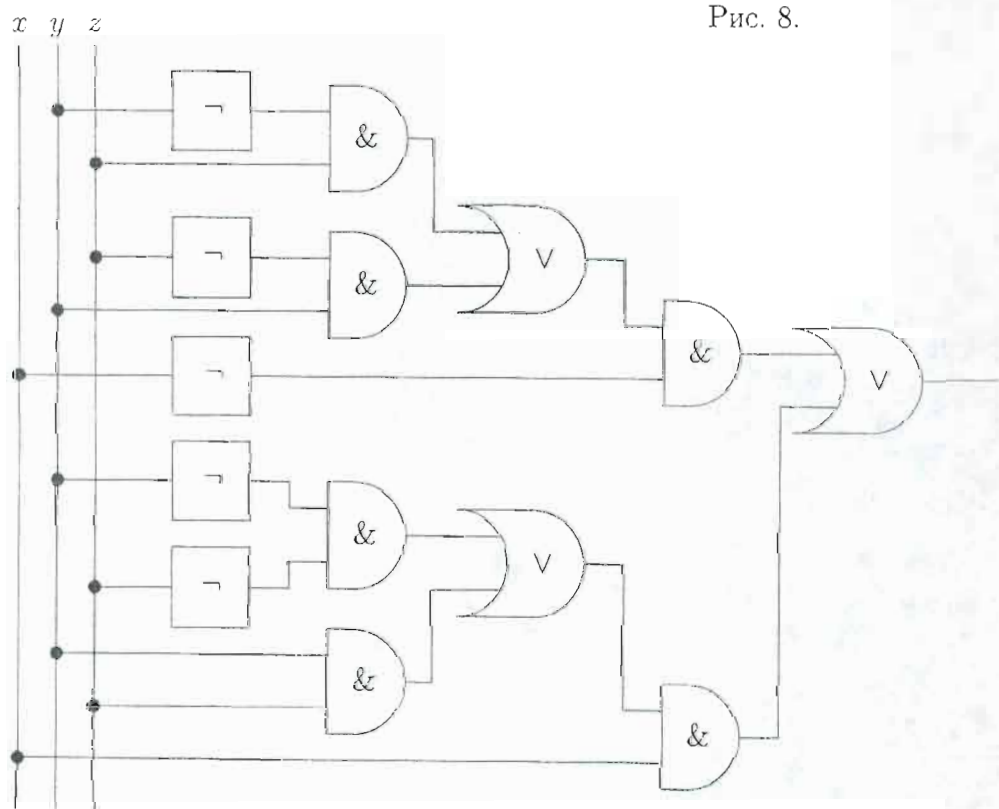


Рис. 9.

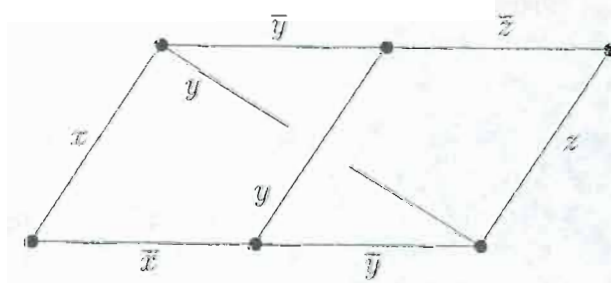


Рис. 10.

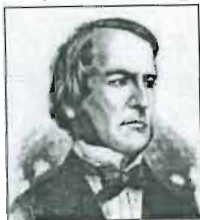
## Биографическая справка

**Адамар Жак Саломон** [Hadamard Jacques Salomon] (1865–1963) —



французский математик, известный своими трудами в теории функций, теории чисел, теории дифференциальных уравнений, механике. В 1896 году он дал первое доказательство асимптотического закона распределения простых чисел. Адамар считается одним из основателей функционального анализа. В теории определителей известно неравенство Адамара для абсолютной величины определителя, следствием которого является равенство, определяющее матрицы Адамара.

**Буль Джордж** [Boole George] (1815–1864) —



английский математик, один из основоположников математической логики. Разработал алгебру логики. Именем Буля названы булевы алгебры — особые алгебраические системы, для элементов которых определены две операции, обладающие специальными свойствами. С именем Буля связаны и булевы функции, с рассмотрения которых начинается пособие.

**Гюйгенс Христиан** [Huygens Christiaan] (1629–1695) —



нидерландский ученый. Изобрел в 1657 году маятниковые часы со спусковым механизмом, установил законы колебания физического маятника, заложил основы теории удара. Открыл кольцо у Сатурна и его спутник Титан. Автор одного из первых трудов по теории вероятностей.

**Дедекинд Юлиус Вильгельм Рихард** [Dedekind Julius Wilhelm Richard] (1831–1916) —



немецкий математик, известный прежде всего трудами по теории алгебраических чисел. Ввел ряд общих концепций, лежащих в основе современной алгебры (дедекиндово кольцо, дедекиндова решетка), в частности ему принадлежит современное определение идеала. Дедекинд — автор одной из первых достаточно строгих теорий действительных чисел, основанной на понятии сечения в упорядоченном поле рациональных чисел.

**Жегалкин Иван Иванович** (1869–1947) —

русский логик и математик, профессор Московского университета, один из создателей советской школы математической логики. В 1927–28 построил логику высказываний в виде арифметики двух чисел — нуля “четное” и единицы “нечетное”, чем достиг большой простоты в решении логических задач. В логике Жегалкина используется не соединительная, а строгая, разделительная дизъюнкция — сложение по модулю 2.

**Кениг Денеш [König Denes] (1884–1944) —**



венгерский математик, в работах которого теория графов впервые появилась как отдельная математическая дисциплина. Сам термин “граф” введен Кенигом в 1936 году.

**Коши Огюстен Луи [Cauchy Augustin Louis] (1789–1857) —**



французский математик, автор свыше 800 трудов по математическому анализу, геометрии, теории чисел и математической физике. Например, в алгебре Коши принадлежит прекрасное доказательство основной теоремы; в теории чисел — доказательство того, что любое натуральное число является  $n$ -угловым числом, или может быть представлено суммой не больше чем  $n$  чисел  $n$ -угловых; в математической физике ему принадлежит обобщенное математическое понятие деформации и упругого напряжения. Особым и доминирующим разделом научного творчества Коши является математический анализ, в частности, проблемы функций комплексного переменного и теория дифференциальных уравнений. С его именем связаны такие понятия, как “определение предела функции по Коши”, “определение непрерывности функции по Коши”, “произведение рядов по Коши”, “признак Коши сходимости рядов”, “метод Коши интегрирования дифференциальных уравнений” и многие другие.

**Лейбниц Готтфрид Вильгельм [Leibniz Gottfried Wilhelm] (1646–1716) —**



немецкий математик, логик и физик. Рекомендовал Петру I организовать академию наук в России. В 1725 году при создании Петербургской Академии наук пользовались планами Лейбница. Он вместе с И. Ньютоном считается создателем дифференциального и интегрального исчисления. В 1684 году в первой своей работе по дифференциальному исчислению Лейбниц ввел понятие и обозначение производной, привел правила дифференцирования суммы, частного, произведения, сложной функции, указал способы определения экстремумов и точек перегиба. В 1686 году он сформулировал понятие и ввел обозначение интеграла, а в 1695 году — формулу определения производной  $n$ -ого порядка произведения. Лейбниц ввел понятие определителя и заложил основы теории определителей. Занимался разработкой универсального языка, пригодного для формулировки различных проблем и лишения неточностей и неопределенностей естественных языков. Создание подобного универсального языка, по замыслу Лейбница, — это первый этап его грандиозной программы создания универсального способа решения различных проблем. Эти идеи Лейбница были реализованы в конце XIX–начале XX вв. Именно Лейбниц ввел такие математические знаки, как  $=$  (равенство) и  $\cdot$  (умножение). В XIX веке идеи Лейбница стали исходной точкой современной математической логики.



**Лукасевич Ян** [Łukasiewicz Jan] (1878–1956) —



польский логик. Построил первую систему многозначной логики. Разработал оригинальный язык для записи логических и алгебраических выражений (бескобочную символику Лукасевича).

**Ньютон Исаак** [Newton Isaac] (1642–1727) —



английский физик и математик, один из создателей дифференциального и интегрального исчисления. Внес большой вклад в разработку основ математического анализа, то есть дал решение таких проблем, как нахождение экстремумов функций, точек перегиба, уравнений касательных к кривым, вычисление длины кривых, площадей, ограниченных кривыми, разработал методы решения простых дифференциальных уравнений (метод касательных или метод Ньютона).

**Парсеваль Марк-Антуан** [Parseval des Chênes Marc-Antoine] (1755–1836) —

французский математик. Основные его труды относились к дифференциальным уравнениям, теории функций действительного переменного. Сформулировал (без доказательства) теорему Парсеваля.

**Паскаль Блез** [Pascal Blaise] (1623–1662) —



французский математик, физик и философ, автор многих теорем эвклидовой геометрии. Паскаль внес вклад в разработку основ теории вероятностей и дифференциального исчисления.

**Пирс Чарлз (Сантьяго) Сандерс** [Peirce Charles (Santiago) Sanders] (1839–1914) —



американский математик и естествоиспытатель. Основные его труды относятся к математической логике (стрелка Пирса), теории вероятностей, алгебре. Основатель семиотики. Ввел (независимо от Г. Фреге) понятие квантора — одного из важнейших понятий современной математической логики.

**Пост Эмиль Леон** [Post Emil Leon] (1897–1954) —



американский математик и логик. Внес значительный вклад в теорию булевых функций, в логику и исчисление высказываний. Им получен ряд фундаментальных результатов в математической логике: одно из наиболее употребительных определений понятий непротиворечивости и полноты формальных систем (исчислений); доказательства функциональной полноты и дедуктивной полноты (в широком и узком смысле) исчисления высказываний; изучение систем многозначной логики с более чем 3 значениями истинности. Посту принадлежит одно из первых (независимое от А.М. Тьюринга) математических определений понятия алгоритма в терминах “абстрактной вычислительной машины” и формулировка основного тезиса теории

алгоритмов о возможности описать любой конкретный алгоритм посредством этого определения. Э. Пост одновременно с А.А. Марковым доказал алгоритмическую неразрешимость проблемы эквивалентности слов для ассоциативных исчислений, что стало одним из первых примеров алгоритмически неразрешимых проблем, сформулированных вне математической логики, и задолго до математического уточнения понятия алгоритма.

**Пэли Раймонд Эдвард Алан Христофер** [Paley Raymond Edward Alan Christopher] (1907–1933) —



американский математик. Основные его труды относятся к теории рядов и интегралов Фурье (теорема Пэли-Винера), ортогональным и гармоническим функциям.

**Стирлинг Джеймс** [Stirling James] (1692–1770) —

шотландский математик, известный своими трудами по теории рядов и исчислению конечных разностей. В 1730 году получил формулу для приближенного вычисления  $n!$ , известную как формула Стирлинга.

**Тьюринг Алан Матисон** [Turing Alan Mathison] (1912–1954) —



английский математик и логик. Ему принадлежит одно из первых математических уточнений интуитивного понятия алгоритма, получившее затем название “машины Тьюринга”. Тьюрингу принадлежит идея универсальной вычислительной машины, воплощенная в современных компьютерах, поэтому он по праву считается одним из создателей современной информатики. Долгие годы было мало из-

вестно еще об одной стороне деятельности Тьюринга — работе в группе по “взлому” шифров немецкой шифровальной машины “Энигма”.

**Уолш Джозеф Леонард** [Walsh Joseph Leonard] (1895–1973) —



американский математик. Основные труды относятся к теории функций и топологии.

**Ферма Пьер** [Fermat Pierre] (1601–1665) —



французский математик, получивший известность благодаря своим трудам по теории чисел. Ферма, как утверждают, занимался чтением математических книг для развлечения и привык писать свои замечания на полях. Он поместил на полях многих книг ряд своих теорем, не заботясь об их доказательстве. Так возникла известная теорема Ферма, не дававшая покоя математикам на протяжении трех с половиной веков. Широкую известность получила и малая теорема Ферма, приведенная им в письме, написанном в 1640 году. Одно из доказательств этой теоремы приведено во второй главе. Ферма наряду с Декартом считают одним из создателей аналити-



ческой геометрии. Он ввел прямоугольную систему координат и доказал, что уравнения первой степени соответствуют прямым, а второй — эллипсам, гиперболам, параболам и кривым, получаемым при сечении конуса плоскостями (конические сечения). Ферма занимался теорией вероятностей, был одним из предшественников Ньютона и Лейбница в области дифференциального и интегрального исчисления.

**Фибоначчи (Леонардо Пизанский)** [Fibonacci (Leonardo Pisano)] (1180–1240) —



итальянский математик, автор “Книги об абакe” (1202), которая несколько веков оставалась основным хранилищем сведений по арифметике и алгебре. Сейчас его имя чаще всего встречается в связи с замечательной числовой последовательностью (см. главу 2).

**Фурье Жан Батист Жозеф** [Fourier Jean Baptiste Joseph] (1768–1830) —



французский математик, заложивший основы теории тригонометрических рядов. Ряды, названные его именем (ряды Фурье), играют большую роль в математике. Фурье занимался математическим анализом, особенно теорией функций, интегральным исчислением и дифференциальными уравнениями.

**Хемминг Ричард Весли** [Hamming Richard Wesley] (1915–1998) —



американский математик, известный своими работами в области теории информации. Его исследования в теории кодирования связаны с кодами определяющими и исправляющими ошибки (коды Хемминга). Им была решена проблема упаковки матриц над конечными полями. Хемминг работал в области теории чисел, интегральных и дифференциальных уравнений. Участвовал в создании одного из

первых компьютеров IBM 650, в исследованиях по производству ядерной бомбы в США (“манхеттонский проект”).

**Холл Маршалл (Младший)** [Hall Marshall Jr] (1910–1990) —



американский математик, хорошо известный своими трудами в теории групп и комбинаторике. В теории групп ему принадлежит решение проблемы Бернсайда. Он показал, что любая конечно порожденная группа, порядок каждого элемента которой делит  $b$ , должна быть конечной. В комбинаторике Холл изучал конечные проективные плоскости и блок-схемы.

**Холл Филип** [Hall Philip] (1904–1982) —



английский математик. Холл занимался исследованиями различных классов групп. В частности, он доказал, что группа порядка  $p^n$ , где  $n > 1$ ,  $p$  — простое число, должна быть простой. Выступал как популяризатор теории групп.

**Цорн Макс Август [Zorn Max August] (1906–1993) —**



немецкий математик. Известность Цорну принесло доказательство “леммы Цорна”, названной его именем. Он рассмотрел теорию полей с точки зрения аксиоматической теории множеств, используя принцип максимума. Кроме теории множеств, Цорн занимался топологией и алгеброй.

**Чёрч Алонзо [Church Alonzo] (1903–1995) —**



американский математик и логик, внесший значительный вклад в основы теории алгоритмов. Чёрч разработал теорию лямбда-исчисления. В статье 1936 года он доказал алгоритмическую неразрешимость исчисления предикатов, решив тем самым одну из самых знаменитых проблем математики начала XX века. Чёрч и Тьюринг показали, что лямбда-исчисления и машины Тьюринга имеют “одинаковые” вычислительные возможности, что привело к формулировке тезиса Чёрча-Тьюринга. Система лямбда-исчислений легла в основу функциональных языков программирования, в частности семейства Лисп (например, Scheme).

**Шеннон Клод Элвуд [Shannon Claude Elwood] (1916–2001) —**



американский инженер и математик. Один из создателей математической теории информации. Внес большой вклад в теорию релейно-контактных схем, математическую теорию связи, кибернетику.

**Шеффер Петер [Schöffner Peter] (до 1430 – около 1503) —**

немецкий типограф и издатель.

**Эйлер Леонард [Euler Leonard] (1707–1783) —**



один из крупнейших математиков XVIII века, родился в Швейцарии, большую часть жизни провел в Петербурге, работая в Петербургской Академии Наук. В списке его трудов более 800 названий. Среди его работ — первые учебники по дифференциальному и интегральному исчислению. В теории чисел он сформулировал проблемы, которые определили направления исследований на десятилетия. Доказал ряд утверждений теории чисел: теоремы Ферма и Эйлера, великую теорему Ферма для показателей 3 и 4. Много работал Эйлер и в области математического анализа. Его имя носит формула  $e^{ix} = \cos x + i \sin x$ , устанавливающая связь тригонометрических и показательной функций, возникающую при использовании комплексных чисел. Разработал теорию логарифмов для комплексных чисел, согласно которой все комплексные числа, кроме нуля, имеют логарифмы, причем каждому числу соответствует бесконечное множество значений логарифма. В геометрии Эйлер положил начало совершенно новой области исследований, выросшей впоследствии в самостоятельную науку — топологию. Имя Эйлера носит формула, связывающая число вершин (V), ребер (P) и граней (Г) выпуклого многогранника:  $V - P + Г = 2$ .

Трудно даже перечислить основные результаты научной деятельности Эйлера. Здесь и геометрия кривых и поверхностей, и первое изложение вариационного исчисления с многочисленными новыми конкретными результатами и многое другое. В 2007 году математический мир отмечает 300-летие со дня рождения Л. Эйлера.

**Яблонский Сергей Всеволодович (1924–1998) —**



российский математик, внесший значительный вклад в дискретную математику, математические вопросы кибернетики и математическую логику. Основные его труды посвящены теории управляющих систем, исследованию функциональных систем с операциями, вопросам контроля и надёжности управляющих систем, изучению алгоритмической сложности синтеза управляющих систем.



# Литература

- [1] Алферов, А.П. *Основы криптографии* / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — М.: Гелиос АРВ, 2002.
- [2] Аршинов, М.Н. *Коды и математика (рассказы о кодировании)* / М.Н. Аршинов, Л.Е. Садовский. — М.: Наука, 1983.
- [3] Биркгоф, Г. *Современная прикладная алгебра* / Г. Биркгоф, Т. Барти. — М.: Мир, 1976.
- [4] Виленкин, Н.Я. *Индукция. Комбинаторика: пособие для учителей* / Н.Я. Виленкин. — М.: Просвещение, 1976.
- [5] Виленкин, Н.Я. *Комбинаторика* / Н.Я. Виленкин. — М.: Наука, 1969.
- [6] Виленкин, Н.Я. *Популярная комбинаторика* / Н.Я. Виленкин. — М.: Наука, 1975.
- [7] Глушков, В.И. *Синтез цифровых автоматов* / В.И. Глушков. — М.: Физматгиз, 1962.
- [8] Грин, Д. *Математические методы анализа алгоритмов* / Д. Грин, Д. Кнут. — М.: Мир, 1987.
- [9] Ежов, И.И. *Элементы комбинаторики* / И.И. Ежов, А.В. Скороход, М.И. Ядренко. — М.: Наука, 1977.
- [10] Емеличев, Е.А. *Лекции по теории графов* / Е.А. Емеличев, О.И. Мельников, В.И. Сарванов, Р.И. Тышкевич. — М.: Наука, 1990.
- [11] Ерусалимский, Я.М. *Дискретная математика: теория, задачи, приложения* / Я.М. Ерусалимский. — 3-е изд. — М.: Вузовская книга, 2000.
- [12] Зыков, А.А. *Основы теории графов* / А.А. Зыков. — М.: Наука, 1987.
- [13] Иванов, Б.Н. *Дискретная математика. Алгоритмы и программы: учеб. пособие* / Б.Н. Иванов. — М.: Лаборатория Базовых Знаний, 2001.
- [14] Камерон, П. *Теория графов, теория кодирования и блок-схемы* / П. Камерон, Дж. ван Линт. — М.: Наука, 1980.

- [15] Коршунов, А.Т. *Основные свойства случайных графов с большим числом вершин и ребер* / А.Д. Коршунов // УМН. — 1985. — Т. 40, вып. 1. — С. 107-173.
- [16] Кострикин, А.И. *Введение в алгебру. Основные структуры алгебры* / А.И. Кострикин. — Т. 3. — М.: Лаборатория Базовых Знаний, 2001.
- [17] Кофман, А. *Введение в прикладную комбинаторику* / А. Кофман. — М.: Наука, 1975.
- [18] Кратко, М.И. *Алгоритмическая неразрешимость одной задачи из теории конечных автоматов* / М.И. Кратко // Алгебра и логика. — Новосибирск, 1964. — Т.3, №2. — С. 33-44.
- [19] Кудрявцев, В.Б. *Введение в теорию конечных автоматов* / В.Б. Кудрявцев, С.В. Алешин, А.С. Подколзин. — М.: Наука, 1985.
- [20] Кузнецов, О.П. *Дискретная математика для инженера* / О.П. Кузнецов. — СПб.; М.; Краснодар: Лань, 2004.
- [21] Кузнецов, О.П. *Дискретная математика для инженера* / О.П. Кузнецов, Г.М. Адельсон-Вельский. — М.: Энергоатом, 1988.
- [22] Кук, Д. *Компьютерная математика* / Д. Кук, Г. Бейз. — М.: Наука, 1990.
- [23] Кучумов, А.И. *Электроника и схемотехника* / А.И. Кучумов. — М.: Гелиос АРВ, 2004.
- [24] Лавров, И.А. *Задачи по теории множеств, математической логике и теории алгоритмов* / И.А. Лавров, Л.Л. Максимова. — М.: Наука, 1975.
- [25] Лаллеман, Ж. *Полугруппы и комбинаторные приложения* / Ж. Лаллеман. — М.: Мир, 1985.
- [26] Липский, В.В. *Комбинаторика для программистов* / В.В. Липский. — М.: Мир, 1973.
- [27] Логачев, О.А. *Булевы функции в теории кодирования и криптографии* / О.А. Логачев, А.А. Сальников, В.В. Яценко. — М.: Изд-во МЦНМО, 2004.
- [28] Марков, Ал.Ал. *Введение в теорию кодирования* / Ал.Ал. Марков. — М.: Наука, 1982.
- [29] Матиясевич, Ю.В. *Диофантовы множества* / Матиясевич Ю.В. // УМК. — Т.22, №5. — 1972. — С. 185-222.
- [30] Мещеряков, М.В. *Избранные лекции по дискретной математике* / М.В. Мещеряков. — Саранск: Изд-во Мордов. ун-та, 2003.



- [31] Новиков, Ф.А. *Дискретная математика для программистов* / Ф.А. Новиков. — СПб.: Питер, 2001.
- [32] Оре, О. *Теория графов* / О. Оре. — М.: Наука, 1980.
- [33] Пентус, А.Е. *Теория формальных языков* / А.Е. Пентус, М.Р. Пентус. — М.: Изд-во МГУ, 2004.
- [34] Прасолов, В.В. *Элементы комбинаторной и дифференциальной топологии* / В.В. Прасолов. — М.: МЦНМО, 2004.
- [35] Редкин, Н.П. *Дискретная математика* / Н.П. Редкин. — СПб.; М.; Краснодар: Лань, 2003.
- [36] Рейнгольд, Э. *Комбинаторные алгоритмы: теория и практика* / Э. Рейнгольд, Ю. Нивергельт, Н. Део. — М.: Мир, 1980.
- [37] Рингель, Г. *Теорема о раскраске карт* / Г. Рингель. — М.: Мир, 1977.
- [38] Риордан, Дж. *Введение в комбинаторный анализ* / Дж. Риордан. — М.: ИЛ, 1963.
- [39] Риордан, Дж. *Комбинаторные тождества* / Дж. Риордан. — М.: Наука, 1982.
- [40] Саломая, А. *Жемчужины теории формальных языков* / А. Саломая. — М.: Мир, 1996.
- [41] Сачков, В.Н. *Введение в комбинаторные методы дискретной математики* / В.Н. Сачков. — М.: Наука, 1982.
- [42] Скопенков, А.Б. *Вокруг критерия Куратовского планарности графов* / А.Б. Скопенков // Математическое просвещение. — Третья серия, вып. 9. — М.: МЦНМО, 2005. — С. 116–129.
- [43] Соколов, В.А. *Формальные языки и грамматики* / В.А. Соколов. — Ярославль: ЯрГУ, 1998.
- [44] Тараканов, В.Е. *Комбинаторные задачи и  $(0,1)$ -матрицы* / В.Е. Тараканов. — М.: Наука, 1985.
- [45] Трахтенброт, Б.А. *Конечные автоматы* / Б.А. Трахтенброт, Я.М. Барздинь. — М.: Наука, 1970.
- [46] Фалевич, Б.Я. *Комбинаторика. Элементы теории графов: учебное пособие* / Б.Я. Фалевич. — Рыбинск: Изд-во РАТИ, 1993.
- [47] Фомичев, В.М. *Дискретная математика и криптология* / В.М. Фомичев. — М.: ДИАЛОГ-МИФИ, 2003.

- [48] Харари, Ф. *Теория графов* / Ф. Харари. — М.: Мир, 1973.
- [49] Холл, М. *Комбинаторика* / М. Холл. — М.: Наука, 1970.
- [50] Хопкрофт, Дж. *Введение в теорию автоматов, языков и вычислений* / Дж. Хопкрофт, Р. Мотвани, Дж. Ульман. — М.: Издательский дом "Вильямс", 2002.
- [51] Эвнин, А.Ю. *Дискретная математика: Конспект лекций* / А.Ю. Эвнин. — Челябинск: Изд-во ЮУрГУ, 1998.
- [52] Яблонский, С.В. *Введение в дискретную математику* / С.В. Яблонский. — М.: Наука, 1986.
- [53] Яблонский, С.В. *Функции алгебры логики и классы Поста* / С.В. Яблонский, Г.П. Гаврилов, В.Б. Кудрявцев. — М.: Наука, 1966.
- [54] Euler, L. *The Königsberg bridges* / L. Euler // Sci. Amer. — 1953. — V 18. — P. 66–70.
- [55] Post, E. *Intoduction to a general theory of elementary propositions* / E. Post // Amer. J. Math. — 1921. — Vol. 43.
- [56] Post, E. *Two-valued iterative systems* / E. Post. — 1941.