

*М.Холл*

## **КОМБИНАТОРИКА**

ИЗДАТЕЛЬСТВО «МИР» Москва 1970

Известный американский математик М. Холл уже знаком советскому читателю по изданным в русском переводе книгам — «Теория групп» (ИЛ, 1962) и «Комбинаторный анализ» (ИЛ, 1963). Настоящая книга является наиболее полным изданием в области комбинаторного анализа. Она состоит из трех основных частей: проблемы перечисления, теоремы выбора и связанные с ними вопросы и проблемы существования и построения блок-схем. Книга написана на высоком научном уровне и освещает самые новейшие достижения в области комбинаторики.

Она доступна весьма широкому кругу читателей и, несомненно, заинтересует математикой различных специальностей.

### **ОГЛАВЛЕНИЕ**

|   |           |
|---|-----------|
| Предисловие редактора перевода                                    | 5         |
| Предисловие   | 7         |
| <b>Глава 1. Перестановки и сочетания</b>                          | <b>9</b>  |
| 1.1. Определения  | 9         |
| 1.2. Приложения к теории вероятностей                             | 13        |
| Задачи  | 16        |
| <b>Глава 2. Формулы обращения</b>                                 | <b>18</b> |
| 2.1. Принцип включения и исключения. Обращение Мёбиуса            | 18        |
| 2.2. Частично упорядоченные множества и их функции Мёбиуса        | 26        |
| Задачи  | 32        |
| <b>Глава 3. Производящие функции и рекуррентные соотношения</b>   | <b>33</b> |
| 3.1. Правила и свойства   | 33        |
| 3.2. Комбинаторные задачи   | 37        |
| Задачи  | 42        |
| <b>Глава 4. Разбиения</b>   | <b>45</b> |
| 4.1. Разбиения. Тождества и арифметические свойства               | 45        |
| 4.2. Асимптотические свойства $p(n)$                              | 59        |
| Задачи  | 63        |
| <b>Глава 5. Системы различных представителей</b>                  | <b>64</b> |
| 5.1. Теоремы Ф. Холла и Д. Кёнига                                 | 64        |
| Задачи  | 78        |
| <b>Глава 6. Теорема Рамсея</b>                                    | <b>79</b> |
| 6.1. Формулировка и доказательство теоремы                        | 79        |
| 6.2. Одно приложение теоремы Рамсея                               | 81        |
| Задачи  | 83        |
| <b>Глава 7. Некоторые экстремальные задачи</b>                    | <b>85</b> |
| 7.1. Задача о назначениях   | 85        |
| 7.2. Теорема Дилуорса   | 90        |
| Задачи  | 94        |
| <b>Глава 8. Выпуклые пространства и линейное программирование</b> | <b>95</b> |

|  |            |
|--|------------|
| 8.1. Выпуклые пространства. Выпуклые конусы и двойственные им пространства | 95         |
| 8.2. Линейные неравенства  | 102        |
| 8.3. Линейное программирование. Симплексный метод                          | 110        |
| <b>Глава 9. Графические методы. Последовательности де Брёйна</b>           | <b>128</b> |
| 9.1. Полные циклы  | 128        |
| 9.2. Теоремы о графах  | 130        |
| 9.3. Доказательство теоремы де Брёйна                                      | 134        |
| <b>Глава 10. Блок-схемы</b>  | <b>140</b> |
| 10.1. Предварительное обсуждение   | 140        |
| 10.2. Элементарные теоремы о блок-схемах                                   | 144        |
| 10.3. Теорема Брука — Райзера — Човла                                      | 149        |
| 10.4. Формулировка теоремы Хассе — Минковского. Приложения                 | 155        |
| <b>Глава 11. Разностные множества</b>                                      | <b>167</b> |
| 11.1. Примеры и определения  | 167        |
| 11.2. Конечные поля  | 172        |
| 11.3. Теорема Зингера  | 178        |
| 11.4. Теорема о множителе  | 183        |
| 11.5. Разностные множества в группах общего вида                           | 189        |
| 11.6. Некоторые семейства разностных множеств                              | 196        |
| <b>Глава 12. Конечные геометрии</b>  | <b>230</b> |
| 12.1. Основания  | 230        |
| 12.2. Конечные геометрии как блок-схемы                                    | 235        |
| 12.3. Конечные плоскости   | 238        |
| 12.4. Некоторые типы конечных плоскостей                                   | 248        |
| <b>Глава 13. Ортогональные латинские квадраты</b>                          | <b>261</b> |
| 13.1. Ортогональность и ортогональные таблицы                              | 261        |
| 13.2. Основные теоремы   | 263        |
| 13.3. Построение ортогональных квадратов.                                  | 269        |
| 13.4. Опровержение предположения Эйлера                                    | 277        |
| <b>Глава 14. Матрицы Адамара</b>   | <b>283</b> |
| 14.1. Конструкции Пэли   | 283        |
| 14.2. Метод Уильямсона   | 299        |
| 14.3. Три новых метода   | 305        |
| <b>Глава 15. Общие методы построения блок-схем</b>                         | <b>308</b> |
| 15.1. Методы построения  | 308        |
| 15.2. Основные определения. Теоремы Ханани                                 | 308        |
| 15.3. Прямые методы построения   | 318        |
| 15.4. Системы троек  | 327        |
| 15.5. Блок-схемы с $k > 3$   | 343        |
| <b>Глава 16. Теоремы о пополнении и вложении</b>                           | <b>348</b> |
| 16.1. Метод Коннора  | 348        |
| 16.2. Коположительные и вполне положительные квадратичные формы            | 365        |
| 16.3. Рациональные пополнения матриц инцидентности                         | 378        |

|   |               |
|---|---------------|
| 16.4. Целые решения уравнений инцидентности   | 389           |
| <i>Приложение I.</i> Уравновешенные неполные блок-схемы с числом повторений каждого элемента от 3 до 15 | 398           |
| <i>Приложение II.</i> Матрицы Адамара типа Уильямсона   | 410           |
| Библиография  | 413           |
| Предметный указатель  | 419           |
| Предметный указатель  |               |
| Автоморфизм блок-схемы  | 167           |
| Адамара матрица   | 283           |
| Аксиомы проективной геометрии   | 230           |
| — плоскости   | 238           |
| Аффинное пространство   | 235           |
| База  | 319           |
| Базисная точка  | 169           |
| Биномиальный коэффициент  | 10, 12        |
| Блок  | 65            |
| — критический   | 66            |
| Блок-схема  | 140, 309      |
| — дополнительная  | 347           |
| — остаточная  | 144           |
| — производная   | 143           |
| — разрешимая  | 274           |
| — с делимостью на группы  | 275           |
| — связь с ортогональными таблицами  | 275, 276      |
| — симметричная  | 143           |
| — уравновешенная относительно пар элементов   | 271           |
| — неполная  | 140           |
| — центрально разрешимая   | 312           |
| — циклическая   | 168           |
| де Брейна последовательности  | 128           |
| де Брейна теорема   | 136           |
| Брука теорема   | 190           |
| Брука — Райзера теорема   | 241           |
| Брука — Райзера — Човла теорема   | 149           |
| Бхаттачария теорема   | 337           |
| Веблена — Веддербёрна система   | 250           |
| Веддербёрна теорема   | 234           |
| Ведущий главный минор   | 159           |
| $m$ -вершина  | 131           |
| Витта теорема   | 381           |
| Включения и исключения принцип (метод)  | 18, 19        |
| Вполне положительная квадратичная форма   | 367           |
| Выделенные блоки  | 312           |
| Выпуклая оболочка множества   | 81            |
| Выпуклое множество  | 95            |
| — пространство  | 95            |
| — тело  | 81, 95        |
| Выпуклый конус  | 97            |
| Галуа поле  | 175           |
| Гаусса — Якоби тождество  | 53            |
| Гиперплоскость  | 96, 179, 234  |
| Голоморф группы   | 198           |
| Границная гиперплоскость  | 96            |
| Граф  | 129           |
| 2-граф  | 135           |
| Групповое кольцо  | 191           |
| — разностное множество  | 170           |
| Гуда теорема  | 134           |
| Дважды связанные блоки  | 356           |
| Двойственное пространство   | 101           |
| Двойственности теорема  | 105           |
| Двойственные задачи линейного программирования  | 105, 110, 111 |
| Двойственный граф   | 135           |
| Дезарга теорема   | 231           |
| Дезаргова плоскость   | 233           |
| Диаграммы разбиения   | 48, 50        |
| Дилуорса теорема  | 90            |
| Дирихле производящая функция  | 43            |
| Дзета-функция   | 29            |
| Дополнение блок-схемы   | 347           |
| Допустимость задачи линейного программирования  | 105, 111      |
| Евклидово пространство  | 95            |
| Задача о беспорядках  | 19            |

- — встречах 20
- — гостях 24
- — кёнигсбергских мостах 133
- — назначениях 85, 108—109
- — супружеских парах 24
- — школьницах 335
- Замыкание множества 96
- Зингера теорема 179
- Зингеровы разностные множества 196
- Изоморфные блок-схемы 167
- Инцидентности матрица 141
  - отношение 230
  - система 140
- Йонсена теорема 388
- Квадратичный вычет 155
  - закон взаимности 156
  - невычет 155
- Кёнига теорема 72
- Киркмана задача 335, 336
- Класс разности 321
- Конгруэнтность 381
- Конечная геометрия 230
- Конечное поле 172
- Коннора метод 349
- Конфигурация 231
- Коположительная квадратичная форма 367
  - — тест для проверки 378
- Кососимметрического типа матрица 290
- Лангранжа теорема 151
- Латинский квадрат 74
  - прямоугольник 73, 74
- Лежандра символ 156
- Линейное программирование 104, 105
- Линейно упорядоченное множество 27
- Линия в матрице 72
- Локально конечное частично упорядоченное множество 27
- Макнейша теорема 263
- Манна теорема 267
- Матрица инцидентности 141
- кососимметрического типа 290
- H*-матрица см. Адамара матрица Мёбиуса функция 21
- Множитель разностного множества 183, 184, 190
- Модулярность 231
- Недезаргова плоскость 233
- Независимые элементы 91
- Неприводимый полином 175
- Несравнимые элементы 90
- Нормализованная матрица Адамара 283
- Норма точки 95
- Общих представителей система 75
- Опорная гиперплоскость 96
- Опорное решение 119
- Оптимальное назначение 85
- Орбита 319
- Ориентированный граф 129
- Ортогональная таблица 262
- Ортогональные векторы 262
  - латинские квадраты 244
  - матрицы 261
- Осевое преобразование 115, 116
- Оси правило выбора 120
- Основное матричное соотношение 144
- Остаточная блок-схема 144
- Отделяющая гиперплоскость 96
- Паппа теорема 231
- Параллельное множество трансверсалей 310
- Параллельные блоки 243
- Первообразный элемент 177
- Перестановка 9, 10
- Петля 129
- Поле 172
- Полиномиальный коэффициент 13
- Полный цикл 128
- Полуполе 254
- Порядок конечной проективной плоскости 241
- Почти-поле 253

- Представление квадратичной формы 381  
Примитивный корень (первообразный элемент) 177  
«Принцип ящиков» 174  
Проективная геометрия 178, 230  
Производная блок-схема 143  
Производящая функция 33  
— экспоненциальная 34  
Прямая сумма матриц 383  
— полей Галуа 227  
Прямое произведение матриц 288  
Путь 129  
Равноблочная компонента 271  
Разбиения целого числа 45, 48, 50  
— арифметический свойства 56  
Разбиения целого числа производящая функция 49  
Различных представителей системы 64, 66  
— алгоритм нахождения 70, 71  
Размерность проективного пространства 230  
 $(v, k, \lambda)$ -разностное множество 168  
Разностных множеств типы 196, 197  
Разрешимая блок-схема 274  
Райзера теорема 146  
Рамсея теорема 79  
Свободное множество блоков 271  
Свойство «здоровой наследственности» 334  
— «незддоровой наследственности» 334  
Связанные блоки 356  
Связный граф 129  
Символ норменного вычета Гильберта 158  
— Хассе 159  
Симметричная блок-схема 143  
Симплексный метод 110, 119  
 $T$ -система (трансверсальная система) 309  
Система троек 327  
Скалярное произведение 100  
Смешанная разность 321  
Сопряженные разбиения 48  
Сочетание 9, 11  
Сравнимые элементы 90  
Стирлинга числа второго рода 42  
— первого рода 42  
Строго зависимое подмножество 93  
Структурная матрица  $S_t$  352  
Тактическая конфигурация 140  
Тернар 249  
Тернарная операция 249  
Трансверсальная система 309  
Уильямсона метод 299  
Уравновешенная неполная блок-схема 140  
Условие С 65, 69  
Фаркаша теорема 102  
Ферма теорема о классах вычетов 174  
Фибоначчи числа 42  
Фишера неравенство 144  
Формула обращения Мёбиуса 22  
Ханани теорема 337  
Характер 289  
Характеристическая матрица блоков 350  
Характеристический полином рекуррентного соотношения 35, 37  
Хассе символ 159  
Хассе—Минковского теорема 160  
Холла системы 251  
Холла Ф. теорема 65  
Хорна форма 376  
Центр блок-схемы 312  
Центральная разрешимость блок-схем 312  
Цепь 26  
Цикл 128, 129  
Циклическая блок-схема 168  
Циклические последовательности 22  
Циклическое разностное множество 168

- Частично упорядоченное множество  
26
- Чистая разность 321
- Штейнера система троек 328
- — — метод построения Мура 330
- Эйлера предположение 265, 277
- Эйлера теорема 131
- — обобщение см. Гуда теорема
- Эйлера тождество 50
- Эквивалентность матриц Адамара  
283
- ортогональных таблиц 263
- Экстремальная точка 96
- — выпуклого конуса 97
- Якоби тождество 55

MARSHALL HALL, JR.

*California Institute of Technology*

---

# COMBINATORIAL THEORY

---



BLAISDELL PUBLISHING COMPANY  
Waltham (Massachusetts) · Toronto · London

1967

## Предисловие редактора перевода

„Комбинаторика“ М. Холла занимает особое место среди вышедших за последние годы на русском языке монографий зарубежных авторов, посвященных комбинаторике. Если „Введение в комбинаторный анализ“ Дж. Риордана содержит довольно полное изложение методов решения перечислительных задач, а в „Комбинаторной математике“ Г. Дж. Райзера в очень хорошем изложении представлены разнообразные, но лишь самые основные, принципиальные стороны комбинаторной теории, то книга М. Холла характерна, прежде всего, тем, что в ней весьма подробно и на высоком математическом уровне рассматриваются сложные и красивые вопросы существования и построения блок-схем, матриц Адамара и латинских квадратов<sup>1)</sup>.

Комбинаторные задачи построения привлекают к себе внимание уже давно (можно вспомнить, например, знаменитую задачу Эйлера о 36 офицерах), но их большое прикладное значение выяснилось сравнительно недавно и явилось, очевидно, дополнительным мощным стимулом, вызвавшим все возрастающее количество комбинаторных исследований, посвященных существованию и построению блок-схем. В книге М. Холла, одного из ярких представителей именно этого направления комбинаторики, представлены многие из полученных (в том числе и самим автором) в недавнее время интересных результатов, таких, как опровержение предположения Эйлера, построение матриц Адамара, построение целого ряда систем разностных множеств и др. Этим вопро-

<sup>1)</sup> Вышедший на русском языке в 1963 г. обзор М. Холла „Комбинаторный анализ“ можно рассматривать как предварительный эскиз настоящей книги..

сам посвящены гл. 10—16, занимающие две трети книги. Другим сторонам комбинаторной теории уделено сравнительно меньшее внимание, что, однако, не мешает рассматривать книгу М. Холла как книгу по „комбинаторике в целом“. Следует отметить, что и в гл. 1—9, наряду с более традиционным материалом, читатель найдет немало нового и интересного, как, например, теорию различных представителей для системы конечных подмножеств бесконечного множества в гл. 5, лаконичное изложение основ линейного программирования в гл. 8, решение с помощью теории графов задачи перечисления полных циклов в гл. 9.

Инициатором перевода книги М. Холла явился член-корреспондент АН СССР А. О. Гельфond, уделявший комбинаторике много внимания, особенно в последнее время. Безвременная кончина прервала работу Александра Осиповича над редактированием книги. Продолжили эту работу его сотрудники из Математического института АН СССР. Следует отметить, что в процессе перевода и редактирования замечено довольно много неточностей и опечаток, которые были исправлены. Всем принявшим участие в работе над русским изданием книги я выражаю свою искреннюю признательность.

B. E. Тараканов

Комбинаторная теория<sup>1)</sup> — название предмета, прежде именовавшегося „комбинаторным анализом“ или „комбинаторикой“; впрочем, этими терминами многие пользуются и до сих пор. Как и во многих разделах математики, границы комбинаторной теории четко не определены, но центральной ее задачей можно считать задачу размещения объектов в соответствии со специальными правилами и нахождения числа способов, которыми это может быть сделано. Если правила очень просты, то основным в этой задаче является подсчет числа возможностей для осуществления искомого размещения. Если же эти правила тонкие или запутанные, главной проблемой становится вопрос существования таких размещений и нахождения методов их построения. Промежуточную область образуют вопросы о возможностях, возникающих при связанных между собой альтернативах, и типичная в этой области теорема утверждает, что максимум при альтернативе одного рода равен минимуму при альтернативе другого рода.

Текст книги делится на три большие части. Первые четыре главы связаны с проблемами перечисления. Главы 5—9 посвящены промежуточной области — теоремам о выборе. В главах 10—16 речь идет о существовании и построении схем.

Теория перечисления подробно изложена в классической работе Мак-Магона (MacMahon P. A., Combinatorial Analysis, London, vol. I, 1915, vol. II, 1916) и

---

<sup>1)</sup> В оригинале книга называется „Комбинаторная теория“. Вместо этого (введенного автором) термина в переводе принят термин „комбинаторика“. — Прим. ред.

в недавней книге Риордана (J. Riordan, *An Introduction to Combinatorial Analysis*, New York, 1958)<sup>1)</sup>. Этот раздел трактуется в первых четырех главах настоящей книги довольно кратко, без какого-либо намерения достигнуть той обстоятельности, с которой он представлен в упомянутых двух книгах. В книге Райзера (H. J. Ryser, *Combinatorial Mathematics*, 1963)<sup>2)</sup> дается сжатое, но элегантное изложение теорем о выборе, а также вопросов построения и существования блок-схем.

При подготовке этой книги большую помощь оказали мне многие лица, в их числе д-р Л. Бомер, проф. Р. Дилуорс, д-р К. Голдберг, проф. Д. Кнут, д-р М. Ньюман и проф. А. У. Таккер. Профессора Г. Биркгоф, Р. Гринвуд и Г. Райзер прочитали книгу в рукописи и дали мне ряд ценных советов, за что я глубоко им признателен. При подготовке рукописи и исправлении технических ошибок неоценимой была помощь мисс К. Гардт, д-ра А. Пфеффера и м-ра Р. Мак-Элайса.

Пасадена, Калифорния

Маршалл Холл

---

<sup>1)</sup> Русский перевод: Риордан Дж., Введение в комбинаторный анализ, ИЛ, М., 1963. — Прим. перев.

<sup>2)</sup> Русский перевод: Райзер Г. Дж., Комбинаторная математика, „Мир“, М., 1966. — Прим. перев.

# Перестановки и сочетания

---

## 1.1. Определения

*Перестановка*<sup>1)</sup> есть упорядоченная выборка элементов из некоторого множества  $S$ .

*Сочетание* есть неупорядоченная выборка элементов из некоторого множества  $S$ .

В перестановках и сочетаниях мы можем как допускать, так и не допускать повторений<sup>2)</sup>. Так, выбирая два из трех элементов  $a, b, c$ , мы получаем девять перестановок с повторениями:

$$aa, ab, ac, ba, bb, bc, ca, cb, cc$$

и шесть перестановок без повторений:

$$ab, ac, ba, bc, ca, cb.$$

Мы имеем также шесть сочетаний с повторениями:

$$aa, bb, cc, ab, ac, bc$$

и три сочетания без повторений:

$$ab, ac, bc.$$

Число перестановок без повторений из  $n$  элементов по  $r$  обозначается через  ${}_nP_r$  и легко вычисляется. В самом деле, в перестановке  $a_1a_2 \dots a_r$  мы можем в качестве  $a_1$  взять любой из  $n$  элементов, в качестве  $a_2$  — любой из остальных  $n - 1$  элементов и, выбрав  $a_1, a_2, \dots, a_{i-1}$ , в качестве  $a_{i+1}$  взять любой из оставшихся  $n - i$

<sup>1)</sup> Или размещение. — Прим. ред.

<sup>2)</sup> По другой терминологии (см. Райзер Г. Дж., Комбинаторная математика, „Мир“, 1966) перестановкой называется только упорядоченная выборка из множества  $S$ , в которой все элементы различны, а сочетанием — только неупорядоченная выборка из  $S$ , все элементы которой различны (т. е. подмножество множества  $S$ ). — Прим. ред.

элементов. Следовательно,

$${}_n P_r = n(n-1)\dots(n-r+1) = \frac{n!}{(n-r)!} = (n)_r. \quad (1.1.1)$$

Сочетание без повторений из  $n$  элементов по  $r$ , например  $a_1 a_2 \dots a_r$ , приводит к  $r!$  различным перестановкам, а именно ко всем  $r!$  перестановкам элементов  $a_1, a_2, \dots, a_r$ . Следовательно, число сочетаний из  $n$  элементов по  $r$ , обозначаемое через  ${}_n C_r$ , равно

$${}_n C_r = \frac{{}_n P_r}{r!} = \frac{n!}{(n-r)! r!} = \binom{n}{r}, \quad (1.1.2)$$

хорошо известному биномиальному коэффициенту. Действительно, в произведении  $(x+y)^n = (x+y)\dots(x+y)$  коэффициент при члене  $x^r y^{n-r}$  — это не что иное, как число способов выбора  $r$  множителей  $x+y$ , из которых берется  $x$ ; при этом из оставшихся  $n-r$  множителей  $x+y$  берется  $y$ . Заметим, что

$${}_n C_r = {}_n C_{n-r}. \quad (1.1.3)$$

Число перестановок с повторениями из  $n$  элементов по  $r$  равно  $n'$ , так как в  $a_1 a_2 \dots a_r$ , для каждого из  $a_1, a_2, \dots, a_r$ , существует  $n$  возможностей выбора.

Чтобы найти число сочетаний с повторениями из  $n$  элементов по  $r$ , мы не можем просто разделить  $n'$  на соответствующий множитель, так как в этом случае различные сочетания могут давать различное число перестановок. Так, беря сочетания из  $a, b, c, d, e$  по три, замечаем, что сочетание  $abc$  дает шесть перестановок, сочетание  $aab$  дает три перестановки, а сочетание  $aaa$  — лишь одну перестановку. Для подсчета используем здесь прием, заключающийся в перечислении элементов другого множества, которое находится во взаимно однозначном соответствии с исходным. К данному сочетанию (например,  $bcd$ ) присоединим все элементы  $a, b, c, d, e$  множества и то, что получается, запишем в следующем порядке:  $abbcdde$ . После этого разделим различные элементы черточками:  $a|bbb|c|dd|e$ . В общем случае к сочетанию с повторениями из  $n$  элементов по  $r$  добавим все  $n$  элементов и напишем полученные  $n+r$  элементов по порядку; после этого разделим различные элементы  $n-1$  черточками. Таким

образом, имея  $n+r$  мест и  $n+r-1$  промежутков между ними, мы должны поставить  $n-1$  черточек. Число возможных способов равно

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{r}. \quad (1.1.4)$$

Но между способами расстановки  $n-1$  черточек в  $n+r-1$  промежутков и сочетаниями с повторениями из  $n$  элементов по  $r$  имеется взаимно однозначное соответствие. Следовательно, число сочетаний с повторениями из  $n$  элементов по  $r$  равно  $\binom{n+r-1}{r}$ .

Выражения для числа сочетаний без повторений и с повторениями из  $n$  элементов по  $r$  сходны между собой. Например, для случая сочетаний из пяти элементов по три эти числа равны

$$\frac{5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3} \quad \text{и} \quad \frac{5 \cdot 6 \cdot 7}{1 \cdot 2 \cdot 3}$$

соответственно; здесь множители в чисителях убывают в одном случае и возрастают в другом.

Число сочетаний с повторениями из  $n$  элементов по  $r$  есть число решений  $(x_1, x_2, \dots, x_n)$  уравнения

$$r = x_1 + x_2 + \dots + x_n \quad (1.1.5)$$

в неотрицательных целых  $x_i$ , где  $x_i$  есть число появлений  $i$ -го элемента в данном сочетании. Это подсказывает и другой, но аналогичный способ подсчета числа сочетаний. Пусть  $y_i = x_i + 1$ ,  $i = 1, \dots, n$ . Тогда уравнение (1.1.5) принимает вид

$$n+r = y_1 + y_2 + \dots + y_n \quad (1.1.6)$$

и число решений  $(y_1, \dots, y_n)$  уравнения (1.1.6) в положительных целых  $y_i$  совпадает с числом решений для (1.1.5) в неотрицательных целых числах. Если мы возьмем  $n+r$  точек и поставим  $n-1$  черточек в  $n+r-1$  промежутках между ними, то можем считать  $y_1$  числом точек в первом множестве,  $y_2$  — числом точек во втором множестве и т. д. Таким образом, мы снова видим, что число решений уравнения (1.1.6) равно  $\binom{n+r-1}{n-1}$ , что в свою очередь равно числу неотрицательных реше-

ний уравнения (1.1.5), а также числу сочетаний с повторениями из  $n$  элементов по  $r$ .

Как еще одно применение этого метода, мы найдем число сочетаний без повторений из  $n$  чисел  $1, 2, \dots, n$  по  $r$ , не содержащих пар соседних чисел. Запишем числа  $1, 2, \dots, n$  в естественном порядке, и после каждого выбираемого числа будем ставить в этой записи черточку. Если имеется  $x_1$  чисел перед первой черточкой,  $x_2$  чисел между первой и второй черточками и, наконец,  $x_{r+1}$  чисел после последней черточки, то тем самым определяется выборка и

$$n = x_1 + x_2 + \dots + x_{r+1}, \quad (1.1.7)$$

где  $x_1 \geq 1, x_2 \geq 2, \dots, x_r \geq 2, x_{r+1} \geq 0$ . Запишем теперь  $n - r + 2 = x_1 + (x_2 - 1) + \dots + (x_r - 1) + (x_{r+1} + 1)$ , (1.1.8) что дает представление числа  $n - r + 2$  в виде суммы  $r + 1$  положительных целых чисел, и число таких представлений равно  $\binom{n-r+1}{r}$  — числу способов расстановки  $r$  черточек в  $n - r + 1$  промежутках.

Имеется очень большое число тождеств, включающих биномиальные коэффициенты; вот некоторые из них:

$$\sum_{k=0}^n \binom{n}{k} = 2^n, \quad (1.1.9a)$$

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0, \quad (1.1.9b)$$

$$\sum_{k=1}^n k (-1)^k \binom{n}{k} = 0, \quad n \geq 1, \quad (1.1.9c)$$

$$\sum_{k=r}^n (-1)^k \binom{k}{r} \binom{n}{k} = 0, \quad n \geq r. \quad (1.1.9d)$$

Все они могут быть получены из соотношения

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

Чтобы получить соотношения (1.1.9a) и (1.1.9b), положим в нем  $x = 1$  и  $x = -1$  соответственно; для получения (1.1.9c) продифференцируем его по  $x$  и затем возьмем  $x = -1$ ; для получения (1.1.9d) продифференцируем  $r$  раз по  $x$ , разделим на  $r!$  и положим  $x = -1$ .

Если мы имеем все возможные перестановки  $a_1 a_2 \dots a_n$  из  $n$  элементов, в которых  $b_1$  элементов первого рода,  $b_2$  элементов второго рода и вообще  $b_i$  элементов  $i$ -го рода ( $i = 1, 2, \dots, r$ ), где, естественно,  $b_1 + b_2 + \dots + b_r = n$ , то мы можем заменить  $b_i$  элементов  $i$ -го рода различными элементами так, чтобы все элементы в перестановке стали различными, и получить  $n!$  перестановок. Каждая исходная перестановка дает  $b_1! b_2! \dots b_r!$  перестановок. Следовательно, число исходных перестановок равно

$$\frac{n!}{b_1! b_2! \dots b_r!}, \quad b_1 + b_2 + \dots + b_r = n, \quad (1.1.10)$$

хорошо известному полиномиальному коэффициенту.

## 1.2. Приложения к теории вероятностей

Предположим, что в некоторой ситуации имеется  $n$  возможных взаимно исключающих исходов, которые мы обозначим через  $x_1, x_2, \dots, x_n$ . Припишем исходу  $x_i$  некоторое число  $p_i = p(x_i)$ , где  $p_i$  — действительное число,  $p_i \geq 0$ , и  $p_1 + p_2 + \dots + p_n = 1$ . Если некоторое событие  $E$  случается при одном из исходов  $x_{i_1}, \dots, x_{i_m}$  и не происходит в других случаях, то определим вероятность события  $E$  равенством  $p(E) = p_{i_1} + \dots + p_{i_m}$ . Присвоение начальных вероятностей  $p_1, \dots, p_n$  является не математической задачей, а оценкой относительного правдоподобия различных исходов, и в любом конкретном случае результат подсчета  $p(E)$  зависит от точности этого присвоения.

Существует много практических ситуаций, в которых представляется разумным рассматривать  $n$  исходов как равновозможные. Тогда мы принимаем  $p_1 = p_2 = \dots = p_n = 1/n$ . В этом случае вероятность события  $E$ , происходящего только при  $m$  возможных исходах, равна

$p(E) = \frac{m}{n}$ . В такой ситуации вычисление  $p(E)$  становится чисто комбинаторной задачей на подсчет  $m$  — числа возможных исходов, дающих событие  $E$ . При произвольном бросании игральной кости, шесть граней которой пронумерованы цифрами от 1 до 6, целесообразно допустить, что выпадение любой ее грани одинаково возможно, если кость имеет равномерную плотность. В этом случае мы принимаем  $p_1 = p_2 = \dots = p_6 = \frac{1}{6}$ , где  $p_i$  — вероятность того, что выпадает грань с номером  $i$ . Если нас интересует лишь выпадение 6, то мы рассматриваем только два возможных исхода, полагая вероятность того, что выпадет 6, равной  $p = \frac{1}{6}$  и вероятность того, что 6 не выпадет, равной  $p' = \frac{5}{6}$ .

Пусть имеется  $N$  урн, пронумерованных от 1 до  $N$ . Разместим в урны произвольным образом  $n$  шаров, где  $n < N$ . Найдем вероятность того, что каждая из урн с номерами от 1 до  $n$  содержит точно по одному шару. Эта вероятность зависит от двух условий: 1) различимы ли шары или нет; 2) имеет ли место принцип исключения, который не позволяет положить второй шар в урну, уже содержащую один шар. Если  $n$  шаров различимы и принцип исключения не имеет места, то существует  $N^n$  способов размещения  $n$  шаров в  $N$  урн и  $n!$  способов размещения их по одному в каждую из урн с номерами 1, ...,  $n$ . Из этих условий и определяется вероятность

$$p(E) = \frac{n!}{N^n}. \quad (1.2.1)$$

Если шары различимы и принцип исключения имеет место, то первый шар может быть помещен в любую из  $N$  урн, следующий — в любую из  $N - 1$  урн,  $i$ -й — в любую из  $N - i + 1$  урн; следовательно, число способов размещения  $n$  шаров в  $N$  урн равно  ${}_N P_n = N(N - 1) \dots (N - n + 1)$ . Эти шары могут быть размещены  $n!$  способами в урнах с номерами 1, ...,  $n$ , и тогда искомая вероятность равна

$$p(E) = \frac{n!}{N P_n} = \frac{1}{\binom{N}{n}}. \quad (1.2.2)$$

Если шары неразличимы и принцип исключения не имеет места, то возникает вопрос о решениях уравнения  $x_1 + x_2 + \dots + x_N = n$  в неотрицательных целых  $x_i$ , где  $x_i$  — число шаров в  $i$ -й урне. Число таких решений, как было отмечено в предыдущем разделе, есть число сочетаний с повторениями из  $N$  элементов по  $n$ , которое равно  $\binom{N+n-1}{n}$ . Одно из решений:

$$x_1 = x_2 = \dots = x_n = 1, \quad x_{n+1} = x_{n+2} = \dots = x_N = 0;$$

в этом случае искомая вероятность равна

$$p(E) = \frac{1}{\binom{N+n-1}{n}}. \quad (1.2.3)$$

С физической точки зрения „неразличимость“ означает, что все сочетания равновозможны.

Если шары неразличимы и имеет место принцип исключения, то число способов размещения шаров есть не что иное, как число сочетаний без повторений из  $N$  элементов по  $n$ , т. е.  $_N C_n = \binom{N}{n}$ . Выбор первых  $n$  урн является единственным возможным для нас способом, и, следовательно, вероятность равна

$$p(E) = \frac{1}{\binom{N}{n}}. \quad (1.2.4)$$

Заметим, что мы получили (1.2.2), т. е. если имеет место принцип исключения, то вероятность не зависит от того, различимы ли шары или нет.

В статистической физике рассматривается некоторая совокупность  $n$  частиц (это могут быть протоны, электроны, мезоны, нейтроны, нейтрино или фотоны); каждая из них может быть в любом из  $N$  „состояний“ (это могут быть энергетические уровни). Макроскопическое состояние этой системы из  $n$  частиц задается вектором  $x = (x_1, x_2, \dots, x_N)$ , где  $x_i$  — число частиц, находящихся в  $i$ -м состоянии. Вероятность любого отдельного макроскопического состояния зависит от того, различимы ли эти частицы и подчиняются ли они принципу исключения Паули, который гласит, что никакие две (нераз-

личимые) частицы не могут находиться в одном и том же состоянии. Если рассматриваемые частицы различимы и не подчиняются принципу исключения, то вероятность любого отдельного макроскопического состояния дается формулой (1.2.1), и тогда говорят, что частицы подчиняются статистике Максвелла — Больцмана. Если частицы неразличимы и не подчиняются принципу исключения, то вероятность дается формулой (1.2.3), и тогда говорят, что частицы подчиняются статистике Бозе — Эйнштейна. Если частицы неразличимы и подчиняются принципу исключения, то вероятность дается формулой (1.2.4), и при этом говорят, что они подчиняются статистике Ферми — Дирака. Электроны, протоны и нейтроны подчиняются статистике Ферми — Дирака. Фотоны и пи-мезоны подчиняются статистике Бозе — Эйнштейна. Случай (1.2.2) различных частиц, подчиняющихся принципу исключения, в физике не встречается.

При высоких температурах, когда число  $N$  велико и различные макроскопические состояния почти одинаково возможны, статистики Ферми — Дирака и Бозе — Эйнштейна по существу совпадают с классической статистикой Максвелла — Больцмана. При низких температурах низкие энергетические уровни возможны чаще, чем высокие, и тогда приведенные выше модели следует различать.

### Задачи

1. Доказать, что

$$\sum_{i=0}^m \binom{r}{i} \binom{s}{m-i} = \binom{r+s}{m}.$$

*Указание.*  $(1+x)^r(1+x)^s = (1+x)^{r+s}$ . Дать другое доказательство этого тождества, рассматривая число способов выбора комиссии в составе  $m$  человек из группы, состоящей из  $r$  мужчин и  $s$  женщин.

2. Флаг составляется из 13 горизонтальных полос красного, белого и голубого цвета, причем любые две соседние полосы должны быть разных цветов. Сколькими способами это можно осуществить?

3. Сколько существует положительных целых чисел, меньших чем  $10^n$  (в десятичной системе), цифры которых расположены в неубывающем порядке?

4. Сколькими способами можно  $n$  одинаковых подарков раздать  $r$  детям: а) без ограничений и б) если каждый ребенок должен получить хотя бы один подарок?

5. Из колоды в  $4n$  карт, которая содержит четыре различные масти, в каждой масти по  $n$  карт,  $n \geq 5$ , занумерованных числами  $1, \dots, n$ , выбраны пять карт. Расположить в порядке возрастания частоты появления, зависящей от  $n$ , следующие наборы:

- а) пять последовательных карт одной масти;
- б) четыре карты из пяти с одинаковым номером;
- в) три карты с одним номером и две карты с другим;
- г) пять карт одной масти;
- д) пять последовательно занумерованных карт;
- е) три карты из пяти с одним и тем же номером;
- ж) две карты с одним номером и две с другим;
- з) две карты из пяти с одним номером.

# Формулы обращения

---

## 2.1. Принцип включения и исключения. Обращение Мёбиуса

Пусть имеется  $N$  элементов и некоторое число свойств  $P(1), P(2), \dots, P(n)$ . Пусть далее  $N_i$  — число элементов со свойством  $P(i)$  и вообще  $N_{i_1 i_2 \dots i_r}$  — число элементов со свойствами  $P(i_1), P(i_2), \dots, P(i_r)$ . Тогда число элементов  $N(0)$ , не обладающих ни одним из указанных свойств, задается формулой обращения

$$N(0) = N - \sum N_i + \sum_{i_1 < i_2} N_{i_1 i_2} + \dots + (-1)^s \sum_{i_1 < i_2 < \dots < i_s} N_{i_1 i_2 \dots i_s} + \dots + (-1)^n N_{12 \dots n}. \quad (2.1.1)$$

Докажем это утверждение. Элемент, не обладающий ни одним из названных свойств, учитывается один раз в члене  $N$  и ни в какие из остальных слагаемых не входит. Элемент  $A$  со свойством  $P(j)$  учитывается по одному разу в  $N$  и  $N_j$ , поэтому дает 1 в члене  $N$ ,  $-1$  в члене  $-\sum_i N_i$  и, следовательно,  $1 - 1 = 0$  в правой части (2.1.1).

Элемент  $A$ , обладающий точно  $r$  свойствами, например  $j_1, \dots, j_r$ , дает 1 в члене

$$\sum_{i_1 < \dots < i_s} N_{i_1 i_2 \dots i_s}, \quad \text{где } s \leq r,$$

для каждого набора  $i_1, i_2, \dots, i_s$  из  $j_1, \dots, j_r$ , т. е. для  $\binom{r}{s}$  наборов. Следовательно, вклад  $A$  в правую часть (2.1.1) равен

$$1 - \binom{r}{1} + \binom{r}{2} - \dots + (-1)^s \binom{r}{s} - \dots + (-1)^r \binom{r}{r} = (1 - 1)^r = 0. \quad (2.1.2)$$

Таким образом, правая часть (2.1.1) учитывает каждый элемент, не имеющий указанных свойств, точно по одному разу, а всякий другой элемент — нуль раз; следовательно, она равна  $N(0)$ , что и требовалось доказать. Использование формулы (2.1.1) называется иногда *методом включения и исключения*.

Тем же путем можно найти число  $N(r)$  элементов с точно  $r$  свойствами. Оно дается выражением

$$N(r) = \sum_{i_1 < \dots < i_r} N_{i_1 \dots i_r} + \dots + (-1)^{s-r} \binom{s}{r} \sum_{i_1 < \dots < i_s} N_{i_1 \dots i_s} + \dots \quad (2.1.3)$$

В правой части (2.1.3) элемент с точно  $r$  свойствами учитывается один раз в первом слагаемом и не учитывается в остальных слагаемых. Элемент с точно  $t$  свойствами, где  $t > r$ , дает  $(-1)^{s-r} \binom{s}{r} \binom{t}{s}$  в слагаемом

$$(-1)^{s-r} \binom{s}{r} \sum_{i_1 < \dots < i_s} N_{i_1 i_2 \dots i_s}.$$

Но из соотношения (1.1.9d)

$$\sum_{s=r}^t (-1)^{s-r} \binom{s}{r} \binom{t}{s} = 0, \quad (2.1.4)$$

что и доказывает формулу (2.1.3).

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

$$1, 2, \dots, i, \dots, n, \quad (2.1.5)$$

$$a_1, a_2, \dots, a_i, \dots, a_n,$$

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  $P(i)$  выражается равенством  $a_i = i$ ,  $i = 1, 2, \dots, n$ . Тогда  $N_{i_1 i_2 \dots i_r} = (n - r)!$  — число перестановок, оставляющих на месте  $r$  определенных символов. Далее,

в  $\sum N_{i_1 i_2 \dots i_r}$  имеется  $\binom{n}{r}$  слагаемых — по числу способов выбора  $i_1, i_2, \dots, i_r$  из  $1, 2, \dots, n$ . Применяя (2.1.1), находим, что

$$N(0) = n! - n(n-1)! + \binom{n}{2}(n-2)! + \dots \\ \dots + (-1)^r \binom{n}{r}(n-r)! + \dots + (-1)^n \cdot 1. \quad (2.1.6)$$

Это выражение можно переписать в виде

$$N(0) = n! \left( 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \dots \right. \\ \left. \dots + (-1)^r \cdot \frac{1}{r!} + \dots + \frac{(-1)^n}{n!} \right). \quad (2.1.7)$$

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  $N(0)$  отличается от  $n!/e$  меньше, чем на  $1/(n+1)$ , и потому  $n!/e$  является весьма хорошим приближением для числа беспорядков из  $n$  символов.

Если нас интересует не только число беспорядков из  $1, 2, \dots, n$ , но также и число перестановок  $a_1 a_2 \dots a_n$  из  $1, 2, \dots, n$ , для которых  $a_i = i$  точно в  $r$  местах для какого-либо из значений  $r = 0, 1, \dots, n$ , то возникает задача, известная под названием „задачи о встречах“. Ее решение получается несложным расширением задачи о беспорядках:  $r$  чисел из  $1, \dots, n$  мы можем выбрать  $\binom{n}{r}$  способами и, выбрав их, умножим на число беспорядков из оставшихся  $n-r$  символов. Это дает число перестановок точно с  $r$  условиями  $a_i = i$ , равное

$$N(r) = \frac{n!}{r!} \left( 1 - 1 + \frac{1}{2!} - \dots + (-1)^{n-r} \cdot \frac{1}{(n-r)!} \right). \quad (2.1.8)$$

Этот результат можно было бы получить также с помощью формулы (2.1.3).

Чтобы указать формулу обращения другого типа, рассмотрим одну арифметическую функцию — *функцию Мёбиуса*  $\mu(n)$ . Она определяется для положительных целых чисел  $n$ . Если  $n > 1$ , то  $n$  имеет единственное представление в виде произведения степеней простых чисел:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad (2.1.9)$$

где  $p_i$  — различные простые числа. Определим  $\mu(n)$  следующим образом:

$$\mu(n) = \begin{cases} 1 & \text{при } n = 1, \\ 0, & \text{если какое-либо } e_i > 1 \text{ в (2.1.9),} \\ (-1)^r, & \text{если } e_1 = e_2 = \dots = e_r = 1 \text{ в (2.1.9).} \end{cases} \quad (2.1.10)$$

**Лемма 2.1.1.**

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1, \end{cases}$$

где суммирование производится по всем положительным делителям  $d$  числа  $n$ .

**Доказательство.** Если  $n = 1$ , то  $d = 1$  — единственный делитель и  $\mu(1) = 1$ . Если  $n > 1$  и  $n$  задано выражением (2.1.9), то пусть  $n^* = p_1 p_2 \dots p_r$ . Тогда делитель  $d$  числа  $n$ , который не является делителем  $n^*$ , будет иметь кратный простой множитель, и мы имеем  $\mu(d) = 0$ . Следовательно,

$$\sum_{d|n} \mu(d) = \sum_{d|n^*} \mu(d). \quad (2.1.11)$$

Но  $\sum_{d|n^*} \mu(d)$  легко вычисляется:

$$1 - r + \binom{r}{2} + \dots + (-1)^k \binom{r}{k} + \dots = (1 - 1)^r = 0, \quad (2.1.12)$$

так как существует  $\binom{r}{k}$  делителей, которые являются произведениями  $k$  различных простых чисел, и для каждого из них  $\mu(d) = (-1)^k$ . Таким образом, лемма доказана.

**Теорема 2.1.1** (формула обращения Мёбиуса). *Пусть  $f(n)$  и  $g(n)$  – функции, определенные для всякого положительного целого  $n$  и удовлетворяющие условию*

$$f(n) = \sum_{d|n} g(d). \quad (2.1.13a)$$

*Тогда можно обратить это соотношение и выразить  $g$  через  $f$ :*

$$g(n) = \sum_{d|n} \mu(d) f(n/d). \quad (2.1.13b)$$

*Из второго соотношения также следует первое.*

**Доказательство.** Мы имеем  $f(n/d) = \sum_{d'|n/d} g(d')$  для всякого  $d|n$ . Поэтому

$$\sum_{d|n} \mu(d) f(n/d) = \sum_{d|n} \mu(d) \sum_{d'|n/d} g(d'). \quad (2.1.14)$$

Пусть  $n = dd'n_1$ . Тогда  $d$  при фиксированном  $d'$  пробегает все значения делителей числа  $n/d'$ . Следовательно,

$$\sum_{d|n} \mu(d) \cdot \sum_{d'|n/d} g(d') = \sum_{d'|n} g(d') \sum_{d|n/d'} \mu(d) = g(n), \quad (2.1.15)$$

так как по лемме

$$\sum_{d|n/d'} \mu(d) = 0,$$

если только  $d' \neq n$ . Таким образом, правая часть формулы (2.1.14) – просто  $g(n)$ , и теорема доказана. Аналогично если дано равенство (2.1.13b), то мы можем подставить значение  $g(d)$  в правую часть (2.1.13a) и убедиться, что она равна  $f(n)$ , доказав тем самым равенство (2.1.13a).

Обращение Мёбиуса может быть использовано при перечислении циклических последовательностей. Если символы  $a_1, a_2, \dots, a_n$  расположены в циклическом порядке, так что за  $a_n$  следует  $a_1$ , то можно считать, что любая из линейных последовательностей  $a_2, a_3, \dots, a_n, a_1; a_3, \dots, a_n, a_1, a_2; \dots; a_n, a_1, \dots, a_{n-1}$  определяет одну и ту же циклическую последовательность. Но  $n$  линейных последовательностей (линейных „слов“), соответствующих одной и той же циклической последова-

тельности, могут не все быть различными. Если  $d$  — делитель числа  $n$  и последовательность  $a_1, a_2, \dots, a_n$  состоит из последовательности  $d$  символов  $a_1, a_2, \dots, a_d$ , повторенной  $n/d$  раз, то после первых  $d$  соответствующие линейные последовательности начинают повторяться. Для каждой циклической последовательности длины  $n$  можно однозначно указать минимальный период  $d$ , так что циклическая последовательность состоит из  $n/d$  повторений последовательности  $d$  символов. Далее, каждая циклическая последовательность длины  $d$  и периода  $d$ , где  $d|n$ , может быть повторена  $n/d$  раз, чтобы получить циклическую последовательность длины  $n$  и периода  $d$ . Каждой из этих последовательностей соответствует в точности  $d$  различных линейных слов длины  $n$ . Для  $r$  различных символов существует  $r^n$  линейных перестановок  $a_1a_2 \dots a_n$ . Если  $M(d)$  — число циклических последовательностей длины и периода  $d$ , то  $dM(d)$  есть число соответствующих линейных последовательностей длины  $n$ . Отсюда имеем равенство

$$\sum_{d|n} dM(d) = r^n. \quad (2.1.16)$$

Если взять  $f(x) = r^x$  и  $g(x) = xM(x)$ , то к (2.1.16) можно применить формулу обращения Мёбиуса и получить, что

$$nM(n) = \sum_{d|n} \mu(d) r^{n/d}, \quad (2.1.17)$$

следовательно,

$$M(n) = \frac{1}{n} \sum_{d|n} \mu(d) r^{n/d}. \quad (2.1.18)$$

Это есть число циклических перестановок длины и периода  $n$ . Если нам нужно найти общее число циклических перестановок длины  $n$ , то, обозначив его через  $T(n)$ , получим

$$T(n) = \sum_{d|n} M(d). \quad (2.1.19)$$

Если мы хотим узнать общее число циклических перестановок  $n$  элементов с определенным числом элементов некоторого рода (скажем,  $b_i$  элементов  $i$ -го рода,  $i=1, \dots, r$ , где  $b_1 + b_2 + \dots + b_r = n$ ), то вспомним, что число линейных перестановок такого типа есть

## Полиномиальный коэффициент

$$\frac{n!}{b_1! \dots b_r!}, \quad b_1 + b_2 + \dots + b_r = n. \quad (2.1.20)$$

Для циклической перестановки длины  $n$  и периода  $d$  такого типа  $d$  будет делителем всех  $b_1, \dots, b_r$ , или, что то же самое, делителем числа  $(b_1, \dots, b_r)$  — наибольшего общего делителя  $b_1, \dots, b_r$ . Таким образом, если  $M(b_1, \dots, b_r)$ ,  $b_1 + b_2 + \dots + b_r = n$ , есть число циклических перестановок длины  $n$  и периода  $p$  с  $b_i$  элементами  $i$ -го рода,  $i = 1, \dots, r$ , то тем же рассуждением, что и выше, придем к равенству

$$M(b_1, \dots, b_r) = \frac{1}{n} \sum_{d \mid (b_1, \dots, b_r)} \mu(d) \frac{(n/d)!}{(b_1/d)! \dots (b_r/d)!}. \quad (2.1.21)$$

„Задача о супружеских парах“<sup>1)</sup> (probleme des ménages) состоит в следующем: хозяйка желает рассадить  $n$  супружеских пар за круглым столом так, чтобы мужчины и женщины чередовались, но чтобы при этом ни один муж не сидел рядом со своей женой. Сколькими способами это можно осуществить? Легко видеть, что этого нельзя сделать, если число пар меньше трех, но для трех и более пар это осуществимо.

Рассадим сначала на местах через одно женщин, обозначая их номерами  $1, 2, \dots, n$  по кругу. Обозначим место слева от  $i$ -й женщины и справа от  $(i+1)$ -й женщины номером  $i$  и номером  $n$  — место между  $n$ -й женщиной и первой. Тогда первый муж может сесть на любое место, кроме  $n$ -го и первого, а  $i$ -й муж — на любое место, кроме  $(i-1)$ -го и  $i$ -го. Если муж с номером  $a_i$  сидит на месте  $i$ , то  $a_1 a_2 \dots a_n$  есть перестановка чисел  $1, 2, \dots, n$ , и наше условие означает, что в таблице

|       |       |         |           |       |
|-------|-------|---------|-----------|-------|
| 1     | 2     | $\dots$ | $n-1$     | $n$   |
| 2     | 3     | $\dots$ | $n$       | 1     |
| $a_1$ | $a_2$ | $\dots$ | $a_{n-1}$ | $a_n$ |

<sup>1)</sup> В ряде переведенных книг эта задача называется „задачей о гостях“. Настоящий перевод больше отвечает как сущности задачи, так и смыслу французского слова *ménage* (супружеская чета). *Прим. ред.*

перестановка  $a_1 a_2 \dots a_n$  должна быть не согласующейся с первыми двумя строчками (т. е.  $a_i \neq i, i+1$ ). Мы находимся, таким образом, в условиях задачи включения и исключения со свойствами  $P(1)$ :  $a_1 = 1, 2; \dots$ ;  $P(i)$ :  $a_i = i, i+1; \dots$ ;  $P(n)$ :  $a_n = n, 1$ . Если  $P(i)$  выполняется для  $r$  значений  $a_{i_1}, \dots, a_{i_r}$ , то существует  $(n-r)!$  способов дополнения перестановки. Таким образом, мы должны сначала подсчитать, сколькими способами можно получить перестановки с  $r$  свойствами  $P(i)$ , или, как мы будем говорить, число способов получения  $r$  попаданий. Число способов получить одно попадание равно  $2n$ , и в силу циклической симметрии (2.1.22) мы можем предположить, что при этом  $n$  будет либо в  $(n-1)$ -м, либо в  $n$ -м столбце. Перепишем теперь оставшиеся числа, записывая столбцы один за другим

в первом случае:

$$\left. \begin{array}{c} 1, 1, 2, 2, 3, \dots, n-2, n-2, n-1 \\ 1, 2, 2, 3, 3, \dots, n-2, n-1, n-1 \end{array} \right\} \quad (2.1.23)$$

и во втором:

$$\left. \begin{array}{c} 1, 2, 2, 3, 3, \dots, n-2, n-1, n-1 \end{array} \right\}$$

При выборе остальных  $r-1$  чисел мы ограничены тем условием, что в последовательностях (2.1.23) мы не можем выбирать два соседних члена, поскольку такой выбор означает либо взятие одного и того же числа дважды, либо взятие обоих элементов из одного столбца (2.1.22). Тем самым мы приходим к задаче о числе способов выбора  $r-1$  элементов, из которых никакие два не являются соседними, в строке с  $2n-3$  элементами. Это число было найдено в гл. 1, и оно равно  $\binom{2n-r-1}{r-1}$ . Его надо умножить на число  $2n$  возможностей первого выбора; но то же самое множество  $r$  значений может быть получено рассмотрением любого из  $r$  значений в качестве первого, следовательно, мы должны еще поделить на  $r$ . Таким образом, искомое число есть

$$\frac{2n}{r} \binom{2n-r-1}{r-1} = \frac{2n}{2n-r} \binom{2n-r}{r}. \quad (2.1.24)$$

Можно теперь применить формулу (2.1.1) и найти, что число  $U_n$  перестановок, не согласующихся с обеими

перестановками  $1, 2, \dots, n$  и  $2, 3, \dots, n, 1$ , дается формулой

$$\begin{aligned} U_n = & n! - 2n(n-1)! + \dots \\ & \dots + (-1)^r \frac{2n}{2n-r} \binom{2n-r}{r} (n-r)! + \dots + (-1)^n \cdot 2. \end{aligned} \quad (2.1.25)$$

Из этого соотношения можно получить рекуррентную формулу

$$(n-2)U_n = n(n-2)U_{n-1} + nU_{n-2} + 4(-1)^{n+1}, \quad (2.1.26)$$

что доказывается без особого труда. Действительно, для  $r=0$  и  $1$  члены в  $(n-2)U_n$  и  $n(n-2)U_{n-1}$  равны. Для  $r=2, \dots, n-1$  имеем тождество, включающее  $r$ -е члены из  $U_n$  и  $U_{n-1}$  и  $(r-2)$ -й член из  $U_{n-2}$ :

$$\begin{aligned} (n-2) \frac{2n}{2n-r} \binom{2n-r}{r} (n-r)! = & \\ = & n(n-2) \frac{2(n-1)}{2n-r-2} \binom{2n-r-2}{r} (n-r-1)! + \\ & + n \frac{2(n-2)}{2n-r-2} \binom{2n-r-2}{r-2} (n-r)!. \end{aligned} \quad (2.1.27)$$

Наконец, беря член с  $r=n$  в  $(n-2)U_n$  и с  $r=n-2$  в  $nU_{n-2}$ , находим, что

$$(n-2)(-1)^n \cdot 2 = n(-1)^{n-2} \cdot 2 + 4(-1)^{n+1}. \quad (2.1.28)$$

Справедливость формулы (2.1.26) тем самым доказана.

## 2.2. Частично упорядоченные множества и их функции Мёбиуса

*Частично упорядоченным множеством*  $P$  называется система  $P\{\dots, x, y, \dots\}$  элементов с отношением порядка  $x \geqslant y$  (читается: „ $x$  включает  $y$ “) для некоторых пар элементов и равенством  $x=y$ , в которой выполнены следующие аксиомы:

РО1.  $x \geqslant x$  для всякого  $x$  из  $P$ .

РО2. Если  $x \geqslant y$  и  $y \geqslant z$ , то  $x \geqslant z$ .

РО3. Если  $x \geqslant y$  и  $y \geqslant x$ , то  $x=y$ .

*Линейно упорядоченное множество*, или *цепь*, удовлетворяет также аксиоме

РО4. Если  $x, y$  — элементы  $P$ , то либо  $x \geqslant y$ , либо  $y \geqslant x$ <sup>1)</sup>.

Как другой вариант записи  $x \geqslant y$ , мы пишем также  $y \leqslant x$  и  $x > y$  (или  $y < x$ ), если  $x \geqslant y$  (или  $y \leqslant x$ ) и  $x \neq y$ .

Частичное упорядочение — понятие весьма общее. Интересны два частных случая:

1. Элементами множества  $P$  являются все подмножества некоторого конечного множества  $T$ , где мы через 0 обозначаем пустое множество, а через 1 — само  $T$ , и  $y \leqslant x$  означает, что  $y$  есть подмножество  $x$ .

2. Элементами множества  $P$  являются целые положительные числа, и  $y \leqslant x$  означает, что  $y$  делит  $x$ .

Легко проверить справедливость аксиом в обоих примерах.

Если  $T$  есть подмножество частично упорядоченного множества  $P$ , то элемент  $x$  множества  $P$ , такой, что  $x \leqslant t$  для каждого  $t$  из  $T$ , называется *нижней гранью* множества  $T$ . Если  $z$  — нижняя грань  $T$ , такая, что  $x \leqslant z$  для любой нижней грани  $x$  из  $T$ , то  $z$  называется *наибольшей нижней гранью*  $T$ . Из РОЗ следует, что если  $T$  имеет наибольшую нижнюю грань, то она единственна. Аналогично если  $x \geqslant t$  для каждого  $t$  из  $T$ , то  $x$  называется *верхней гранью* множества  $T$ , и если  $z$  — верхняя грань  $T$ , такая, что  $x \geqslant z$  для всякой верхней грани  $x$ , то  $z$  называется *наименьшей верхней гранью*; она также единственна, если существует. Если множество  $P$  само имеет наибольшую нижнюю грань, то она называется *нулевым элементом*  $P$ , а если  $P$  имеет наименьшую верхнюю грань, то она называется *наибольшим элементом* (или иногда *единичным элементом*)  $P$ .

Интервал  $[x, y]$ , где  $x \leqslant y$ , есть множество элементов  $w$ , таких, что  $x \leqslant w \leqslant y$ . Если в интервале  $[x, y]$  нет элементов, кроме  $x$  и  $y$ , то будем говорить, что  $y$  покрывает  $x$ . Частично упорядоченное множество  $P$  называется *локально конечным*, если число элементов в каждом интервале  $[x, y]$  конечно.

<sup>1)</sup> Частично упорядоченное множество, удовлетворяющее аксиоме РО4, называется также *совершенно упорядоченным множеством*. — Прим. ред.

Функция Мёбиуса и обращение Мёбиуса были первоначально определены Вейснером [1] и Ф. Холлом [2] для функций над локально конечными частично упорядоченными множествами. Эта идея недавно получила значительное развитие в работе Рота [1]. Основываясь на этой работе, дадим здесь краткое изложение этого вопроса.

Рассмотрим класс функций  $f(x, y)$ , принимающих действительные значения и определенных для  $x, y \in P$ , где  $P$  — некоторое локально конечное частично упорядоченное множество. Потребуем, чтобы  $f(x, y) = 0$ , если  $x \leq y$ . Сумма двух таких функций, а также умножение на скаляры определяется обычным образом. Произведение  $h = fg$  определяется следующим образом:

$$h(x, y) = \sum_{x \leq z \leq y} f(x, z) g(z, y), \quad x, y \text{ фиксированы.} \quad (2.2.1)$$

Это произведение определено корректно, так как в силу локальной конечности  $P$  сумма в правой части конечна. Посредством операций взятия суммы, умножения на скаляры и умножения по правилу (2.2.1) на функциях  $f(x, y)$  определена алгебра инцидентности  $A(P)$  множества  $P$ . Легко проверить, что умножение в  $A(P)$ , определенное выше, ассоциативно и дистрибутивно и что  $A(P)$  имеет единицу — функцию дельта Кронекера:  $\delta(x, x) = 1$ ,  $\delta(x, y) = 0$  при  $x \neq y$ .

**Лемма 2.2.1.** *Функция  $f(x, y)$  в алгебре  $A(P)$  имеет как левую, так и правую обратные функции в том и только том случае, когда  $f(x, x) \neq 0$  для любого  $x \in P$ .*

**Доказательство.** В формуле (2.2.1) возьмем  $h(x, y) = \delta(x, y)$  и при данном  $f$  попытаемся найти  $g$ . Поскольку для этого требуется, чтобы  $1 = \delta(x, x) = f(x, x)g(x, x)$  при любом  $x$ , то условие  $f(x, x) \neq 0$  для любого  $x \in P$ , очевидно, необходимо. Таким образом, полагаем  $f(x, x) \neq 0$  для каждого  $x$ , и тогда  $g(x, x) = f(x, x)^{-1}$  при любом  $x$ . Чтобы определить  $g(x, y)$  при  $x < y$ , мы можем допустить по индукции, что уже нашли  $g(z, y)$  для всех  $z$ , удовлетворяющих

соотношению  $x < z \leqslant y$ . Тогда

$$h(x, y) = \delta(x, y) = 0 = \sum_{x \leqslant z \leqslant y} f(x, z) g(z, y),$$

и, следовательно,

$$-f(x, x)g(x, y) = \sum_{x < z \leqslant y} f(x, z)g(z, y). \quad (2.2.2)$$

Мы можем отсюда найти  $g(x, y)$ , так как  $f(x, x) \neq 0$  и все слагаемые конечной суммы в правой части известны. Таким образом,  $f$  имеет правую обратную функцию. Аналогично, применив предположение индукции к членам с  $x \leqslant z < y$ , можно использовать (2.2.1), поменяв ролями  $f$  и  $g$ , чтобы показать, что  $f$  имеет левую обратную функцию. Но если  $fg_1 = 1 = \delta(x, y)$  и  $g_2f = 1$ , то, обычным способом,  $g_2 = g_2 \cdot 1 = g_2(fg_1) = (g_2f)g_1 = 1g_1 = g_1$ , т. е. левая и правая обратные функции совпадают.

**Определение.** Пусть  $P$  — локально конечное частично упорядоченное множество и  $A(P)$  — его алгебра инцидентности. *Дзета-функция*  $\zeta(x, y)$  алгебры  $A(P)$  есть такая функция, для которой  $\zeta(x, y) = 1$  при  $x \leqslant y$  и  $\zeta(x, y) = 0$  в остальных случаях. *Функцией Мёбиуса*  $\mu(x, y)$  алгебры  $A(P)$  называется функция, обратная к дзета-функции.

Так как  $\zeta(x, x) = 1 \neq 0$  при любом  $x$ , то в силу леммы 2.2.1  $\zeta(x, y)$  имеет обратную функцию  $\mu(x, y)$ , которая является для нее как левой обратной, так и правой обратной. Следовательно,

$$\mu(x, x) = 1 \text{ при любом } x \text{ из } P. \quad (2.2.3)$$

Для фиксированных  $x$  и  $y$ ,  $x < y$ , получаем

$$\mu(x, y) = - \sum_{x \leqslant z < y} \mu(x, z); \quad (2.2.4)$$

$$\mu(x, y) = - \sum_{x < z \leqslant y} \mu(z, y). \quad (2.2.5)$$

Здесь (2.2.4) выражает функцию Мёбиуса как левую обратную, а (2.2.5) — как правую обратную для дзета-функции.

Теорема об обращении Мёбиуса:

Теорема 2.2.1. Пусть  $P$  — локально конечное частично упорядоченное множество с нулевым элементом 0, функция  $f(x)$  задана для всех  $x$  из  $P$  и  $g(x)$  определяется через  $f(x)$  формулой

$$g(x) = \sum_{y \leqslant x} f(y) \text{ для всех } x \text{ из } P. \quad (2.2.6)$$

Тогда если  $\mu(y, z)$  — функция Мёбиуса множества  $P$ , то

$$f(x) = \sum_{y \leqslant x} g(y) \mu(y, x) \text{ для всех } x \text{ из } P. \quad (2.2.7)$$

Доказательство. Так как каждый интервал  $[0, x]$  конечен, то суммы в (2.2.6) и (2.2.7) определены корректно. Для фиксированного  $x$  рассмотрим сумму

$$S = \sum_{y \leqslant x} g(y) \mu(y, x) = \sum_{y \leqslant x} \left( \sum_{z \leqslant y} f(z) \right) \mu(y, x), \quad (2.2.8)$$

где мы  $g(y)$  заменили правой частью (2.2.6). Изменим теперь порядок суммирования и получим

$$\begin{aligned} S &= \sum_{z \leqslant y} f(z) \sum_{y \leqslant x} \mu(y, x) = \sum_z f(z) \zeta(z, y) \sum_{y \leqslant x} \mu(y, x) = \\ &= \sum_z f(z) \sum_{z \leqslant y \leqslant x} \zeta(z, y) \mu(y, x) = \sum_z f(z) \delta(z, x) = f(x). \end{aligned} \quad (2.2.9)$$

Так как  $S = f(x)$ , то утверждение теоремы — равенство (2.2.7) — доказано.

Определим теперь функцию Мёбиуса для двух частных случаев, упомянутых в начале этого раздела.

В первом случае  $P$  есть частично упорядоченное множество всех подмножеств конечного множества  $T$ , упорядоченных по включению. Мы утверждаем, что для двух подмножеств  $x, y, x \leqslant y$ , множества  $T$

$$\mu(x, y) = (-1)^{n(y) - n(x)}, \quad (2.2.10)$$

где  $n(x)$ ,  $n(y)$  — число элементов в  $x$  и в  $y$  соответственно. Это утверждение, конечно, справедливо, если  $n(y) - n(x) = 0$  или 1. Допустим по индукции, что формула (2.2.10) верна при  $n(y) - n(x) \leqslant r - 1$ , и рассмотрим случай, когда  $n(y) - n(x) = r$ . Тогда равенство (2.2.4)

принимает вид

$$\mu(x, y) = -1 + \binom{r}{1} - \binom{r}{2} + \dots$$

$$\dots - \binom{r}{j} (-1)^j + \dots - \binom{r}{r-1} (-1)^{r-1}, \quad (2.2.11)$$

так как существует  $\binom{r}{j}$  элементов  $z$ , где  $x \leq z < y$ , с  $n(z) - n(x) = j$ , а именно подмножества множества  $T$ , получаемые присоединением к  $x$   $j$  из  $r$  элементов  $y$ , не входящих в  $x$ . Сравнение (2.2.11) с биномиальным разложением  $(1 - 1)^r = 0$  дает  $\mu(x, y) = (-1)^r$ , что и требовалось доказать.

Пусть  $T$  — множество чисел  $1, 2, \dots, n$ , которым сопоставлены свойства  $P(1), P(2), \dots, P(n)$ . Пусть  $K$  — множество из  $N$  элементов, каждый из которых имеет свойства  $P(i)$ ,  $i \in x$  для некоторого подмножества  $x$  из  $T$ . Пусть  $f(x)$  — число элементов  $K$ , имеющих в точности свойства  $P(i)$ ,  $i \notin x$  ( $x$  — подмножество  $T$ ). Тогда если мы полагаем

$$g(x) = \sum_{y \leq x} f(y), \quad (2.2.12)$$

то функция  $g(x)$  — это число элементов  $K$ , имеющих все свойства  $P(i)$  для  $i \notin x$  и, быть может, еще другие. При  $x = T$  формула обращения (2.2.7) дает

$$f(T) = g(T) - \sum_{n(y)=n-1} g(y) + \dots + (-1)^j \sum_{n(y)=n-j} g(y) + \dots \\ \dots + (-1)^n \sum_{n(y)=0} g(y). \quad (2.2.13)$$

Но  $f(T) = N(0)$  есть число элементов, не имеющих ни одного из указанных свойств, а  $g(T) = N$ , так как  $g(T)$  равно числу элементов, имеющих свойства из пустого множества свойств и, возможно, еще другие. Если  $n(y) = n - j$ , то  $g(y)$  равно числу элементов, имеющих  $j$  свойств  $P(i)$  для всех  $i$ , не принадлежащих  $y$ , и, возможно, еще другие. Это показывает, что (2.2.13) есть не что иное, как принцип включения и исключения (2.1.1).

Во втором случае  $P$  — частично упорядоченное множество целых положительных чисел, где  $x \leq y$  означает, что  $x$  делит  $y$ .

Здесь если  $x \leq z \leq y$ , то  $z = xd$ , где  $d|(y/x)$ , и, таким образом, элементы отрезка  $[x, y]$  соответствуют делителям числа  $y/x$ . Заметим, что число 1 есть нулевой элемент  $P$ . Сравнение равенства (2.2.4) с леммой, предшествовавшей теореме 2.1.1, показывает, что в этом случае  $\mu(x, y) = \mu(y/x)$ . Таким образом, теорема 2.1.1 об обращении Мёбиуса есть частный случай теоремы 2.2.1 для множества целых положительных чисел, частично упорядоченных отношением делимости.

### Задачи

1. Пусть  $A$  есть  $(n \times n)$ -матрица с нулями на главной диагонали и единицами на остальных местах. Детерминант  $A$  равен  $(-1)^{n-1}(n-1)$ . (Это будет показано в разд. 10.2.) Сколько из  $n!$  членов в разложении определителя  $A$  будет равно  $+1$ ,  $-1$  и  $0$  соответственно?

2. Данна таблица:

|       |       |       |       |       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 0     | 1     | 2     | 3     | 4     | 5     | 6     | 7     | 8     | 9     |
| 1     | 2     | 3     | 4     | 0     | 6     | 7     | 8     | 9     | 5     |
| $a_0$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ | $a_8$ | $a_9$ |

Сколькими способами можно выбрать перестановку  $a_0 \dots a_9$  чисел  $0, 1, \dots, 9$  так, чтобы ни в одном столбце этой таблицы не было повторяющихся чисел?

3. Доказать, что  $U_n$  в (2.1.25) приближенно равно  $n!/e^2$ .

4. Функция  $\Lambda(n)$  определяется для целых положительных  $n$  формулой

$$\sum_{d|n} \Lambda(d) = \log n.$$

Доказать, что  $\Lambda(n) = \log p$ , если  $n = p^e$ ,  $p$  простое, и  $\Lambda(n) = 0$  в остальных случаях.

5. Найти функции Мёбиуса двух частично упорядоченных множеств  $P_1, P_2$  с пятью элементами  $0, a, b, c, 1$ , где: а) в  $P_1$   $0 \leq a \leq 1, 0 \leq b \leq 1, 0 \leq c \leq 1$  и других включений нет; б) в  $P_2$   $0 \leq a \leq 1, 0 \leq b \leq c \leq 1$  и других включений нет.

# Производящие функции и рекуррентные соотношения

## 3.1. Правила и свойства

Если  $u_0, u_1, u_2, \dots, u_n, \dots$  — некоторая последовательность чисел, то с этой последовательностью можно связать производящую функцию  $g(x)$ , определенную по следующему правилу:

$$g(x) = u_0 + u_1x + u_2x^2 + \dots + u_nx^n + \dots \quad (3.1.1)$$

Если этот ряд имеет круг сходимости радиуса  $R > 0$ , то может случиться, что свойства функции  $g(x)$  дадут нам возможность вычислить коэффициенты  $u_n$  (или хотя бы оценить порядок их величины) или, быть может, получить иную ценную информацию. Если  $h(x)$  — производящая функция последовательности  $v_0, v_1, v_2, \dots, v_n, \dots$ , то

$$h(x) = v_0 + v_1x + v_2x^2 + \dots + v_nx^n + \dots \quad (3.1.2)$$

Если мы сложим теперь равенство (3.1.1), умноженное на  $c$ , и (3.1.2), умноженное на  $d$ , то получим

$$\begin{aligned} cg(x) + dh(x) &= (cu_0 + dv_0) + (cu_1 + dv_1)x + \\ &\quad + (cu_2 + dv_2)x^2 + \dots + (cu_n + dv_n)x^n + \dots \end{aligned} \quad (3.1.3)$$

Перемножив функции  $g$  и  $h$ , получим

$$g(x)h(x) = w_0 + w_1x + w_2x^2 + \dots + w_nx^n + \dots, \quad (3.1.4)$$

где

$$w_n = u_0v_n + u_1v_{n-1} + \dots + u_{n-1}v_1 + u_nv_0 \quad (3.1.5)$$

для любого  $n = 1, 2, 3, \dots$

Даже если ряды для  $g(x)$  и  $h(x)$  не сходятся, мы можем рассматривать формулы (3.1.3), (3.1.4) и (3.1.5) как определения формальных операций над формальными рядами. Легко проверить, что так определенные сложение, умножение на скаляры и перемножение рядов

удовлетворяют законам ассоциативности, коммутативности и дистрибутивности. Кроме того, если  $u_0 \neq 0$  и если взять  $v_0 = u_0^{-1}$ , то (3.1.5) можно использовать как рекуррентное соотношение для определения таких  $v_1, v_2, \dots$ , что  $g(x)h(x) = 1$ .

Вместо производящей функции  $g(x)$ , связанной с  $u_0, u_1, \dots, u_n, \dots$ , можно рассматривать экспоненциальную производящую функцию  $G(x)$ , связанную с этой последовательностью следующим правилом:

$$G(x) = u_0 + u_1 x + \frac{u_2 x^2}{2!} + \dots + \frac{u_n x^n}{n!} + \dots \quad (3.1.6)$$

Пусть  $H(x)$  аналогичным образом связана с  $v_0, v_1, \dots$ ,

$$H(x) = v_0 + v_1 x + \frac{v_2 x^2}{2!} + \dots + \frac{v_n x^n}{n!} + \dots \quad (3.1.7)$$

Тогда для произведения  $G(x)H(x) = K(x)$  имеем

$$G(x)H(x) = K(x) = w_0 + w_1 x + \frac{w_2 x^2}{2!} + \dots + \frac{w_n x^n}{n!} + \dots, \quad (3.1.8)$$

где

$$w_n = u_0 v_n + \binom{n}{1} u_1 v_{n-1} + \dots + \binom{n}{r} u_r v_{n-r} + \dots + \binom{n}{n} u_n v_0, \quad (3.1.9)$$

или символически

$$w^n = (u + v)^n. \quad (3.1.10)$$

Символическую формулу (3.1.10) надо понимать так, что после разложения  $(u + v)^n$  по формуле бинома все показатели степени заменяются на индексы.

Предположим, что последовательность  $u_0, u_1, u_2, \dots, u_n, \dots$  удовлетворяет рекуррентному соотношению порядка  $r$ :

$$u_{n+r} = a_1 u_{n+r-1} + a_2 u_{n+r-2} + \dots + a_r u_n, \quad n = 0, 1, 2, \dots, \quad (3.1.11)$$

где  $a_i, i = 1, \dots, r$ , — постоянные. Тогда, если  $g(x)$  — производящая функция для последовательности  $\{u_n\}$  и если через  $k(x)$  обозначен полином

$$k(x) = 1 - a_1 x - a_2 x^2 - \dots - a_r x^r, \quad (3.1.12)$$

то, очевидно,

$$g(x)k(x) = c_0 + c_1x + c_2x^2 + \dots + c_{r-1}x^{r-1} = C(x), \quad (3.1.13)$$

где  $C(x)$  — полином степени не выше  $r - 1$ . Действительно, если  $c_{n+r}$  есть коэффициент при  $x^{n+r}$ ,  $n \geq 0$ , в произведении  $g(x)k(x)$ , то в силу (3.1.11)

$$c_{n+r} = u_{n+r} - a_1u_{n+r-1} - \dots - a_ru_n = 0. \quad (3.1.14)$$

Таким образом, для последовательности  $\{u_n\}$ , удовлетворяющей линейному рекуррентному соотношению (3.1.11), производящая функция  $g(x)$  есть рациональная функция:

$$g(x) = \frac{C(x)}{k(x)}. \quad (3.1.15)$$

С линейным рекуррентным соотношением (3.1.11) мы связываем *характеристический полином*

$$f(x) = x^r - a_1x^{r-1} - \dots - a_r. \quad (3.1.16)$$

Без ограничения общности можно предположить, что  $a_r \neq 0$ , так как если  $a_r = 0$ , то рекуррентное соотношение будет порядка, меньшего чем  $r$ . Рассмотрим разложение  $f(x)$  на линейные множители:

$$f(x) = (x - a_1)^{e_1} \dots (x - a_s)^{e_s}, \quad e_1 + e_2 + \dots + e_s = r, \quad (3.1.17)$$

где  $a_1, \dots, a_s$  — корни (возможно, комплексные) полинома  $f(x)$ . Сравнивая  $f(x)$  из формулы (3.1.16) и  $k(x)$  из формулы (3.1.12), мы видим, что

$$k(x) = x^r f\left(\frac{1}{x}\right), \quad (3.1.18)$$

и в соответствии с разложением (3.1.17) для  $f(x)$  получаем разложение на множители для  $k(x)$ :

$$k(x) = (1 - a_1x)^{e_1} \dots (1 - a_sx)^{e_s}, \quad e_1 + e_2 + \dots + e_s = r. \quad (3.1.19)$$

Мы можем, рациональную функцию  $g(x) = C(x)/k(x)$  выразить в виде суммы простых дробей

$$g(x) = \frac{C(x)}{k(x)} = \sum_{l=1}^s \sum_{k=1}^{e_l} \frac{\beta_{lk}}{(1 - \alpha_l x)^k}, \quad (3.1.20)$$

где  $\beta_{lk}$  — подходящие постоянные.

Таким образом, (3.1.20) дает выражение производящей функции как суммы функций вида

$$\frac{\beta}{(1 - \alpha x)^k} = \beta (1 - \alpha x)^{-k}. \quad (3.1.21)$$

Разлагая выражение (3.1.21) по формуле бинома, получаем, что

$$\begin{aligned} \beta (1 - \alpha x)^{-k} &= \beta \left( 1 + (-k)(-\alpha x) + \dots \right. \\ &\quad \left. \dots + \frac{(-k) \dots (-k - n + 1) (-\alpha x)^n}{n!} + \dots \right). \end{aligned} \quad (3.1.22)$$

В этом выражении коэффициент при  $x^n$  равен

$$\frac{\beta (n+k-1) \dots k}{n!} \alpha^n = \beta \binom{n+k-1}{n} \alpha^n = \beta \binom{n+k-1}{k-1} \alpha^n. \quad (3.1.23)$$

Заметим, что

$$\sum_{k=1}^{e_l} \beta_{lk} \binom{n+k-1}{k-1} \alpha_i^n = P_l(n) \alpha_i^n, \quad (3.1.24)$$

где  $P_l(n)$  — полином от  $n$  степени не выше  $e_l - 1$ , и что любой полином  $P_l(n)$  может быть получен соответствующим выбором постоянных  $\beta_{lk}$ . Таким образом, (3.1.20) можно записать в виде

$$g(x) = \sum_{n=0}^{\infty} u_n x^n = \sum_{n=0}^{\infty} \sum_{i=1}^s P_l(n) \alpha_i^n x^n, \quad (3.1.25)$$

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

$$u_n = \sum_{i=1}^s P_l(n) \alpha_i^n, \quad (3.1.26)$$

где степень  $P_l(n)$  не выше  $e_l - 1$ .

Сформулируем полученный результат в виде теоремы.

**Теорема 3.1.1.** Пусть последовательность  $u_0, u_1, u_2, \dots, u_n, \dots$  удовлетворяет линейному рекуррентному соотношению с постоянными коэффициентами

$$u_{n+r} = a_1 u_{n+r-1} + \dots + a_r u_n, \quad n \geq 0.$$

Назовем  $f(x) = x^r - a_1 x^{r-1} - \dots - a_r$  характеристическим полиномом этого рекуррентного соотношения, и пусть

$$f(x) = (x - a_1)^{e_1} \dots (x - a_s)^{e_s}, \quad e_1 + e_2 + \dots + e_s = r,$$

— разложение  $f(x)$  на линейные множители. Тогда

$$u_n = \sum_{i=1}^s P_i(n) a_i^n$$

для всех  $n$ , где  $P_i(n)$  — полином степени не выше  $e_i - 1$  относительно  $n$ . Коэффициенты полинома  $P_i(n)$  определяются начальными значениями  $u_0, u_1, \dots, u_{r-1}$  последовательности  $\{u_n\}$ .

### 3.2. Комбинаторные задачи

Рассмотрим комбинаторную задачу, решение которой зависит от линейного рекуррентного соотношения. Пусть  $u_t, t \geq 2$ , — число способов найти перестановку  $a_1 a_2 \dots a_t$  чисел  $1, 2, \dots, t$ , такую, что для каждого  $i$  число  $a_i$  находится в  $i$ -м столбце таблицы:

$$\begin{array}{ccccccccc} 1 & 2 & \dots & t-3 & t-2 & t-1 \\ 1 & 2 & 3 & \dots & t-2 & t-1 & t \\ 2 & 3 & 4 & \dots & t-1 & t \end{array} \quad (3.2.1)$$

Непосредственно находим, что  $u_2 = 2$ ,  $u_3 = 3$ ,  $u_4 = 5$ . Число  $t$  должно быть использовано либо в  $t$ -м, либо в  $(t-1)$ -м столбце. Таким образом, имеем две возможности:

$$\begin{array}{ccccccccc} 1 & 2 & \dots & t-3 & t-2 & t \\ 1 & 2 & 3 & \dots & t-2 & t-1 \\ 2 & 3 & 4 & \dots & t-1 \end{array} \quad (3.2.2)$$

или

$$\begin{array}{ccccccccc} 1 & 2 & \dots & t-3 & t & t-1 \\ 1 & 2 & 3 & \dots & t-2 \\ 2 & 3 & 4 & \dots \end{array} \quad (3.2.3)$$

В обоих случаях выбранные числа выделены жирным шрифтом. В (3.2.2) мы исключили  $t$  из  $(t-1)$ -го столбца, так как оно не может быть там использовано. Так как в (3.2.3)  $t$  выбрано в  $(t-1)$ -м столбце, то  $t-1$  мы должны выбрать в  $t$ -м столбце и затем исключить  $t-1$  из  $(t-2)$ -го столбца. Число способов выбора в (3.2.2) чисел  $1, 2, \dots, t-1$  равно  $u_{t-1}$ , а число способов выбора в (3.2.3) равно  $u_{t-2}$ . Следовательно, складывая их, получаем все способы выбора в (3.2.1):

$$u_t = u_{t-1} + u_{t-2}, \quad (3.2.4)$$

т. е. линейное рекуррентное соотношение второго порядка для  $u_t$ . Хотя эта задача не имеет смысла при  $t=0$  или 1, значения  $u_0=1, u_1=1$  согласуются с рекуррентным соотношением (3.2.4), и мы имеем последовательность значений  $u_0=1, u_1=1, u_2=2, u_3=3, u_4=5, \dots$ . Характеристический полином для (3.2.4) имеет вид

$$f(x) = x^2 - x - 1 = (x - \alpha_1)(x - \alpha_2), \quad (3.2.5)$$

где

$$\alpha_1 = \frac{1 + \sqrt{5}}{2}, \quad \alpha_2 = \frac{1 - \sqrt{5}}{2}. \quad (3.2.6)$$

По теореме 3.1.1 и из начальных значений легко найти, что

$$u_n = \frac{1}{\sqrt{5}} (\alpha_1^{n+1} - \alpha_2^{n+1}). \quad (3.2.7)$$

Другая, более естественная, комбинаторная задача также сводится к вычислению  $u_t$ . Каково число  $z_n$ ,  $n \geq 3$ , перестановок  $a_1 a_2 \dots a_n$  из  $1, 2, \dots, n$ , таких, что  $a_i$  находится в  $i$ -м столбце следующей таблицы?

$$\begin{array}{ccccccccc} 1 & 2 & 3 & \dots & n-3 & n-2 & n-1 & n \\ 2 & 3 & 4 & \dots & n-2 & n-1 & n & 1 \\ 3 & 4 & 5 & \dots & n-1 & n & 1 & 2 \end{array} \quad (3.2.8)$$

Множество всех таких перестановок может быть разбито на подмножества в зависимости от номера столбца, из которого выбирается  $n$ , и если это не  $(n - 1)$ -й столбец, то также в зависимости от того,  $n - 1$  или 1 выбираются в  $(n - 1)$ -м столбце. Выбор того или иного числа обозначим в последних трех столбцах жирным шрифтом, как показано ниже:

$$(a) \begin{matrix} n-2 & n-1 & n \\ n-1 & n & 1 \\ n & 1 & 2 \end{matrix} \quad (b) \begin{matrix} n-2 & n-1 & n \\ n-1 & n & 1 \\ n & 1 & 2 \end{matrix} \quad (3.2.9)$$

$$(c) \begin{matrix} n-2 & n-1 & n \\ n-1 & n & 1 \\ n & 1 & 2 \end{matrix} \quad (d) \begin{matrix} n-2 & n-1 & n \\ n-1 & n & 1 \\ n & 1 & 2 \end{matrix} \quad (e) \begin{matrix} n-2 & n-1 & n \\ n-1 & n & 1 \\ n & 1 & 2 \end{matrix}$$

Случай (а) оставляет единственную возможность выбора, а именно верхней строки (3.2.8), ибо 1 можно выбрать лишь из первого столбца. После этого 2 остается только во втором столбце, и аналогично мы вынуждены выбирать 3, 4, ...,  $n - 2$  в первой строке. В случае (б) нам приходится выбирать из

$$\begin{aligned} & 2 \ 3 \dots n-3 \ n-2 \\ & 2 \ 3 \ 4 \dots n-2 \ n-1 \\ & 3 \ 4 \ 5 \dots n-1 \end{aligned} \quad (3.2.10)$$

и число способов выбора равно  $u_{n-2}$ . В случае (с) выбор чисел производится из таблицы для  $u_{n-1}$ . В случае (д) возможен лишь один выбор, а именно — третьей строки (3.2.8), так как  $n - 1$  можно выбрать лишь из  $(n - 3)$ -го столбца; аналогично  $n - 2, n - 3, \dots, 2$  должны быть выбраны в третьей строке. В случае (е) выбор чисел производится из таблицы для  $u_{n-2}$ . Следовательно, общее число  $z_n$  искомых перестановок для (3.2.8) задается формулой

$$z_n = 1 + u_{n-2} + u_{n-1} + 1 + u_{n-2} = u_n + u_{n-2} + 2 = a_1^n + a_2^n + 2, \quad (3.2.11)$$

где, как и прежде,

$$a_1 = \frac{1 + \sqrt{5}}{2}, \quad a_2 = \frac{1 - \sqrt{5}}{2}.$$

Число  $u_n$  беспорядков из  $1, 2, \dots, n$ , вычисленное в (2.1.6), также может быть найдено посредством рекуррентной формулы. Рассмотрим перестановку (беспорядок)

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}. \quad (3.2.12)$$

Если  $a_1 = j$ , то рассмотрим частичную перестановку

$$\begin{pmatrix} 2 & \dots & j & \dots & n \\ a_2 & \dots & a_j & \dots & a_n \end{pmatrix}. \quad (3.2.13)$$

Здесь надо рассмотреть два случая. Первый — перестановки с  $a_i \neq 1$ , второй — с  $a_j = 1$ . Эти случаи в совокупности являются исчерпывающими и взаимно исключают друг друга. В первом случае имеем перестановку

$$\begin{pmatrix} 2 & \dots & i & \dots & j & \dots & n \\ a_2 & \dots & 1 & \dots & a_i & \dots & a_n \end{pmatrix}, \quad i \neq j, \quad (3.2.14)$$

которую можно связать с беспорядком из  $2, \dots, n$ :

$$\begin{pmatrix} 2 & \dots & i & \dots & j & \dots & n \\ a_2 & \dots & j & \dots & a_i & \dots & a_n \end{pmatrix}. \quad (3.2.15)$$

Обратно, каждый беспорядок из  $2, \dots, n$  вида (3.2.15) приводит к  $n-1$  беспорядкам из  $1, 2, \dots, n$  первого рода, если в качестве  $j$  брать поочередно  $2, \dots, n$ . Во втором случае, с  $a_j = 1$ , частичная перестановка (3.2.13) принимает вид

$$\begin{pmatrix} 2 & \dots & j & \dots & n \\ a_2 & \dots & 1 & \dots & a_n \end{pmatrix}. \quad (3.2.16)$$

Если мы исключим столбец  $\binom{j}{1}$ , то останется беспорядок из  $2, \dots, j-1, j+1, \dots, n$ ; обратно, для каждого  $j=2, \dots, n$  такие беспорядки из  $n-2$  чисел приводят к беспорядкам из  $1, \dots, n$  второго типа. Тем самым

приходим к рекуррентному соотношению

$$u_n = (n-1)u_{n-1} + (n-1)u_{n-2}. \quad (3.2.17)$$

Легко можно проверить, что это соотношение дает те же самые числа, что и формула (2.1.6).

Последовательность  $x_1x_2 \dots x_n$  может быть получена при помощи бинарного неассоциативного произведения несколькими способами. Чему равно это число способов  $u_n$ ? Для  $n=3, 4$  существуют следующие возможности:

$$\begin{aligned} & x_1(x_2x_3), \quad (x_1x_2)x_3; \\ & x_1(x_2(x_3x_4)), \quad x_1((x_2x_3)x_4), \\ & (x_1x_2)(x_3x_4), \\ & (x_1(x_2x_3))x_4, \quad ((x_1x_2)x_3)x_4. \end{aligned} \quad (3.2.18)$$

Таким образом,  $u_3 = 2$ ,  $u_4 = 5$ . Мы имеем также  $u_2 = 1$  и условимся считать  $u_1 = 1$ . Последовательность  $x_1x_2 \dots x_n$  получается в конечном счете как произведение некоторой композиции из первых  $r$  символов на некоторую композицию из последних  $n-r$  символов для какого-либо  $r$ :  $(x_1 \dots x_r)(x_{r+1} \dots x_n)$ . Первые  $r$  символов могут быть скомбинированы  $u_r$  способами (условие  $u_1 = 1$  здесь как раз подходит), а последние  $n-r$  символов  $u_{n-r}$  способами. Таким образом,

$$u_n = u_1u_{n-1} + u_2u_{n-2} + \dots + u_{n-1}u_1, \quad n \geq 2. \quad (3.2.19)$$

Запишем производящую функцию  $f(x)$  в виде

$$f(x) = u_1x + u_2x^2 + \dots + u_nx^n + \dots, \quad (3.2.20)$$

оставив в стороне вопрос о сходимости. Рекуррентное соотношение (3.2.19) формально эквивалентно соотношению

$$(f(x))^2 = -x + f(x). \quad (3.2.21)$$

Заметим, что  $u_1 = 1$  и что рекуррентное соотношение (3.2.19) выполняется только для  $n \geq 2$ ; это учтено членом  $-x$  в правой части (3.2.21). Решая (3.2.21) как квадратное уравнение относительно  $f(x)$ , получаем, что

$$f(x) = \frac{1 - \sqrt{1 - 4x}}{2}. \quad (3.2.22)$$

Здесь мы берем знак минус, так как ряд для  $f(x)$  не имеет постоянного члена. Разложим правую часть (3.2.22) в ряд по степеням  $x$  и найдем коэффициент  $v_n$  при  $x^n$ :

$$v_n = \frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)\dots((3-2n)/2)(-4)^n\left(-\frac{1}{2}\right)}{n!}. \quad (3.2.23)$$

Это выражение упрощается так:

$$v_n = \frac{(2n-2)!}{n!(n-1)!}. \quad (3.2.24)$$

Заметим теперь, что ряд для функции  $f(x)$ , заданной формулой (3.2.22), сходится при  $|x| < \frac{1}{4}$ , и для этих значений выполнено равенство (3.2.21), а следовательно, имеет место рекуррентное соотношение (3.2.19) (с  $v_n$  вместо  $u_n$ ). Но так как  $u_1 = v_1 = 1$ , то  $u_n = v_n$  для всех  $n \geq 1$  и, таким образом,

$$u_n = \frac{(2n-2)!}{n!(n-1)!} \quad (3.2.25)$$

для всех  $n \geq 2$ . Заметим, что доказать сходимость ряда (3.2.20), используя только соотношение (3.2.19), чрезвычайно сложно.

### Задачи

1. Числа в последовательности  $u_0, u_1, \dots, u_n, \dots$ , где  $u_0 = 1$ ,  $u_1 = 2$  и  $u_{n+2} = u_{n+1} + u_n$ , называются числами Фибоначчи. Показать, что всякое положительное целое число  $N$  имеет единственное представление

$$N = \sum_{i=1}^{\infty} a_i u_i,$$

где  $a_i = 0$  или  $1$  и  $a_i a_{i+1} = 0$ ,  $i \geq 1$ .

2. Числа  $s(n, r)$  и  $S(n, r)$ , называемые числами Стирлинга первого и второго рода соответственно, определяются соотношениями

$$(x)_n = x(x-1)\dots(x-n+1) = \sum_{r=0}^n s(n, r)x^r, \quad n > 0,$$

и

$$x^n = \sum_{r=0}^n S(n, r) (x)_r, \quad n > 0.$$

Здесь мы принимаем  $x^0 = (x)_0 = 1$ . Показать, что

$$\sum_r S(n, r) s(r, m) = \delta_{nm},$$

где  $\delta_{nm}$  — дельта Кронекера,  $\delta_{nn} = 1$ ,  $\delta_{nm} = 0$ , если  $n \neq m$ .  
Вывести отсюда, что одно из двух соотношений

$$(a) \quad a_n = \sum_r s(n, r) b_r, \quad n = 1, 2, \dots,$$

$$(b) \quad b_n = \sum_r S(n, r) a_r, \quad n = 1, 2, \dots,$$

влечет за собой другое.

3. Применить соотношение  $(x)_{m+1} = (x - m)(x)_m$  к доказательству рекуррентных соотношений для чисел Стирлинга первого и второго рода:

$$s(n+1, r) = s(n, r-1) - ns(n, r),$$

$$S(n+1, r) = S(n, r-1) + rS(n, r).$$

4. Пусть  $P_n = \sum_{r=0}^n (n)_r$  — общее число перестановок из  $n$  различных элементов.

(а) Показать, что  $P_n$  удовлетворяет рекуррентному соотношению

$$P_n = nP_{n-1} + 1, \quad n \geq 1, \quad P_0 = 1.$$

(б) Показать, что  $P_n = n! \sum_{r=0}^n \frac{1}{r!}$  и что для  $n \geq 1$  число  $P_n$  есть ближайшее целое к  $n! e$ .

(в) Показать, что  $\sum_{n=0}^{\infty} P_n \frac{x^n}{n!} = e^x/(1-x)$ .

5. Производящая функция Дирихле  $A(s)$  для последовательности чисел  $a_1, a_2, \dots$  — это формальный ряд

$$A(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Пусть

$$B(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s},$$

определен сумму

$$A(s) + B(s) = C(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

где  $c_n = a_n + b_n$ , и произведение

$$A(s)B(s) = V(s) = \sum_{n=1}^{\infty} \frac{v_n}{n^s},$$

где

$$v_n = \sum_{d \mid n} a_d b_{n/d}.$$

(а) Доказать, что так определенное произведение коммутативно и ассоциативно.

(б) Показать, что если  $i_1 = 1, 0 = i_2 = i_3 = \dots$ , то ряд  $I(s)$  определяет единицу относительно этого умножения.

(с) Показать, что при  $a_1 \neq 0$  для ряда  $A(s)$  имеется обратный ряд  $B(s)$ , удовлетворяющий равенству

$$A(s)B(s) = I(s).$$

6. Определим дзета-функцию

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Показать, что ряд, обратный к  $\zeta(s)$ , представляется в виде

$$\zeta(s)^{-1} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

где  $\mu(n)$  — функция Мёбиуса, определенная в (2.1.10). Если  $a_n = g(n)$ ,  $b_n = f(n)$  для всех  $n$  и  $B(s) = A(s)\zeta(s)$ , то  $A(s) = B(s)\zeta(s)^{-1}$ . Показать, что это соответствует формуле обращения Мёбиуса (теорема 2.1.1).

# Разбиения

---

## 4.1. Разбиения. Тождества и арифметические свойства

*Разбиением* целого положительного числа  $n$  называется представление  $n$  в виде суммы целых положительных чисел

$$n = x_1 + x_2 + \dots + x_k, \quad x_i > 0, \quad i = 1, \dots, k. \quad (4.1.1)$$

Легко найти число упорядоченных разбиений  $n$  на  $k$  частей: это будет число способов, которыми можно разместить  $k - 1$  черточек в  $n - 1$  промежутках между  $n$  точками. Оно равно  $\binom{n-1}{k-1}$ . Если число частей  $k$  не фиксировать, то черточку в каждом из промежутков можно как поместить, так и не поместить, и общее число упорядоченных разбиений равно  $2^{n-1}$ .

Теория неупорядоченных разбиений значительно сложнее и ставит ряд интересных проблем. Обозначим через  $p_k(n)$  число (неупорядоченных) разбиений  $n$  на  $k$  частей. Неупорядоченное разбиение  $n$  на  $k$  частей можно представить в стандартной форме, выписывая части в убывающем порядке. Таким образом,  $p_k(n)$  — это число решений в целых положительных  $x_i$  уравнения

$$n = x_1 + x_2 + \dots + x_k, \quad x_1 \geq x_2 \geq \dots \geq x_k \geq 1. \quad (4.1.2)$$

Нетрудно подсчитать  $p_k(n)$  для всех  $n$  при малых значениях  $k$ , но с возрастанием  $k$  вычисления становятся все более утомительными. Согласно уравнению (4.1.2), мы имеем

$$n - k = (x_1 - 1) + (x_2 - 1) + \dots + (x_k - 1), \quad (4.1.3)$$

где  $x_1 \geq x_2 \geq \dots \geq x_k \geq 1$ . Положив  $y_i = x_i - 1$ ,  $i = 1, \dots, k$ , получим

$$n - k = y_1 + y_2 + \dots + y_k, \quad y_1 \geq y_2 \geq \dots \geq y_k \geq 0. \quad (4.1.4)$$

Однако если  $y_s > 0$ , а  $y_{s+1} = \dots = y_k = 0$ , то формула (4.1.4) дает разбиение  $n - k$  на  $s$  частей. Таким образом, число решений уравнения (4.1.4) равно числу разбиений  $n - k$  на самое большое  $k$  частей; другими словами, это число равно  $p_k(n - k) + p_{k-1}(n - k) + \dots + p_1(n - k)$ . Сравнивая (4.1.4) с (4.1.2), получаем, что

$$p_k(n) = p_k(n - k) + p_{k-1}(n - k) + \dots + p_1(n - k). \quad (4.1.5)$$

Это рекуррентное соотношение определяет  $p_k(n)$  при начальных условиях  $p_k(n) = 0$  для  $n < k$  и  $p_k(k) = 1$ , так как единственный способ представить  $k$  в виде суммы  $k$  положительных целых чисел — это записать его в виде суммы  $k$  единиц. Мы можем использовать (4.1.5) для построения таблицы значений  $p_k(n)$ , как это сделано в табл. 4.1.

Таблица 4.1

Значения  $p_k(n)$ 

| $n \backslash k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|------------------|---|---|---|---|---|---|---|
| 1                | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2                | 0 | 1 | 1 | 2 | 2 | 3 | 3 |
| 3                | 0 | 0 | 1 | 1 | 2 | 3 | 4 |
| 4                | 0 | 0 | 0 | 1 | 1 | 2 | 3 |
| 5                | 0 | 0 | 0 | 0 | 1 | 1 | 2 |
| 6                | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 7                | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

Мы можем также использовать рекуррентное соотношение (4.1.5) для вычисления  $p_k(n)$  при малых значениях  $k$  и любом  $n$ . Очевидно,  $p_1(n) = 1$  для всех  $n \geq 1$ . Записав теперь

$$p_2(n) = p_2(n - 2) + p_1(n - 2) = p_2(n - 2) + 1,$$

находим, что  $p_2(n) = n/2$  для четных  $n$  и  $p_2(n) = (n - 1)/2$  для нечетных  $n$ , поскольку  $p_2(1) = 0$  и  $p_2(2) = 1$ ;  $p_3(n)$  можно выразить в виде полинома второй степени относительно  $n$ , коэффициенты которого зависят от класса

вычетов  $n$  по модулю 6. Получаем следующие значения  $p_k(n)$  для  $k = 1, 2, 3$ :

$$p_1(n) = 1;$$

$$p_2(n) = \begin{cases} \frac{n}{2}, & n \equiv 0 \pmod{2}, \\ \frac{n-1}{2}, & n \equiv 1 \pmod{2}; \end{cases} \quad (4.1.6)$$

$$p_3(n) = \begin{cases} \frac{n^2}{12}, & n \equiv 0 \pmod{6}, \\ \frac{n^2}{12} - \frac{1}{12}, & n \equiv 1 \pmod{6}, \\ \frac{n^2}{12} - \frac{1}{3}, & n \equiv 2 \pmod{6}, \\ \frac{n^2}{12} + \frac{1}{4}, & n \equiv 3 \pmod{6}, \\ \frac{n^2}{12} - \frac{1}{3}, & n \equiv 4 \pmod{6}, \\ \frac{n^2}{12} - \frac{1}{12}, & n \equiv 5 \pmod{6}. \end{cases}$$

Без особого труда можно показать, что число  $p_k(n)$  является полиномом степени  $k-1$ , старший член которого равен  $n^{k-1}/(k-1)!k!$ , и что коэффициенты  $p_k(n)$  зависят от класса вычетов  $n$  по  $\text{mod } k!$ . При  $k=1, 2, 3$  это верно по (4.1.6). Применим индукцию по  $k$ . Если  $n \equiv n_0 \pmod{k!}$ , то  $n-k \equiv n_0-k \pmod{k!}$  и в равенстве (4.1.5) каждое слагаемое суммы  $p_{k-1}(n-k) + \dots + p_1(n-k)$  есть полином от  $n$ , а вся сумма есть полином со старшим членом  $n^{k-2}/(k-2)!(k-1)!$ . Но тогда

$$p_k(n) - p_k(n-k) = \frac{n^{k-2}}{(k-2)!(k-1)!} + R_{k-3}(n), \quad (4.1.7)$$

где  $R_{k-3}(n)$  — полином от  $n$  степени не выше  $k-3$ . Точно так же получаем, что

$$p_k(n-ik) - p_k(n-(i+1)k) = \frac{n^{k-2}}{(k-2)!(k-1)!} + R_{k-3}^i(n) \quad (4.1.8)$$

для  $i = 1, 2, \dots, (k-1)! - 1$ . Суммируя, приходим к равенству

$$p_k(n) - p_k(n - k!) = \frac{n^{k-2}}{(k-2)!} + S_{k-3}(n), \quad (4.1.9)$$

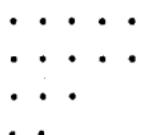
где  $S_{k-3}(n)$  — некоторый полином от  $n$  степени не выше  $k-3$ . Уравнение (4.1.9) определяет теперь все значения  $p_k(n)$  с  $n \equiv n_0 \pmod{k!}$  через наименьшее значение  $p_k(n_0)$ . Нетрудно, однако, заметить, что решение (4.1.9) имеет вид

$$p_k(n) = \frac{n^{k-1}}{(k-1)!k!} + R_{k-2}(n), \quad n \equiv n_0 \pmod{k!}, \quad (4.1.10)$$

где  $R_{k-2}(n)$  — полином от  $n$  степени не выше  $k-2$ . Таким образом, формула (4.1.10) доказана по индукции.

Вспомним теперь, что число упорядоченных разбиений  $n$  на  $k$  частей равно  $\binom{n-1}{k-1}$  — полиному степени  $k-1$  относительно  $n$  со старшим членом  $n^{k-1}/(k-1)!$ . Если  $k$  частей различны, то каждое неупорядоченное разбиение дает  $k!$  упорядоченных разбиений. Полином  $(1/k!)\binom{n-1}{k-1}$  от  $n$  имеет степень  $k-1$ , и его старший член равен  $n^{k-1}/(k-1)!k!$ ; сравнение с (4.1.10) показывает, что для больших  $n$  в большинстве (в некотором смысле) разбиений  $n$  на  $k$  частей все  $k$  частей различны.

С разбиением числа  $n$  мы можем связать некоторую диаграмму, изображая каждую часть строкой из соответствующего количества точек и помещая в верхнюю строку наибольшую часть, а затем остальные части в порядке убывания. Таким образом, разбиение  $15 = 5 + 5 + 3 + 2$  мы представляем следующей диаграммой:



Начала всех строк образуют, как показано, один столбец. Диаграмму можно читать также по столбцам, и тогда разбиение имеет вид  $15 = 4 + 4 + 3 + 2 + 2$ . Два разбиения, связанные таким образом, называются *сопряженными*. Очевидно, отношение сопряженности симметрично.

**Теорема 4.1.1.** Число разбиений целого числа  $n$  на  $k$  частей равно числу разбиений  $n$  на части, наибольшая из которых есть  $k$ .

**Доказательство.** Сопряженное разбиение для разбиения с  $k$  частями есть разбиение, наибольшая часть которого равна  $k$ , и обратно.

Мы обратимся теперь ко всевозможным разбиениям  $n$ , обозначив их число через  $p(n)$ . Если расположить части в убывающем порядке, то, поскольку существует не более  $n$  частей, получаем, что  $p(n)$  есть число решений в целых числах уравнения

$$n = x_1 + x_2 + \dots + x_n, \quad x_1 \geq x_2 \geq \dots \geq x_n \geq 0. \quad (4.1.11)$$

Мы можем также описать разбиение  $n$  числом  $y_k$  частей величины  $k$  ( $k = 1, 2, \dots, n$ ). Тогда  $p(n)$  есть также число решений в целых числах уравнения

$$n = 1y_1 + 2y_2 + \dots + ny_n, \quad y_i \geq 0, \quad i = 1, \dots, n. \quad (4.1.12)$$

**Теорема 4.1.2.** Производящая функция для  $p(n)$ ,

$$f(x) = 1 + p(1)x + p(2)x^2 + \dots + p(n)x^n + \dots,$$

имеет вид

$$P(x) = \prod_{i=1}^{\infty} (1 - x^i)^{-1}.$$

**Доказательство.** Запишем разложение  $(1 - x^i)^{-1} = 1 + x^i + x^{2i} + \dots + x^{ri} + \dots$ . Каждое представление  $n$  вида (4.1.12) дает член  $x^n$  в произведении

$$P(x) = \prod_{i=1}^{\infty} (1 - x^i)^{-1},$$

если взять  $x^{iy_j}$  из сомножителя  $(1 - x^j)^{-1}$ ; обратно: каждое  $x^n$  в разложении  $P(x)$  получается таким способом. Следовательно,

$$P(x) = \sum_{n=0}^{\infty} p(n)x^n,$$

если принять  $p(0) = 1$ . Разбиения

$$\begin{aligned}
 1 &= 1, & 4 &= 4, & 5 &= 5, \\
 2 &= 2, & 4 &= 3 + 1, & 5 &= 4 + 1, \\
 2 &= 1 + 1, & 4 &= 2 + 2, & 5 &= 3 + 2, \\
 3 &= 3, & 4 &= 2 + 1 + 1, & 5 &= 3 + 1 + 1, \\
 3 &= 2 + 1, & 4 &= 1 + 1 + 1 + 1, & 5 &= 2 + 2 + 1, \\
 3 &= 1 + 1 + 1, & & & 5 &= 2 + 1 + 1 + 1, \\
 & & & & 5 &= 1 + 1 + 1 + 1 + 1
 \end{aligned} \tag{4.1.13}$$

непосредственно дают нам значения

$$p(1) = 1, \quad p(2) = 2, \quad p(3) = 3, \quad p(4) = 5, \quad p(5) = 7. \tag{4.1.14}$$

Функция  $\varphi(x) = \prod_{i=1}^{\infty} (1 - x^i)$ , обратная к  $P(x)$ , является производящей функцией коэффициентов  $c_n$  ряда

$$\varphi(x) = \prod_{i=1}^{\infty} (1 - x^i) = \sum_{n=0}^{\infty} c_n x^n, \quad c_0 = 1, \tag{4.1.15}$$

где  $c_n$  имеет комбинаторную интерпретацию

$$c_n = p_q(n) - p_u(n), \tag{4.1.16}$$

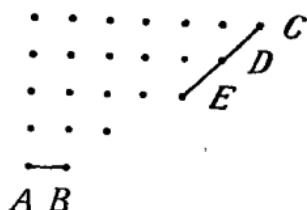
$p_q(n)$  — число разбиений  $n$  на четное число различных частей,  $p_u(n)$  — число разбиений  $n$  на нечетное число различных частей. Эту интерпретацию можно использовать для вычисления  $c_n$ .

**Теорема 4.1.3** (тождество Эйлера). *Справедливо тождество*

$$\prod_{i=1}^{\infty} (1 - x^i) = 1 + \sum_{k=1}^{\infty} (-1)^k (x^{(3k^2-k)/2} + x^{(3k^2+k)/2}).$$

**Доказательство.** Приводимое доказательство принадлежит Франклину [1]. Оно использует комбинаторную природу коэффициента  $c_n$ , которая отражается равенством (4.1.16). Возьмем диаграмму, представляющую разбиение  $n$  на неравные части в порядке убывания величины. Назовем самую нижнюю строку основанием  $b$  этой диаграммы. Из  $C$ , крайней справа точки верхней строки, проведем через точки нашей диаграммы насколько возможно длинную прямую с угловым коэффициентом 1; может случиться, разумеется, что она будет

содержать только одну точку. Эту линию назовем наклонной  $s$ :



В приводимой диаграмме основание  $b$  есть линия  $AB$ , а  $CDE$  — наклонная  $s$ . Будем пользоваться буквами  $b$  и  $s$  также для обозначения числа точек в основании и наклонной соответственно. Например,  $b = 2$ ,  $s = 3$  означает, что  $b$  содержит две, а  $s$  — три точки.

Определим теперь две операции на диаграммах и обозначим их через  $\alpha$  и  $\beta$ :

- 1)  $\alpha$ . Если  $b \leq s$  и если основание и наклонная не имеют общей точки, то перемещаем основание, присоединяя его точки к первым строкам, чтобы образовать новую наклонную. Если основание и наклонная пересекаются и  $b \leq s - 1$ , эта операция все еще возможна.
- 2)  $\beta$ . Если  $b > s$ , то перемещаем наклонную и рассматриваем ее в качестве нового основания. Это возможно, если основание и наклонная не пересекаются. Если основание и наклонная пересекаются, то это все еще возможно при  $b \geq s + 2$ .

Так как для  $\alpha$  требуется  $b \leq s$ , а для  $\beta$  требуется  $b > s$ , то к произвольной диаграмме  $D$  можно применить самое большее одну из операций  $\alpha$ ,  $\beta$ . Далее, легко проверить, что если операция  $\alpha$  допустима, то, применяя  $\alpha$  к  $D$ , мы получим диаграмму  $D'$ , для которой допустима операция  $\beta$ , и применение  $\beta$  к  $D'$  дает  $D$ . Аналогично если  $\beta$  можно применить к  $D$ , чтобы получить  $D''$ , то  $\alpha$  можно применить к  $D''$ , чтобы получить  $D$ . Таким образом, эти операции устанавливают взаимно однозначное соответствие между разбиениями на четное число различных частей и разбиениями на нечетное число различных частей во всех случаях, когда эти операции применимы. Если  $b \leq s$ , то  $\alpha$  нельзя применить только тогда, когда основание и наклонная пересекаются и

$b = s = k$ . В этом случае разбиение имеет вид

$$n = k + (k + 1) + \dots + (2k - 1) = \frac{3k^2 - k}{2}. \quad (4.1.17)$$

Если  $b > s$ , в нельзя применить только тогда, когда основание и наклонная пересекаются и  $b - 1 = s = k$ . Здесь разбиение имеет вид

$$n = (k + 1) + (k + 2) + \dots + 2k = \frac{3k^2 + k}{2}. \quad (4.1.18)$$

Таким образом,  $p_q(n) = p_u(n)$  и  $c_n = 0$ , если только  $n$  не имеет вида  $(3k^2 \pm k)/2$ ; в случае  $n = (3k^2 \pm k)/2$  существует одно разбиение на  $k$  частей, заданное либо формулой (4.1.17), либо формулой (4.1.18), и его вкладом в  $c_n$  является  $(-1)^k$ ; следовательно,  $c_n = (-1)^k$  для  $n = (3k^2 \pm k)/2$ . Таким образом, мы показали, что

$$c_n = \begin{cases} 0, & \text{если } n \neq (3k^2 \pm k)/2, \\ (-1)^k, & \text{если } n = (3k^2 \pm k)/2. \end{cases} \quad (4.1.19)$$

Значит, коэффициенты  $c_n$  в (4.1.15) вычисляются по (4.1.19), и теорема 4.1.3 доказана.

Теоремы 4.1.2 и 4.1.3 дают тождество

$$\left[ 1 + \sum_{k=1}^{\infty} (-1)^k (x^{(3k^2-k)/2} + x^{(3k^2+k)/2}) \right] \left[ \sum_{n=0}^{\infty} p(n) x^n \right] = 1, \quad (4.1.20)$$

если учесть, что  $p(0) = 1$ . Это тождество можно использовать для получения рекуррентного соотношения  $p(n)$ , вычисляя коэффициент при  $x^n$ ,  $n \geq 1$ , в левой части (4.1.20) и полагая его равным нулю. Тогда получится

$$\begin{aligned} p(n) &= p(n-1) + p(n-2) - p(n-5) - p(n-7) + \dots \\ &\dots + (-1)^{k-1} p\left(n - \frac{3k^2 - k}{2}\right) + (-1)^{k-1} p\left(n - \frac{3k^2 + k}{2}\right) + \dots, \end{aligned} \quad (4.1.21)$$

причем все аргументы в правой части неотрицательны и учитывается условие  $p(0) = 1$ . Этим способом можно вычислить значения  $p(n)$ , как показано в табл. 4.2.

Теорему 4.1.3 и другие результаты можно вывести из некоторого более общего тождества.

Таблица 4.2

Значения  $p(n)$ 

| $\sum n$ | $p(n)$ | $n$  | $p(n)$  | $n$ | $p(n)$    | $n$ | $p(n)$      |
|----------|--------|------|---------|-----|-----------|-----|-------------|
| 1        | 1      | 26   | 2 436   | 51  | 239 943   | 76  | 9 289 091   |
| 2        | 2      | 27   | 3 010   | 52  | 281 589   | 77  | 10 619 863  |
| 3        | 3      | 28   | 3 718   | 53  | 329 931   | 78  | 12 132 164  |
| 4        | 5      | 29   | 4 565   | 54  | 386 155   | 79  | 13 848 650  |
| 5        | 7      | 30   | 5 604   | 55  | 451 276   | 80  | 15 796 476  |
| 6        | 11     | 31   | 6 842   | 56  | 526 823   | 81  | 18 004 327  |
| 7        | 15     | 6 32 | 8 349   | 57  | 614 154   | 82  | 20 506 255  |
| 8        | 22     | 33   | 10 143  | 58  | 715 220   | 83  | 23 338 469  |
| 9        | 30     | 34   | 12 310  | 59  | 831 820   | 84  | 26 543 660  |
| 10       | 42     | 35   | 14 883  | 60  | 966 467   | 85  | 30 167 357  |
| 11       | 56     | 36   | 17 977  | 61  | 1 121 505 | 86  | 34 262 902  |
| 12       | 77     | 37   | 21 637  | 62  | 1 300 156 | 87  | 38 887 673  |
| 13       | 101    | 38   | 26 015  | 63  | 1 505 499 | 88  | 44 108 109  |
| 14       | 135    | 39   | 31 185  | 64  | 1 741 630 | 89  | 49 995 925  |
| 15       | 176    | 40   | 37 338  | 65  | 2 012 558 | 90  | 56 634 173  |
| 16       | 231    | 41   | 44 583  | 66  | 2 323 520 | 91  | 64 112 359  |
| 17       | 297    | 42   | 53 174  | 67  | 2 679 689 | 92  | 72 533 807  |
| 18       | 385    | 43   | 63 261  | 68  | 3 087 735 | 93  | 82 010 177  |
| 19       | 490    | 44   | 75 175  | 69  | 3 554 345 | 94  | 92 669 720  |
| 20       | 627    | 45   | 89 134  | 70  | 4 087 968 | 95  | 104 651 419 |
| 21       | 792    | 46   | 105 558 | 71  | 4 697 205 | 96  | 118 114 304 |
| 22       | 1002   | 47   | 124 754 | 72  | 5 392 783 | 97  | 133 230 930 |
| 23       | 1255   | 48   | 147 273 | 73  | 6 185 689 | 98  | 150 198 136 |
| 24       | 1575   | 49   | 173 525 | 74  | 7 089 500 | 99  | 169 229 875 |
| 25       | 1958   | 50   | 204 226 | 75  | 8 118 264 | 100 | 190 569 292 |

Теорема 4.1.4 (тождество Гаусса — Якоби). Следующее тождество справедливо при всех  $z \neq 0$  и всех  $q$  с  $|q| < 1$ :

$$\prod_{k=1}^{\infty} (1 - q^{2k})(1 - q^{2k-1}z^2)(1 - q^{2k-1}z^{-2}) = \\ = \sum_{k=-\infty}^{+\infty} (-1)^k z^{2k} q^{k^2}. \quad (4.1.22)$$

**Доказательство.** Запишем

$$\varphi(z) = \prod_{k=1}^n (1 - q^{2k-1}z^2)(1 - q^{2k-1}z^{-2}). \quad (4.1.23)$$

Непосредственно проверяется, что

$$\varphi(qz)(-qz^2 + q^{2n}) = \varphi(z)(1 - q^{2n+1}z^2). \quad (4.1.24)$$

Справедливо также равенство

$$\begin{aligned} \varphi(z) = A_0 - A_1(z^2 + z^{-2}) + A_2(z^4 + z^{-4}) + \dots \\ \dots + (-1)^n A_n(z^{2n} + z^{-2n}), \end{aligned} \quad (4.1.25)$$

где  $A_i$  — полиномы от  $q$  и

$$A_n = q^{1+3+\dots+2n-1} = q^{n^2}. \quad (4.1.26)$$

Подставляя (4.1.25) в (4.1.24) и приравнивая коэффициенты при  $z^{-2k+2}$ , получаем

$$A_k = A_{k-1}q^{2k-1} \frac{1 - q^{2n-2k+2}}{1 - q^{2n+2k}}. \quad (4.1.27)$$

Из (4.1.26) и (4.1.27) находим  $A_k$ :

$$\begin{aligned} A_k = \frac{q^{k^2}}{(1 - q^2)(1 - q^4)\dots(1 - q^{2n})} \prod_{2s=2n-2k+2}^{2n} (1 - q^{2s}) \times \\ \times \prod_{2s=2n+2k+2}^{4n} (1 - q^{2s}); \end{aligned} \quad (4.1.28)$$

эта величина при  $n \rightarrow \infty$  стремится к

$$\frac{q^{k^2}}{(1 - q^2)(1 - q^4)\dots}. \quad (4.1.29)$$

Из (4.1.28) получаем, что

$$\begin{aligned} \prod_{k=1}^n (1 - q^{2k})(1 - q^{2k-1}z^2)(1 - q^{2k-1}z^{-2}) = \\ = \sum_{k=-n}^{+n} (-1)^k z^{2k} q^{k^2} B_k, \end{aligned} \quad (4.1.30)$$

где  $B_k$  определяется равенством

$$B_k = \prod_{2s=2n-2k+2}^{2n} (1 - q^{2s}) \prod_{2s=2n+2k+2}^{4n} (1 - q^{2s}). \quad (4.1.31)$$

Для любого  $k \lim_{n \rightarrow \infty} B_k = 1$ . Переходя к пределу, устанавливаем справедливость теоремы.

Из тождества Гаусса — Якоби без труда получается теорема 4.1.3, если заменить  $q, z$  на  $q^{3/2}, q^{1/4}$  соответственно:

$$\prod_{k=1}^{\infty} (1 - q^{3k})(1 - q^{3k-1})(1 - q^{3k-2}) = \sum_{-\infty < k < +\infty} (-1)^k q^{(3k^2+k)/2}; \quad (4.1.32)$$

это иная запись тождества теоремы 4.1.3. Выведем еще одну формулу Якоби.

**Теорема 4.1.5** (тождество Якоби). *Справедливо тождество*

$$\prod_{k=1}^{\infty} (1 - q^k)^3 = 1 + \sum_{k=1}^{\infty} (-1)^k (2k+1) q^{k(k+1)/2}. \quad (4.1.33)$$

**Доказательство.** Хотя произведение в левой части можно связать с разбиениями на части, ни одна из которых не может быть использована более трех раз, никакое комбинаторное доказательство этого тождества автору не известно.

В формуле (4.1.22) заменим  $q, z$  на  $q^{1/2}, q^{1/4+\varepsilon}$  соответственно и возьмем  $\varepsilon$  сколь угодно малым. Тогда получим

$$\begin{aligned} \prod_{k=1}^{\infty} (1 - q^k)(1 - q^{k+2\varepsilon})(1 - q^{k-1-2\varepsilon}) &= \\ &= \sum_{-\infty < k < +\infty} (-1)^k q^{k/2+2\varepsilon k} q^{k^2/2}. \end{aligned} \quad (4.1.34)$$

Множитель  $(1 - q^{-2\varepsilon})$  в левой части можно записать в виде

$$1 - e^{-2\varepsilon \log q} = 1 - (1 - 2\varepsilon \log q + \dots) = 2\varepsilon \log q + \dots, \quad (4.1.35)$$

где последующие члены содержат более высокие степени  $\varepsilon$ . Аналогично для члена из правой части

$$q^{2\varepsilon k} = 1 + (2k \log q) \varepsilon + \dots, \quad (4.1.36)$$

где снова последующие члены содержат более высокие степени  $\epsilon$ . В сумме

$$\sum_{-\infty < k < +\infty} (-1)^k (1 + 2k\epsilon \log q + \dots) q^{(k^2+k)/2} \quad (4.1.37)$$

члены, не содержащие  $\epsilon$ , обращаются в нуль, так как слагаемые с  $k=r$  и  $k=-r-1$  сокращаются, и формула (4.1.34) принимает вид

$$(2\epsilon \log q + \dots) \prod_{k=1}^{\infty} (1 - q^k)(1 - q^{k+2\epsilon}) \prod_{k=2}^{\infty} (1 - q^{k-1-2\epsilon}) = \\ = \sum_{-\infty < k < +\infty} (-1)^k (2k\epsilon \log q + \dots) q^{(k^2+k)/2}. \quad (4.1.38)$$

Если мы теперь разделим на  $2\epsilon \log q$  и затем устрим  $\epsilon$  к нулю, то получим равенство

$$\prod_{k=1}^{\infty} (1 - q^k)^3 = \sum_{-\infty < k < +\infty} (-1)^k \cdot k q^{(k^2+k)/2}, \quad (4.1.39)$$

что и доказывает формулу Якоби.

Рамануджан, индийский гений-самоучка, „открытый“ Харди, впервые подметил некоторые любопытные арифметические свойства числа разбиений  $p(n)$ . Это

$$p(5m+4) \equiv 0 \pmod{5}, \quad (4.1.40a)$$

$$p(7m+5) \equiv 0 \pmod{7}, \quad (4.1.40b)$$

$$p(11m+6) \equiv 0 \pmod{11}. \quad (4.1.40c)$$

Мы докажем первые два из них, как это было сделано Рамануджаном, используя тождества Эйлера и Якоби. В силу этих тождеств

$$q \{(1-q)(1-q^2)\dots\}^4 = \\ = q \{(1-q)(1-q^2)\dots\} \{(1-q)(1-q^2)\dots\}^3 = \\ = q(1-q-q^2+q^5+q^7+\dots)(1-3q+5q^3-7q^6+\dots). \quad (4.1.41)$$

Запишем это в таком виде:

$$q \{(1-q)(1-q^2)\dots\}^4 = \sum_r \sum_s (-1)^{r+s} (2s+1) q^{E(r,s)}, \quad (4.1.42)$$

где

$$E(r, s) = 1 + \frac{1}{2} r(3r+1) + \frac{1}{2} s(s+1) \quad (4.1.43)$$

и  $r$  пробегает значения от  $-\infty$  до  $+\infty$ , в то время как  $s$  изменяется от 0 до  $\infty$ . Пусть  $E(r, s)$  кратно 5. Отсюда вытекает, что

$$2(r+1)^2 + (2s+1)^2 = 8E(r, s) - 10r^2 - 5 \quad (4.1.44)$$

также кратно 5. Но

$$2(r+1)^2 \equiv 0, 2, 3 \pmod{5}, \quad (2s+1)^2 \equiv 0, 1, 4 \pmod{5}. \quad (4.1.45)$$

Следовательно,  $E(r, s) \equiv 0 \pmod{5}$  только тогда, когда

$$r+1 \equiv 2s+1 \equiv 0 \pmod{5}. \quad (4.1.46)$$

Поэтому в формуле (4.1.42) показатель  $E(r, s)$  кратен 5 лишь тогда, когда коэффициент  $2s+1$  также кратен 5. Значит, в

$$q \{(1-q)(1-q^2)\dots\}^4$$

коэффициент при  $q^{5m+5}$  кратен 5. В биномиальном разложении  $(1-q)^{-5}$  все коэффициенты делятся на 5 за исключением коэффициентов при степенях 1,  $q^5$ ,  $q^{10}$ , ..., которые сравнимы с 1 по мод 5. Мы выразим это так:

$$\frac{1}{(1-q)^5} \equiv \frac{1}{1-q^5} \pmod{5}, \quad (4.1.47)$$

или

$$\frac{1-q^5}{(1-q)^5} \equiv 1 \pmod{5}, \quad (4.1.48)$$

где сравнения означают, что все коэффициенты полиномов сравнимы по мод 5. Следовательно, коэффициент при  $q^{5m+5}$  в

$$\begin{aligned} & q \frac{(1-q^5)(1-q^{10})\dots}{(1-q)(1-q^2)\dots} = \\ & = q \frac{\{(1-q)(1-q^2)\dots\}^4 (1-q^5)(1-q^{10})\dots}{\{(1-q)(1-q^2)\dots\}^5} \end{aligned} \quad (4.1.49)$$

кратен 5, а значит, и коэффициент при  $q^{5m+5}$  в

$$\frac{q}{(1-q)(1-q^2)\dots} \quad (4.1.50)$$

кратен 5; но он совпадает с  $p(5m + 4)$ . Этим доказано (4.1.40а). Точно так же мы можем использовать квадрат тождества Якоби, чтобы доказать (4.1.40б). Никакого столь же простого доказательства формулы (4.1.40с) не известно<sup>1)</sup>.

Производящая функция  $P(x) = \sum_{n=1}^{\infty} p(n)x^n$  связана с арифметикой еще и другим способом; а именно она связана с функцией  $\sigma(n)$  делителей числа  $n$ , определяемой равенством

$$\sigma(n) = \sum_{d|n} d. \quad (4.1.51)$$

Пусть

$$P(x) = \sum_{k=1}^{\infty} (1 - x^k)^{-1} \quad (4.1.52)$$

— производящая функция. Тогда

$$\log(P(x)) = \sum_{k=1}^{\infty} -\log(1 - x^k). \quad (4.1.53)$$

Если взять теперь производную от (4.1.53) по  $x$  и умножить результат на  $x$ , то получим равенство

$$\frac{xP'(x)}{P(x)} = \sum_{k=1}^{\infty} \frac{kx^k}{1 - x^k}. \quad (4.1.54)$$

Из разложения по степеням  $x$   $k$ -го члена в правой части видно, что его вклад в коэффициент при каждой степени  $x^{mk}$  равен  $k$ . Следовательно, коэффициент при  $x^n$  в правой части есть  $\sigma(n)$ , сумма всех делителей числа  $n$ . Таким образом,

$$\frac{xP'(x)}{P(x)} = \sum_{n=1}^{\infty} \sigma(n)x^n. \quad (4.1.55)$$

<sup>1)</sup> Элементарное доказательство сравнения (4.1.40 с) получено недавно Винквиистом (Winquist L., *J. of combinatorial theory*, 6 (1969), № 1, 56—59). — Прим. ред.

## 4.2. Асимптотические свойства $p(n)$

Если мы зададим себе вопрос о том, как велико  $p(n)$  для больших значений  $n$ , то столкнемся с задачей, относящейся по существу к аналитической теории чисел. И хотя эта тема выходит тем самым за рамки настоящей книги, полученные результаты столь привлекательны, что мы вкратце их изложим.

Функция делителей  $\sigma(n)$  обладает весьма нерегулярным ростом, однако ее среднее значение достаточно гладко растет. Если мы определим  $s(n)$  посредством равенства

$$s(n) = \sum_{k=1}^n \sigma(k), \quad (4.2.1)$$

то несложный подсчет показывает, что

$$s(n) = \sum_{h=1}^n \frac{1}{2} \left\{ \left[ \frac{n}{h} \right]^2 + \left[ \frac{n}{h} \right] \right\}, \quad (4.2.2)$$

где  $[x]$  означает наибольшее целое, не превосходящее  $x$ . Так как ряд

$$\sum_{h=1}^{\infty} \frac{1}{h^2} \quad (4.2.3)$$

сходится и имеет суммой  $\pi^2/6$ , то мы можем получить довольно хорошую оценку  $s(n)$ , а именно

$$\frac{\pi^2 n^2}{12} - \frac{n}{2} \log n - \frac{3n}{2} < s(n) < \frac{\pi^2 n^2}{12} + \frac{n}{2} \log n + \frac{n}{2}. \quad (4.2.4)$$

Так как

$$(1-x)^{-1} \sum_{n=1}^{\infty} \sigma(n) x^n = \sum_{n=1}^{\infty} s(n) x^n, \quad (4.2.5)$$

то мы можем представить равенство (4.1.55) в виде

$$\frac{xP'(x)}{P(x)} = (1-x) \sum_{n=1}^{\infty} s(n) x^n. \quad (4.2.6)$$

С помощью довольно элементарных вычислений мы можем, используя в (4.2.6) оценку (4.2.4) для  $s(n)$ , вывести, что асимптотически

$$\log p(n) \sim A \sqrt{n}, \quad A = \pi \sqrt{\frac{2}{3}}, \quad (4.2.7)$$

где  $f(n) \sim g(n)$  означает, что

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1.$$

Вывод формулы (4.2.7) из (4.2.4) и (4.2.6) — процесс весьма длительный, и мы его здесь не приводим, поскольку результат получается довольно слабый. В действительности асимптотическое значение  $p(n)$  дается выражением

$$p(n) \sim \frac{1}{4n \sqrt{3}} e^{AV\sqrt{n}}. \quad (4.2.8)$$

Ряд  $P(x)$  сходится в единичном круге и имеет единичную окружность границей круга сходимости. По теореме Коши имеем

$$p(n) = \frac{1}{2\pi i} \int_C \frac{P(x)}{x^{n+1}} dx, \quad (4.2.9)$$

где  $C$  — контур, включающий начало координат. Харди и Рамануджан [1] изучали асимптотическое значение  $p(n)$ , используя (4.2.9) и некоторые функциональные равенства. В частности, если комплексные числа  $x$ ,  $x'$  с  $|x|, |x'| < 1$  связаны соотношением

$$\log \frac{1}{x} \log \frac{1}{x'} = 4\pi^2 \quad \text{или} \quad x' = \exp \left\{ \frac{-4\pi^2}{\log(1/x)} \right\}, \quad (4.2.10)$$

то имеет место тождество

$$P(x) = \frac{x^{1/24}}{\sqrt{2\pi}} \sqrt{\log \frac{1}{x}} \exp \left\{ \frac{\pi^2}{6 \log(1/x)} \right\} P(x'). \quad (4.2.11)$$

Если  $x$  действительно и близко к 1, то  $x'$  чрезвычайно мало и  $P(x')$  практически равно 1, так что (4.2.11) эффективно выражает  $P(x)$  через элементарные функции. Существуют аналогичные формулы, связанные с корнями

из единицы, так что если  $x$  находится вблизи  $x_{p,q} = \exp(2\pi i(p/q))$  для взаимно простых  $p$  и  $q$ , то мы можем с большой точностью аппроксимировать  $P(x)$  элементарными функциями.

Взяв в качестве  $C$  в формуле (4.2.9) окружность радиуса  $1 - 1/n$  и подставив (4.2.11) в (4.2.9), заменив при этом  $P(x')$  на 1 (с ошибкой порядка  $e^{H\sqrt{n}}$ , где  $H < A = \pi \sqrt{\frac{2}{3}}$ ), Харди и Рамануджан вывели формулу

$$p(n) = \frac{1}{2\pi\sqrt{2}} \frac{d}{dn} \left( \frac{e^{A\lambda_n}}{\lambda_n} \right) + O(e^{H\sqrt{n}}), \quad (4.2.12)$$

где

$$\lambda_n = \sqrt{n - \frac{1}{24}}. \quad (4.2.13)$$

Символ  $O$  в (4.2.12) — частный случай общего обозначения  $f(n) = O(g(n))$ , означающего, что существует такая постоянная  $K$ , что

$$\limsup_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| \leq K.$$

Оценка (4.2.12) заключает в себе (4.2.8), но является гораздо более точной.

Формула (4.2.12) может быть значительно улучшена. Когда  $x$  приближается к  $x_{p,q}$  по радиусу,  $P(x)$  ведет себя, в грубом приближении, подобно  $\exp\{\pi^2/6q^2(1-|x|)\}$ . Таким образом, в интеграле (4.2.9) „рациональные особенности“  $x_{p,q}$  являются наиболее весомыми особенностями, и следует ожидать, что их значения в интеграле (4.2.9) будут перевешивать остальное. Это привело Харди и Рамануджана к поискам формулы вида

$$p(n) = P_1(n) + P_2(n) + \dots + P_Q(n) + R(n), \quad (4.2.14)$$

где  $P_1(n)$  — доминирующий член в (4.2.12),  $P_q(n)$  для  $q = 2, \dots, Q$  устроены одинаково и в  $P_q(n)$  собраны значения вблизи рациональных точек со знаменателем  $q$ , а  $R(n)$  — остаточный член. Так как Мак-Магон вычислил  $p(n)$  для значений  $n$  вплоть до 200, представлялось

естественным проверить формулы для  $n = 200$ . К своему удивлению Харди и Рамануджан нашли, что восемь членов их формулы дают  $p(200)$  с ошибкой всего лишь 0,004. Таким образом, численный анализ Мак-Магона, как назвали бы мы его теперь, стимулировал дальнейшее развитие теории Харди и Рамануджана, и они сумели показать существование таких постоянных  $a, M$ , что

$$p(n) = \sum_{q < a\sqrt{n}} P_q(n) + R(n), \quad (4.2.15)$$

где

$$|R(n)| < Mn^{-1/4}. \quad (4.2.16)$$

Таким образом, была получена формула, которая точно описывала бы  $p(n)$ , если только  $a$  и  $M$  были бы найдены. Пытаясь упростить методы Харди и Рамануджана, Радемахер [1], сделав незначительные изменения, нашел сходящийся ряд для  $p(n)$ . Положив

$$\psi_q(n) = \frac{q^{1/2}}{\pi\sqrt{2}} \cdot \frac{d}{dn} \left\{ \frac{\operatorname{sh}(A\lambda_n/q)}{\lambda_n} \right\}, \quad A = \pi \sqrt{\frac{2}{3}}, \quad (4.2.17)$$

и

$$L_q(n) = \sum_p w_{p,q} \exp\left(\frac{-2np\pi i}{q}\right), \quad (4.2.18)$$

где  $w_{p,q}$  — некоторый корень 24-й степени из единицы, Радемахер доказал, что

$$p(n) = \sum_{q=1}^{\infty} L_q(n) \psi_q(n) \quad (4.2.19)$$

и что остаток после  $Q$  членов меньше, чем

$$CQ^{-1/2} + D \left(\frac{Q}{n}\right)^{1/2} \operatorname{sh}\left(\frac{An^{1/2}}{Q}\right), \quad (4.2.20)$$

где  $C$  и  $D$  — постоянные, для которых он нашел точные значения. Для  $Q$  порядка  $\sqrt{n}$  этот результат аналогичен (4.2.15) и (4.2.16). Но в одном важном отношении результат Радемахера лучше, ибо, как было показано Лемером [1], бесконечные ряды Харди и Рамануджана не сходятся.

## Задачи

1. Вычислить  $p(101)$ ,  $p(102)$ ,  $p(103)$ ,  $p(104)$  и  $p(105)$ . Проверить эти значения, используя сравнения (4.1.40).

2. Показать, что  $p^*(n) = p(n) - p(n-1)$  для  $n \geq 1$  есть число разбиений  $n$  на части, большие единицы. Опираясь на свойства  $p^*(n)$ , показать, что  $p(n+2) - 2p(n+1) + p(n) \geq 0$  при  $n \geq 0$ .

3. Доказать, что число разбиений любого положительного целого числа  $n$  на различные части равно числу разбиений  $n$  на нечетные части, показав, что

$$(1+x)(1+x^2)\dots(1+x^i)\dots = \frac{1}{(1-x)(1-x^3)\dots(1-x^{2i-1})\dots}.$$

4. Доказать посредством комбинаторных рассуждений, что

$$(1+x)(1+x^3)\dots(1+x^{2n-1})\dots = \\ = 1 + \frac{x}{1-x^2} + \frac{x^4}{(1-x^2)(1-x^4)} + \dots + \frac{x^{n^2}}{(1-x^2)\dots(1-x^{2n})} + \dots$$

5. Показать, что

$$f_1(n, k) = \frac{1}{k!} \binom{n-1}{k-1} \leq p_k(n)$$

для всех  $n \geq 1$  и  $k \geq 1$ . Указать в явном виде такую функцию  $f_2(n, k)$ , что  $p_k(n) \leq f_2(n, k)$  для всех  $n \geq 1$ ,  $k \geq 1$  и при фиксированном  $k$  отношение  $f_2(n, k)/f_1(n, k)$  стремится к 1, когда  $n \rightarrow \infty$ .

6. Выразить  $p_4(n)$  через полиномы от  $n$ , коэффициенты которых зависят от класса вычетов  $n$  по модулю 12.

# Системы различных представителей

---

## 5.1. Теоремы Ф. Холла и Д. Кёнига

Следующая задача является типичной для этой главы. Даны пять множеств:

$$\begin{aligned}
 S_1 &= \{1, 2, 3\}, \\
 S_2 &= \{1, 2, 4\}, \\
 S_3 &= \{1, 2, 5\}, \\
 S_4 &= \{3, 4, 5, 6\}, \\
 S_5 &= \{3, 4, 5, 6\},
 \end{aligned} \tag{5.1.1}$$

требуется выбрать такие различные числа  $x_1, x_2, x_3, x_4, x_5$ , что  $x_i \in S_i$ ,  $i = 1, \dots, 5$ . Одним из способов выбора является  $x_1 = 1$ ,  $x_2 = 2$ ,  $x_3 = 5$ ,  $x_4 = 3$ ,  $x_5 = 4$ . Но если взять множества

$$\begin{aligned}
 T_1 &= \{1, 2\}, \\
 T_2 &= \{1, 2\}, \\
 T_3 &= \{1, 2\}, \\
 T_4 &= \{3, 4, 5, 6\}, \\
 T_5 &= \{3, 4, 5, 6\},
 \end{aligned} \tag{5.1.2}$$

то такой выбор оказывается невозможным, так как нельзя выбрать три различных числа из множеств  $T_1, T_2, T_3$ , содержащих лишь два числа: 1 и 2. Возникает вопрос: при каких условиях подмножества  $S_i$ ,  $i = 1, \dots, n$ , множества  $S$  обладают различными представителями  $x_i$ ,  $i = 1, \dots, n$ , т. е.  $x_i \in S_i$  и  $x_i \neq x_j$ , если  $i \neq j$ ? Заметим, что не требуется, чтобы  $S_i$  и  $S_j$  с  $i \neq j$  были различными подмножествами множества  $S$ . Как видно из (5.1.2), очевидное необходимое условие для существования различных представителей состоит в том, чтобы

в совокупности всех элементов произвольных  $k$  множеств  $S_i$  содержалось не менее  $k$  различных элементов. Мы будем, когда это удобно, систему различных представителей обозначать сокращенно с. р. п. Примечателен тот факт (доказанный впервые Ф. Холлом [1] в 1935 г.), что это очевидное необходимое условие для существования различных представителей является также достаточным.

**Теорема 5.1.1** (Филипп Холл). *Пусть  $I$  — конечное множество индексов,  $I = \{1, 2, \dots, n\}$ , и  $S_i$  для каждого  $i \in I$  — подмножество некоторого множества  $S$ . Необходимым и достаточным условием существования различных представителей  $x_i$ ,  $i = 1, \dots, n$ ,  $x_i \in S_i$ ,  $x_i \neq x_j$  при  $i \neq j$ , является условие С: для каждого  $k = 1, \dots, n$  и каждой последовательности  $k$  различных индексов  $i_1, \dots, i_k$  в совокупности всех элементов подмножеств  $S_{i_1}, \dots, S_{i_k}$  содержится не менее  $k$  различных элементов.*

**Доказательство.** Мы уже выяснили необходимость условия С для существования различных представителей, и теперь надо доказать его достаточность. Заметим, что если каждое  $S_i$  содержит единственный элемент  $x_i$ , то выполнение условия С означает, что  $x_1, \dots, x_n$  различны и, значит, являются различными представителями. Нашей основной операцией будет такое вычеркивание некоторых элементов из некоторых подмножеств  $S_i$ , что для получающихся в результате подмножеств  $\bar{S}_i \subseteq S_i$ ,  $i = 1, \dots, n$ , условие С все еще выполняется. Если после ряда вычеркиваний, каждое из которых сохраняет условие С, остаются множества  $\bar{S}_i$ , содержащие каждое по единственному элементу  $x_i$ , то  $x_1, \dots, x_n$  будут различными представителями, и наша теорема будет доказана.

В качестве первого тривиального вычеркивания, которое не нарушает условия С, мы можем удалить из каждого множества  $S_i$ , содержащего более  $n$  элементов, все, кроме  $n$  элементов. Назовем множество  $r$  подмножеств  $S_{i_1}, \dots, S_{i_r}$  блоком и обозначим его через  $B_{r,s}$ , где  $s$  — число различных элементов в подмножествах

$S_{i_1}, \dots, S_{i_r}$ . Тогда условие С 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  $B_{0,0}$ . Мы можем определить также объединение и пересечение блоков. Предположим, что  $A_1, \dots, A_m, C_{m+1}, \dots, C_r$  — подмножества  $S_i$  в блоке  $B_{r,s}$  и что  $A_1, \dots, A_m, D_{m+1}, \dots, D_t$  — подмножества в блоке  $B_{t,v}$ , где  $A_1, \dots, A_m$  — все подмножества, общие для обоих блоков (напомним, что подмножества  $S_i, S_j$  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  $A_1, \dots, A_m$ , а объединение  $B_{r,s} \cup B_{t,v}$  — как блок, подмножествами которого являются  $A_1, \dots, A_m, C_{m+1}, \dots, C_r, D_{m+1}, \dots, D_t$ ; это будет блок  $B_{y,z}$  с  $y = r + t - u$ .

**Лемма 5.1.1.** *Если условие С 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 С 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 доказана.

**Лемма 5.1.2.** *Если  $B_{k,k}$  — критический блок, то вычеркивание элементов  $B_{k,k}$  из множеств, не принадлежащих  $B_{k,k}$ , не нарушает условия С.*

**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

$B_{r,s} \cap B_{k,k} = B_{u,v}$ ,  $B_r, B_s \cup_{k,k} = B_{y,z}$  и  $B_{r,s}$  состоит из множеств  $A_1, \dots, A_m, C_{m+1}, \dots, C_r$ , а  $B_{k,k}$  — из множеств  $A_1, \dots, A_m, D_{m+1}, \dots, D_k$ , где  $A_1, \dots, A_m$  — все множества, общие для обоих блоков. Тогда  $B_{u,v}$  состоит из  $A_1, \dots, A_m$ , а  $B_{y,z}$  — из

$$A_1, \dots, A_m, C_{m+1}, \dots, C_r, D_{m+1}, \dots, D_k.$$

После вычеркивания получим блок  $(B_{r,s})' = B'_{r,s'}$ , состоящий из

$$A_1, \dots, A_m, C'_{m+1}, \dots, C'_r.$$

Но так как  $C_{m+1}, \dots, C_r$  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  $C'_{m+1}, \dots, C'_r$ . Поскольку  $y=r+k-u$  и  $z \geq y$ ,  $v \geq u$ , то

$$s' = v+z-k \geq u+y-k = r.$$

Таким образом,  $s' \geq r$ , т. е. и после вычеркивания условие С все еще выполняется.

Докажем теперь нашу теорему, используя индукцию по числу  $n$  множеств, поскольку теорема тривиальна при  $n=1$ . Предположим сначала, что в системе подмножеств  $U = \{S_1, \dots, S_n\}$  имеется критический блок  $B_{k,k}$ , не совпадающий со всей системой, т. е.  $1 \leq k < n$ . Вычеркнув, если необходимо, элементы  $B_{k,k}$  из остальных множеств, можем считать, что  $U$  состоит из  $B_{k,k}$  и блока  $B'_{n-k,v}$ , которые не имеют общих элементов. По лемме 5.1.2 условие С не нарушается и по индукции  $B_{k,k}$  и  $B'_{n-k,v}$  имеют оба с. р. п., а так как они не пересекаются, то в совокупности дают с. р. п. для  $U$ . Предположим далее, что в системе  $U = \{S_1, \dots, S_n\}$  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 С выполняется для системы из  $n-1$  остальных множеств; таким образом, по индукции они имеют с. р. п., которая вместе с выбранным выше представителем одного множества образует с. р. п. для всей системы. Тем самым доказательство теоремы завершено.

**Следствие теоремы 5.1.1.** *Если  $n$  множеств  $S_1, \dots, S_n$  имеют с. р. п. 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 с. р. п., а при  $t < n$  существует не меньше, чем  $t!$  различных с. р. п.*

Это следствие получается при более тщательном рассмотрении доказательства. Должно существовать хотя бы одно множество, в котором в качестве представителя можно выбрать любой элемент, ибо 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  $S_1$ . Выбор представителя в  $S_1$  можно осуществить не менее чем  $t$  способами. Вычеркнем теперь элемент, выбранный в качестве представителя для  $S_1$ , из  $S_2, \dots, S_n$  и получим множества  $S'_2, \dots, S'_n$ , которые обладают с. р. п. и в которых наименьшее множество содержит не меньше, чем  $t-1$  элементов. Продолжая дальше таким же образом, мы можем получить не меньше, чем  $t(t-1)\dots(t-n+1)$  с. р. п., если  $t \geq n$ , и не меньше чем  $t!$  с. р. п., если  $t < n$ .

Предыдущее доказательство не является первоначальным доказательством Ф. Холла, а принадлежит автору. Его можно использовать, чтобы распространить теорему 5.1.1 на тот случай, когда система  $U$  содержит бесконечно много множеств  $S_i$ , каждое из которых конечно. Если мы имеем бесконечно много множеств, среди которых могут быть бесконечные множества, то не ясно, какое условие гарантирует существование с. р. п. Например, если мы имеем систему из множеств  $S_0 =$

$= \{1, 2, 3, \dots\}$  и  $S_i = \{i\}, i = 1, 2, \dots$ , то эта система не имеет с. р. п., так как представители для  $S_i, i = 1, 2, \dots$ , выбираются однозначно и не остается ни одного элемента, который представлял бы только  $S_0$ . Однако для любого  $k$ , конечного или бесконечного, любые  $k$  из данных выше множеств содержат среди своих элементов не менее  $k$  различных. Таким образом, требование конечности для множеств в следующей теореме не является излишним.

**Теорема 5.1.2.** Пусть для каждого  $i$  из системы индексов  $I$  задано конечное подмножество  $S_i$  множества  $S$ . Система  $U = \{S_i\}, i \in I$ , имеет систему различных представителей тогда и только тогда, когда выполняется следующее условие С: для каждого конечного  $k$  и любого выбора  $k$  различных индексов  $i_1, i_2, \dots, i_k$  в совокупности всех элементов подмножеств  $S_{i_1}, S_{i_2}, \dots, S_{i_k}$  имеется не менее  $k$  различных элементов.

**Доказательство.** Мы можем ввести частичное упорядочение для вычеркиваний, полагая  $D_1 \leq D_2$  для вычеркиваний  $D_1$  и  $D_2$ , если каждый элемент, вычеркнутый из некоторого множества по  $D_1$ , вычеркнут и по  $D_2$ . Нас интересуют вычеркивания, которые не нарушают условия С. Если все вычеркивания  $D_1 \leq D_2 \leq \dots \leq D_i \leq \dots$  в возрастающей цепи не нарушают условия С, то пусть  $D$  обозначает вычеркивание, которое состоит в том, что элемент  $b$  вычеркивается из множества  $S$ , если только это происходит при каком-нибудь  $D_i$  из возрастающей цепи. Тогда мы утверждаем, что  $D$  также не нарушает условия С, ибо для любого блока  $B_{r,s}$  из  $U$  (поскольку  $r$  и  $s$  конечны) лишь конечное число вычеркиваний в цепи действует на  $B_{r,s}$ , и, значит, существует последнее вычеркивание  $D_n$ , действующее на него. Но при  $D_n$  блок  $(B_{r,s})' = B'_{r,s}$  по предположению еще удовлетворяет условию С:  $s' \geq r$ . Следовательно,  $D$  не нарушает условия С. По лемме Цорна для всех вычеркиваний, не нарушающих условия С, тогда существует максимальное такое вычеркивание  $D$ . Мы покажем, что если произвести это вычеркивание  $D$ , то в каждом множестве  $S'_i$  остается единственный элемент, и эти элементы

образуют, следовательно, с. р. п. для исходной системы  $U$ .

Действительно, если существует некоторый элемент  $a_1$ , не принадлежащий никакому критическому блоку, то вычеркнем  $a_1$  из каждого множества  $S_i$ , содержащего  $a_1$ . При таком вычеркивании блок  $B_{r,s}$  заменяется на  $B'_{r,s'}$ , где  $s' = s$ , если  $a_1$  не является элементом какого-нибудь множества из  $B_{r,s}$ , и  $s' = s - 1$ , если  $a_1$  — элемент множества из  $B_{r,s}$ . Но в последнем случае, по предположению,  $s > r$ , следовательно,  $s' \geq s - 1 \geq r$ , и условие С выполняется после такого вычеркивания. К любому критическому блоку  $B_{k,k}$  применима лемма 5.1.2 и если вычеркнуть элементы  $B_{k,k}$  из всех остальных множеств, то условие С не нарушится<sup>1)</sup>. По теореме 5.1.1 критический блок  $B_{k,k}$ , будучи конечным, при выполнении условия С обладает с. р. п. Если теперь в  $B_{k,k}$  выбрать с. р. п. и затем вычеркнуть в каждом множестве из  $B_{k,k}$  все элементы, кроме выбранного представителя, то условие С во всей системе  $U$  не нарушится. Поэтому после вычеркивания  $D$  каждый элемент находится в критическом блоке, и в любом критическом блоке каждое множество состоит только из одного элемента.

Таким образом, для максимального вычеркивания  $D$ , не нарушающего условия С, каждое множество  $S'_i$  состоит из единственного элемента, и эти элементы образуют с. р. п. для системы  $U$ . Доказательство теоремы завершено.

Если даны  $n$  подмножеств  $S_1, \dots, S_n$  множества  $S$ , то проверка для них справедливости условия С, вообще говоря, практически невозможна, так как она сводится к рассмотрению  $2^n - 1$  подмножеств. Мы дадим алгоритм, который не требует предварительных проверок и либо заканчивается нахождением искомой системы различных представлений, либо дает  $k$  множеств, которые не содержат среди своих элементов  $k$  различных.

\* Выберем произвольный элемент  $a_1$  из  $S_1$  и, пока возможно, будем выбирать элементы  $a_i$  из  $S_i$ , отличающиеся

<sup>1)</sup> Поэтому (ввиду максимальности  $D$ ) ни одно из подмножеств, входящих в  $B_{k,k}$ , не имеет общих элементов ни с одним из подмножеств, не входящих в  $B_{k,k}$ . — Прим. ред.

от ранее выбранных  $a_1, \dots, a_{i-1}$ . Если этот процесс может быть продолжен вплоть до  $S_n$ , то получим с. р. п. Этого не произойдет, если мы дойдем до множества  $S_r$ , все элементы  $b_1, \dots, b_t$  которого были использованы в качестве представителей. Образуем теперь список  $T_1$ , выписывая подряд  $b_1, \dots, b_t$ . Второй список,  $T_2$ , будет состоять из  $T_1$ , за которым следуют элементы множества  $S(b_1)$ , имеющего представителем  $b_1$ , не принадлежащие  $T_1$ ; обозначим их через  $b_{t+1}, \dots, b_s$ . Это дополнительное множество элементов может, разумеется, оказаться и пустым. Вообще если построен список  $T_i$ , то мы образуем список  $T_{i+1}$ , помещая за  $T_i$  элементы (которые еще не были выписаны) множества  $S(b_i)$ , имеющего представителем  $b_i$ . Если на некотором шаге мы выписываем элемент  $b_u$ , который не был использован в качестве представителя, то  $b_u$  не находится в списке  $T_1$ , но находится в некотором списке  $T_{u_2+1}$ , будучи включен туда в качестве элемента из  $S(b_{u_2})$ , не содержащегося в  $T_{u_2}$ . Здесь  $u_2 < u$ , и если  $b_{u_2}$  не находится в  $T_1$ , то  $b_{u_2}$  находится в множестве  $S(b_{u_3})$  с  $u_3 < u_2$ . Далее,

$$b_u \in S(b_{u_2}), b_{u_2} \in S(b_{u_3}), \dots, b_{u_{s-1}} \in S(b_{u_s}) \text{ и } b_{u_s} \in T_1.$$

Таким образом, мы можем использовать  $b_u$  в качестве представителя  $S(b_{u_2})$ , и вообще  $b_{u_t}$  в качестве представителя  $S(b_{u_{t+1}})$ , освобождая  $b_{u_s}$  для представления  $S_r$ . У нас по-прежнему есть различные представители для  $S_1, \dots, S_{r-1}$ , но теперь имеется также представитель и для  $S_r$ . Повторное применение этой процедуры может дать полную с. р. п. Однако описанным методом действовать невозможно, если мы приходим к конечному списку  $T_m$  с элементами  $b_1, \dots, b_{k-1}$ , где каждый элемент  $b_i$  был использован в качестве представителя множества  $S(b_i)$ ,  $i = 1, \dots, k-1$ , и все элементы этих множеств включены в список. Но тогда эти  $k-1$  множества вместе с  $S_r$ , для которого не найден представитель, образуют систему из  $k$  множеств, и так как они в совокупности содержат лишь  $k-1$  различных элементов, то условие С нарушается. Этот алгоритм можно без труда запрограммировать на электронно-вычислительных машинах.

Из этого алгоритма вытекает следующий факт, не являющийся очевидным следствием теоремы 5.1.1.

**Теорема 5.1.3.** Пусть  $U = \{S_1, \dots, S_i, \dots, S_n\}$  — упорядоченная совокупность подмножеств множества  $S$ . Если  $S_1, \dots, S_r$  имеют различных представителей  $a_1, \dots, a_r$ , и если  $U$  имеет с. р. п., то  $U$  имеет с. р. п., содержащую  $a_1, \dots, a_r$ , хотя и не обязательно в качестве представителей  $S_1, \dots, S_r$ .

Заметим, что в (5.1.1) в качестве представителей  $S_1, S_2, S_3$  можно взять 3, 4, 5, но в с. р. п. они не могут быть все представителями именно этих множеств.

**Теорема Кёнига [1]** о матрицах по существу эквивалентна теореме Ф. Холла. Воспользуемся термином „линия“ для обозначения либо строки, либо столбца в матрице.

**Теорема 5.1.4 (Кёниг).** 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,  $m \geq M$ . Мы можем воспользоваться теоремой Ф. Холла, чтобы доказать обратное неравенство  $M \geq m$ . Предположим, что минимальное покрытие  $m$  линиями состоит из  $r$  строк и  $s$  столбцов, где  $r + s = m$ . Мы можем переставить строки и столбцы так, чтобы указанные линии были первыми  $r$  строками и первыми  $s$  столбцами соответственно; так как перестановки строк и столбцов, очевидно, не влияют на значения  $M$  и  $m$ . 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  $i$ -й строкой находятся единицы.

Мы утверждаем, что множества  $S_i$  удовлетворяют условию С, ибо 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 С, и по теореме Ф. Холла они имеют  $r$  различных представителей, т. е. 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  $m = M$ , и теорема доказана.

Обратно, легко вывести теорему Ф. Холла из теоремы Кёнига. Если даны множества  $S_1, \dots, S_n$  с элементами  $x_1, \dots, x_m$ , то образуем матрицу  $A = (a_{ij})$ , где  $a_{ij} = 1$ , если  $x_j$  находится в  $S_i$ , 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 С нарушается. Но если минимальное покрытие линиями содержит  $r + s = n$  линий, то по теореме Кёнига имеется  $n$  единиц, из которых никакие две не лежат на одной линии, и соответствующие этим единицам элементы образуют с. р. п. для  $S_1, \dots, S_n$ .

Теорию различных представителей можно применить к изучению латинских прямоугольников и латинских квадратов. Назовем таблицу

$$\begin{array}{cccccc}
 a_{11} & a_{12} & \dots & a_{1n} \\
 a_{21} & a_{22} & \dots & a_{2n} \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 a_{r1} & a_{r2} & \dots & a_{rn}
 \end{array} \tag{5.1.3}$$

**латинским** ( $r \times n$ )-**прямоугольником**, если каждая строка есть некоторая перестановка чисел  $1, 2, \dots, n$  и в каждом столбце ни одно число не повторяется. В общем случае  $r \leq n$ ; если  $r = n$ , то такая таблица называется **латинским квадратом** и каждое число  $1, 2, \dots, n$  появляется точно один раз в каждой строке и каждом столбце. Возникает естественный вопрос: если  $r < n$ , то можно ли добавить еще одну строку к табл. (5.1.3), чтобы получить латинский  $((r+1) \times n)$ -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 мы уже видели, что это число есть целое, ближайшее к  $n!/e$ . Если есть две строки

$$\begin{array}{ccccccccc} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1, \end{array} \quad (5.1.4)$$

то число способов добавления третьей строки — это „задача о супружеских парах“, рассмотренная в гл. 2, и оно приближенно равно  $n!/e^2$ . Эрдёшем и Капланским [1] было показано, что если  $r$  мало в сравнении с  $n$ , в частности если  $r < \sqrt[3]{n}$ , то число способов добавления строки приближенно равно  $n!/e^r$ . Следующая теорема дает нижнюю границу для всех значений  $r$ , которая почти наверняка занижена при  $r \leq n - 3$ .

**Теорема 5.1.5.** Число способов добавления строки к латинскому ( $r \times n$ )-прямоугольнику, дающих в результате латинский  $((r+1) \times n)$ -прямоугольник, не меньше  $(n-r)!$ .

**Доказательство.** Пусть  $S_i$ ,  $i = 1, \dots, n$ , — множество чисел, которые не появляются в  $i$ -м столбце данного латинского ( $r \times n$ )-прямоугольника  $R$ . Тогда с. р. п. множество  $S_i$  можно добавить к  $R$  в качестве строки, чтобы получить латинский  $((r+1) \times n)$ -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  $R$  для получения латинского  $((r+1) \times n)$ -прямоугольника, будет с. р. п. для множеств  $S_i$ .

Задача состоит теперь в том, чтобы показать, что множества  $S_i$  имеют с. р. п., и найти число возможных с. р. п. Множество  $S_i$  состоит из  $n - r$  чисел, не содержащихся в  $i$ -м столбце  $R$ . Каждое число 1, 2, ...,  $n$  появляется  $r$  раз в  $R$  и, следовательно,  $n - r$  раз в множествах  $S_1, \dots, S_n$ , взятых вместе. Набор  $k$  из этих множеств  $S_1, \dots, S_r$  будет содержать  $k(n - r)$  чисел с учетом кратностей. Но так как ни одно из этих чисел не появляется более чем  $n - r$  раз, то среди элементов этих  $k$  множеств должно быть не менее  $k$  различных чисел. Следовательно, условие С удовлетворяется. Так как каждое из множеств  $S_i$  содержит  $n - r$  элементов, то по следствию теоремы 5.1.1 существует не меньше  $(n - r)!$  с. р. п., и теорема доказана.

Следующим приложением теоремы о различных представителях служит

**Теорема 5.1.6 (об общих представителях).** *Если некоторое множество  $S$  представлено как сумма конечного числа  $n$  подмножеств двумя способами*

$$S = A_1 + A_2 + \dots + A_n = B_1 + B_2 + \dots + B_n$$

*и если никакие  $k$  из множеств  $A_i$  не содержатся в менее чем  $k$  множествах  $B_j$  для каждого  $k = 1, 2, \dots, n$ , то существуют элементы  $x_1, \dots, x_n$ , которые являются одновременно представителями и для  $A_i$ , и для  $B_j$ .*

**Доказательство.** Для каждого  $A_i$  определим множество  $S_i$  как множество всех таких индексов  $j$ , что пересечение  $A_i \cap B_j$  не пусто. Условие теоремы есть как раз условие С для множеств  $S_i$ . Если  $j_1, j_2, \dots, j_n$  — различные представители для множеств  $S_i$ , то выберем элемент  $x_i$  в пересечении  $A_i \cap B_{j_i}$ . Тогда  $x_1, \dots, x_n$  являются одновременно представителями и  $A_i$ , и  $B_j$ . Условие теоремы тривиальным образом необходимо; как только что показано, оно также достаточно для существования общих представителей. Очевидно, что это условие фактически симметрично относительно  $A_i$  и  $B_j$ .

Заметим, что эта теорема справедлива и при бесконечном  $n$ , если только подмножества конечны, так как тогда применима теорема 5.1.2.

Эта теорема имеет интересное приложение в теории групп.

**Теорема 5.1.7.** *Если  $H$  — конечная подгруппа группы  $G$ , то существует множество элементов, которые являются общими представителями для правых смежных классов по  $H$  и левых смежных классов по  $H$ .*

**Доказательство.** И правые  $x_iH$ , и левые  $Hy_i$  смежные классы имеют одинаковое число элементов, равное числу элементов в подгруппе  $H$ . Поэтому условие теоремы 5.1.6 тривиальным образом выполняется, и отсюда следует утверждение теоремы 5.1.7. Общие представители правых и левых смежных классов существуют и при некоторых других условиях на подгруппу. Эта проблема довольно подробно была исследована Оре [1].

**Теорема 5.1.8.** *В бесконечномерном векторном пространстве любые два базиса имеют одинаковую мощность.*

**Доказательство.** Пусть  $x_i$ ,  $i \in I$ , и  $y_j$ ,  $j \in J$ , — два базиса векторного пространства  $V$  над полем  $F$ . Если каждое  $x_i$  выразить как линейную комбинацию элементов  $y_j$ , то получим множество  $S_i$ , состоящее из  $y_j$ , связанных с  $x_i$ , а именно тех  $y_j$ , которые в выражение  $x_i$  через  $y_j$  входят с ненулевым коэффициентом. Множества  $S_i$ ,  $i \in I$ , конечны и должны удовлетворять условию С, так как если бы в какой-либо совокупности  $k$  множеств  $S_i$  содержалось меньше чем  $k$   $y_j$ , то соответствующие  $x_i$  были бы линейно зависимы. Следовательно, мы можем выбрать различные  $y_j$  из множеств  $S_i$ , и тогда мощность множества  $J$  не меньше мощности множества  $I$ . Точно так же мощность  $I$  не меньше, чем мощность  $J$ , и, значит, эти мощности совпадают.

Теорему о различных представителях можно применить для получения сведений о матрицах. Следующая теорема является важным примером такого применения.

**Теорема 5.1.9.** Пусть  $A = (a_{ij})$ ,  $i = 1, \dots, n$ ,  $j = 1, \dots, n$  —  $(n \times n)$ -матрица, где  $a_{ij}$  — неотрицательные действительные числа, такие, что каждая строка и каждый столбец имеют одну и ту же сумму. Тогда  $A$  представляется суммой матриц перестановки, умноженных на неотрицательные числа.

**Доказательство.** Матрица перестановки  $P$  — это квадратная матрица из нулей и единиц с единственной единицей в каждой строке и в каждом столбце. Нам надо доказать, что если  $A = (a_{ij})$ , где

$$\sum_{i=1}^n a_{ij} = t, \quad j = 1, \dots, n,$$

$$\sum_{j=1}^n a_{ij} = t, \quad i = 1, \dots, n,$$

$$a_{ij} \geq 0,$$

то

$$A = u_1 P_1 + u_2 P_2 + \dots + u_s P_s, \quad u_i \geq 0,$$

где  $P_1, P_2, \dots, P_s$  — матрицы перестановки. Будем доказывать это индукцией по числу  $w$  ненулевых элементов в  $A$ . Если  $A \neq 0$ , то  $w \geq n$ , и если  $w = n$ , то легко видеть, что  $A = tP$ , где  $P$  — матрица перестановки. Для каждого  $i = 1, \dots, n$  обозначим через  $S_i$  множество таких индексов  $j$ , что  $a_{ij} > 0$ . Мы утверждаем, что множества  $S_i$  удовлетворяют условию С. Действительно, если предположить, что какие-либо  $k$  множеств  $S_i$ , взятые вместе, содержат не более  $k - 1$  индексов  $j$ , то положительные числа в соответствующих  $k$  строках лежат не более чем в  $k - 1$  столбцах. Если мы сложим эти числа по строкам, то получим  $kt$ , в то время как сумма по столбцам не превысит  $(k - 1)t$ . Это противоречие показывает, что условие С должно выполняться. Далее, пусть  $j_1, \dots, j_n$  — различные представители для  $S_1, \dots, S_n$ . Это означает, что  $a_{ij_i} > 0$  для  $i = 1, \dots, n$ , и так как  $j_1, \dots, j_n$  различны, они представляют собой перестановку чисел  $1, \dots, n$ . Поэтому матрица  $P_1 = (c_{ij})$ , где  $c_{ij_i} = 1$ ,  $c_{ij} = 0$  при  $j \neq j_i$ , — матрица перестановки. Если  $u_1$  — минимум  $a_{ij_i}$ ,  $i = 1, \dots, n$ , то  $A_1 = A - u_1 P_1$  — матрица с неотрицательными элементами, в которой

каждая строка и каждый столбец имеют сумму  $t - u_1$ . Далее, согласно выбору  $u_1$ , в  $A_1$  меньше ненулевых элементов, чем в  $A$ , и по индукции существуют матрицы перестановки  $P_2, \dots, P_s$  и неотрицательные числа  $u_2, \dots, u_s$ , такие, что  $A_1 = u_2 P_2 + \dots + u_s P_s$ ; следовательно,  $A = u_1 P_1 + u_2 P_2 + \dots + u_s P_s$ , что и требовалось доказать. Это завершает доказательство теоремы.

### Задачи

1. Взяв столбцы следующих таблиц в качестве множеств, показать, что существует соответственно 31 и 24 с. р. п.:

|               |               |
|---------------|---------------|
| 1 2 3 4 5 6 7 | 1 2 3 4 5 6 7 |
| 2 3 4 5 6 7 1 | 2 3 4 5 6 7 1 |
| 3 4 5 6 7 1 2 | 4 5 6 7 1 2 3 |

2. Множества  $S_1, S_2, \dots, S_n$  содержат соответственно  $2, 3, \dots, n+1$  элементов. Показать, что существует не менее  $2^n$  с. р. п. Указать примеры таких множеств, для которых существует точно  $2^n$  с. р. п.

3. Пусть  $S_1, \dots, S_n$  — это  $n$  множеств, имеющих с. р. п. Предположим, что  $a_1, \dots, a_t, t < n$ , — с. р. п. для  $S_1, \dots, S_t$ . Доказать, что  $S_1, \dots, S_n$  имеют с. р. п., включающую элементы  $a_1, \dots, a_t$ , но не обязательно в качестве представителей множеств  $S_1, \dots, S_t$ . Дать пример множеств  $S_1, \dots, S_n$  и элементов  $a_1, \dots, a_t$ , которые представляют  $S_1, \dots, S_t$ , но не могут быть представителями  $S_1, \dots, S_t$  ни в какой с. р. п. для  $S_1, \dots, S_n$ .

4. Пусть  $A$  есть  $(n \times n)$ -матрица из неотрицательных действительных чисел, такая, что каждая строка и каждый столбец имеют одну и ту же сумму. Доказать, что  $A$  может быть представлена суммой не более чем  $n^2 - 2n + 2$  матриц перестановки, умноженных на неотрицательные числа. (В действительности это наилучшая возможная граница.)

# Теорема Рамсея

---

## 6.1. Формулировка и доказательство теоремы

Пусть имеется шесть точек, связанных попарно дугами, окрашенными в красный или голубой цвет. Докажем, что существуют три точки, такие, что дуги образуемого ими треугольника окрашены в один и тот же цвет. Мы можем показать это следующим образом. Возьмем какую-нибудь точку  $P_0$  и рассмотрим пять дуг, соединяющих  $P_0$  с остальными пятью точками. Три из этих дуг должны быть одного и того же цвета (например, красного), обозначим их через  $P_0P_1$ ,  $P_0P_2$ ,  $P_0P_3$ . Если какая-нибудь из дуг  $P_1P_2$ ,  $P_1P_3$  или  $P_2P_3$  красная, то эта дуга вместе с двумя дугами, соединяющими ее концы с  $P_0$ , образует красный треугольник. В противном случае все три дуги  $P_1P_2$ ,  $P_1P_3$  и  $P_2P_3$  голубые, и тогда  $P_1P_2P_3$  — голубой треугольник. Это есть решение поставленной задачи, и легко видеть, что шесть — минимальное число точек, гарантирующее наличие треугольника одного цвета. Следующий перечень дает пример множества из пяти точек, соединенных попарно красными или голубыми дугами так, что при этом не образуется треугольника одного цвета:

$$\begin{array}{ll}
 P_1P_2 \text{ — красная,} & P_2P_4 \text{ — красная,} \\
 P_1P_3 \text{ — красная,} & P_2P_5 \text{ — голубая,} \\
 P_1P_4 \text{ — голубая,} & P_3P_4 \text{ — голубая,} \\
 P_1P_5 \text{ — голубая,} & P_3P_5 \text{ — красная,} \\
 P_2P_3 \text{ — голубая,} & P_4P_5 \text{ — красная.}
 \end{array}$$

Как сама проблема, так и ее решение, данное выше, допускают значительное обобщение. Обобщение, данное здесь, известно как теорема Рамсея.

**Теорема 6.1.1 (теорема Рамсея [1]).** Пусть  $S$  — множество, содержащее  $N$  элементов, и  $T$  — семейство

всех подмножеств множества  $S$ , содержащих в точности  $r$  элементов. Разобьем  $T$  на два (не пересекающихся) семейства  $\alpha$  и  $\beta$ . Пусть  $p, q, r$  — целые числа,  $p \geq r, q \geq r, r \geq 1$ . Тогда существует такое минимальное число  $n(p, q, r)$ , зависящее только от  $p, q, r$  и не зависящее от множества  $S$ , что если  $N \geq n(p, q, r)$ , то либо существует подмножество  $A$  из  $p$  элементов, все  $r$ -подмножества которого находятся в семействе  $\alpha$ , либо существует подмножество  $B$  из  $q$  элементов, все  $r$ -подмножества которого находятся в семействе  $\beta$ .

**Доказательство.** Заметим, что задача, решенная выше, показывает, что  $n(3, 3, 2)$  не превосходит 6, а приведенный пример показывает, что  $n(3, 3, 2)$  больше 5. Таким образом,  $n(3, 3, 2) = 6$ .

Переходим теперь к доказательству теоремы. Воспользуемся методом полной индукции относительно  $p, q, r$ , предполагая теорему справедливой для  $r - 1$  и любых значений  $p^* \geq r - 1, q^* \geq r - 1$ , а также для  $r$  и троек  $p', q, r$ , где  $p' < p$ , и троек  $p, q', r$ , где  $q' < q$ . Нужно вычислить начальные значения  $n(p, q, 1)$ ,  $n(r, q, r)$  и  $n(p, r, r)$ . Нетрудно заметить, что  $n(p, q, 1) = p + q - 1$ . Действительно, если  $N \geq p + q - 1$  и  $\alpha$  содержит не более  $p - 1$  элементов, то  $\beta$  содержит не менее  $N - (p - 1) \geq q$  элементов, т. е.  $n(p, q, 1) \leq p + q - 1$ . Если же  $N \leq p + q - 2$ , то мы можем взять такое разбиение, что  $\alpha$  состоит не более чем из  $p - 1$  элементов, а  $\beta$  — не более чем из  $q - 1$  элементов, и утверждение теоремы не выполняется. Покажем далее, что  $n(r, q, r) = q$ . Действительно, пусть  $N \geq q$ . Если  $\alpha$  не пусто, то любое  $r$ -подмножество из  $\alpha$  дает утверждение теоремы. Если же  $\alpha$  пусто, то все  $r$ -подмножества содержатся в  $\beta$  и, следовательно, утверждение теоремы опять справедливо. При  $N < q$ , если все  $r$ -подмножества отнести к  $\beta$ , то утверждение теоремы не верно. Точно так же  $n(p, r, r) = p$ . Обозначим теперь  $p_1 = n(p - 1, q, r), q_1 = (p, q - 1, r)$ . Мы утверждаем, что  $n(p, q, r) \leq n(p_1, q_1, r - 1) + 1$ .

Пусть  $S$  — множество из  $N \geq n(p_1, q_1, r - 1) + 1$  элементов. Выберем в  $S$  некоторый элемент  $a_0$ , и пусть  $S' = S - a_0$ . Разобьем совокупность всех  $(r - 1)$ -подмножеств множества  $S'$  на два семейства  $\alpha'$  и  $\beta'$  следующим

образом: будем считать, что  $(r-1)$ -подмножество принадлежит семейству  $\alpha'$ , если оно вместе с  $a_0$  образует  $r$ -подмножество из семейства  $\alpha$ ;  $(r-1)$ -подмножество принадлежит семейству  $\beta'$ , если оно вместе с  $a_0$  образует  $r$ -подмножество из семейства  $\beta$ . Так как  $S'$  имеет не меньше  $n(p_1, q_1, r-1)$  элементов, то по индукции  $S'$  содержит либо множество из  $p_1$  элементов, все  $(r-1)$ -подмножества которого принадлежат  $\alpha'$ , либо множество из  $q_1$  элементов, все  $(r-1)$ -подмножества которого принадлежат  $\beta'$ . Поскольку  $p_1 = n(p-1, q, r)$ , то в первом случае, если множество из  $p_1$  элементов содержит подмножество из  $q$  элементов, все  $r$ -подмножества которого принадлежат  $\beta$ , то эти  $q$  элементов удовлетворяют нашему требованию. В противном случае это множество из  $p_1$  элементов содержит подмножество из  $p-1$  элементов, все  $r$ -подмножества которого принадлежат  $\alpha$ , и это  $(p-1)$ -подмножество, взятое вместе с  $a_0$ , образует  $r$ -подмножество в  $S$ , все  $r$ -подмножества которого принадлежат  $\alpha$ ; снова наше требование удовлетворено. Аналогичное рассуждение применяем и тогда, когда  $S'$  содержит множество из  $q_1 = n(p, q-1, r)$  элементов, все  $(r-1)$ -подмножества которого принадлежат  $\beta'$ . Таким образом, мы показали, что  $n(p, q, r) \leq n(p_1, q_1, r-1) + 1$  с  $p_1 = n(p-1, q, r)$ ,  $q_1 = n(p, q-1, r)$ , и теорема доказана.

## 6.2. Одно приложение теоремы Рамсея

Как приложение теоремы Рамсея, Эрдёш и Секереш [1] получили следующий результат:

**Теорема 6.2.1.** Для данного целого числа  $n$  существует целое число  $N = N(n)$ , такое, что любые  $N$  точек в плоскости, из которых никакие три не лежат на одной прямой, содержат  $n$  точек, образующих выпуклый  $n$ -угольник.

**Доказательство.** Более подробно выпуклые тела мы будем изучать в гл. 8. Тело называется *выпуклым*, если любой прямолинейный отрезок, соединяющий две его точки, лежит целиком внутри тела. Выпуклой оболочкой какого-либо множества точек называется наименьшее выпуклое тело, содержащее все эти точки. Для

конечного множества точек в плоскости, не все из которых находятся на одной прямой, выпуклой оболочкой является многоугольник, содержащий все эти точки либо на своей границе, либо внутри себя.

**Лемма 6.2.1.** *Из пяти точек в плоскости, никакие три из которых не лежат на одной прямой, четыре являются вершинами выпуклого четырехугольника.*

**Доказательство.** Если выпуклая оболочка для пяти точек есть четырехугольник или пятиугольник, то лемма очевидна. Если выпуклая оболочка — треугольник  $ABC$ , а две другие точки  $D, E$  находятся внутри него, то продолжение отрезка  $DE$  пересечет две из сторон треугольника и не пересечет третьей, например  $BC$ . Тогда точки  $B, C, D, E$  образуют вершины выпуклого четырехугольника.

**Лемма 6.2.2.** *Если все четырехугольники, образованные из  $n$  точек, никакие три из которых не лежат на одной прямой, выпуклы, то эти  $n$  точек являются вершинами выпуклого  $n$ -угольника.*

**Доказательство.** Утверждение тривиально для  $n = 4$ , и мы проведем доказательство индукцией по  $n$ . Предположим, что  $n \geqslant 5$  и что все четырехугольники, образованные из  $A_1, \dots, A_n$ , выпуклы. Тогда по предположению индукции точки  $A_1, \dots, A_{n-1}$  являются вершинами выпуклого  $(n-1)$ -угольника  $C_{n-1}$ , и мы можем предположить, что его вершины упорядочены вдоль периметра. Пусть сначала  $A_n$  лежит внутри  $C_{n-1}$ . Тогда  $A_n$  должна находиться внутри одного из треугольников  $A_1A_2A_3, A_1A_3A_4, \dots, A_1A_iA_{i+1}, \dots, A_1A_{n-2}A_{n-1}$ .

Если  $A_n$  находится внутри треугольника  $A_1A_iA_{i+1}$ , то четыре точки  $A_1, A_i, A_{i+1}, A_n$  не образуют выпуклый четырехугольник, что противоречит предположению. (Заметим, что, поскольку никакие три точки не лежат на одной прямой,  $A_n$  не может лежать на стороне какого-либо из этих треугольников.) Следовательно,  $A_n$  должна лежать вне многоугольника  $C_{n-1}$ . Соединим  $A_n$  с каждой из точек  $A_1, \dots, A_{n-1}$  отрезками. Так как  $A_n$  лежит вне  $C_{n-1}$ , существуют две экстремальные прямые

(скажем,  $A_nA_i$  и  $A_nA_j$ ), образующие угол, который заключает внутри себя выпуклый многоугольник  $C_{n-1}$ . Если  $A_i$  и  $A_j$  — не последовательные вершины, то треугольник  $A_nA_iA_j$  будет содержать еще одну точку  $A_k$  внутри себя, так что четыре точки  $A_n, A_i, A_j, A_k$  не будут образовывать выпуклый четырехугольник; но это противоречит предположению. Следовательно,  $A_i$  и  $A_j$  — последовательные вершины, и, помещая  $A_n$  между ними, получаем выпуклый  $n$ -угольник. Лемма доказана.

После установления этих геометрических лемм теорема 6.2.1 следует почти непосредственно из теоремы Рамсея, примененной к множеству из  $N$  точек в плоскости, из которых никакие три не лежат на одной прямой, и разбиению четырехугольников на семейство  $\alpha$  выпуклых четырехугольников и семейство  $\beta$  вогнутых четырехугольников. В этом случае теорема Рамсея утверждает, что если  $N \geq N(n, 5, 4)$ , то существует либо  $n$ -угольник, все четырехугольники которого выпуклы, либо пятиугольник, все четырехугольники которого вогнуты. По лемме 6.2.1 последнее невозможно, и, значит, выполняется первое. Таким образом, по лемме 6.2.2 эти  $n$  точек образуют вершины выпуклого  $n$ -угольника, и теорема доказана.

### Задачи

1. Дано шесть точек, соединенных попарно либо голубой, либо красной дугой. Назовем треугольник хроматическим, если три его дуги одного и того же цвета. Показать, что существует не менее двух хроматических треугольников.

2. Используя результат задачи 1, показать, что если имеется семь точек, соединенных попарно голубой или красной дугой, то существует не менее трех хроматических треугольников.

3. Доказать, что  $n(k, m, 2) = n(m, k, 2)$ , если  $m \geq 2$ ,  $k \geq 2$ .

4. Доказать для  $k \geq 2$ ,  $m \geq 2$ , что

$$n(k, m, 2) \geq \binom{k+m-2}{k-1} = \binom{k+m-2}{m-1}.$$

5. Сформулировать и доказать естественное обобщение теоремы Рамсея для множества  $S$ ,  $r$ -подмножества которого разбиты на  $m$  (попарно не пересекающихся) семейств  $a_1, a_2, \dots, a_m$ .

6. Доказать, что  $n(3, 4, 2) \leq 9$ , где  $\alpha$  — красный цвет, а  $\beta$  — голубой. Показать, что это утверждение справедливо, если в некоторой вершине имеется четыре красные дуги или шесть голубых. Показать, что такая ситуация, при которой в каждой вершине имеется три красных и пять голубых дуг, невозможна ввиду нечетности чисел 3, 5 и 9.

7. Доказать, что  $n(3, 4, 2) > 8$ , и, значит,  $n(3, 4, 2) = 9$ , беря в качестве вершин вычеты по модулю 8: 0, 1, ..., 7 и окрашивая дугу, соединяющую  $i$  и  $j$  в зависимости только от разности  $i - j \pmod{8}$ . Заметим, что цвет, соответствующий  $d \equiv i - j$  и  $-d \equiv j - i$ , должен быть одинаков.

8. Показать, что  $n(4, 4, 2) > 17$ , беря в качестве вершин вычеты 0, 1, ..., 16 ( $\pmod{17}$ ) и считая голубой дугу, соединяющую  $i$  и  $j$ , если  $i - j \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17}$ , и красной в остальных случаях. Отсюда делаем вывод, что  $n(4, 4, 2) = 18$ .

# Некоторые экстремальные задачи

---

## 7.1. Задача о назначениях

Теорема о различных представителях оказывается полезной при решении некоторых задач, которые на первый взгляд не имеют никакого отношения к различным представителям. Одной из них является задача о назначениях. Предположим, что мы имеем  $n$  мест, которые должны быть заняты  $n$  людьми, и  $a_{ij}$  — мера ценности  $i$ -го человека на  $j$ -м месте. Любое назначение определяется перестановкой

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

где  $j_i = \pi(i)$  — место, на которое назначается  $i$ -й человек. Оптимальным является назначение, которое максимизирует  $\sum_i a_{i\pi(i)}$ . Имеется всего  $n!$  перестановок, которые нужно испытать. Однако, даже если  $n$  сравнительно невелико, осуществить практически такое число испытаний невозможно. Значение следующей теоремы двояко: во-первых, она позволяет найти решение за относительно малое число шагов и, во-вторых, дает метод, позволяющий непосредственно проверить, что найденное решение действительно является оптимальным.

**Теорема 7.1.1.** Пусть  $A = (a_{ij})$  есть  $(n \times n)$ -матрица действительных чисел. Тогда максимум суммы

$$\sum_{i=1}^n a_{i\pi(i)}$$

по всем перестановкам  $\pi$  равен минимуму суммы

$$\sum_{i=1}^n u_i + \sum_{j=1}^n v_j$$

по всем числам  $u_i$  и  $v_j$ , таким, что  $u_i + v_j \geq a_{ij}$  для всех  $i$  и  $j$ ,  $1 \leq i, j \leq n$ . Это общее значение для сумм достигается, когда  $u_i + v_{\pi(i)} = a_{i\pi(i)}$ ,  $i = 1, \dots, n$ , и соответствующая перестановка  $\pi$  дает решение задачи о назначениях.

Доказательство. Если дана матрица  $A = (a_{ij})$ , то мы всегда можем найти числа  $u_i$ ,  $v_j$ , удовлетворяющие условию  $u_i + v_j \geq a_{ij}$ ,  $i, j = 1, 2, \dots, n$ , взяв, например, все  $v_j$  равными нулю, а  $u_i$  — максимуму  $a_{ij}$ ,  $j = 1, \dots, n$ . Для любой перестановки  $\pi$  тогда имеем  $u_i + v_{\pi(i)} \geq a_{i\pi(i)}$ ; следовательно, суммируя по  $i$ , получаем

$$\sum_{i=1}^n u_i + \sum_{j=1}^n v_j \geq \sum_{i=1}^n a_{i\pi(i)}.$$

Отсюда минимум  $m$  для сумм

$$\sum_{i=1}^n u_i + \sum_{j=1}^n v_j$$

существует, а для максимума  $M$  сумм

$$\sum_{i=1}^n a_{i\pi(i)}$$

по всем перестановкам должно выполняться условие  $m \geq M$ . Нам нужно доказать, что  $m = M$ .

Вначале предположим, что меры ценности  $a_{ij}$  — целые числа. Каковы бы ни были числа  $u_i$  и  $v_j$ , удовлетворяющие неравенствам  $u_i + v_j \geq a_{ij}$  при всех  $i, j$ , мы можем, сохранив  $v_j$  фиксированными, уменьшить  $u_i$ , если это необходимо, так, чтобы для каждого  $i$  существовало хотя бы одно  $j$ , такое, что  $u_i + v_j = a_{ij}$ . Для данного выбора  $u_i$  и  $v_j$  и для каждого  $i = 1, \dots, n$  обозначим через  $S_i$  множество таких индексов  $j$ , что  $u_i + v_j = a_{ij}$ . Если множества  $S_i$  имеют систему различных представителей (с. р. п.)  $j_1, j_2, \dots, j_n$ , то  $u_i + v_{j_i} = a_{ij_i}$  и перестановка  $\pi(i) = j_i$ ,  $i = 1, \dots, n$ , дает решение задачи о назначениях. Если с. р. п. не существует,

то условие С (см. гл. 5) нарушается и мы можем найти  $k$  множеств  $S_i$ ,  $i \in K$ , где  $K$  — множество из  $k$  индексов, таких, что существует не более  $k - 1$  различных значений  $j$  во всех множествах  $S_i$ ,  $i \in K$ . (Заметим, что указанный в гл. 5 алгоритм для отыскания с. р. п. дает возможность найти множества, нарушающие условие С, если оно нарушается.) Обозначим через  $J$  подмножество индексов, таких, что  $j \in J$  тогда и только тогда, когда  $j \in S_i$  при некотором  $i \in K$ . Нарушение условия С означает, что  $J$  содержит не более  $k - 1$  индексов  $j$ . Заменим теперь  $u_i$  и  $v_j$  новыми значениями, полагая

$$\begin{aligned} u_i^* &= u_i - 1, \text{ если } i \in K, \\ u_i^* &= u_i, \quad \text{если } i \notin K, \\ v_j^* &= v_j + 1, \text{ если } j \in J, \\ v_j^* &= v_j, \quad \text{если } j \notin J. \end{aligned} \tag{7.1.1}$$

Пусть в  $J$  имеется  $t < k$  индексов. Тогда новые значения  $u_i^*$  и  $v_j^*$  удовлетворяют соотношению

$$\sum_{i=1}^n u_i^* + \sum_{j=1}^n v_j^* = \sum_{i=1}^n u_i + \sum_{j=1}^n v_j - k + t, \tag{7.1.2}$$

и, поскольку  $t < k$ , сумма  $\sum u_i + \sum v_j$  уменьшается на  $k - t$ . Мы утверждаем также, что

$$u_i^* + v_j^* \geq a_{ij} \quad \text{при всех } i, j. \tag{7.1.3}$$

Действительно, из формул (7.1.1) следует, что (7.1.3), несомненно, выполняется, если  $i \notin K$ . Пусть  $i \in K$ . Если  $j \in J$ , то

$$u_i^* + v_j^* = (u_i - 1) + (v_j + 1) = u_i + v_j \geq a_{ij}. \tag{7.1.4}$$

Но если  $j \notin J$ , то из определения  $S_i$  получаем

$$u_i + v_j > a_{ij}, \text{ или } u_i + v_j \geq a_{ij} + 1, \tag{7.1.5}$$

следовательно,

$$u_i^* + v_j^* = u_i + v_j - 1 \geq a_{ij}. \tag{7.1.6}$$

Если условие С выполняется при этом новом выборе  $u_i$  и  $v_j$ , то мы приходим к решению теоремы и задачи о назначениях. Если же нет, то, действуя, как прежде, находим новые значения для  $u_i$  и  $v_j$ , при которых сумма  $\sum u_i + \sum v_j$  уменьшается, а условие  $u_i + v_j \geq a_{ij}$  при всех  $i, j$  по-прежнему выполняется. Так как исходные числа  $u_i$  и  $v_j$  можно было взять целыми и так как сумма  $\sum u_i + \sum v_j$  уменьшалась каждый раз на целое положительное число, то процесс должен оборваться на конечном этапе, что доказывает нашу теорему и дает искомое решение задачи о назначениях.

Заметим, что если при некотором выборе  $u_i$  и  $v_j$  имеется с. р. п.  $j_1, j_2, \dots, j_n$  множеств  $S_i$ , то, конечно, имеется и решение задачи о назначениях, причем

$$a_{1j_1} + a_{2j_2} + \dots + a_{nj_n} = \sum u_i + \sum v_j.$$

Если, однако,  $f_1, f_2, \dots, f_n$  — какая-либо другая перестановка, то  $u_i + v_{f_i} \geq a_{if_i}$  и равенство выполняется только при  $f_i \in S_i$ ,  $i = 1, 2, \dots, n$ . Следовательно,

$$a_{1f_1} + a_{2f_2} + \dots + a_{nf_n} \leq \sum u_i + \sum v_j,$$

и равенство выполняется только тогда, когда  $f_1, f_2, \dots, f_n$  — с. р. п. множеств  $S_i$ . Другими словами, выбор  $u_i$  и  $v_j$ , дающий оптимальное назначение, будет приводить ко всем оптимальным назначениям путем нахождения всех с. р. п. множеств  $S_i$ .

Этот процесс без труда можно видоизменить, чтобы доказать теорему и решить задачу о назначениях для нецелых значений  $a_{ij}$ . Заменим сначала  $a_{ij}$  целыми  $\bar{a}_{ij}$ , где  $\bar{a}_{ij} \geq a_{ij} > \bar{a}_{ij} - 1$ . Затем, как и выше, можно найти перестановку  $j_1, \dots, j_n$  и целые числа  $u_i, v_j$ , такие, что

$$\bar{a}_{1j_1} + \bar{a}_{2j_2} + \dots + \bar{a}_{nj_n} = \sum u_i + \sum v_j = m_1 \quad (7.1.7)$$

и

$$u_i + v_j \geq \bar{a}_{ij}, \quad 1 \leq i, j \leq n. \quad (7.1.8)$$

Заметим, что в силу выбора  $\bar{a}_{ij}$

$$a_{1j_1} + a_{2j_2} + \dots + a_{nj_n} > m_1 - n \quad (7.1.9)$$

и что для любой перестановки  $f_1, \dots, f_n$

$$a_{1f_1} + a_{2f_2} + \dots + a_{nf_n} \leq \bar{a}_{1f_1} + \dots + \bar{a}_{nf_n} \leq m_1. \quad (7.1.10)$$

Выберем теперь натуральное число  $N$  и заменим  $a_{ij}$  на  $g_N(a_{ij})$ , где  $g_N(a_{ij})$  – рациональное число с знаменателем  $N$ , удовлетворяющее неравенствам

$$g_N(a_{ij}) \geq a_{ij} > g_N(a_{ij}) - \frac{1}{N}. \quad (7.1.11)$$

Если мы изменим правило (7.1.1) следующим образом:

$$\begin{aligned} u_i^* &= u_i - \frac{1}{N}, & \text{если } i \in K, \\ u_i^* &= u_i, & \text{если } i \notin K, \\ v_j^* &= v_j + \frac{1}{N}, & \text{если } j \in J, \\ v_j^* &= v_j, & \text{если } j \notin J, \end{aligned} \quad (7.1.12)$$

то доказательство проводится, как ранее, и мы найдем перестановку  $j_1, \dots, j_n$  и рациональные числа  $u_i, v_j$  со знаменателем  $N$ , такие, что

$$g_N(a_{1j_1}) + \dots + g_N(a_{nj_n}) = \sum u_i + \sum v_j = m_N \quad (7.1.13)$$

и

$$u_i + v_j \geq g_N(a_{ij}) \geq a_{ij}, \quad 1 \leq i, j \leq n. \quad (7.1.14)$$

Итак,

$$a_{1j_1} + \dots + a_{nj_n} > m_N - \frac{n}{N}, \quad (7.1.15)$$

и для любой перестановки  $f_1, \dots, f_n$

$$a_{1f_1} + \dots + a_{nf_n} \leq m_n. \quad (7.1.16)$$

Очевидно, если  $a_{ij}$  рациональны, то мы непосредственно приходим к решению, а если нет, то взятием все больших и больших знаменателей  $N$  мы в пределе из соотношений (7.1.15) и (7.1.16) получим решение задачи о назначениях. Действительно, возьмем такую последовательность значений для  $N$  (скажем, 2, 4, 8, ...), чтобы каждое последующее значение было кратно предыдущему, и возьмем окончательные значения  $u_i$  и  $v_j$  для каждого предыдущего значения  $N$  в качестве исходных

для следующего значения  $N$ . Заметим, что в нашем процессе на каждом шаге те  $u_i$ , которые изменяются, убывают, а те  $v_j$ , которые изменяются, возрастают, но ни те, ни другие не изменяются более чем на  $1/N$ . Следовательно, в пределе имеем:

$$\sum u_i + \sum v_j = m = M = a_{1l_1} + \dots + a_{nl_n}, \quad (7.1.17)$$

и теорема полностью доказана.

## 7.2. Теорема Дилуорса

Следующая теорема Дилуорса [1] дает экстремальное свойство частично упорядоченных множеств, которое аналогично теореме Кёнига (теорема 5.1.4) о матрицах из нулей и единиц.

В разделе 2.2 гл. 2 мы дали определение частично упорядоченного множества. В этом разделе мы будем записывать отношение порядка в частично упорядоченном множестве  $P$  символом  $\leq$ , и если  $a \leq b$  для  $a, b$  из  $P$ , то будем говорить, что  $a$  содержится в  $b$ . Два элемента частично упорядоченного множества называются *сравнимыми*, если они образуют цепь, в противном случае они называются *несравнимыми*.

**Теорема 7.2.1 (Дилуорс).** Пусть дано частично упорядоченное множество  $P$ . Минимальное число непересекающихся цепей, которые в совокупности содержат все элементы  $P$ , равно максимально возможному числу элементов в подмножестве множества  $P$ , состоящем из попарно несравнимых элементов, если это число конечно.

**Доказательство.** Пусть  $m$  — минимальное число непересекающихся цепей, содержащих все элементы множества  $P$ , и пусть  $M$  — максимальное число элементов в множестве  $S$ , элементы которого попарно несравнимы. Если  $x_1, \dots, x_M$  попарно несравнимы, то никакая цепь не может содержать двух из этих элементов, и тривиальным образом

$$m \geq M. \quad (7.2.1)$$

Мы должны доказать обратное неравенство. Таким образом, наша теорема сводится к следующей лемме.

**Лемма 7.2.1.** Если  $P$  — частично упорядоченное множество и если любые  $k+1$  элементов ( $k$  конечно) содержат сравнимую пару, то в  $P$  существует множество не более чем из  $k$  непересекающихся цепей, которые в совокупности содержат все элементы  $P$ .

Сначала докажем лемму для случая, когда  $P$  конечно. Используем индукцию по числу  $n$  элементов множества  $P$ . Предположим, что лемма верна, когда число элементов в  $P$  меньше  $n$ . Если существует  $t$  непересекающихся цепей  $C_1, C_2, \dots, C_t$ , которые в совокупности содержат все элементы  $P$ , то мы скажем, что  $P$  есть сумма  $C_1, \dots, C_t$ , и обозначим это:  $P = C_1 + C_2 + \dots + C_t$ . Если подмножество  $S$  элементов из  $P$  не содержит сравнимой пары, то мы скажем, что эти элементы независимы. В этих терминах наша лемма гласит: если  $k$  — максимальное число независимых элементов в  $P$ , то  $P$  есть сумма  $k$  цепей. Вычертим произвольный элемент  $b$  из  $P$ . Тогда  $P^* = P - b$  — частично упорядоченное множество, в котором максимальное число независимых элементов равно либо  $k-1$ , либо  $k$ . По индуктивному предположению  $P^*$  — сумма соответственно  $k-1$  или  $k$  цепей. Если это число есть  $k-1$ , то  $k-1$  цепей вместе с  $b$  в качестве еще одной цепи имеют  $P$  своей суммой, и наша лемма доказана. Поэтому мы предполагаем, что  $P^*$  есть сумма  $k$  цепей:

$$P - b = P^* = C_1 + C_2 + \dots + C_k. \quad (7.2.2)$$

Рассмотрим теперь соотношения между цепями  $C_1, \dots, C_k$  и элементом  $b$  в  $P$ . Пусть  $U_i$  для каждого  $i = 1, 2, \dots, k$  есть подмножество, состоящее из всех элементов цепи  $C_i$ , содержащих  $b$ ,  $L_i$  — подмножество, состоящее из всех элементов цепи  $C_i$ , содержащихся в  $b$ , и  $N_i$  — подмножество, состоящее из всех элементов цепи  $C_i$ , не сравнимых с  $b$ . Введем следующие обозначения:

$$\begin{aligned} U &= U_1 + U_2 + \dots + U_k, \\ L &= L_1 + L_2 + \dots + L_k, \\ N &= N_1 + N_2 + \dots + N_k. \end{aligned} \quad (7.2.3)$$

Здесь

$$C_i = U_i + N_i + L_i, \quad i = 1, \dots, k.$$

Заметим, что  $l_i \subseteq b \subseteq u_j$  для любых  $l_i \in L_i$  и  $u_j \in U_j$  и для всех  $i$  и  $j$ . Таким образом, если  $N_i$  при некотором  $i$  пусто, то  $L_i + b + U_i = C'_i$  — цепь и  $C_1 + \dots + C'_i + \dots + C_k = P$ , и наша теорема доказана. Следовательно, можно предположить, что ни одно  $N_i$  не пусто.

Покажем теперь, что при некотором  $m$  максимальное число независимых элементов в  $N + U - U_m$  меньше  $k$ . В самом деле, предположим, что для каждого  $j = 1, 2, \dots, k$  множество  $N + U - U_j$  содержит подмножество  $S_j$  из  $k$  независимых элементов. Так как множество  $S_j$  содержит  $k$  независимых элементов, оно содержит точно по одному элементу из цепей  $C_1, C_2, \dots, C_k$ , и так как  $S_j$  не содержит элементов из  $U_j$ , то отсюда следует, что  $S_j$  содержит точно один элемент из  $N_j$ . Далее, в сумме множеств  $S = S_1 + S_2 + \dots + S_j + \dots + S_k$  ( $S_j$  могут и пересекаться) обозначим через  $s_i$ ,  $i = 1, \dots, k$ , минимальный элемент цепи  $C_i$ , принадлежащий  $S$ . Элемент  $s_i$  содержится в  $N_i$ , так как  $S_i$  содержит один элемент из  $N_i$ , а каждый элемент из  $N_i$  содержится в каждом элементе из  $U_i$ . Допустим, что  $s_i \equiv s_j$  при некоторых  $i \neq j$ . Пусть  $s_r \in S_r$  для некоторого  $r$ ,  $1 \leq r \leq k$ , и  $t_i$  — элемент множества  $S_r$ , принадлежащий  $C_i$ . В силу минимальности  $s_i$  имеем  $t_i \equiv s_i$ . Но тогда  $t_i \equiv s_i \equiv s_j$ , что противоречит независимости элементов  $t_i$  и  $s_j$  множества  $S_r$ . Следовательно, ни при каких  $i \neq j$  не может быть  $s_i \equiv s_j$ , и потому элементы  $s_1, s_2, \dots, s_k$  независимы. Так как  $s_i$  принадлежит  $N_i$  для  $i = 1, \dots, k$ , элементы  $s_1, s_2, \dots, s_k, b$  суть  $k+1$  независимых элементов множества  $P$ . Но было дано, что в  $P$  не содержится  $k+1$  независимых элементов, и, следовательно, предположение, что каждое из множеств  $N + U - U_j$ ,  $j = 1, \dots, k$ , содержит  $k$  независимых элементов, неверно. Значит,  $N + U - U_m$  при некотором  $m$  содержит меньше чем  $k$  независимых элементов. Аналогично доказывается, что  $N + L - L_w$  при некотором  $w$  содержит меньше чем  $k$  независимых элементов.

Пусть  $T$  — подмножество, состоящее из независимых элементов множества

$$(N + U - U_m) + (N + L - L_w) = P^* - U_m - L_w.$$

Множество  $T$  не может содержать одновременно элемент  $x$  из  $U - U_m$  и элемент  $y$  из  $L - L_w$ , так как тогда  $x \equiv b \equiv y$ , что противоречит независимости элементов  $T$ . Но тогда  $T$  содержит либо в  $N + U - U_m$ , либо в  $N + L - L_w$ , и поэтому  $T$  имеет не более  $k - 1$  элементов. По предположению индукции  $P^* - U_m - L_w$  есть сумма не более чем  $k - 1$  цепей:  $P^* - U_m - L_w = C_1^* + C_2^* + \dots + C_{k-1}^*$ . Но  $C_k^* = U_m + b + L_w$  — цепь, и

$$P = C_1^* + C_2^* + \dots + C_k^*. \quad (7.2.4)$$

Это доказывает лемму и теорему для конечного  $P$ .

Если  $P$  бесконечно, то мы проводим индукцию по  $k$ . Заключение тривиально при  $k = 1$ . Допустим, что лемма выполняется для всех частично упорядоченных множеств, имеющих не более  $k - 1$  чрезвычайно независимых элементов, и что  $P$  содержит  $k$  независимых элементов. Подмножество  $C$  множества  $P$  называется *строго зависимым*, если для каждого конечного подмножества  $S$  множества  $P$  существует представление  $S$  в виде суммы не более чем  $k$  непересекающихся цепей, одна из которых содержит все элементы подмножества  $C$ , принадлежащие  $S$ . Очевидно,  $C$  должно быть цепью. Свойство строгой зависимости есть свойство конечного характера (в смысле определения Тьюки [1, стр. 7]), и, следовательно, для него справедлив принцип максимальности, т. е. в  $P$  существует максимальное строго зависимое множество  $C_1$ . Допустим, что  $P - C_1$  содержит  $k$  независимых элементов  $a_1, a_2, \dots, a_k$ . Максимальность  $C_1$  означает, что ни одно из множеств  $C_1 + a_1, C_1 + a_2, \dots, C_1 + a_k$  не является строго зависимым. Следовательно, для каждого  $i = 1, \dots, k$  существует конечное множество  $S_i$ , такое, что элементы из множества  $C_1 + a_i$ , принадлежащие  $S_i$ , не находятся в одной цепи, как бы  $S_i$  ни было представлено в виде суммы  $k$  непересекающихся цепей. При этом  $S_i$  должно содержать элемент  $a_i$ , поскольку  $C_1$  строго зависимо.

Рассмотрим теперь  $S = S_1 + S_2 + \dots + S_k$ . Множество  $S$  содержит все элементы  $a_1, a_2, \dots, a_k$ , и так как

С конечно, мы ввиду строгой зависимости  $C_1$  можем записать  $S$  в виде такой суммы  $k$  непересекающихся цепей  $S = K_1 + \dots + K_k$ , что все элементы  $C_1$ , содержащиеся в  $S$ , лежат в одной из них, скажем, в  $K_1$ . Но так как элементы  $a_1, \dots, a_k$  независимы, они все лежат в разных цепях, и один из них (скажем,  $a_r$ ) лежит в  $K_1$ . Таким образом, пересечения  $K_1, \dots, K_k$  с  $S_r$  — это непересекающиеся цепи  $T_1, \dots, T_k$ , так что  $S_r = T_1 + \dots + T_k$ , и все элементы множества  $C_1 + a_r$ , лежащие в  $S_r$ , принадлежат  $T_1$ . Но это противоречит нашему выбору  $S_r$ . Следовательно, невозможно, чтобы  $a_1, \dots, a_k$  были независимы. Таким образом,  $P - C_1$  содержит не более чем  $k - 1$  независимых элементов. По предположению индукции  $P - C_1 = C_2 + \dots + C_k$  и

$$P = C_1 + C_2 + \dots + C_k, \quad (7.2.5)$$

что доказывает лемму и теорему.

### Задачи

1. Найти  $(5 \times 5)$ -матрицу мер ценности для задачи о назначениях, такую, что ни одна из двух наибольших мер ценности не может быть использована при оптимальном назначении.
2. В задаче о назначении четырех лиц на четыре места меры ценности  $a_{ij}$ ,  $i, j = 1, 2, 3, 4$ , — это упорядоченные некоторым образом числа  $1, 2, \dots, 16$ . Показать, что сумма мер ценности при оптимальном назначении не меньше 34, и привести пример матрицы с такими мерами ценности, для которой 34 — оптимальное значение.
3. В процессе эксперимента исследуется некоторое число белых мышей. Если имеется  $mn + 1$  мышей, то показать, что либо а) имеется последовательность  $m + 1$  мышей, каждая из которых является потомком следующей, либо б) существует  $n + 1$  мышей, ни одна из которых не является потомком другой.

# Выпуклые пространства и линейное программирование

## 8.1. Выпуклые пространства. Выпуклые конусы и двойственные им пространства

Обозначим через  $E_n$   $n$ -мерное евклидово пространство ( $n$  конечно) над полем действительных чисел. Точка в  $E_n$  есть вектор  $x = (x_1, x_2, \dots, x_n)$ , где  $x_i$  — действительные числа. Нормой точки  $x$  называется величина  $|x| = \sqrt{x_1^2 + x_2^2 + \dots + x_n^2}$ , а расстоянием между точками  $x$  и  $y$  — величина  $|x - y|$ .

*Выпуклым пространством<sup>1)</sup>*  $C$  называется такое множество точек в  $E_n$ , что если  $x \in C$ ,  $y \in C$ , то  $ax + (1 - a)y \in C$ , где  $0 \leq a \leq 1$ . Геометрически это означает, что если две точки принадлежат  $C$ , то прямолинейный отрезок, соединяющий их, также принадлежит  $C$ .

*Лемма 8.1.1.* *Если  $x_1, \dots, x_m$  принадлежат выпуклому пространству  $C$ , то  $x = a_1x_1 + a_2x_2 + \dots + a_mx_m$  также принадлежит  $C$ , если  $a_i$  — действительные числа и*

$$a_i \geq 0, \quad \sum_{i=1}^m a_i = 1.$$

Доказательство проводим индукцией по  $m$ . Утверждение тривиально при  $m = 1$  и совпадает с определением выпуклости при  $m = 2$ . Если  $a_1 = 0$  или 1, то по индукции  $x \in C$ . Если же  $a_1 \neq 0, 1$ , то пусть  $b = 1 - a_1$  и  $b_i = a_i/b$ ,  $i = 2, \dots, m$ . Тогда  $b_i \geq 0$ ,  $i = 2, \dots, m$ , и  $\sum_{i=2}^m b_i = 1$ , следовательно, в силу индуктивного предположения  $b_2x_2 + \dots + b_mx_m = y \in C$ . Но тогда  $a_1x_1 + (1 - a_1)y = a_1x_1 + by = a_1x_1 + a_2x_2 + \dots + a_mx_m = x \in C$ .

<sup>1)</sup> Выпуклые пространства автор называет в дальнейшем также выпуклыми телами и выпуклыми множествами. — Прим. ред.

Под *окрестностью* точки  $x$  будем, как обычно, понимать открытый шар, состоящий из всех точек  $y$ , таких, что  $|x - y| < \epsilon$  при некотором  $\epsilon > 0$ . Точка  $x$  называется *пределной* точкой множества  $C$  из  $E_n$ , если существует такая последовательность точек  $x_m$ ,  $m = 1, 2, \dots$ , этого множества  $C$ , что

$$\lim_{m \rightarrow \infty} x_m = x,$$

т. е. если для всякого  $\epsilon > 0$  существует такое  $N$ , зависящее от  $\epsilon$ , что  $|x_m - x| < \epsilon$  при всех  $m \geq N$ . Заметим, что допускается равенство  $x_m = x$ . *Замыкание*  $\bar{S}$  множества  $S$  состоит из всех точек  $S$  и всех предельных точек  $S$ . *Граница* множества  $S$  состоит из точек  $y$ , таких, что каждая окрестность точки  $y$  содержит как точки, принадлежащие  $S$ , так и точки, не принадлежащие  $S$ .

Приведенные термины применимы к общим множествам точек. Мы используем также некоторые специфические термины, относящиеся к выпуклым пространствам. *Экстремальной* точкой  $x$  выпуклого пространства  $C$  называется такая точка  $x \in C$ , что если  $x = ay + (1 - a)z$ ,  $0 < a < 1$ ,  $y, z \in C$ , то  $y = z = x$ . Гиперплоскость

$$u_1x_1 + u_2x_2 + \dots + u_nx_n = u_0,$$

которую мы будем записывать в виде  $f(x) = u_0$ , называется *граничной гиперплоскостью* выпуклого пространства  $C$ , если  $f(y) > u_0$  для всякого  $y \in \bar{C}$ . Скажем, что гиперплоскость  $f(x) = u_0$  *отделяет* точку  $w$  от  $\bar{C}$ , если  $f(w) < u_0$  и  $f(y) > u_0$  при всяком  $y \in \bar{C}$ . Гиперплоскость  $f(x) = u_0$  называется *опорной гиперплоскостью* выпуклого пространства  $C$ , если  $f(y) \geq u_0$  при всяком  $y \in \bar{C}$  и если наибольшая нижняя грань  $f(y)$  при  $y \in \bar{C}$  равна  $u_0$ . Например, если  $C$  лежит в плоскости и ограничено одной ветвью гиперболы, то асимптота гиперболы есть *опорная гиперплоскость* для  $C$ . Другим примером опорных гиперплоскостей могут служить касательные к выпуклым телам. Через экстремальную точку может проходить несколько опорных гиперплоскостей. Так, через вершину квадрата, которая является экстремальной точкой этого квадрата, проходит много опорных прямых.

Частный случай выпуклого тела — выпуклый конус. Выпуклое тело  $C$  называется *выпуклым конусом*, если для каждого  $x \in C$  и любого действительного числа  $b \geq 0$  имеем  $bx \in C$ . Введем для выпуклого конуса несколько иное определение экстремальной точки. Скажем, что  $x \in C$  есть экстремальная точка выпуклого конуса  $C$ , если из  $x = ay + (1 - a)z$ ,  $0 < a < 1$ ,  $y \in C$ ,  $z \in C$ , следует, что  $y = ux$ ,  $z = vx$  при некоторых действительных  $u \geq 0$ ,  $v \geq 0$ .

Многие из обычных геометрических объектов являются выпуклыми телами. Нас здесь будут интересовать также и другие выпуклые пространства, которые обычно не рассматриваются с геометрической точки зрения. Так, *mn* действительных чисел, являющихся элементами  $(m \times n)$ -матрицы  $A = (a_{ij})$ , можно выписать в некотором порядке как координаты точки в  $E_{mn}$ . Множество всех таких матриц образует полное пространство  $E_{mn}$ , в то время как матрицы с неотрицательными элементами образуют выпуклый конус. Аналогично дважды стохастические матрицы, т. е.  $(n \times n)$ -матрицы  $A = (a_{ij})$ , удовлетворяющие условиям

$$a_{ij} \geq 0, \quad \sum_i a_{ij} = 1, \quad j = 1, \dots, n, \quad \sum_j a_{ij} = 1, \quad i = 1, \dots, n,$$

образуют выпуклое пространство. Симметрические  $(n \times n)$ -матрицы  $A = (a_{ij})$ ,  $a_{ij} = a_{ji}$ , образуют выпуклый конус; симметрические матрицы, для которых соответствующая квадратичная форма

$$Q = \sum_{i,j} a_{ij} x_i x_j$$

полупределена, также образуют выпуклый конус.

**Теорема 8.1.1.** *Если  $C$  — выпуклое множество<sup>1)</sup>, то замыкание  $\bar{C}$  множества  $C$  есть также выпуклое множество.*

**Доказательство.** Если  $x \in \bar{C}$ ,  $y \in \bar{C}$ , то существуют последовательности  $\{x_m\}$ ,  $\{y_m\}$  точек  $C$ , такие, что

$$\lim_{m \rightarrow \infty} x_m = x, \quad \lim_{m \rightarrow \infty} y_m = y.$$

<sup>1)</sup> См. примечание на стр. 95. — Прим. ред.

Но тогда при  $0 \leq a \leq 1$  имеем также

$$\lim_{m \rightarrow \infty} (ax_m + (1 - a)y_m) = ax + (1 - a)y.$$

Поэтому каждая точка прямой, соединяющей  $x$  и  $y$ , есть снова точка из  $\bar{C}$ , а это и есть утверждение теоремы.

**Теорема 8.1.2.** *Если  $C$  – выпуклое множество и  $P$  – точка, не лежащая в  $\bar{C}$ , то существует гиперплоскость, отделяющая  $P$  от  $\bar{C}$ .*

**Доказательство.** Пусть  $s$  – произвольная точка  $C$ . Тогда точки  $x$ , такие, что  $|P - x| \leq |P - s| = b$ , образуют замкнутый шар радиуса  $b$  с центром  $P$ , который представляет собой компактное множество. Следовательно, существует точка  $Q \in \bar{C}$ , ближайшая к  $P$ , т. е. такая, что  $|P - Q|$  минимально среди всех  $Q \in \bar{C}$ . Кроме того,  $Q$  единственна, так как если  $Q_1, Q_2$  – две точки из  $\bar{C}$  на одном и том же расстоянии от  $P$ , то  $PQ_1Q_2$  – равнобедренный треугольник с равными сторонами  $PQ_1$  и  $PQ_2$ . Но если  $Q_1 \neq Q_2$ , то середина отрезка  $Q_1Q_2$  есть точка из  $\bar{C}$ , находящаяся ближе к  $P$ , чем  $Q_1$  или  $Q_2$ .

Пусть теперь  $f(x) = u_1x_1 + u_2x_2 + \dots + u_nx_n = u_0$  – гиперплоскость, перпендикулярная к отрезку  $PQ$  и делящая его пополам. Тогда  $f(P) = u_0$  и  $f(Q) = u_0$  имеют противоположные знаки, и мы можем считать, что  $f(P) < u_0$  и  $f(Q) > u_0$ , умножая, если нужно, на  $-1$ . Чтобы показать, что гиперплоскость  $f(x) = u_0$  отделяет  $P$  от  $\bar{C}$ , достаточно доказать, что она не содержит ни одной точки из  $\bar{C}$ . Предположим обратное: пусть  $S$  – точка гиперплоскости  $f(x) = u_0$  и  $S \in \bar{C}$ . Тогда  $S$  находится дальше от  $P$ , чем  $Q$ ; в частности,  $S$  не является серединой отрезка  $PQ$ , так что  $PSQ$  – равнобедренный треугольник с равными сторонами  $PS$  и  $SQ$  и с третьей стороной  $PQ$ , которая короче первых двух. Но тогда все три угла треугольника  $PSQ$  острые, и, значит, перпендикуляр из  $P$  к  $SQ$  пересекает отрезок  $SQ$  в точке  $T$ . Так как  $S$  и  $Q$  обе лежат в  $\bar{C}$ ,  $T$  также является точ-

кой  $\bar{C}$ . Но  $P\bar{T}$  короче  $PQ$ , что противоречит выбору точки  $Q$ . Это означает, что гиперплоскость  $f(x) = u_0$  не содержит ни одной точки из  $\bar{C}$ . Так как  $f(Q) > u_0$  и  $f(P) < u_0$ , отсюда следует, что  $f(y) > u_0$  при всяком  $y \in \bar{C}$ , и потому  $f(x) = u_0$  — гиперплоскость, отделяющая  $P$  от  $\bar{C}$ .

Следующая, несколько более тонкая теорема аналогична доказанной.

**Теорема 8.1.3.** *Пусть  $P$  — точка на границе замыкания  $\bar{C}$  выпуклого пространства  $C$ . Тогда существует опорная гиперплоскость пространства  $C$ , проходящая через  $P$ .*

**Доказательство.** Так как  $P$  лежит на границе  $\bar{C}$ , всякая окрестность точки  $P$  содержит точку, не лежащую в  $\bar{C}$ . Следовательно, мы можем найти бесконечную последовательность  $\{z_m\}$ ,  $m = 1, 2, \dots$ , точек, не лежащих в  $\bar{C}$ , такую, что  $\lim_{m \rightarrow \infty} z_m = P$ . По теореме 8.1.2 для каждой точки существует гиперплоскость  $f_m(x) = u_{m0}$ , отделяющая  $z_m$  от  $\bar{C}$ . Предполагаем, что каждая такая гиперплоскость задана своим нормальным уравнением

$$f_m(x) = u_{1m}x_1 + \dots + u_{nm}x_n,$$

где  $u_{1m}^2 + \dots + u_{nm}^2 = 1$  и  $f_m(y) > u_{m0}$  при всяком  $y \in \bar{C}$ . Так как точки  $u^{(m)} = (u_{1m}, u_{2m}, \dots, u_{nm})$  лежат на единичной сфере, являющейся компактным множеством, то существует некоторая сходящаяся подпоследовательность последовательности точек  $u^{(m)}$ ,  $m = 1, \dots, k, \dots$ , с пределом  $(u_1, u_2, \dots, u_n)$ . Пусть это будет подпоследовательность с индексами  $m_j$ ,  $j = 1, 2, \dots$ . Тогда

$$\lim_{j \rightarrow \infty} f_{m_j}(x) = f(x) = u_1x_1 + u_2x_2 + \dots + u_nx_n.$$

Так как

$$\lim_{j \rightarrow \infty} z_{m_j} = P$$

$$f_{m_j}(z_j) < u_{m_j 0} < f_{m_j}(P), \text{ то}$$

$$\lim_{j \rightarrow \infty} u_{m_j 0} = u_0,$$

где  $f(P) = u_0$ . Для каждого  $y \in \bar{C}$  мы имели  $f_{m_j}(y) > u_{m_j 0}$ .

Следовательно, в пределе, при  $j \rightarrow \infty$ ,  $f(y) \geq u_0$ . Таким образом, гиперплоскость  $f(x) = u_0$  есть опорная гиперплоскость для  $C$ , проходящая через  $P$ , так как  $f(y) \geq u_0$  при всяком  $y \in C$  и  $f(P) = u_0$ , где  $P$  — либо точка пространства  $C$ , либо предельная точка для  $C$ .

**Лемма 8.1.2.** *Если  $P$  — граничная точка замыкания  $\bar{C}$  выпуклого конуса  $C$ , то опорная гиперплоскость выпуклого пространства  $C$ , проходящая через  $P$ , проходит также через начало координат.*

**Доказательство.** Если  $P$  — начало, то доказывать нечего. Пусть  $P \neq (0, \dots, 0)$  и  $f(x) = u_0$  — опорная гиперплоскость, проходящая через  $P$ , где  $f(P) = u_0$ . Тогда  $cP$  есть точка пространства  $\bar{C}$  для любого  $c > 0$ , следовательно,  $f(cP) = cf(P) \geq u_0$ , так как  $f(x) = u_0$  есть опорная плоскость. Поскольку  $f(P) = u_0$ , это означает, что  $cu_0 \geq u_0$  при любом  $c > 0$ . Это возможно только при  $u_0 = 0$ , следовательно, гиперплоскость имеет уравнение  $f(x) = 0$  и обязательно проходит через начало координат.

**Скалярное произведение**  $(x, y)$  векторов  $x = (x_1, \dots, x_n)$  и  $y = (y_1, \dots, y_n)$  определим как обычно:

$$(x, y) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n. \quad (8.1.1)$$

Отметим следующие свойства скалярного произведения:

$$\begin{aligned} (x, y) &= (y, x), \\ (bx, y) &= (x, by) = b(x, y) \quad (b — \text{действительное число}), \\ (x + y, z) &= (x, z) + (y, z). \end{aligned} \quad (8.1.2)$$

**Теорема 8.1.4.** *Если  $S$  — некоторое непустое множество векторов  $\{x\}$ , то множество  $T$  векторов  $y$ , таких, что  $(x, y) \geq 0$  для всякого  $x \in S$ , есть замкнутый выпуклый конус.*

**Доказательство.** Утверждение теоремы почти очевидно, так как для векторов  $y_1, y_2$ , удовлетворяющих условиям  $(x, y_1) \geq 0$  и  $(x, y_2) \geq 0$  при всяком  $x \in S$ ,

и для любых положительных чисел  $a, b$  имеем

$$(x, ay_1 + by_2) = a(x, y_1) + b(x, y_2) \geq 0$$

при всяком  $x \in S$ . Аналогично если

$$\lim_{m \rightarrow \infty} y_m = y \quad \text{и} \quad (x, y_m) \geq 0,$$

то  $(x, y) \geq 0$  при всяком  $x \in S$ . Теорема доказана.

**Определение.** Если  $C$  — замкнутый выпуклый конус, то множество точек  $y$ , таких, что  $(x, y) \geq 0$  при всяком  $x \in C$ , называется *двойственным пространством* для  $C$  и обозначается через  $C^*$ ; пространство  $C^*$  является замкнутым выпуклым конусом (по теореме 8.1.4).

**Теорема 8.1.5.** *Если  $C$  — замкнутый выпуклый конус и  $C^*$  — двойственный ему конус, то  $(C^*)^* = C$ .*

**Доказательство.** Это — основная теорема, но мы увидим, что она почти эквивалентна теореме отделимости 8.1.2. Из определения двойственного пространства имеем

$$\begin{aligned} C^* &= \{y \mid (x, y) \geq 0 \text{ для всех } x \in C\}, \\ (C^*)^* &= \{z \mid (y, z) \geq 0 \text{ для всех } y \in C^*\}. \end{aligned} \quad (8.1.3)$$

Из симметричности скалярного произведения следует, что каждый вектор  $x \in C$  удовлетворяет условию  $(y, x) \geq 0$  при всяком  $y \in C^*$ , поэтому  $C \subseteq (C^*)^*$ . Мы должны доказать обратное включение. Если  $z$  — вектор (точка) из  $(C^*)^*$ , который не лежит в  $\bar{C} = C$ , то по теореме 8.1.2 существует гиперплоскость  $f(x) = u_0$ , которая отделяет  $z$  от  $\bar{C} = C$ , так что  $f(z) < u_0$ , а при всяком  $x \in C$   $f(x) > u_0$ . Поскольку начало  $O$  принадлежит  $C$ , то  $0 = f(O) > u_0$ , т. е.  $u_0$  отрицательно. Так как  $f(x) = u_1 x_1 + u_2 x_2 + \dots + u_n x_n \geq 0$  для всех  $x \in C$  (в противном случае существовало бы такое  $c > 0$ , что  $f(cx) < u_0$ ), то отсюда следует, что  $u = (u_1, u_2, \dots, u_n) \in C^*$ , но  $f(z) = (u, z) < u_0 < 0$ , т. е.  $z \notin (C^*)^*$ . Получили противоречие. Следовательно,  $(C^*)^* \subseteq C$  и  $C = (C^*)^*$ .

## 8.2. Линейные неравенства

Обратимся теперь к теории линейных неравенств, или линейному программированию, как стало принято ее называть. Если  $x = (x_1, \dots, x_m)$  — произвольный вектор, то мы будем писать

$$x \geqslant 0, \text{ если } x_i \geqslant 0, i = 1, \dots, m;$$

$$x \geqslant 0, \text{ если } x \geqslant 0 \text{ и } x \neq 0;$$

$$x > 0, \text{ если } x_i > 0, i = 1, \dots, m.$$

Определим неравенства  $x \geqslant y$ ,  $x \geqslant y$  и  $x > y$  в соответствии с соотношением между  $x - y$  и 0.

Если  $A = (a_{ij})$ ,  $i = 1, \dots, m$ ,  $j = 1, \dots, n$ , есть  $(m \times n)$ -матрица и  $x = (x_1, \dots, x_m)$  таков, что  $x \geqslant 0$ , то множество всех векторов  $xA$ , как легко видеть, есть выпуклый конус  $C$  пространства  $E_n$ , определенный строками матрицы  $A$ . Если  $r_1, r_2, \dots, r_m$  — строки  $A$ , то  $xA = x_1r_1 + x_2r_2 + \dots + x_mr_m$ .

Пусть вектор-столбец  $w^t$  есть транспонированный вектор  $w = (w_1, \dots, w_n)$ . Утверждение  $Aw^t \geqslant 0$  эквивалентно тому, что скалярные произведения  $(r_i, w) \geqslant 0$  для  $i = 1, \dots, m$ . В силу линейности скалярного произведения по каждому сомножителю  $(y, w) \geqslant 0$  при всяком  $y \in C$ , т. е.  $w$  принадлежит  $C^*$ , двойственному конусу для  $C$ . Заметим, что  $C$  — замкнутый выпуклый конус. Мы можем теперь сформулировать теорему 8.1.5 в матричной форме. Эта теорема восходит к Фаркашу [1].

**Теорема 8.2.1 (Фаркаш).** Пусть  $A$  есть  $(m \times n)$ -матрица, и пусть  $y = (y_1, \dots, y_n)$  — такой вектор, что  $yw^t = (y, w) \geqslant 0$  для всякого вектора  $w = (w_1, \dots, w_n)$ , удовлетворяющего неравенству  $Aw^t \geqslant 0$ . Тогда  $y$  имеет вид

$$y = xA, \text{ где } x = (x_1, \dots, x_m) \geqslant 0.$$

**Доказательство.** Пусть  $C$  — замкнутый выпуклый конус, определяемый строками  $A$ , т. е.  $C$  состоит из всех векторов  $x_1r_1 + \dots + x_mr_m$ , где  $r_1, \dots, r_m$  — строки  $A$  и  $x_i \geqslant 0$ ,  $i = 1, 2, \dots, m$ . Тогда предположение теоремы означает, что  $y \in (C^*)^*$ , а заключение — что  $y \in C$ . Поэтому теорема 8.2.1 следует из теоремы 8.1.5.

Следующая теорема представляет собой более сильную, неоднородную форму теоремы 8.2.1.

**Теорема 8.2.2.** Пусть  $A$  есть  $(m \times n)$ -матрица,  $d = (d_1, \dots, d_m)$  — некоторый вектор и  $k$  — скаляр. Предположим, что хотя бы для одного вектора  $w = (w_1, \dots, w_n)$  выполняется соотношение

$$Aw^t \geqq d^t. \quad (8.2.1)$$

Тогда вектор  $y = (y_1, \dots, y_n)$  удовлетворяет соотношению

$$yw^t = (y, w) \geqq k \quad (8.2.2)$$

при всех  $w$ , удовлетворяющих условию (8.2.1), в том и только том случае, когда существует вектор  $x = (x_1, \dots, x_m) \geqq 0$ , такой, что

$$y = xA \quad \text{и} \quad xd^t \geqq k. \quad (8.2.3)$$

**Доказательство.** Если (8.2.3) выполняется, то сразу получаем

$$yw^t = xAw^t \geqq xd^t \geqq k. \quad (8.2.4)$$

Докажем обратное. Для этого придадим задаче однородную форму, чтобы можно было применить теорему 8.2.1. Если ввести обозначения

$$A' = \begin{pmatrix} A & -d^t \\ 0 & 1 \end{pmatrix}, \quad w' = (w_1, \dots, w_n, z_0), \quad y' = (y_1, \dots, y_n, -k), \quad (8.2.5)$$

то (8.2.1) принимает вид

$$A'w'^t \geqq 0 \quad \text{при} \quad z_0 = 1, \quad (8.2.6)$$

а (8.2.2) — вид

$$y'w'^t \geqq 0 \quad \text{при} \quad z_0 = 1. \quad (8.2.7)$$

Если бы при этом получилось, что

$$y' = x'A' \quad \text{с} \quad x' = (x_1, \dots, x_m, x_{m+1}) \geqq 0, \quad (8.2.8)$$

то

$$y = xA \quad \text{и} \quad -xd^t + x_{m+1} = -k, \quad \text{или} \quad xd^t = k + x_{m+1} \geqq k,$$

что эквивалентно формуле (8.2.3). За исключением ограничения  $z_0 = 1$ , предположения (8.2.6) и (8.2.7) — это как

раз предположения теоремы 8.2.1, и (8.2.8) является заключением этой теоремы. Необходимо ослабить действие указанного ограничения. Если  $w' = (w_1, \dots, w_n, z_0)$ , где  $z_0 > 0$ , удовлетворяет (8.2.6), то  $w'' = (1/z_0) w' = \left(\frac{w_1}{z_0}, \dots, \frac{w_n}{z_0}, 1\right)$  также удовлетворяет этому условию, а следовательно, и условию (8.2.7). Поэтому, умножая на  $z_0$ , мы находим, что  $w'$  также удовлетворяет (8.2.7). Таким образом, доказано, что всякий раз, когда

$A' w'^t \geqq 0$  для  $w' = (w_1, \dots, w_n, z_0)$ , где  $z_0 > 0$ , (8.2.9)  
то

$$y' w'^t \geqq 0, \quad (8.2.10)$$

и мы хотим получить, что

$$y' = x' A', \text{ где } x' = (x_1, \dots, x_m, x_{m+1}) \geqq 0. \quad (8.2.11)$$

Если (8.2.9.) влечет за собой (8.2.10) также в случае  $z_0 = 0$ , то формула (8.2.11) вытекает из теоремы 8.2.1 (ввиду (8.2.5)). Остается рассмотреть предположение, что для некоторого  $w'' = (w''_1, \dots, w''_n, 0)$ , где  $z_0 = 0$ , формула (8.2.9) справедлива, а (8.2.10) нет, т. е.

$$A' w''^t \geqq 0 \text{ и } y' w''^t < 0. \quad (8.2.12)$$

Возьмем тогда  $w'_0$  с  $z_0 = 1$ , для которого выполняются (8.2.6) и (8.2.7), и образуем  $w'$  по формуле

$$w' = w'' + x_0 w'_0, \text{ где } x_0 > 0. \quad (8.2.13)$$

Вектор  $w'$  удовлетворяет (8.2.9), а следовательно, и (8.2.10), т. е.

$$y' w'^t \geqq 0, \text{ или } y' (w'' + x_0 w'_0)^t \geqq 0. \quad (8.2.14)$$

Отсюда

$$y' w''^t \geqq -x_0 y' w'_0^t. \quad (8.2.15)$$

Но  $y' w''^t < 0$ , а  $y' w'_0^t \geqq 0$ , и (8.2.15) не выполняется при некотором достаточно малом положительном  $x_0$ . Таким образом, ситуация (8.2.12) не может возникнуть, и (8.2.9) влечет за собой (8.2.10) и в случае  $z_0 = 0$ . По теореме 8.2.1 заключаем, что соотношение (8.2.11) выполняется, и теорема полностью доказана.

Линейное программирование — это проблема максимизации или минимизации некоторой линейной формы, когда переменные подчинены соотношениям, записываемым в виде линейных неравенств. Трактовка, приводимая здесь, принадлежит Флуду [1]. Впервые проблема была рассмотрена в работе Гейла, Куна и Таккера [1].

Предположим, что даны  $(r \times s)$ -матрица  $A = (a_{ij})$  и два вектора  $b = (b_1, \dots, b_r)$  и  $c = (c_1, \dots, c_s)$ . Рассмотрим теперь две задачи.

*Задача I.* Найти вектор  $x = (x_1, \dots, x_s)$ , который минимизирует

$$cx^t = (c, x) \quad (8.2.16)$$

и удовлетворяет неравенствам

$$Ax^t \geqq b^t, \quad x \geqq 0. \quad (8.2.17)$$

*Задача II.* Найти вектор  $y = (y_1, \dots, y_r)$ , который максимизирует

$$yb^t = (y, b) \quad (8.2.18)$$

и удовлетворяет неравенствам

$$yA \leqq c, \quad y \geqq 0. \quad (8.2.19)$$

Эти две задачи называются *двойственными* одна другой. Если существует вектор  $x$ , удовлетворяющий соотношениям (8.2.17), то задача I называется допустимой, а  $x$  — допустимым вектором. Так же определяется допустимость для задачи II.

**Теорема 8.2.3 (теорема двойственности).** *Задачи I и II обладают решениями тогда и только тогда, когда обе задачи допустимы. Далее, если  $t$  — минимальное значение для  $cx^t$  в задаче I, а  $M$  — максимальное значение для  $yb^t$  в задаче II, то  $t = M$ . Если одна из задач имеет решение, то другая задача также имеет решение.*

**Доказательство.** Предположим сначала, что обе задачи допустимы. Тогда существуют  $x = (x_1, \dots, x_s)$  и  $y = (y_1, \dots, y_r)$ , для которых выполняются неравенства

$$Ax^t \geqq b^t, \quad x \geqq 0, \quad (8.2.20a)$$

$$yA \leqq c, \quad y \geqq 0. \quad (8.2.20b)$$

Отсюда

$$cx^t \geq yAx^t \geq yb^t. \quad (8.2.21)$$

Следовательно,  $cx^t$  ограничено снизу числом  $yb^t$  при всяком допустимом  $y$ , а  $yb^t$  ограничено сверху числом  $cx^t$  при всяком допустимом  $x$ . Следовательно, существуют наибольшая нижняя грань  $m$  для  $cx^t$  и наименьшая верхняя грань  $M$  для  $yb^t$ , которые связаны соотношением

$$m \geq M. \quad (8.2.22)$$

В нашем доказательстве будет использована теорема 8.2.2, но, чтобы ее применить, нам нужно заменить два неравенства (8.2.20a) одним. Определим  $(r+s)$ -мерный вектор  $b_0 = (b_1, \dots, b_r, 0, \dots, 0)$  путем добавления  $s$  нулей к  $b$ . Аналогично построим  $[(r+s) \times s]$ -матрицу  $A_0$  путем добавления к  $A$   $s$  строк, которые образуют единичную  $(s \times s)$ -матрицу. Тогда

$$A_0x^t = \begin{pmatrix} A \\ I_s \end{pmatrix}x^t \geq b_0^t = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \quad (8.2.23)$$

Это неравенство в точности эквивалентно двум неравенствам (8.2.20a):  $Ax^t \geq b^t$ ,  $x \geq 0$ . Поэтому если  $m$  — наибольшая нижняя грань для  $cx^t$ , то

$$cx^t \geq m \quad (8.2.24)$$

для всех  $x$ , удовлетворяющих (8.2.23). Мы находимся теперь в условиях теоремы 8.2.2 и можем заключить, что существует такой вектор  $y_0$ , что

$$y_0 = (u_1, \dots, u_r, v_1, \dots, v_s), \quad y_0 \geq 0,$$

$$c = y_0 A_0, \quad y_0 b_0^t \geq m. \quad (8.2.25)$$

Если ввести обозначения

$$u = (u_1, \dots, u_r), \quad v = (v_1, \dots, v_s), \quad (8.2.26)$$

то результат (8.2.25) можно выразить в следующем виде:

$$c = uA + v, \quad u \geq 0, \quad v \geq 0, \quad ub^t \geq m. \quad (8.2.27)$$

Но из формул (8.2.22) и (8.2.27) имеем

$$\begin{aligned} uA &\leqq c, \\ ub^t &\geq m \geq M \geq ub^t. \end{aligned} \quad (8.2.28)$$

Отсюда

$$ub^t = m = M, \quad (8.2.29)$$

и  $y = u$  есть решение задачи II.

Аналогично если построить матрицу

$$B_0 = (A, -I_r), \quad (8.2.30)$$

добавив к  $A$   $r$  столбцов, которые образуют матрицу  $-I_r$ , где  $I_r$  — единичная  $(r \times r)$ -матрица, то два неравенства (8.2.20b)  $yA \leqq c$  и  $y \geq 0$  эквивалентны одному

$$(-B_0^t)y^t \geq -c_0^t, \quad (8.2.31)$$

где  $c_0 = (c_1, \dots, c_s, 0, \dots, 0)$  есть  $(s+r)$ -мерный вектор, полученный добавлением  $r$  нулей к  $c$ . Отсюда как следствие соотношения (8.2.21) получаем, что

$$-by^t \geq -M \quad (8.2.32)$$

для всех векторов  $y$ , удовлетворяющих (8.2.31). Мы можем теперь применить теорему 8.2.2 и заключить, что существует такой вектор  $d = (w_1, \dots, w_s, z_1, \dots, z_r)$ , что

$$d \geq 0, \quad -b = d(-B_0^t), \quad d(-c_0^t) \geq -M. \quad (8.2.33)$$

Если ввести обозначения

$$w = (w_1, \dots, w_s), \quad z = (z_1, \dots, z_r), \quad (8.2.34)$$

то (8.2.33) принимает вид

$$w \geq 0, \quad z \geq 0, \quad b = wA' - z, \quad wc' \leq M. \quad (8.2.35)$$

Но тогда  $w A^t \geqq b$ :

$$A w^t \geqq b^t, \quad c w^t \leq M \leq m \leq c w^t, \quad w \geqq 0. \quad (8.2.36)$$

Таким образом,  $x = w$  решает задачу I, и вновь показано, что  $M = m$ .

Итак, мы показали, что если обе задачи допустимы, то они обе имеют решения, и при этом минимум  $m$  для задачи I равен максимуму  $M$  для задачи II. Заметим, что из существования  $m$  в (8.2.24) вытекает, что  $y = u$  в (8.2.26) есть решение задачи II, а из существования  $M$  в (8.2.32) вытекает, что  $x = w$  в (8.2.34) есть решение задачи I. Таким образом, если одна из задач имеет решение, то и другая задача имеет решение, и все утверждения теоремы теперь доказаны.

На прямолинейном отрезке в  $n$ -мерном пространстве линейная функция координат либо постоянна, либо принимает на нем минимум на одном конце отрезка и максимум на другом его конце. Таким образом, линейная функция на выпуклом пространстве, ограниченная сверху (или снизу), будет принимать в нем максимум (или минимум) в экстремальной точке. Очевидно, матрицы перестановки являются экстремальными точками пространства дважды стохастических матриц, и теорема 5.1.9 показывает, что в этом пространстве других экстремальных точек нет. Следовательно, максимум или минимум линейной функции на пространстве дважды стохастических матриц достигается на матрице перестановки. Используя это замечание, мы попытаемся найти другой подход к задаче о назначениях — с помощью теоремы двойственности. Будет показано, что числа  $u_i$  и  $v_j$ , которые несколько „таинственно“ появились в теореме 7.1.1, вполне естественно возникают из задачи, двойственной задаче о назначениях.

Пусть  $A = (a_{ij})$ ,  $i, j = 1, \dots, n$ , — матрица мер ценности при назначениях, рассматриваемая в теореме 7.1.1. Определим  $n^2$  чисел  $b$  равенством  $b_{i+(j-1)n} = a_{ij}$ . Введем также переменные  $z_{ij}$ ,  $i, j = 1, \dots, n$ , и переменные  $y_1, \dots, y_n$ , где  $y_{i+(j-1)n} = z_{ij}$ . Определим теперь такие

$(n^2 \times 4n)$  = матрицу  $K$  и вектор  $c$ :

$$K = \begin{bmatrix} J_1 & -J_1 & I_n & -I_n \\ J_2 & -J_2 & I_n & -I_n \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ J_n & -J_n & I_n & -I_n \end{bmatrix}, \quad c = (i_n, -i_n, i_n, -i_n), \quad (8.2.37)$$

где  $I_n$  – единичная  $(n \times n)$ -матрица,  $J_i$  –  $(n \times n)$ -матрица с единицами в  $i$ -м столбце и нулями на остальных местах и  $i_n$  – вектор-строка из  $n$  единиц. Возьмем  $y = (y_1, \dots, y_{n^2})$ . Тогда условие

$$yK \leq c, \quad y \geq 0, \quad (8.2.38)$$

означает, что матрица  $Z = (z_{ij})$  дважды стохастическая, поскольку тогда элементы  $Z$  неотрицательны, суммы по строкам и столбцам  $Z$  не превосходят +1, а суммы противоположных значений по строкам и столбцам не превосходят -1. Следовательно, при

$$b = (b_1, \dots, b_{n^2}), \quad b_{i+(j-1)n} = a_{ij} \quad (8.2.39)$$

проблема максимизации  $yb^t$  есть в точности проблема максимизации

$$\sum_{i,j} a_{ij} z_{ij},$$

где  $Z = (z_{ij})$  – дважды стохастическая матрица. Мы знаем, что эта задача имеет решение, которое должно быть матрицей перестановки, так как матрицы перестановки – экстремальные точки пространства дважды стохастических матриц. Таким образом, задача о назначениях есть в точности задача нахождения максимума скалярного произведения  $(y, b) = yb^t$ , если  $y$  удовлетворяет неравенствам (8.2.38). Это указанная выше задача II. Двойственная задача I состоит в том, чтобы найти минимум для  $cx^t$ , где  $x = (x_1, \dots, x_{4n})$  – вектор, удовлетворяющий неравенствам

$$Kx^t \geq b^t, \quad x \geq 0. \quad (8.2.40)$$

Если обозначить  $u_i = x_i - x_{n+i}$  для  $i = 1, \dots, n$  и  $v_j = x_{2n+j} - x_{3n+j}$  для  $j = 1, \dots, n$ , то неравенство (8.2.40)

принимает вид

$$u_i + v_j \geq a_{ij}, \quad i, j = 1, \dots, n, \quad (8.2.41)$$

и теорема двойственности утверждает, что минимум  $m$  для

$$cx^t = \sum_i u_i + \sum_j v_j,$$

где  $x$  подчинен условиям (8.2.41), есть максимум  $M$  для

$$\sum_{i,j} z_{ij} a_{ij},$$

где  $Z = (z_{ij})$  — матрица перестановки. Доказательство этого утверждения — основная часть доказательства теоремы 7.1.1.

### 8.3. Линейное программирование. Симплексный метод

Задачи I и II из предыдущего раздела связаны с максимизацией (или минимизацией) линейной формы от действительных переменных  $x_1, \dots, x_r$ , подчиненных некоторым линейным неравенствам и дополнительному условию  $x_i \geq 0, i = 1, 2, \dots, r$ . В этом разделе мы рассмотрим более общую задачу, в которой переменные не обязательно являются неотрицательными. Мы изложим также метод, принадлежащий Данцигу [1] и называемый „симплексным методом“, который дает конструктивное решение этой задачи, когда решение существует. Мы назовем эту общую задачу задачей III и определим также задачу IV, двойственную ей в том же смысле, в котором были двойственны задачи I и II.

*Задача III.* Найти вектор  $z = (z_1, \dots, z_m)$ , который максимизирует линейную функцию

$$b_1 z_1 + b_2 z_2 + \dots + b_m z_m = u \quad (8.3.1)$$

и удовлетворяет неравенствам

$$\begin{aligned} a_{11} z_1 + a_{21} z_2 + \dots + a_{m1} z_m + c_1 &\geq 0, \\ a_{12} z_1 + a_{22} z_2 + \dots + a_{m2} z_m + c_2 &\geq 0, \\ \dots &\dots \dots \dots \dots \dots \dots \\ a_{1n} z_1 + a_{2n} z_2 + \dots + a_{mn} z_m + c_n &\geq 0. \end{aligned} \quad (8.3.2)$$

**Задача IV.** Найти вектор  $y = (y_1, \dots, y_n)$ ,  $y \geq 0$ , который минимизирует функцию

$$c_1 y_1 + c_2 y_2 + \dots + c_n y_n = v \quad (8.3.3)$$

и удовлетворяет уравнениям

$$\begin{aligned} a_{11} y_1 + a_{12} y_2 + \dots + a_{1n} y_n + b_1 &= 0, \\ a_{21} y_1 + a_{22} y_2 + \dots + a_{2n} y_n + b_2 &= 0, \\ \vdots &\vdots \\ a_{m1} y_1 + a_{m2} y_2 + \dots + a_{mn} y_n + b_m &= 0. \end{aligned} \quad (8.3.4)$$

Мы скажем, что задача III допустима, если существует вектор  $z = (z_1, \dots, z_m)$ , удовлетворяющий неравенствам (8.3.2), и что задача IV допустима, если существует вектор  $y = (y_1, \dots, y_n)$ ,  $y \geq 0$ , удовлетворяющий уравнениям (8.3.4).

**Теорема 8.3.1.** Задачи III и IV обладают решениями тогда и только тогда, когда обе задачи допустимы. При этом для решений имеем  $u = v$ . Если одна из задач имеет решение, то другая задача также имеет решение.

**Доказательство.** Для доказательства видоизменим задачи таким образом, чтобы можно было применить теорему двойственности. Пусть

$$\begin{aligned} z &= (z_1, \dots, z_m), \quad y = (y_1, \dots, y_n), \quad b = (b_1, \dots, b_m), \\ c &= (c_1, \dots, c_n), \quad A = (a_{ij}), \quad i = 1, \dots, m, \quad j = 1, \dots, n. \end{aligned}$$

Определим также

$$x = (x_1, \dots, x_m, x_{m+1}, \dots, x_{2m}),$$

где  $x_{m+i} - x_i = z_i$ ,  $i = 1, \dots, m$ , и  $x \geq 0$ , и пусть

$$x^1 = (x_1, \dots, x_m), \quad x^2 = (x_{m+1}, \dots, x_{2m}),$$

так что  $x^2 - x^1 = z$ , и  $d = (-b_1, \dots, -b_m, b_1, \dots, b_m) = [-b, b]$ . Определим, наконец,  $(2m \times n)$ -матрицу  $A_1$ :

$$A_1 = \begin{bmatrix} A \\ -A \end{bmatrix}. \quad (8.3.5)$$

Сформулируем теперь двойственные задачи в терминах этих векторов и матриц,

*Задача I.* Найти  $y = (y_1, \dots, y_n)$ , который минимизирует

$$cy^t = m' \quad (8.3.6)$$

и удовлетворяет неравенствам

$$y \geq 0, \quad A_1 y^t \geq d^t. \quad (8.3.7)$$

*Задача II.* Найти  $x = (x_1, \dots, x_m, x_{m+1}, \dots, x_{2m})$ , который максимизирует

$$x d^t = M' \quad (8.3.8)$$

и удовлетворяет неравенствам

$$x \geq 0, \quad x A_1 \leq c. \quad (8.3.9)$$

К этим двум задачам применима теорема двойственности. Здесь неравенство (8.3.7) имеет вид

$$y \geq 0, \quad \begin{bmatrix} Ay^t \\ -Ay^t \end{bmatrix} \geq \begin{bmatrix} -b^t \\ b^t \end{bmatrix}, \quad (8.3.10)$$

откуда  $Ay^t \geq -b$  и  $-Ay^t \geq b$ , что эквивалентно равенству  $Ay^t + b = 0$ , матричной форме системы уравнений (8.3.4), а  $cy^t = m'$  — то же самое, что и (8.3.3) с  $m' = v$ . Соотношения (8.3.9) принимают вид

$$x^1 A - x^2 A \leq c, \quad (8.3.11)$$

или  $-zA \leq c$ , что иначе можно записать так:

$$zA + c \geq 0, \quad (8.3.12)$$

а это матричная форма системы неравенств (8.3.2). Наконец, (8.3.8) принимает вид

$$-x^1 b^t + x^2 b^t = M', \quad (8.3.13)$$

или

$$zb^t = M', \quad (8.3.14)$$

а это не что иное, как (8.3.1) с  $M' = u$ . Таким образом, в новой форме задача II есть задача III, а задача I есть задача IV. Тем самым теорема 8.3.1 сводится к теореме двойственности 8.2.3, и доказательство теоремы 8.3.1 завершено.

Нам больше не нужны переменные  $x_i$ , использованные при доказательстве теоремы 8.3.1, поэтому теперь

через  $x_1, \dots, x_n$  обозначим левые части неравенств (8.3.2):

$$\begin{aligned}x_1 &= a_{11}z_1 + a_{21}z_2 + \dots + a_{m1}z_m + c_1 \geq 0, \\x_2 &= a_{12}z_1 + a_{22}z_2 + \dots + a_{m2}z_m + c_2 \geq 0, \\&\dots \\x_n &= a_{1n}z_1 + a_{2n}z_2 + \dots + a_{mn}z_m + c_n \geq 0.\end{aligned}\quad (8.3.15)$$

Здесь, разумеется,  $x_i \geq 0$ ,  $i = 1, \dots, n$ . В следующей теореме устанавливается простое тождество, которое не содержит  $z_i$  в явном виде.

**Теорема 8.3.2.** Для  $x_i$  из (8.3.15) и  $y_j$  из (8.3.4) выполняется следующее тождество:

$$x_1y_1 + x_2y_2 + \dots + x_ny_n = -u + v. \quad (8.3.16)$$

**Доказательство.** Заменяя  $x_i$  в левой части (8.3.16) их значениями из (8.3.15) и используя (8.3.4), получаем

$$\begin{aligned}\sum_{j=1}^n y_j \left( \sum_{i=1}^m a_{ij}z_i + c_j \right) &= \sum_{i=1}^m z_i \left( \sum_{j=1}^n a_{ij}y_j \right) + \sum_{j=1}^n y_j c_j = \\&= -\sum_{i=1}^m b_i z_i + \sum_{j=1}^n c_j y_j = -u + v.\end{aligned}\quad (8.3.17)$$

**Следствие.** Если  $z = (z_1, z_2, \dots, z_m)$ ,  $y = (y_1, y_2, \dots, y_n)$  — решения задач III и IV соответственно, то  $x_i y_i = 0$ ,  $i = 1, \dots, n$ , где  $x_i$  заданы соотношениями (8.3.15).

Это видно непосредственно из (8.3.16), так как для существования решения, как мы знаем, необходимо, чтобы  $u = v$ , а поскольку  $x_i \geq 0$ ,  $y_i \geq 0$ ,  $i = 1, \dots, n$ , это означает, что каждое слагаемое  $x_i y_i$  в левой части (8.3.16) должно быть равно нулю. Следовательно, если решение имеется, то при каждом  $i$  ( $i = 1, \dots, n$ ) либо  $x_i = 0$ , либо  $y_i = 0$ , либо  $x_i = y_i = 0$ . Далее, (8.3.16) показывает, что для любых допустимых значений для задач III и IV мы имеем

$$b_1 z_1 + b_2 z_2 + \dots + b_m z_m = u \leq v = c_1 y_1 + c_2 y_2 + \dots + c_n y_n. \quad (8.3.18)$$

Таким образом, любой допустимый вектор  $u$  дает верхнюю границу (скажем,  $v_0$ ) для всех возможных  $u$ , а любой допустимый вектор  $z$  дает нижнюю границу (скажем,  $u_0$ ) для всех возможных  $v$ . Следовательно, всякий раз, когда для каких-либо допустимых векторов обеих задач мы имеем  $u = v$ , эти векторы дают решение обеих задач. Таким образом, наши задачи свелись к комбинаторной проблеме нахождения такого подмножества  $I = \{i_1, \dots, i_r\}$  множества  $\{1, 2, \dots, n\}$ , что, полагая  $x_i = 0$  при  $i \notin I$  и  $y_j = 0$  при  $j \notin I$ , мы приходим к допустимым векторам для обеих задач.

В изложенном ниже простом методе нахождения решения мы следуем Таккеру [1] и принстонским лекциям Балинского. Схема

$$\begin{array}{c|ccccc|c} & \dots & \eta^* & \dots & \eta & \dots & \\ \hline x^* & \dots & a & \dots & b & \dots & = -y^* \\ x & \dots & c & \dots & d & \dots & = -y \\ \hline & \dots & \xi^* & \dots & \xi & \dots & \end{array} \quad (8.3.19)$$

является удобной формой одновременного представления следующих двух систем линейных уравнений:

### 1. Система по строкам

$$\begin{array}{c} \vdots \qquad \vdots \qquad \vdots \\ \vdots \qquad \vdots \qquad \vdots \\ \vdots \qquad \vdots \qquad \vdots \\ \dots + a\eta^* + \dots + b\eta + \dots = -y^* \\ \vdots \qquad \vdots \qquad \vdots \\ \vdots \qquad \vdots \qquad \vdots \\ \dots + c\eta^* + \dots + d\eta + \dots = -y \\ \vdots \qquad \vdots \qquad \vdots \\ \vdots \qquad \vdots \qquad \vdots \end{array}, \quad (8.3.20a)$$

в которой зависимые символы  $-y$  (переменные или числа) выражаются как линейные комбинации независимых  $\eta$ .

## 2. Система по столбцам

$$\begin{array}{ccccccc} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdots + x^* a + \cdots + x c + \cdots = \xi^* & & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdots + x^* b + \cdots + x d + \cdots = \xi^* & & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}, \quad (8.3.20b)$$

в которой зависимые символы  $\xi$  выражаются в виде линейных комбинаций независимых  $x$ .

„Осьевое преобразование“ с „осью“<sup>1)</sup>  $a \neq 0$  разрешает обе системы линейных уравнений — систему по строкам относительно  $\eta^*$ , а систему по столбцам относительно  $x^*$ , где  $\eta^*$  и  $x^*$  — независимые, а  $y^*$  и  $\xi^*$  — зависимые символы. Разрешая систему по строкам относительно  $-\eta^*$ , получаем

$$\cdots + a^{-1} y^* + \cdots + b a^{-1} \eta + \cdots = -\eta^* \quad (8.3.21)$$

и, подставляя это выражение для  $\eta^*$  в другие уравнения по строкам, получаем

$$\begin{array}{ccccccc} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdots + a^{-1} y^* + \cdots + b a^{-1} \eta + \cdots = -\eta^* & & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdots - c a^{-1} y^* + \cdots + (d - c a^{-1} b) \eta + \cdots = -y & & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array} \quad (8.3.22)$$

<sup>1)</sup> В оригинале «a pivot transformation» и «pivot entry» соответственно. — Прим. перев.

Аналогично разрешая систему по столбцам относительно  $x^*$ , приходим к равенству

$$\dots + \xi^* a^{-1} - \dots - xca^{-1} + \dots = x^* \quad (8.3.23)$$

и, подставляя выражение для  $x^*$  в остальные уравнения по столбцам, получаем:

$$\begin{array}{c} \dots \\ \vdots \\ \dots + \xi^* a^{-1} - \dots - xca^{-1} + \dots = x^* \\ \vdots \\ \dots \\ \vdots \\ \dots + \xi^* ba^{-1} + \dots + x(d - ca^{-1}b) + \dots = \xi \\ \vdots \\ \dots \end{array} \quad (8.3.24)$$

Осьевое преобразование с осью  $a \neq 0$  — это преобразование, которое заменяет схему (8.3.19) схемой

$$\begin{array}{c} \dots \quad y^* \quad \dots \quad \eta \quad \dots \\ \hline \xi^* \quad \dots \quad a^{-1} \quad \dots \quad a^{-1}b \quad \dots \quad = -\eta^* \\ \hline x \quad \dots \quad -ca^{-1} \quad \dots \quad d - ca^{-1}b \quad \dots \quad = -y \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \dots = x^* \quad \dots = \xi \quad \dots \end{array} \quad (8.3.25)$$

Преобразованная схема (8.3.25) соответствует системе уравнений по строкам (8.3.22) и системе по столбцам (8.3.24). Здесь уравнения (8.3.20a) заменились на (8.3.22) путем разрешения относительно  $-\eta^*$ , а уравнения (8.3.20b) заменились на (8.3.24) путем разрешения относительно  $x^*$ .

Другими словами, схема (8.3.25) получена из схемы (8.3.19) посредством операций:

1) замена символов, соответствующих оси  $a$ ; а именно  $\eta^*$  заменяется на  $y^*$  и  $-y^*$  на  $-\eta^*$  в системе по строкам и  $x^*$  заменяется на  $\xi^*$  и  $\xi^*$  на  $x^*$  в системе по столбцам;

2) все остальные символы не изменяются;

3) ось  $a$  заменяется на обратный элемент  $a^{-1}$ ; каждый другой элемент  $b$  в той же строке, что и  $a$ , заменяется на  $a^{-1}b$ ; каждый элемент  $c$  в том же столбце, что и  $a$ , заменяется на  $-ca^{-1}$ ; все прочие элементы  $d$  заменяются на  $d - ca^{-1}b$ , где  $b$  — элемент, лежащий в той же строке, что и  $a$ , и в том же столбце, что и  $d$ , а  $c$  — элемент из той же строки, что и  $d$ , и того же столбца, что и  $a$ , так что  $a, b, c, d$  образуют прямоугольник [см. (8.3.19)].

Необходимо подчеркнуть, что единственный результат осевого преобразования — это представление двух линейных систем в терминах других множеств независимых и зависимых символов. Мы воспользуемся понятиями схемы и осевого преобразования, чтобы решить пару двойственных задач типа III и IV, а затем рассмотрим в общем виде симплексный метод, который по существу является алгоритмом для решения таких задач. Он может быть использован для непосредственного доказательства теоремы 8.3.1.

**Задача (типа III).** Даны неравенства

$$\begin{aligned}x_1 &= -z_1 - z_2 + 2 \geqslant 0, \\x_2 &= z_1 + z_2 - 1 \geqslant 0, \\x_3 &= z_1 + 2z_2 - 2 \geqslant 0, \\x_4 &= -z_1 + 1 \geqslant 0, \\x_5 &= -6z_1 - 5z_2 + 10 \geqslant 0;\end{aligned}\tag{8.3.26}$$

максимизировать

$$u = 3z_1 + 2z_2.\tag{8.3.27}$$

Можно записать задачу, двойственную данной.

**Двойственная задача (типа IV).** Даны уравнения

$$\begin{aligned}-y_1 + y_2 + y_3 - y_4 - 6y_5 + 3 &= 0, \\-y_1 + y_2 + 2y_3 - 5y_5 + 2 &= 0,\end{aligned}\tag{8.3.28}$$

где  $y_i$  подчинены условиям

$$y_1 \geqslant 0, y_2 \geqslant 0, y_3 \geqslant 0, y_4 \geqslant 0, y_5 \geqslant 0;\tag{8.3.29}$$

минимизировать

$$v = 2y_1 - y_2 - 2y_3 + y_4 + 10y_5. \quad (8.3.30)$$

Обе задачи одновременно описывает единую схему

$$\begin{array}{cccccc|c} & y_1 & y_2 & y_3 & y_4 & y_5 & 1 \\ \hline z_1 & -1^* & 1 & 1 & -1 & -6 & 3 & = 0 \\ z_2 & -1 & 1 & 2 & 0 & -5 & 2 & = 0 \quad (x_i \geq 0, y_i \geq 0) \\ 1 & 2 & -1 & -2 & 1 & 10 & 0 & = v = \min \\ \hline & = x_1 & = x_2 & = x_3 & = x_4 & = x_5 & = u = \max & (8.3.31) \end{array}$$

По ней можно проверить непосредственно тождество из теоремы 8.3.2:

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 + u = v. \quad (8.3.32)$$

Будем искать решения обеих двойственных задач. Сначала исключим переменные  $z_1$  и  $z_2$ , на которые не наложено ограничений. Исключая  $z_1$  при помощи осевого преобразования с осью  $-1$ , отмеченной звездочкой в (8.3.31), получаем

$$\begin{array}{cccccc|c} & 0 & y_2 & y_3 & y_4 & y_5 & 1 \\ \hline x_1 & -1 & -1 & -1 & 1 & 6 & -3 & = -y_1 \\ z_2 & -1 & 0 & 1^* & 1 & 1 & -1 & = 0 \quad (x_i \geq 0, y_i \geq 0) \\ 1 & 2 & 1 & 0 & -1 & -2 & 6 & = v = \min \\ \hline & = z_1 & = x_2 & = x_3 & = x_4 & = x_5 & = u = \max & (8.3.33) \end{array}$$

Теперь исключим  $z_2$  аналогичным преобразованием с осью  $1$ , отмеченной звездочкой в (8.3.33):

$$\begin{array}{cccccc|c} & 0 & y_2 & 0 & y_4 & y_5 & 1 \\ \hline x_1 & -2 & -1 & 1 & 2 & 7 & -4 & = -y_1 \\ x_3 & -1 & 0 & 1 & 1 & 1 & -1 & = -y_3 \quad (x_i \geq 0, y_i \geq 0) \\ 1 & 2 & 1 & 0 & -1 & -2 & 6 & = v = \min \\ \hline & = z_1 & = x_2 & = z_2 & = x_4 & = x_5 & = u = \max & (8.3.34) \end{array}$$

Нулевые „переменные“ не входят в уравнения по строкам, но соответствующие столбцы служат для выражения переменных без ограничений  $z_1$  и  $z_2$  через переменные с ограничением ( $\geq 0$ )  $x_1$  и  $x_3$ .

Мы можем теперь придать задаче каноническую форму, в которой переменные без ограничений выражены через переменные с ограничением и имеется единая схема, представляющая пару систем линейных уравнений относительно переменных с ограничением. Итак, перепишем (8.3.34) в канонической форме с помощью линейных уравнений

$$\begin{aligned} z_1 &= -2x_1 - x_3 + 2, \\ z_2 &= \quad x_1 + x_3 \end{aligned} \tag{8.3.35}$$

и следующей схемы:

$$\begin{array}{ccccc} y_2 & y_4 & y_5 & 1 & \\ \hline x_1 & -1 & 2 & 7 & -4 \\ x_3 & 0 & 1 & 1 & -1 \\ 1 & 1 & -1 & -2 & 6 \end{array} = \begin{array}{l} -y_1 \\ -y_3 \\ v = \min \end{array} \quad (x_i \geq 0, y_i \geq 0)$$

$$= x_2 = x_4 = x_5 = u = \max \tag{8.3.36}$$

Если мы приравняем нулю все независимые переменные в системах, которые представляет эта схема,  $x_1 = x_3 = 0$ ,  $y_2 = y_4 = y_5 = 0$ , то мы получим так называемое *опорное решение* для (8.3.32) с  $u = v$ . Значения остальных переменных мы можем получить из окаймляющей строки и окаймляющего столбца нашей схемы, а именно  $x_2 = 1$ ,  $x_4 = -1$ ,  $x_5 = -2$ ,  $y_1 = 4$ ,  $y_3 = 1$  и  $u = v = 6$ .

Поскольку для полученного опорного решения все  $y_i \geq 0$ , вектор  $y = (4, 0, 1, 0, 0)$  является допустимым по программе для строк и дает  $v = 6$ . Однако соответствующий вектор  $x$  из опорного решения не является допустимым по программе для столбцов, так как среди  $x_i$  имеются отрицательные величины, и поэтому мы не достигли искомого минимума  $v$  для программы по строкам.

Симплексный метод использует осевое преобразование, которое сохраняет допустимость программы по

строкам для опорного решения и не увеличивает значения  $v$ . Рассмотрим влияние осевого преобразования с осью  $a_{rs}$  на столбец, которому принадлежит ось, и столбец правых частей:

$$\begin{array}{l}
 a_{1s} \dots b_1 \quad - a_{1s}a_{rs}^{-1} \dots b_1 - a_{1s}a_{rs}^{-1}b_r \\
 \vdots \quad \vdots \quad \vdots \quad \vdots \\
 \vdots \quad \vdots \quad \vdots \quad \vdots \\
 \vdots \quad \vdots \quad \vdots \quad \vdots \\
 a_{is} \dots b_i \quad - a_{is}a_{rs}^{-1} \dots b_i - a_{is}a_{rs}^{-1}b_r \\
 \vdots \quad \vdots \quad \vdots \quad \vdots \\
 \vdots \quad \vdots \quad \vdots \quad \vdots \\
 a_{rs}^* \dots b_r \quad a_{rs}^{-1} \dots b_r a_{rs}^{-1} \\
 \vdots \quad \vdots \quad \vdots \quad \vdots \\
 \vdots \quad \vdots \quad \vdots \quad \vdots \\
 a_{ms} \dots b_m \quad - a_{ms}a_{rs}^{-1} \dots b_m - a_{ms}a_{rs}^{-1}b_r \\
 c_s \dots d \quad - c_s a_{rs}^{-1} \dots d - c_s a_{rs}^{-1}b_r
 \end{array} \rightarrow \quad (8.3.37)$$

Числа  $b_1, \dots, b_m$  неположительны, и мы хотим, чтобы новые правые части были неположительны. Мы хотим также, чтобы новое значение  $u = v$  было меньше предыдущего, для чего необходимо, чтобы  $d - c_s a_{rs}^{-1}b_r \leq d$ . Последнее будет достигнуто, если  $a_{rs} > 0$ ,  $c_s \leq 0$ , и тогда неравенство  $b_i - a_{is}a_{rs}^{-1}b_r \leq 0$ ,  $i \neq r$ , выполняется наверняка при  $a_{is} \leq 0$ , а при  $a_{is} > 0$  — только если  $a_{is}^{-1}b_i \leq a_{rs}^{-1}b_r$ . Заметим, что если  $c_s \geq 0$  в каждом столбце, то наше полное решение допустимо также по столбцам, и мы имеем решение двойственной задачи. Далее, если  $c_s < 0$  и  $a_{1s}, \dots, a_{ms} \leq 0$ , то

$$x_s = a_{1s}x_{i_1} + \dots + a_{ms}x_{i_m} + c_s,$$

и  $x_s < 0$  при любом выборе остальных  $x_i \geq 0$ ; в этом случае программа по столбцам решения не имеет. Тем самым получаем правило для выбора оси осевого преобразования, когда есть опорное решение, допустимое по строкам.

*Правило выбора оси для схемы, допустимой по строкам:* в качестве оси следует выбирать положительное  $a_{rs}$

в столбце с  $c_s < 0$ , такое, что  $a_{rs}^{-1} b_r \geq a_{is}^{-1} b_i$  при  $a_{is} > 0$ ,  $i \neq s$ .

Так, в схеме (8.3.36) в качестве оси можно выбрать 1 в строке  $x_3$  и столбце  $y_4$ . Преобразуя относительно этой оси, получаем

$$\begin{array}{c|cccc|c} & y_2 & y_3 & y_5 & 1 \\ \hline x_1 & -1 & -2 & 5^* & -2 & = -y_1 \\ x_4 & 0 & 1 & 1 & -1 & = -y_4 \\ 1 & 1 & 1 & -1 & 5 & = v = \min \\ \hline & x_2 & x_3 & x_5 & u = \max & \end{array} \quad (8.3.38)$$

Беря 5 (отмечено звездочкой) в качестве следующей подходящей оси, находим

$$\begin{array}{c|cccc|c} & y_2 & y_3 & y_1 & 1 \\ \hline x_5 & \frac{-1}{5} & \frac{-2}{5} & \frac{1}{5} & \frac{-2}{5} & = -y_5 \\ x_4 & \frac{1}{5} & \frac{7}{5} & \frac{-1}{5} & \frac{-3}{5} & = -y_4 \\ 1 & \frac{4}{5} & \frac{3}{5} & \frac{1}{5} & \frac{23}{5} & = v = \min \\ \hline & x_2 & x_3 & x_1 & u = \max & \end{array} \quad (8.3.39)$$

В (8.3.39) опорное решение дает допустимые значения как по строкам, так и по столбцам, и наши двойственные задачи решены. Решения таковы:

$$x_1 = \frac{1}{5}, \quad x_2 = \frac{4}{5}, \quad x_3 = \frac{3}{5}, \quad x_4 = 0, \quad x_5 = 0.$$

$$y_1 = 0, \quad y_2 = 0, \quad y_3 = 0, \quad y_4 = \frac{3}{5}, \quad y_5 = \frac{2}{5}. \quad (8.3.40)$$

$$u = v = \frac{23}{5}.$$

$$z_1 = 1, \quad z_2 = \frac{4}{5}.$$

Значения  $z_1$  и  $z_2$  получены подстановкой найденных  $x_i$  в (8.3.35). В общем случае схема, представляющая

двойственные задачи III и IV, имеет вид

$$\begin{array}{c|ccccc}
 & y_1 & y_2 & \dots & y_N & 1 \\
 \hline
 z_1 & a_{11} & a_{12} & \dots & a_{1N} & b_1 = 0 \\
 z_2 & a_{21} & a_{22} & \dots & a_{2N} & b_2 = 0 \\
 \vdots & \vdots & \vdots & & \vdots & \vdots \\
 z_M & a_{M1} & a_{M2} & \dots & a_{MN} & b_M = 0 \\
 1 & c_1 & c_2 & \dots & c_N & d = v = \min
 \end{array}$$

$$= x_1 = x_2 = \dots = x_N = u = \max \quad (8.3.41)$$

Первый этап нахождения решения состоит в том, чтобы исключить как можно больше переменных без ограничений  $z_i$ . Этот процесс осуществляется осевыми преобразованиями и продолжается до тех пор, пока в схеме можно найти ненулевой элемент в столбце с  $y$  наверху и в строке с нулем справа. В результате приходим к схеме вида

$$\begin{array}{c|ccccc}
 & y'_{m+1} & \dots & y'_{m+n} & 0 & \dots 0 & 1 \\
 \hline
 x'_1 & a'_{11} & \dots & a'_{1n} & a'_{1, n+1} & \dots & a'_{1N} & b'_1 = -y'_1 \\
 \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
 x'_m & a'_{m1} & \dots & a'_{mn} & a'_{m, n+1} & \dots & a'_{mN} & b'_m = -y'_m \\
 \hline
 z'_{m+1} & 0 & \dots & 0 & a'_{m+1, n+1} & \dots & a'_{m+1, N} & b'_{m+1} = 0 \\
 \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
 z'_M & 0 & \dots & 0 & a'_{M, n+1} & \dots & a'_{MN} & b'_M = 0 \\
 \hline
 1 & c'_1 & \dots & c'_n & c'_{n+1} & \dots & c'_N & d' = v = \min
 \end{array}$$

$$= x'_{m+1} = x'_{m+n} = z'_1 = z'_m = u = \max$$

$$x'_i \geq 0, \quad y'_i \geq 0 \quad (m+n=N) \quad (8.3.42)$$

В этой схеме переменные со штрихами — это размещенные иначе первоначальные переменные из (8.3.41), а строки и столбцы переставлены в соответствии с положением нулей внутри схемы и нулевых символов. Уравнения для строк  $m+1, \dots, M$  имеют вид

$$0 = b'_j, \quad j = m+1, \dots, M.$$

Следовательно, если какое-либо из  $b'_j, j = m+1, \dots, M$ , отлично от нуля, то мы приходим к противоречию:  $0 = b'_j \neq 0$ , и система по строкам несовместна.

С другой стороны, если  $b'_j = 0$  при  $j = m+1, \dots, M$ , то уравнения по строкам сводятся к тривиальному уравнению  $0 = 0$  и могут быть отброшены из системы по строкам. Столбцы от  $n+1$  до  $N$  являются теперь линейными уравнениями, выражающими  $z'_1, \dots, z'_m$  через переменные с ограничениями  $x'_1, \dots, x'_m$  и переменные  $z'_{m+1}, \dots, z'_M$ , которые являются теперь произвольными параметрами. Остается рассмотреть только соотношения относительно  $x'_1, \dots, x'_{m+n}$  и  $y'_1, \dots, y'_{m+n}$ , где все переменные подчинены ограничениям ( $\geq 0$ ), и мы имеем следующую каноническую форму для двойственных задач (или программ):

$$\begin{array}{ccccc} & y_{m+1} & \dots & y_{m+n} & 1 \\ \begin{array}{c} x_1 \\ \vdots \\ \vdots \\ x_m \\ 1 \end{array} & \left| \begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{array} \right| & = -y_1 & & \\ & \hline & \left| \begin{array}{ccc|c} c_1 & \dots & c_n & d \end{array} \right| & = v = \min & \\ & & = x_{m+1} \dots = x_{m+n} = u = \max & & \end{array} \quad (8.3.43)$$

Для простоты мы опустили штрихи у переменных. Ключевое тождество

$$x_1 y_1 + \dots + x_{m+n} y_{m+n} + u = v$$

будет выполняться. Задача теперь состоит в том, чтобы найти по схеме, полученной из (8.3.43), последователь-

ностью осевых преобразований, допустимое решение (если таковое существует) для обеих задач, такое, что  $x_i y_i = 0$ ,  $i = 1, \dots, m+n$ , и  $x_i \geq 0$ ,  $y_i \geq 0$ ,  $i = 1, \dots, m+n$ . Чтобы упростить обозначения, в этой части нашего рассуждения будем обозначать через + положительное число и  $\oplus$  – неотрицательное число; аналогично через – и  $\ominus$  обозначим отрицательное и неположительное числа соответственно. Если мы можем от (8.3.43) прийти к схеме вида

$$\begin{array}{c} 1 \\ \boxed{\quad} \quad | \quad \ominus \\ \vdots \\ \vdots \\ \ominus \end{array}, \quad (8.3.44)$$

$$1 \quad \boxed{\oplus \dots \oplus} \quad | \quad = v = \min$$

$$= u = \max$$

полагая независимые переменные равными нулю, то мы тем самым получаем допустимое опорное решение для обеих программ, т. е. решение обеих двойственных задач. Если на некотором шаге мы имеем строку вида

$$\begin{array}{c} 1 \\ \boxed{\oplus \dots \oplus} \quad | \quad + \end{array} \quad (8.3.45)$$

или столбец вида

$$\begin{array}{c} \boxed{\ominus \dots \ominus} \\ | \\ \vdots \\ \vdots \\ \ominus \end{array}, \quad (8.3.46)$$

$$1 \quad \boxed{-}$$

то для системы по строкам или системы по столбцам нарушается требование  $-y_i \leq 0$  или  $+x_i \geq 0$ ,  $i = 1, 2, \dots, m+n$ , допустимости по строкам или по столбцам соответственно.

Предположим, что в схеме (8.3.43) нет строк вида (8.3.45) и столбцов вида (8.3.46). Если  $b_1 \leq 0, \dots, b_m \leq 0$ , то опорное решение допустимо по строкам. Если опорное решение не допустимо по столбцам, то  $c_s < 0$  для некоторого  $s$  и в столбце элемента  $c_s$  должны быть положительные числа, ибо в противном случае этот столбец имеет вид (8.3.46) и программа по столбцам вообще не допустима. Выберем тогда в качестве оси такой элемент  $a_{rs}$  в этом столбце, что

$$a_{rs} > 0 \text{ и } a_{rs}^{-1}b_r \geq a_{is}^{-1}b_i \text{ при любом } a_{is} > 0. \quad (8.3.47)$$

Как это было замечено на примере, такой выбор обеспечивает допустимость нового опорного решения по строкам и, если  $b_r < 0$ , дает новое значение  $v$ , строго меньшее, чем предыдущее.

Аналогично, если  $c_1 \geq 0, \dots, c_n \geq 0$ , то опорное решение допустимо по столбцу, и если каждое  $b$  неположительно, то мы имеем допустимые решения для обеих задач и на этом кончаем. Если же  $b_r > 0$ , то пусть строка элемента  $b_r$  отлична от (8.3.45). Тогда в этой строке есть отрицательные числа, и мы можем выбрать такую ось  $a_{rs}$ , что

$$a_{rs} < 0, \quad a_{rs}^{-1}c_s \geq a_{rj}^{-1}c_j \quad \text{для любого } a_{rj} < 0. \quad (8.3.48)$$

При этом если  $c_s > 0$ , то новое значение  $v$  строго больше предыдущего. Для схемы, которая допустима либо по строкам, либо по столбцам, последовательность таких осевых преобразований либо выявляет недопустимую строку или столбец и тогда решения не существует, либо приводит к схеме вида (8.3.44) и, следовательно, решению обеих двойственных задач.

Разумеется, каноническая форма (8.3.43) может оказаться недопустимой как по строкам, так и по столбцам. Переставим строки так, чтобы  $k$  неположительных  $b$  поместить сверху; тогда получим схему

$$\begin{array}{c|c|c}
 & y_{m+1} \cdots y_{m+n} & 1 \\
 \hline
 x_1 & & \ominus \\
 \cdot & & \cdot \\
 \cdot & & \cdot \\
 x_k & & \ominus \\
 \hline
 x_{k+1} & & + \\
 \hline
 \cdot & & \cdot \\
 \cdot & & \cdot \\
 x_m & & + \\
 \hline
 1 & c_1 & \cdots & c_n & = v \\
 & & & & = u
 \end{array} = -y_{k+1} \quad (8.3.49)$$

Рассмотрим теперь первые  $k+1$  строк этой схемы как допустимую по строкам программу и постараемся минимизировать  $-y_{k+1}$ . Если на каком-нибудь шаге мы достигнем неположительного значения для  $-y_{k+1}$ , то мы получим уже  $k+1$  строк, а не  $k$  в виде допустимой по строкам программы и продолжим процесс, стремясь представить в допустимой форме как можно больше строк. Если же не достигнем, то придем к схеме одного из следующих видов:

$$\begin{array}{c|c}
 \ominus & \ominus \\
 \cdot & \cdot \\
 \cdot & \cdot \\
 \ominus & \ominus \\
 \hline
 -* & + \\
 \hline
 & \\
 \hline
 1 & = v \\
 & = u
 \end{array} = -y_{k+1} \quad \text{или} \quad
 \begin{array}{c|c}
 & \ominus \\
 \cdot & \cdot \\
 \cdot & \cdot \\
 \ominus & \ominus \\
 \hline
 \oplus \dots \oplus & + \\
 \hline
 & \\
 \end{array} = -y_{k+1} \quad (8.3.50)$$

Вторая из этих схем содержит недопустимую строку (8.3.45). Если в первой схеме мы выберем в качестве оси отмеченное звездочкой отрицательное число, то легко проверить, что этот выбор дает  $k+1$  или еще больше допустимых строк. Таким образом, описаны способы действия во всех возможных случаях.

# Графические методы. Последовательности де Брёйна

---

## 9.1. Полные циклы

Циклом называется последовательность символов  $a_1a_2 \dots a_r$ , взятых в таком порядке, что  $a_1$  следует за  $a_r$ , и все последовательности  $a_2 \dots a_ra_1, \dots, a_ra_1 \dots a_{r-1}$  — это один и тот же цикл  $a_1a_2 \dots a_r$ . Существует множество комбинаторных задач о циклах, но здесь мы рассмотрим только одну. Если  $n$  — положительное целое число и  $N = 2^n$ , то цикл  $a_1a_2 \dots a_N$ , составленный из нулей и единиц, называется *полным циклом*, если подпоследовательности

$$a_i a_{i+1} \dots a_{i+n-1}, \quad i = 1, \dots, N,$$

состоят из всех возможных  $N = 2^n$  упорядоченных последовательностей  $b_1 \dots b_n$  из нулей и единиц. При  $n = 1, 2, 3$  имеются следующие полные циклы:

$$\begin{aligned} n = 1: & 01, \\ n = 2: & 0011, \\ n = 3: & 00010111, \\ & 00011101. \end{aligned} \tag{9.1.1}$$

При  $n = 4$  существует точно 16 полных циклов. Задача состоит в том, чтобы доказать существование полных циклов длины  $N = 2^n$  и, если это возможно, найти их число.

Решение этой задачи дает теорема, принадлежащая де Брёйну [1]. По этой причине полные циклы называются также *последовательностями де Брёйна*.

**Теорема де Брёйна.** Для всякого положительного целого числа  $n$  существует точно  $2^{2^{n-1}-n}$  полных циклов длины  $N = 2^n$ .

Доказательство этой теоремы будет дано в разделе 9.3. Здесь же мы дадим графическую интерпретацию полных циклов.

**Определение.** Графом  $G$  называется множество точек  $\{p_i\}$  и дуг  $\{A_j\}$ . Каждая дуга  $A_j$  соединяет две точки  $p_i$  и  $p_k$ , называемые ее концевыми точками.

Мы не требуем, чтобы две концевые точки дуги были различными. Если концевые точки дуги совпадают, то она называется *петлей*. Две точки могут как вообще не соединяться дугой, так и соединяться одной или большим числом дуг. Мы будем рассматривать только конечные графы, т. е. имеющие конечное число точек и дуг. Пусть  $p_1, \dots, p_n$  — такая последовательность точек в графе  $G$ , что существуют дуги  $A_i$ , соединяющие  $p_i$  и  $p_{i+1}$  для  $i = 1, \dots, n-1$ . Последовательность дуг  $A_1, \dots, A_{n-1}$  называется *путем*, и мы говорим, что точки  $p_1$  и  $p_n$  *связаны*. Граф  $G$  называется *связным*, если каждая пара точек в  $G$  связана.

С дугой  $A_i$ , соединяющей  $p_i$  и  $p_k$ , можно также связать направление, если одну из точек,  $p_i$ , назвать началом дуги  $A_i$ , а другую,  $p_k$ , — ее концом. Ориентированный граф — это граф, все дуги которого имеют направление. При определении пути  $A_1, A_2, \dots, A_n$  в ориентированном графе требуется, чтобы при любом  $i = 1, \dots, n-1$  конец дуги  $A_i$  был началом дуги  $A_{i+1}$ . Такой путь называется циклом, если конец дуги  $A_n$  есть начало  $A_1$ . Последовательность дуг в цикле берется в циклическом порядке, т. е., например,  $A_2, \dots, A_n, A_1$  отождествляется с  $A_1, A_2, \dots, A_n$ . Пусть каждой из  $2^{n-1}$  последовательностей  $c_1 \dots c_{n-1}$  из нулей и единиц длины  $n-1$  сопоставлена точка  $p_i = (c_1, \dots, c_{n-1})$  и каждой последовательности  $b_1, b_2, \dots, b_{n-1}, b_n$  длины  $n$  сопоставлена направленная дуга, началом которой является точка  $(b_1, b_2, \dots, b_{n-1})$ , а концом точка  $(b_2, \dots, b_{n-1}, b_n)$ . Обозначим такой граф через  $G_n$ . На рис. 9.1 показаны графы  $G_2$  и  $G_3$ , стрелки указывают направление дуг.

Заметим, что граф  $G_n$  связан, так как подпоследовательности длины  $n$  в последовательности  $c_1 \dots c_{n-1} d_1 \dots d_{n-1}$  дают путь, ведущий из  $(c_1, \dots, c_{n-1})$  в  $(d_1, \dots, d_{n-1})$ . В множестве всех последовательностей

$b_1b_2 \dots b_{n-1}b_n$  каждая подпоследовательность длины  $n-1$  встречается дважды в качестве  $b_1b_2 \dots b_{n-1}$  и дважды в качестве  $b_2 \dots b_{n-1}b_n$ . Следовательно, каждая точка в  $G_n$  является началом точно двух дуг и концом точно двух дуг. Если  $N = 2^n$ , то полному циклу  $a_1a_2 \dots a_N$  можно сопоставить путь в  $G_n$ , составленный из дуг  $A_i$ ,  $a_ia_{i+1} \dots a_{i+n-1}$ ,  $i = 1, \dots, N$ . Это есть путь, поскольку для всякого  $i$  конец дуги  $A_i$  есть начало дуги  $A_{i+1}$ . Кроме того, это цикл, так как конец  $A_N$  есть начало  $A_1$ .

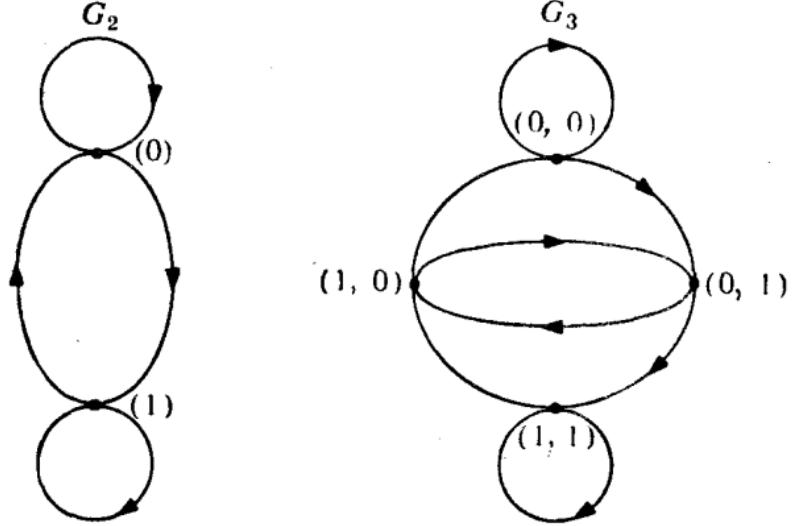


Рис. 9.1. Графы  $G_2$  и  $G_3$ .

В этот цикл каждая дуга графа  $G_n$  входит точно один раз. Обратно, ориентированный цикл в  $G_n$ , содержащий каждую дугу точно один раз, сразу приводит к построению полного цикла  $a_1a_2 \dots a_N$ , если проходить по порядку дуги  $a_ia_{i+1} \dots a_{i+n-1}$ ,  $i = 1, \dots, N$ . Поэтому задача построения полных циклов  $a_1a_2 \dots a_N$ , составленных из нулей и единиц, эквивалентна нахождению циклов в  $G_n$ , в которых каждая дуга проходится точно один раз, и такие циклы мы также будем называть полными циклами.

## 9.2. Теоремы о графах

Сначала опишем несколько свойств неориентированных графов; некоторые из них справедливы и для ориентированных графов. Точка  $p$  графа называется

$m$ -вершиной, если  $m$  — концевая точка для  $m$  дуг. Назовем  $m$  четной вершиной, если  $m$  четно.

**Лемма 9.2.1.** *Любой граф содержит четное число нечетных вершин.*

**Доказательство.** Если имеется  $x_i$  точек, которые являются  $i$ -вершинами, то  $x_1 + 2x_2 + \dots + kx_k = 2A$ , где  $A$  — число дуг (так как в левой части подсчитывается число концевых точек дуг, а каждая дуга имеет точно две концевые точки). Из этого равенства следует, что  $x_1 + x_3 + x_5 + \dots + x_{2y+1}$  — четное число, что и требовалось доказать.

**Теорема 9.2.1 (Эйлер).** *Цикл, проходящий через каждую дугу графа точно один раз, существует тогда и только тогда, когда граф связан и все его вершины четны.*

**Доказательство.** Если существует цикл, проходящий через каждую дугу графа  $G$  точно один раз, то  $G$ , очевидно, связан. Кроме того, каждый раз, когда цикл проходит через некоторую точку, мы приходим в эту точку по одной дуге, а выходим по другой, и, значит, каждая вершина четна. Предположим теперь, что граф  $G$  связан и что каждая вершина четна. Пусть  $P$  — путь в  $G$ , который является максимальным (в смысле использования наибольшего возможного числа дуг). Покажем, что  $P$  — искомый цикл, содержащий все дуги графа. Во-первых,  $P$  — цикл. Предположим, что, напротив,  $P$  есть  $A_1, A_2, \dots, A_m$  и  $A_m$  заканчивается в точке  $q$ , которая не является начальной для  $A_1$ . Но каждый раз, когда цикл проходит через  $q$ , использовались две дуги с концами в  $q$ . Это дает нечетное число дуг, для которых  $q$  — концевая точка; но поскольку  $q$  — четная вершина, то должна существовать еще одна дуга в  $q$ , значит, можно добавить к  $P$  дугу  $A_{m+1}$ , и получается более длинный путь, что противоречит предположению. Следовательно,  $P$  — цикл.

Во-вторых, допустим, что существует некоторая точка  $q$  в  $P$  и дуга  $B$  с концом в  $q$ , не использованная в  $P$ . Перенумеровывая дуги, если это необходимо, можем сделать  $q$  концом для  $A_m$  и началом для  $A_1$ .

Далее, напишем  $B = B_1$ , соединяя  $q = q_1$  с некоторой точкой  $q_2$ . Тогда  $A_1, A_2, \dots, A_m, B_1$  — путь, превосходящий по длине  $P$ , что противоречит нашему выбору  $P$ . Мы показали тем самым, что  $P$  — цикл и что каждая дуга, проходящая через всякую точку  $P$ , содержится в  $P$ . Мы утверждаем теперь, что  $P$  проходит через каждую точку графа  $G$ ; в самом деле, если  $p$  — точка из  $G$ , не содержащаяся в  $P$ , то пусть  $q$  — точка, содержащаяся в  $P$ . Так как граф  $G$  связный, существует путь  $U_1, U_2, \dots, U_w$ , где  $U_i$  соединяет точки  $x_i$  и  $x_{i+1}$  и  $x_1 = q, x_{w+1} = p$ . Но поскольку  $q$  — точка из  $P$ , дуга  $U_1$ , соединяющая  $x_1 = q$  и  $x_2$ , содержитя в  $P$ . Значит,  $x_2$  — точка  $P$ , а тогда и дуга  $U_2$  также содержитя в  $P$ . Продолжая рассуждение для  $x_3, \dots, x_{w+1} = p$ , получим, что  $p$  — точка  $P$ , что противоречит нашему выбору точки  $p$ . Следовательно,  $P$  содержит все точки  $G$ , а значит, и все дуги  $G$ , и теорема доказана.

**Теорема 9.2.2.** *Если граф  $G$  связан и имеет точно  $2s > 0$  нечетных вершин, то существуют  $s$  и не существует меньшего числа путей  $P_1, \dots, P_s$ , которые в совокупности содержат все дуги  $G$  точно по одному разу. Каждый из путей  $P_1, \dots, P_s$  начинается в одной нечетной вершине и кончается в другой нечетной вершине.*

**Доказательство.** По лемме 9.2.1, если имеются нечетные вершины, то их должно быть четное число. Если это число есть  $2s$ , то разобьем их на  $s$  пар и образуем новый граф  $G_1$ , добавляя  $s$  новых дуг к  $G$  так, что каждая дуга соединяет пару указанных вершин. Тогда  $G_1$  есть связный граф, все вершины которого четны. По теореме 9.2.1 существует цикл  $C$  в  $G_1$ , проходящий по всем дугам  $G_1$  точно по одному разу. Если мы из  $C$  удалим  $s$  дуг, не принадлежащих  $G$ , то оставшиеся дуги составят  $s$  путей, проходящих по всем дугам  $G$ , причем каждый путь начинается в одной нечетной вершине и кончается в другой нечетной вершине. Заметим, что в любой совокупности путей  $P_i$ , содержащей все дуги  $G$ , каждая нечетная вершина должна быть концом пути, и, значит, при  $2s$  нечетных вершинах нельзя пройти все дуги  $G$ , используя меньше чем  $s$  путей.

Простым приложением этой теоремы является известная задача о кенигсбергских мостах, впервые решенная Эйлером. На реке, протекающей по городу, находятся два острова. Имеется мост между островами, по

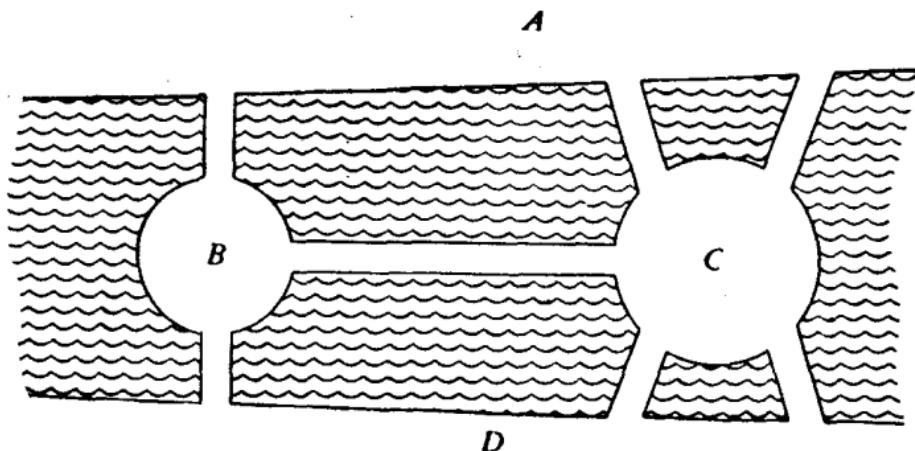


Рис. 9.2. Задача о кенигсбергских мостах.

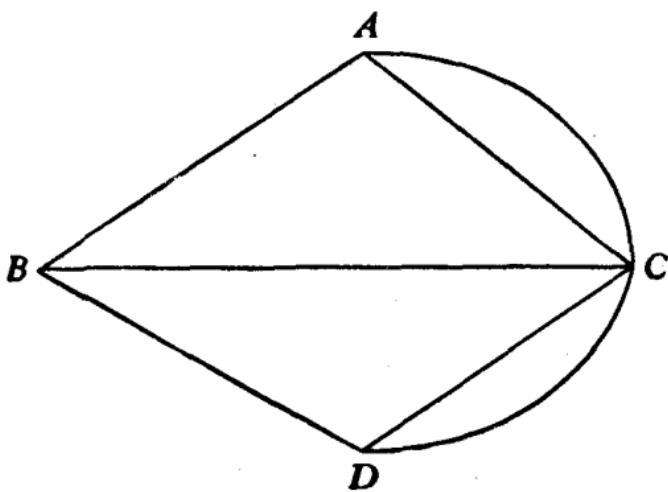


Рис. 9.3. Граф для задачи о мостах.

два моста на каждый берег от большого острова и по одному мосту на каждый берег от меньшего острова. Задача состоит в том, чтобы пройти по всем семи мостам, ни один мост не проходя дважды. На рис. 9.2 показано расположение мостов. Если за точки графа принять берега и оба острова, то мы увидим, что эта

задача есть задача о нахождении пути, при котором все дуги на рис. 9.3 проходятся по одному разу. Так как все четыре вершины этого графа нечетны, теорема 9.2.2 показывает, что требуется по меньшей мере два отдельных пути, чтобы пройти по всем дугам, и следовательно, исходная задача о прохождении по всем семи мостам, не проходя какого-либо моста дважды, не имеет решения.

### 9.3. Доказательство теоремы де Брёйна

Обобщение теоремы 9.2.1, принадлежащее Гуду [1], показывает, что всегда существует хотя бы один полный цикл  $a_1 a_2 \dots a_N$ , где  $N = 2^n$ .

**Теорема 9.3.1 (Гуд).** *Если  $G$  — связный ориентированный граф и если для каждой точки  $G$  число выходящих из нее дуг совпадает с числом входящих в нее дуг, то существует ориентированный цикл в  $G$ , который проходит каждую дугу  $G$  в указанном на ней направлении, ни одну из дуг не проходя дважды.*

**Доказательство.** Теорема доказывается по существу так же, как теорема 9.2.1. Пусть  $P = A_1, A_2, \dots, A_m$  — максимальный ориентированный путь в  $G$ , где  $A_i$  начинается в  $p_i$  и кончается в  $p_{i+1}$  для  $i = 1, \dots, m$  и все дуги  $A_1, \dots, A_m$  различны. Если  $p_{m+1} \neq p_1$ , то каждый раз, когда  $p_{m+1}$  проходится в  $P$ , путь входит в нее по одной дуге и выходит по другой. Но тогда в  $P$  дуг, входящих в  $p_{m+1}$ , оказывается больше, чем выходящих, и, значит, по нашему предположению, должна быть еще одна дуга  $A_{m+1}$ , выходящая из  $p_{m+1}$ , откуда следует, что  $P$  — не максимальный путь. Следовательно,  $p_{m+1} = p_1$  и  $P$  — цикл.

Если для точки  $q$  из  $P$  существует дуга  $B_1$ , не принадлежащая  $P$ , то можно предположить, что эта дуга выходит из  $q$ ; изменяя нумерацию, если это необходимо, получаем, что  $q = p_1 = p_{m+1}$ . Но тогда  $A_1, A_2, \dots, A_m, B_1$  — более длинный путь, что противоречит выбору  $P$ . Следовательно, если  $P$  — максимальный путь, то  $P$  есть ориентированный цикл, содержащий все дуги, которые проходят через любую точку  $P$ . А так как  $G$  — связный

граф, то  $P$  содержит все дуги графа  $G$ . Следовательно,  $P$  — искомый ориентированный цикл, проходящий каждую дугу  $G$  точно один раз в заданном на ней направлении.

В разделе 9.1 мы заметили, что граф  $G_n$ , сопоставленный полным циклам, связан и что в каждой его точке имеется две дуги, входящие в нее, и две дуги, выходящие из нее. Следовательно, по теореме 9.3.1 при каждом целом положительном  $n$  существует хотя бы один полный цикл  $a_1 a_2 \dots a_N$ , если  $N = 2^n$ . Но теорема 9.3.1 не дает числа полных циклов. Суть доказательства де Брёйна состоит в выяснении связи между графиками  $G_n$  и  $G_{n+1}$  и нахождении соотношения между количеством полных циклов в  $G_n$  и в  $G_{n+1}$ .

Назовем ориентированный граф  $G$  *2-графом*, если в каждой его точке существуют две дуги, выходящие из нее, и две входящие в нее. Наши графы  $G_n$  являются 2-графами. Если дан 2-граф  $G$ , то определим *двойственный граф*  $G^*$  по следующим правилам:

1. Каждой дуге  $B_0$  из  $G$  соотнесем точку  $b_0$  из  $G^*$ .
2. Если  $B_1$  — дуга из  $G$ , начало которой есть конец дуги  $B_0$ , то в  $G^*$  имеется дуга  $U_{01}$  с началом в  $b_0$  и концом в  $b_1$ .
3. Точки и дуги в  $G^*$  определяются по  $G$  правилами 1 и 2 и никакими другими.

Легко видеть, что  $G^*$  есть также 2-граф с удвоенным по сравнению с  $G$  числом точек (таково число дуг в  $G$ ). Кроме того (и это весьма важно в доказательстве де Брёйна),  $G_{n+1}$  есть *двойственный граф* к  $G_n$ , ибо произвольная последовательность из  $n+1$  нулей и единиц

$$b_1, b_2, b_3, \dots, b_{n-1}, b_n, b_{n+1}$$

определяет в  $G_n$  точки

$$\begin{aligned} (b_1, b_2, b_3, \dots, b_{n-1}) &= x_1, \\ (b_2, b_3, \dots, b_{n-1}, b_n) &= x_2, \\ (b_3, \dots, b_{n-1}, b_n, b_{n+1}) &= x_3; \end{aligned}$$

дуги в  $G_n$  — это точки в  $G_{n+1}$ :

$$\begin{aligned} (b_1, b_2, b_3, \dots, b_{n-1}, b_n) &= B_0 = b_0, \\ (b_2, b_3, \dots, b_n, b_{n+1}) &= B_1 = b_1; \end{aligned}$$

тогда в  $G_{n+1}$  имеется дуга

$$(b_1, b_2, b_3, \dots, b_{n-1}, b_n, b_{n+1}) = U_{01}.$$

Ввиду этого теорема де Брёйна следует из теоремы 9.3.2.

**Теорема 9.3.2.** *Если  $G$  есть 2-граф с  $m$  точками, имеющий в точности  $M$  полных циклов, то  $G^*$  имеет в точности  $2^{m-1}M$  полных циклов.*

**Следствие** (теорема де Брёйна).  *$G_n$  имеет в точности  $2^{2^{n-1}-n}$  полных циклов.*

**Доказательство** следствия из теоремы 9.3.2. Граф  $G_n$  имеет  $2^{n-1}$  точек — точки  $(c_1, \dots, c_{n-1})$ . В  $G_2$  имеется в точности один полный цикл. Поэтому следствие получается из теоремы индукцией по  $n$ , если учесть тот факт, что  $G_{n+1} = G_n^*$ .

**Доказательство** теоремы. Следя де Брёйну, обозначим через  $|G|$  число полных циклов в  $G$ . При этом циклы  $A_1, A_2, \dots, A_m$  и  $A_2, \dots, A_m, A_1$  рассматриваются как один и тот же цикл. Заметим, что  $|G|=0$ , если  $G$  несвязен. Заметим также, что теорема 9.3.2 есть обобщение следствия. Таким образом, мы имеем здесь пример весьма типичной ситуации, когда доказательство важного результата зависит от доказательства его подходящего обобщения.

Доказательство будем проводить индукцией по  $m$ . Если  $m=1$ , то  $G$  имеет единственную точку  $p$  и две петли  $A_1$  и  $A_2$  от  $p$  к  $p$ . В этом случае  $G^*$  есть граф  $G_2$ , имеющий  $2^{1-1}=1$  полный цикл. В общем случае предположим сначала, что в каждой точке имеется петля. Тогда (предполагая, что  $G$  связан) граф  $G$  описать несложно. Он имеет точки  $p_1, p_2, \dots, p_m$ , петли  $A_i: p_i \rightarrow p_i$  в точках  $p_i$  и дуги  $B_i: p_i \rightarrow p_{i+1}$ , где индексы берутся по модулю  $m$ . Граф  $G^*$  имеет  $2m$  точек  $a_i, b_i, i=1, \dots, m$ , дуги  $U_i: a_i \rightarrow a_i$ ,  $V_i: a_i \rightarrow b_i$ ,  $W_i: b_i \rightarrow a_{i+1}$  и  $X_i: b_i \rightarrow b_{i+1}$ . Очевидно, в полном цикле для  $G^*$  дуга  $U_i$  должна располагаться между  $W_{i-1}$  (предшествует  $U_i$ ) и  $V_i$  (следует за  $U_i$ ). Но путь  $W_{i-1}, U_i, V_i$ , как и дуга  $X_{i-1}$ , ведет от  $b_{i-1}$  к  $b_i$ . Следовательно, при прохождении полного цикла в  $G^*$  каждая из вершин  $b_1, b_2, \dots, b_m$  встретится

дважды, причем в первый раз мы можем попасть в  $b_i$ , используя один из двух возможных путей от  $b_{i-1}$  к  $b_i$ , и тогда другой путь используется во второй раз. Это дает точно  $2^{m-1}$  полных циклов.

Предположим теперь, что  $G$  имеет точку  $x$  без петли. Пусть  $P, Q$  — дуги, входящие в  $x$ , а  $R, S$  — дуги, выходящие из  $x$ :

$G$

$$\begin{array}{ll} P: a \rightarrow x, & R: x \rightarrow c, \\ Q: b \rightarrow x, & S: x \rightarrow d. \end{array}$$

Здесь  $P, Q, R, S$  различны, но некоторые из точек  $a, b, c, d$  могут совпадать между собой, но не с  $x$ .

Мы можем, удалив  $x$ , образовать из  $G$  новый 2-граф двумя способами, полагая либо  $P = R, Q = S$ , либо  $P = S, Q = R$ . Обозначим эти два графа через  $G_1$  и  $G_2$  соответственно. Каждый полный цикл в  $G$  соответствует полному циклу либо в  $G_1$ , либо в  $G_2$  (но не в обоих) в зависимости от способа прохождения точки  $x$ . Таким образом,  $|G| = |G_1| + |G_2|$ :

$$\begin{array}{ll} G_1 & G_2 \\ P = R: a \rightarrow c, & P = S: a \rightarrow d, \\ Q = S: b \rightarrow d, & Q = R: b \rightarrow c. \end{array}$$

Каждый из графов  $G_1$  и  $G_2$  имеет  $m - 1$  точек, и, следовательно, по индукции

$$|G^*| = 2^{m-2} |G_1|, \quad |G_2^*| = 2^{m-2} |G_2|.$$

Докажем, что  $|G^*| = 2|G_1^*| + 2|G_2^*|$ . Пусть  $p, q, r, s$  — точки  $G^*$ , соответствующие дугам  $P, Q, R, S$  в  $G$ . Тогда

$$\begin{array}{lll} G^* & G_1^* & G_2^* \\ X_1: p \rightarrow r, & p = r, & p = s, \\ X_2: p \rightarrow s, & q = s, & q = r. \\ X_3: q \rightarrow r, \\ X_4: q \rightarrow s, \end{array}$$

Здесь  $G_1^*$  и  $G_2^*$  могут быть получены из  $G^*$  вычеркиванием четырех дуг  $X_1, X_2, X_3, X_4$  и отождествлением  $p$

и  $q$  с  $r$  и  $s$ , как указано. В полный цикл графа  $G^*$  входят четыре дуги  $X_i$ , а также четыре пути, ведущие от  $r$  к  $s$  к  $p$  и  $q$ . Поэтому при каждом полном цикле реализуется одна из следующих трех возможностей:

Случай 1

$$\begin{aligned} C_1: r \rightarrow p, \\ C_2: r \rightarrow q, \\ C_3: s \rightarrow p, \\ C_4: s \rightarrow q, \end{aligned}$$

Случай 2

$$\begin{aligned} D_1: r \rightarrow p, \\ D_2: r \rightarrow p, \\ D_3: s \rightarrow q, \\ D_4: s \rightarrow q, \end{aligned}$$

Случай 3

$$\begin{aligned} E_1: r \rightarrow q, \\ E_2: r \rightarrow q, \\ E_3: s \rightarrow p, \\ E_4: s \rightarrow p. \end{aligned}$$

Используя, например, пути случая 1, имеем четыре полных цикла в  $G^*$ , а именно:

$$\begin{array}{cccccccc} X_1, & C_1, & X_2, & C_4, & X_3, & C_2, & X_4, & C_3; \\ X_1, & C_2, & X_3, & C_1, & X_2, & C_4, & X_4, & C_3; \\ X_1, & C_2, & X_4, & C_3, & X_2, & C_4, & X_3, & C_1; \\ X_1, & C_2, & X_4, & C_4, & X_3, & C_1, & X_2, & C_3. \end{array}$$

Использовать пути  $C$  для образования полных циклов в  $G_1^*$  и  $G_2^*$  можно лишь следующим образом:

$$\begin{aligned} G_1^*: & C_1, C_2, C_4, C_3; \\ G_2^*: & C_1, C_3, C_4, C_2. \end{aligned}$$

В случае 2 мы имеем следующие четыре полных цикла в  $G^*$ :

$$\begin{array}{cccccccc} X_1, & D_1, & X_2, & D_3, & X_4, & D_4, & X_3, & D_2; \\ X_1, & D_1, & X_2, & D_4, & X_4, & D_3, & X_3, & D_2; \\ X_1, & D_2, & X_2, & D_3, & X_4, & D_4, & X_3, & D_1; \\ X_1, & D_2, & X_2, & D_4, & X_4, & D_3, & X_3, & D_1. \end{array}$$

Эти пути не дают связного цикла в  $G_1^*$ , зато в  $G_2^*$  мы имеем два полных цикла:

$$\begin{aligned} G_2^*: & D_1, D_3, D_2, D_4; \\ & D_1, D_4, D_2, D_3. \end{aligned}$$

Аналогично пути случая 3 дают четыре полных цикла для  $G^*$ , два — для  $G_1^*$  и ни одного для  $G_2^*$ . Заметим, что

все полные циклы для  $G_1^*$  и  $G_2^*$  составлены из путей  $C_i$ ,  $D_i$  или  $E_i$ . Следовательно, в любом случае

$$|G^*| = 2|G_1^*| + 2|G_2^*|.$$

По индукции

$$|G_1^*| = 2^{m-2}|G_1| \quad \text{и} \quad |G_2^*| = 2^{m-2}|G_2|.$$

Так как  $|G| = |G_1| + |G_2|$ , то

$$|G^*| = 2^{m-1}|G_1| + 2^{m-1}|G_2| = 2^{m-1}|G|,$$

и теорема доказана.

## Блок-схемы

---

### 10.1. Предварительное обсуждение

В комбинаторном анализе проблемой весьма общего характера является проблема размещения элементов в заданном числе множеств таким образом, чтобы  $i$ -й элемент появлялся  $r_i$  раз во всей совокупности этих множеств, чтобы  $j$ -е множество содержало  $k_j$  элементов и чтобы пары, тройки и тому подобные наборы элементов появлялись определенное число раз. Такое размещение может быть названо „системой инцидентности“ или „тактической конфигурацией“.

Здесь мы будем рассматривать системы инцидентности частного вида, которые называются неполными уравновешенными блок-схемами, хотя большей частью мы для краткости будем называть их блок-схемами или просто схемами.

**Определение.** Уравновешенной неполной блок-схемой называется такое размещение  $v$  различных элементов по  $b$  блокам, что каждый блок содержит точно  $k$  различных элементов, каждый элемент появляется точно в  $r$  различных блоках и каждая пара различных элементов  $a_i, a_j$  появляется точно в  $\lambda$  блоках.

Каждый из  $b$  блоков  $B_1, \dots, B_b$  содержит  $k$  элементов, но различные блоки  $B_i$  и  $B_j$  могут содержать одни и те же элементы. Таким образом, блок-схема — это не просто совокупность подмножеств некоторого множества, а некоторая конструкция из элементов и блоков с отношением инцидентности, указывающим, какие элементы какому блоку принадлежат. Термин „уравновешенная неполная блок-схема“, применяемый в статистике, происходит из теории планирования экспериментов. Множе-

ство всех  $vC_k$ , сочетаний из  $v$  элементов по  $k$ , взятых в качестве блоков, — это полная блок-схема. А часть этих сочетаний, в которых каждая пара элементов  $a_i, a_j$  появляется одно и то же число раз, является неполной, но уравновешенной, поскольку это касается сравнений между парами.

Между пятью параметрами блок-схемы имеются два элементарных соотношения:

$$bk = vr, \quad (10.1.1a)$$

$$r(k-1) = \lambda(v-1). \quad (10.1.1b)$$

Доказываются они просто. В первом случае подсчитывается двумя способами общее число инциденций; каждый из  $b$  блоков содержит  $k$  элементов, и каждый из  $v$  элементов принадлежит точно  $r$  блокам. Во втором — подсчитываются появления пар, содержащих фиксированный элемент  $a_1$ . Элемент  $a_1$  появляется в  $r$  блоках, и в каждом из них образует пары с остальными  $k-1$  элементами, но, с другой стороны,  $a_1$  образует  $\lambda$  пар с каждым из всех  $v-1$  остальных элементов.

Блок-схема описывается своей матрицей инцидентности. Если  $a_1, \dots, a_v$  — элементы и  $B_1, \dots, B_b$  — блоки, то матрица инцидентности  $A = (a_{ij})$ ,  $i = 1, \dots, v$ ,  $j = 1, \dots, b$ , строится так:

$$a_{ij} = \begin{cases} 1, & \text{если } a_i \in B_j, \\ 0, & \text{если } a_i \notin B_j. \end{cases} \quad (10.1.2)$$

Основные требования для блок-схемы выражаются матричными уравнениями:

$$AA^T = B = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \ddots & \ddots & \vdots \\ \lambda & \dots & \dots & r \end{pmatrix} = (r - \lambda)I_v + \lambda J_v, \quad w_v A = k w_b. \quad (10.1.3)$$

Здесь  $J_v = (v \times v)$ -матрица из единиц, а  $w_v$  и  $w_b$  — векторы из  $v$  и  $b$  единиц соответственно. Элемент  $b_{ij}$  матрицы  $B$  есть скалярное произведение  $i$ -й и  $j$ -й строк  $A$ . Таким образом,  $b_{ii} = r$  — это число единиц в  $i$ -й строке  $A$ . Если же  $j \neq i$ , то  $i$ -я и  $j$ -я строки имеют 1 в столбце  $t$  тогда и только тогда, когда  $a_i$  и  $a_j$  оба принадлежат  $B_t$ . Значит, недиагональный элемент  $b_{ij}$  матрицы  $B$  — это число появлений пары  $a_i, a_j$ ; в каждом случае он равен  $\lambda$ . Соотношение  $w_v A = k w_b$  выражает тот факт, что в каждом столбце имеется  $k$  единиц. Обратно,  $(v \times b)$ -матрица  $A$  из нулей и единиц, удовлетворяющая (10.1.3), есть матрица инцидентности блок-схемы с параметрами  $b, v, r, k, \lambda$ .

Соотношение  $AA^T = B$  можно, конечно, сформулировать в виде соотношения между квадратичными формами. Сопоставим элементам неизвестные  $x_1, \dots, x_v$ , а блоку  $B_j$  — линейную форму  $L_j$ :

$$L_j = \sum_{i=1}^v a_{ij} x_i, \quad j = 1, \dots, b, \quad (10.1.4)$$

где  $a_{ij}$  — элементы матрицы  $A$  (см. 10.1.2). Тогда (10.1.3) принимает вид

$$L_1^2 + \dots + L_b^2 = (r - \lambda)(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2. \quad (10.1.5)$$

Ниже приведены три примера блок-схем:

1. Для  $v = b = 7, r = k = 3, \lambda = 1$ :

$$\begin{array}{ll} B_0: 0, 1, 3; & B_3: 3, 4, 6; \\ B_1: 1, 2, 4; & B_4: 4, 5, 0; \\ B_2: 2, 3, 5; & B_5: 5, 6, 1; \quad B_6: 6, 0, 2. \end{array}$$

2. Для  $b = 12, v = 9, r = 4, k = 3, \lambda = 1$ :

$$\begin{array}{llll} B_1: 1, 2, 3; & B_4: 1, 4, 7; & B_7: 1, 5, 9; & B_{10}: 1, 6, 8; \\ B_2: 4, 5, 6; & B_5: 2, 5, 8; & B_8: 2, 6, 7; & B_{11}: 2, 4, 9; \\ B_3: 7, 8, 9; & B_6: 3, 6, 9; & B_9: 3, 4, 8; & B_{12}: 3, 5, 7. \end{array}$$

3. Для  $v = b = 15$ ,  $r = k = 7$ ,  $\lambda = 3$ :

|           |          |                 |
|-----------|----------|-----------------|
| $B_0:$    | 0, 1, 2, | 3, 4, 5, 6;     |
| $B_1:$    | 0, 1, 2  | 7, 8, 9, 10;    |
| $B_2:$    | 0, 1, 2  | 11, 12, 13, 14; |
| $B_3:$    | 0, 3, 4  | 7, 8, 11, 12;   |
| $B_4:$    | 0, 3, 4  | 9, 10, 13, 14;  |
| $B_5:$    | 0, 5, 6  | 7, 8, 13, 14;   |
| $B_6:$    | 0, 5, 6  | 9, 10, 11, 12;  |
| $B_7:$    | 1, 3, 5  | 7, 9, 11, 13;   |
| $B_8:$    | 1, 3, 6  | 7, 10, 12, 14;  |
| $B_9:$    | 1, 4, 5  | 8, 10, 11, 14;  |
| $B_{10}:$ | 1, 4, 6  | 8, 9, 12, 14;   |
| $B_{11}:$ | 2, 3, 5  | 8, 10, 12, 13;  |
| $B_{12}:$ | 2, 3, 6  | 8, 9, 11, 14;   |
| $B_{13}:$ | 2, 4, 5  | 7, 9, 12, 14;   |
| $B_{14}:$ | 2, 4, 6  | 7, 10, 11, 13.  |

Блок-схема называется *симметричной*, если  $v = b$  (и, значит,  $k = r$ ); первая и третья из приведенных схем как раз этого типа. Вторая схема не симметрична, но имеет дополнительное свойство другого рода. В приведенной записи блоки из примера 2 разделены на четыре группы по три блока в каждой группе, причем каждая группа содержит все девять элементов. Схема с таким свойством называется *разрешимой блок-схемой*. Мы покажем в следующем разделе, что симметричная схема всегда обладает еще одним свойством: любые два различных блока имеют точно  $\lambda$  общих элементов. Это свойство дает возможность построить из каждой симметричной блок-схемы еще две схемы, что можно проиллюстрировать на третьем примере.

Возьмем один из блоков (скажем,  $B_0$ ) и построим блоки  $B'_1, \dots, B'_{b-1}$ , где  $B'_i$  содержит  $\lambda$  элементов, общих для  $B_0$  и  $B_i$ ,  $i = 1, \dots, b - 1$ . Получим схему, которая называется *производной схемой*. Если исходная схема имела параметры  $v = b$ ,  $r = k$ ,  $\lambda$ , то производная схема имеет параметры

$$v' = k, \quad b' = b - 1 = v - 1, \quad r' = r - 1 = k - 1, \\ k' = \lambda, \quad \lambda' = \lambda - 1,$$

В нашем примере параметры производной схемы — это  $v' = 7$ ,  $b' = 14$ ,  $r' = 6$ ,  $k' = 3$ ,  $\lambda' = 2$ , и ее элементы — это 0, 1, 2, 3, 4, 5, 6, появляющиеся в блоках  $B_1, \dots, B_{14}$ . Если вычеркнуть  $B_0$  и его элементы из блоков  $B_1, \dots, B_{14}$ , то полученные таким образом блоки  $B_1^*, \dots, B_{14}^*$ , составленные из элементов 7, 8, 9, 10, 11, 12, 13, 14, образуют *остаточную схему*. Параметры остаточной схемы — это  $v^* = v - k$ ,  $b^* = b - 1 = v - 1$ ,  $k^* = k - \lambda$ ,  $r^* = r = k$ ,  $\lambda^* = \lambda$ . В нашем примере  $v^* = 8$ ,  $b^* = 14$ ,  $k^* = 4$ ,  $r^* = 7$ ,  $\lambda^* = 3$ .

## 10.2. Элементарные теоремы о блок-схемах

Основным соотношением для матрицы инцидентности блок-схемы является

$$AA^T = B = (r - \lambda)I + \lambda J = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \vdots \\ \lambda & \dots & \dots & r \end{pmatrix}. \quad (10.2.1)$$

Можно без труда вычислить детерминант  $B$  и найти, что

$$\det B = (r - \lambda)^{v-1} (v\lambda - \lambda + r). \quad (10.2.2)$$

Чтобы получить это выражение, вычтем первый столбец из всех остальных и затем прибавим 2-ю, 3-ю, ...,  $v$ -ю строки к первой. Тогда все элементы выше главной диагонали оказываются равными нулю; на главной диагонали первый элемент есть  $r + (v - 1)\lambda$ , а остальные равны  $r - \lambda$ . Это и дает (10.2.2). Если  $r = \lambda$ , то схема тривиальна, так как тогда элемент  $a_i$  может появляться только вместе с каждым другим элементом  $a_j$ , и каждый блок содержит все  $v$  элементов. В противном случае  $r > \lambda$  и  $B$  невырождена. Отсюда можно получить неравенство Фишера

$$b \geqslant v, \text{ и, следовательно, } r \geqslant k, \quad (10.2.3)$$

ибо ранг  $A$  не превосходит  $b$ , в то время как ранг  $B$  равен  $v$ . Но ранг произведения матриц не может превышать ранга сомножителя, и потому  $b \geqslant v$ .

Следующая теорема доказывается легко, но имеет очень сильные следствия.

**Теорема 10.2.1.** *Если в симметричной схеме  $v$  четно, то  $k - \lambda$  есть точный квадрат.*

**Доказательство.** Так как  $b = v$ , то  $A$  — квадратная матрица и из формулы (10.2.1) получаем

$$(\det A)^2 = \det B = (k - \lambda)^{v-1} (v\lambda - \lambda + k). \quad (10.2.4)$$

Поскольку  $k(k-1) = \lambda(v-1)$ , то  $v\lambda - \lambda + k = k^2$ . Но тогда другой множитель в выражении для  $\det B$ , а именно  $(k - \lambda)^{v-1}$ , также должен быть квадратом, а так как  $v$  четно, то это означает, что  $k - \lambda$  есть квадрат, что и требовалось доказать. Эта теорема показывает, что соотношения (10.1.1) для параметров блок-схемы не являются достаточными условиями ее существования. Например, параметры  $b = v = 22$ ,  $r = k = 7$ ,  $\lambda = 2$  удовлетворяют условиям (10.1.1), и схема (если бы она существовала) должна была бы быть симметричной. Но  $v = 22$  четно, а  $k - \lambda = 5$  не есть квадрат, и поэтому такой схемы не существует.

Следующая теорема дает основное свойство симметричных схем.

**Теорема 10.2.2.** *Если  $A$  — матрица инцидентности симметричной блок-схемы, то  $A$  удовлетворяет следующим четырем соотношениям:*

$$AA^T = B = (k - \lambda)I + \lambda J, \quad (10.2.5)$$

$$A^TA = B = (k - \lambda)I + \lambda J, \quad (10.2.6)$$

$$AJ = kJ, \quad (10.2.7)$$

$$JA = kJ. \quad (10.2.8)$$

Из них формула (10.2.5) — это фактически (10.2.1), если вспомнить, что  $b = v$ ,  $k = r$ , а соотношение (10.2.7) означает, что каждая строка в  $A$  содержит  $k$  единиц, т. е. каждый элемент содержится в  $r = k$  блоках. Равенство (10.2.8) означает, что каждый столбец в  $A$  содержит  $k$  единиц, т. е. число элементов в каждом блоке равно  $k$ . Таким образом, остается только показать, что выполняется

(10.2.6). Для этого достаточно показать, что (10.2.6) является следствием (10.2.5), (10.2.7) и (10.2.8). Это просто теорема о матрицах, что показывает следующая теорема, в которой предполагается значительно меньше.

**Теорема 10.2.3 (Райзер).** Пусть  $A$  — невырожденная  $(v \times v)$ -матрица, которая удовлетворяет либо (10.2.5), либо (10.2.6), а также либо (10.2.7), либо (10.2.8). Тогда  $A$  удовлетворяет всем четырем равенствам (10.2.5)–(10.2.8). Кроме того,  $v, k, \lambda$  удовлетворяют соотношению  $k^2 - k = \lambda(v - 1)$ .

**Доказательство.** Так как  $\det B = (k - \lambda)^{v-1} (v\lambda - \lambda + k)$ , невырожденность  $A$  означает просто, что  $k - \lambda \neq 0$ ,  $v\lambda - \lambda + k \neq 0$ . Допустим, что выполняются (10.2.5) и (10.2.7). Тогда нам дана невырожденная матрица  $A$  и

$$AA^T = (k - \lambda)I + \lambda J, \quad AJ = kJ. \quad (10.2.9)$$

Найдем теперь:  $A^{-1}(AJ) = A^{-1}(kJ)$ , следовательно,  $J = kA^{-1}J$ , а потому  $k \neq 0$  и  $A^{-1}J = k^{-1}J$ . Имеем также  $(AJ)^T = (kJ)^T$ , или  $J A^T = kJ$ , так как  $J^T = J$ . Замечая, что  $J^2 = vJ$ , получим

$$\begin{aligned} A^T &= A^{-1}(AA^T) = (k - \lambda)A^{-1} + \lambda A^{-1}J = \\ &= (k - \lambda)A^{-1} + \lambda k^{-1}J; \end{aligned}$$

$$\begin{aligned} kJ &= JA^T = (k - \lambda)JA^{-1} + \lambda k^{-1}J^2 = \\ &= (k - \lambda)JA^{-1} + \lambda k^{-1}vJ. \end{aligned}$$

Таким образом,

$$JA^{-1} = \frac{k - \lambda k^{-1}v}{k - \lambda} J = mJ,$$

где через  $m$  обозначена постоянная. Следовательно,

$$\begin{aligned} J &= mA, \\ vJ &= J^2 = (mA)J = mJ(AJ) = \\ &= mJ(kJ) = mkJ^2 = mkvJ. \end{aligned}$$

Это дает  $v = mkv$ , т. е.  $mk = 1$ ,  $m = k^{-1}$ . Но  $m(k - \lambda) = k - \lambda k^{-1}v$ . Подставляя  $m = k^{-1}$ , получим  $k^{-1}(k - \lambda) =$

$= k - \lambda k^{-1}v$  и, умножив на  $k$ , приходим к соотношению  $k - \lambda = k^2 - \lambda v$ , или

$$k^2 - k = \lambda(v - 1), \quad (10.2.10)$$

что и требовалось доказать. Равенство  $JA^{-1} = mJ = k^{-1}J$  дает также  $J = k^{-1}JA$ , или

$$JA = kJ, \quad (10.2.11)$$

— соотношение (10.2.8), которое требовалось доказать. Мы можем теперь вернуться к равенству

$$A^T = (k - \lambda) A^{-1} + \lambda k^{-1} J$$

и, умножив справа на  $A$ , получить соотношение

$$\begin{aligned} A^T A &= (k - \lambda) I + \lambda k^{-1} JA = \\ &= (k - \lambda) I + \lambda k^{-1} (kJ) = \\ &= (k - \lambda) I + \lambda J, \end{aligned} \quad (10.2.12)$$

которое является требуемым соотношением (10.2.6).

Мы показали, что если  $A$  невырождена, из соотношений (10.2.5) и (10.2.7) следуют (10.2.6) и (10.2.8) и соотношение  $k^2 - k = \lambda(v - 1)$ .

Предположим теперь, что выполняются (10.2.5) и (10.2.8) и что  $A$  невырождена. Тогда

$$AA^T = (k - \lambda) I + \lambda J,$$

$$JA = kJ.$$

Этот случай несколько проще первого. Имеем

$$J(AA^T) = (k - \lambda) J + \lambda J^2,$$

$$kJA^T = (k - \lambda) J + \lambda v J = mJ, \quad m = k - \lambda + \lambda v,$$

$$kJ(A^T J) = mJ^2,$$

$$kJ(JA)^\dagger = mJ^2,$$

$$kJ(kJ)^T = mJ^2,$$

$$k^2 J^2 = mJ^2,$$

следовательно,  $k^2 = m = k - \lambda + \lambda v$ , т. е.  $k^2 - k = \lambda(v - 1)$ , что и требовалось доказать. Далее,  $kJA^T = mJ = k^2 J$ ,  $k \neq 0$ ,

так как  $A$  невырождена. Тогда  $JA^T = kJ$ , что дает

$$AJ = (JA^T)^T = (kJ)^T = kJ,$$

т. е. требуемое соотношение (10.2.7). Наконец,

$$A^T A = A^{-1} (AA^T) A = (k - \lambda) I + \lambda A^{-1} JA.$$

Но при  $AJ = kJ = JA$  имеем  $A^{-1} JA = J$ , следовательно,  $A^T A = (k - \lambda) I + \lambda J$ , т. е. получено соотношение (10.2.6). Таким образом, из (10.2.5) и (10.2.8) следуют остальные соотношения.

Наконец, если в предыдущих рассуждениях заменить  $A$  на  $A^T$ , то получится, что из формулы (10.2.6) и либо (10.2.7), либо (10.2.8) следуют остальные соотношения, и доказательство теоремы завершено.

Из теорем 10.2.2 и 10.2.3 вытекает несколько важных следствий. Если  $A$  — матрица инцидентности симметричной схемы, то соотношение  $A^T A = (k - \lambda) I + \lambda J$  показывает, что любые два различных блока схемы имеют точно  $\lambda$  общих элементов — факт, упомянутый в разделе 10.1, доказательство которого мы обещали дать в этом разделе. Точнее, эти соотношения означают, что  $A^T$  также является матрицей инцидентности блок-схемы. Если  $D$  — заданная схема с элементами  $a_1, \dots, a_v$  и блоками  $B_1, \dots, B_v$ , то  $A^T$  — матрица инцидентности *двойственной* схемы  $D'$  с элементами  $b_1, \dots, b_v$  и блоками  $A_1, \dots, A_v$ . Можно установить соответствие между  $D$  и  $D'$  следующим образом:

$$\begin{aligned} a_i &\rightleftharpoons A_i, \\ B_j &\rightleftharpoons b_j \end{aligned} \tag{10.2.13}$$

и определить  $D'$  правилом:  $b_j \equiv A_i$  тогда и только тогда, когда  $a_i \in B_j$  в  $D$ .

В первом из примеров в конце разд. 10.1 двойственная схема  $D'$  эквивалентна исходной схеме, в чем легко убедиться, перенумеровав надлежащим образом элементы и блоки. Но в третьем примере двойственная схема  $D'$ , хотя и имеет параметры  $v = b = 15$ ,  $r = k = 7$ ,  $\lambda = 3$ , но не эквивалентна исходной схеме  $D$  ни при каком перенумеровании элементов и блоков. Действительно, в  $D$  следующие тройки элементов: 0, 1, 2; 0, 3, 4;

0, 5, 6; 0, 7, 8; 0, 9, 10; 0, 11, 12; 0, 13, 14, и только они, обладают тем свойством, что входят каждая в три блока. Заметим, что все они содержат элемент 0. В  $D'$  каждая из троек элементов  $b_0, b_1, b_2; b_0, b_3, b_4; b_0, b_5, b_6; b_1, b_3, b_5; b_1, b_4, b_6; b_2, b_3, b_6; b_2, b_4, b_5$  является общей трем блокам, и никакая другая тройка не обладает этим свойством. Но эти множества троек не имеют общего элемента, а при перенумеровании элементов и блоков пересекающиеся тройки должны переходить также в пересекающиеся тройки. Следовательно, никакое перенумерование элементов и блоков не сделает  $D'$  эквивалентной  $D$ .

### 10.3. Теорема Брука — Райзера — Човла

Наиболее важная теорема существования для симметричных блок-схем принадлежит Бруку, Райзеру и Човла.

**Теорема 10.3.1.** *Если существует симметричная блок-схема с параметрами  $v, k, \lambda$ , то, полагая  $n = k - \lambda$ , получаем:*

1) если  $v$  четно, то  $n$  есть квадрат;

2) если  $v$  нечетно, то уравнение  $z^2 = nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2$  имеет решение в целых числах  $x, y, z$ , не равных одновременно нулю.

Условие 1 уже доказано (теорема 10.2.1). Теорема 10.3.1 для случая  $\lambda = 1$ , когда схема является конечной проективной плоскостью, впервые была доказана в 1949 г. Бруком и Райзером [1]. В 1950 г. эта теорема в своей полной форме была доказана Човла и Райзером [1], а Шрикханде [1] независимо от них в том же году доказал также условие 1. Арифметические соображения исключают многие параметры, которые удовлетворяют условию  $k(k-1) = \lambda(v-1)$ . Например, если  $v = 43, k = 7, \lambda = 1$ , применение условия 2 приводит к уравнению  $z^2 = 6x^2 - y^2$ , или  $z^2 + y^2 = 6x^2$ , которое не имеет ненулевого решения в целых  $x, y, z$ . Следовательно, симметричной схемы с параметрами  $v = 43, k = 7, \lambda = 1$  не существует. Следует отметить, что это наиболее сильное из известных условие существования симметричных схем.

Возможно даже, что необходимые условия теоремы Брука — Райзера — Човла являются в действительности достаточными для существования схемы. До сих пор нет примера, который показывал бы тем или иным способом, что не существует симметричной схемы для значений параметров  $v, k, \lambda$ , удовлетворяющих равенству  $k(k-1) = \lambda(v-1)$  и условиям Брука — Райзера — Човла. Существует, разумеется, много параметров, для которых существование схемы находится под сомнением. В частности, очень интересен вопрос о существовании проективной плоскости порядка 10 — симметричной схемы с параметрами  $v = 111, k = 11, \lambda = 1, n = 10$ .

Основным наблюдением Брука и Райзера было то, что для симметричных схем соотношение (10.1.5) принимает вид

$$L_1^2 + \dots + L_v^2 = (k - \lambda)(x_1^2 + \dots + x_v^2) + \\ + \lambda(x_1 + \dots + x_v)^2 = Q, \quad (10.3.1)$$

где

$$L_j = \sum_{i=1}^v a_{ij} x_i, \quad (10.3.2)$$

$a_{ij}$  — числа 0 или 1. Используя лишь рациональность коэффициентов форм  $L_j$ , получаем, что из существования симметричной блок-схемы следует рациональная эквивалентность формы  $Q$ , заданной правой частью формулы (10.3.1), сумме квадратов  $L_1^2 + \dots + L_v^2$ . О рациональной эквивалентности квадратичных форм имеются сильные и глубокие результаты Хассе и Минковского. Приложение этих результатов к (10.3.1) и дает теорему 10.3.1. Работа Човла — Райзера, которой мы в основном будем следовать, дает более элементарное доказательство теоремы 10.3.1, хотя для других целей нам нужны результаты Хассе — Минковского во всей полноте.

Для доказательства теоремы нам понадобятся одна арифметическая теорема и одно тождество. Это тождество

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2, \quad (10.3.3)$$

где

$$\begin{aligned}y_1 &= b_1x_1 - b_2x_2 - b_3x_3 - b_4x_4, \\y_2 &= b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4, \\y_3 &= b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4, \\y_4 &= b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4.\end{aligned}\tag{10.3.4}$$

Оно наиболее естественно припоминается в связи с кватернионами, хотя исторически это тождество предшествует открытию кватернионов Гамильтоном. Если имеется система единиц  $1, i, j, k$ , где  $i^2 = j^2 = k^2 = -1$ ,  $ij = k$ ,  $jk = i$ ,  $ki = j$ ,  $ji = -k$ ,  $kj = -i$ ,  $ik = -j$ , то правило умножения кватернионов принимает вид

$$(b_1 + b_2i + b_3j + b_4k)(x_1 + x_2i + x_3j + x_4k) = y_1 + y_2i + y_3j + y_4k,\tag{10.3.5}$$

где  $y_1, y_2, y_3, y_4$  заданы равенствами (10.3.4), и если мы определим норму  $N(\beta)$  кватерниона  $\beta = b_1 + b_2i + b_3j + b_4k$  равенством

$$N(\beta) = b_1^2 + b_2^2 + b_3^2 + b_4^2,\tag{10.3.6}$$

то тождество (10.3.3) принимает вид

$$N(\beta)N(\xi) = N(\beta\xi).\tag{10.3.7}$$

Арифметическая теорема принадлежит Лагранжу. За доказательством мы отсылаем читателя к книге Харди и Райта [1, стр. 302].

**Теорема Лагранжа.** *Каждое положительное целое число  $n$  можно представить в виде суммы квадратов четырех целых чисел:*

$$n = b_1^2 + b_2^2 + b_3^2 + b_4^2.$$

Заметим, что если  $b_1, b_2, b_3, b_4$  — целые числа и  $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$ , то в (10.3.4) определитель линейных форм от  $x_i$  равен  $n^2$ . Следовательно, мы можем выразить  $x_i$  как линейные формы от  $y_i$  с рациональными коэффициентами, имеющими в знаменателе  $n^2$ .

Продолжим доказательство теоремы Брука — Райзера — Човла. Для числа  $n = k - \lambda$  по теореме Лагранжа

имеем  $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$  с целыми  $b_1, b_2, b_3, b_4$ . Тогда (10.3.1) принимает вид

$$L_1^2 + \dots + L_v^2 = n(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2. \quad (10.3.8)$$

Так как при  $v$  четном теорема уже доказана (по теореме 10.2.1), то считаем  $v$  нечетным и предположим сначала, что  $v \equiv 1 \pmod{4}$ . Преобразуем теперь правую часть (10.3.8) с помощью тождества

$$n(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2) = y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2, \quad (10.3.9)$$

где использовано представление  $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$  и тождество (10.3.3), в котором  $y_i$  и  $x_i$  связаны между собой, как в (10.3.4). Применим (10.3.9) к  $x$ , взятым по четыре, и поскольку  $v \equiv 1 \pmod{4}$ , одно  $x$  останется свободным:

$$L_1^2 + \dots + L_v^2 = y_1^2 + y_2^2 + \dots + y_{v-1}^2 + nx_v^2 + \lambda(x_1 + \dots + x_v)^2. \quad (10.3.10)$$

Полагаем теперь  $y_v = x_v$  и, выражая  $x_i$  через  $y_i$ , получаем рациональное тождество относительно независимых неизвестных  $y_1, \dots, y_v$ :

$$L_1^2 + \dots + L_v^2 = y_1^2 + \dots + y_{v-1}^2 + ny_v^2 + \lambda w^2, \quad (10.3.11)$$

где  $L_1, \dots, L_v$  и  $w = x_1 + x_2 + \dots + x_v$  – рациональные линейные формы от  $y_1, \dots, y_v$ . Пусть  $L_1 = c_{11}y_1 + \dots + c_{1v}y_v$ . Если  $c_{11} \neq 1$ , то мы можем принять  $L_1 = y_1$  в качестве соотношения, определяющего  $y_1$  как линейную форму от  $y_2, \dots, y_v$ . Если  $c_{11} = 1$ , то полагаем  $L_1 = -y_1$ . В любом случае  $y_1$  выражается как рациональная линейная форма от  $y_2, \dots, y_v$ , и справедливо равенство  $L_1^2 = y_1^2$ . Тогда (10.3.11) принимает вид

$$L_2^2 + \dots + L_v^2 = y_2^2 + \dots + y_{v-1}^2 + ny_v^2 + \lambda w^2, \quad (10.3.12)$$

т. е. становится тождеством относительно  $y_2, \dots, y_v$ . Аналогично мы можем выразить  $y_2$  в виде линейной формы от  $y_3, \dots, y_v$ , полагая  $L_2 = \pm y_2$ . Продолжая этот процесс для  $L_3, \dots, L_{v-1}$ , мы, наконец, получим, что

$$L_v^2 = ny_v^2 + \lambda w^2, \quad (10.3.13)$$

где  $L_v$  и  $w$  — рациональные кратные  $y_v$ , которое по-прежнему остается независимым. Последнее существенно, так как соотношение (10.3.13) ничего не дало бы нам, если бы  $L_v$ ,  $y_v$  и  $w$  были тождественно равны нулю. Взяв в качестве  $y_v$  целое число  $x$ , кратное знаменателям в  $L_v$  и  $w$ , мы получаем соотношение для целых чисел  $x, y, z$  с  $x \neq 0$ :

$$z^2 = nx^2 + \lambda y^2. \quad (10.3.14)$$

Это равенство есть следствие существования схемы с  $v \equiv 1 \pmod{4}$ .

Если  $v \equiv 3 \pmod{4}$ , то пусть  $x_{v+1}$  — новое неизвестное. Прибавляя  $nx_{v+1}^2$  к обеим частям равенства (10.3.8) и используя (10.3.9), приходим к форме

$$L_1^2 + \dots + L_v^2 + nx_{v+1}^2 = y_1^2 + \dots + y_{v+1}^2 + \lambda w^2. \quad (10.3.15)$$

Действуя, как прежде, находим, что

$$nx^2 = y_{v+1}^2 + \lambda w^2, \quad (10.3.16)$$

где  $x, w$  рационально зависят от независимого неизвестного  $y_{v+1}$ . Мы можем взять  $y_{v+1}$  кратным знаменателям в  $x$  и  $w$ , и это даст нам ненулевое решение в целых числах уравнения

$$z^2 = nx^2 - \lambda y^2. \quad (10.3.17)$$

Теперь можем соединить (10.3.14) и (10.3.17) в одно соотношение

$$z^2 = nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2. \quad (10.3.18)$$

Тем самым доказана вторая часть, а следовательно, и вся теорема 10.3.1.

Основное уравнение инцидентности для симметричной схемы имеет вид

$$AA^T = (k - \lambda) I + \lambda J. \quad (10.3.19)$$

В терминах квадратичных форм его можно записать в виде

$$L_1^2 + \dots + L_v^2 = (k - \lambda)(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2, \quad (10.3.20)$$

где

$$L_j = \sum_{i=1}^v a_{ij} x_i. \quad (10.3.21)$$

Теорема Брука — Райзера — Човла дает необходимые условия для существования рациональной матрицы  $A$ , удовлетворяющей (10.3.19), или, что то же самое, для существования рациональных линейных форм  $L_j$ , удовлетворяющих (10.3.20). Эти условия являются в действительности достаточными для рационального решения (10.3.19) или (10.3.20). Доказательство этого основывается на глубоких результатах Хассе — Минковского, которые будут приведены в следующем разделе. Но в двух случаях достаточность может быть показана непосредственно. Прежде всего, если  $k - \lambda = n$  есть квадрат, то легко проверить, что

$$A = \sqrt{n} I + \frac{k - \sqrt{n}}{v} J, \quad (10.3.22)$$

$$L_j = \sqrt{n} x_j + \frac{k - \sqrt{n}}{v} (x_1 + \dots + x_v), \quad j = 1, \dots, v,$$

— рациональные решения уравнений (10.3.19) и (10.3.20) соответственно. Это доказывает достаточность условия 1 теоремы 10.3.1, когда  $v$  четно, и, разумеется, включает случаи, когда  $v$  нечетно, а  $n$  — квадрат. Когда  $\lambda = 1$ , мы можем написать  $k = n + 1$ , и тогда  $v = n^2 + n + 1$ . Тождество (10.3.20) можно переписать в виде

$$\begin{aligned} L_1^2 + \dots + L_v^2 &= n \left( x_2 + \frac{x_1}{n} \right)^2 + \\ &+ n \left( x_3 + \frac{x_1}{n} \right)^2 + \dots + n \left( x_v + \frac{x_1}{n} \right)^2 + (x_2 + \dots + x_v)^2. \end{aligned} \quad (10.3.23)$$

Необходимо заметить здесь, что коэффициент при  $x_1^2$  в правой части (10.3.23) равен  $(v - 1)/n = (n^2 + n)/n = n + 1$ , что согласуется с (10.3.20). Когда  $v \equiv 1 \pmod{4}$ , тождество

$$n(u_i^2 + u_{i+1}^2 + u_{i+2}^2 + u_{i+3}^2) = y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2,$$

примененное к правой части равенства (10.3.23), приводит его к виду

$$L_1^2 + \dots + L_v^2 = y_1^2 + \dots + y_v^2, \quad (10.3.24)$$

где  $y_v = x_2 + \dots + x_v$ , и мы непосредственно получаем  $L_i = y_i$ ,  $i = 1, \dots, v$ , в качестве рационального решения (10.3.20). Очевидно,  $v \equiv 1 \pmod{4}$ , когда  $n \equiv 0, 3 \pmod{4}$ . Если же  $n \equiv 1, 2 \pmod{4}$ , то  $v \equiv 3 \pmod{4}$ , и по условию 2 теоремы уравнение

$$z^2 = nx^2 - y^2 \quad (10.3.25)$$

имеет ненулевые решения в целых числах. Тогда  $x \neq 0$  и  $n = r^2 + s^2$ ,  $r = y/x$ ,  $s = z/x$  и можно воспользоваться тождеством

$$(r^2 + s^2)(u_i^2 + u_{i+1}^2) = (ru_i + su_{i+1})^2 + (ru_{i+1} - su_i)^2, \quad (10.3.26)$$

чтобы привести (10.3.23) к виду

$$L_1^2 + \dots + L_v^2 = y_1^2 + \dots + y_v^2. \quad (10.3.27)$$

Снова  $L_i = y_i$ ,  $i = 1, \dots, v$ , дает рациональное решение (10.3.8). Когда  $v$  нечетно и  $\lambda > 1$ , то, по-видимому, не существует равенства, аналогичного (10.3.23), которое давало бы простое доказательство достаточности условий Брука — Райзера — Човла для рационального решения (10.3.8).

## 10.4. Формулировка теоремы Хассе — Минковского. Приложения

В этом разделе мы сформулируем несколько теорем из теории чисел, которые необходимы для нашей дальнейшей работы в комбинаторном анализе. Никаких доказательств приводиться не будет, но будут указаны источники, где соответствующие доказательства можно найти.

Пусть  $p$  — нечетное простое число. Числа  $b \not\equiv 0 \pmod{p}$  делятся на два класса, называемые *квадратичными вычетами* и *квадратичными невычетами*, в зависимости от того, имеет ли сравнение  $x^2 \equiv b \pmod{p}$  решение  $x \pmod{p}$  или нет. Так, по модулю 7 число 2 является квадратичным вычетом, а 3 — квадратичным невычетом,

так как  $4^2 \equiv 2 \pmod{7}$ , а  $x^2 \equiv 3 \pmod{7}$  не имеет решения. Это свойство выражается посредством символа Лежандра  $\left(\frac{b}{p}\right)$  следующим образом:

$$\left(\frac{b}{p}\right) = +1, \text{ если } b \text{ есть квадратичный вычет по } \pmod{p}, \quad (10.4.1a)$$

$$\left(\frac{b}{p}\right) = -1, \text{ если } b \text{ есть квадратичный невычет по } \pmod{p}. \quad (10.4.1b)$$

Таким образом,  $\left(\frac{2}{7}\right) = +1$  и  $\left(\frac{3}{7}\right) = -1$ . Если  $b \equiv 0 \pmod{p}$ , то можно условиться писать  $\left(\frac{b}{p}\right) = 0$ . Следующие теоремы выражают некоторые из основных свойств квадратичных вычетов и невычетов. Доказательства можно найти в книге Харди и Райта [1, стр. 68]<sup>1)</sup>.

**Теорема 10.4.1.** *Если  $p$  – нечетное простое число, то*

$$b \equiv c \pmod{p} \text{ влечет за собой } \left(\frac{b}{p}\right) = \left(\frac{c}{p}\right), \quad (10.4.2)$$

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}, \quad (10.4.3)$$

$$\left(\frac{bc}{p}\right) = \left(\frac{b}{p}\right) \left(\frac{c}{p}\right). \quad (10.4.4)$$

Эта теорема включает утверждение, что произведение двух невычетов есть вычет. Так,  $\left(\frac{3}{7}\right) = -1$ ,  $\left(\frac{6}{7}\right) = -1$ , но  $3 \cdot 6 = 18 \equiv 4 \pmod{7}$  и  $2^2 \equiv 4 \pmod{7}$ . Имеются также некоторые более глубокие соотношения между символами  $\left(\frac{b}{p}\right)$  для различных простых  $p$ . Они принадлежат Гауссу, а второе и третье из следующих ниже соотношений известны под названием „квадратичного закона взаимности“.

<sup>1)</sup> См. также И. М. Виноградов „Основы теории чисел“, М.-Л., 1952. – Прим. ред.

**Теорема 10.4.2.** Если  $p$  и  $q$  — два нечетных простых числа, то

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad (10.4.5)$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad (10.4.6)$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \quad (10.4.7)$$

Теоремы 10.4.1 и 10.4.2 не только выражают глубокие свойства квадратичных вычетов, но и позволяют относительно просто вычислять символ  $\left(\frac{b}{p}\right)$ . Так,  $\left(\frac{26}{83}\right) = \left(\frac{2}{83}\right)\left(\frac{13}{83}\right)$ . Здесь, в силу равенства (10.4.6),  $\left(\frac{2}{83}\right) = -1$ . Согласно (10.4.7),  $\left(\frac{13}{83}\right)\left(\frac{83}{13}\right) = +1$ . Следовательно,  $\left(\frac{13}{83}\right) = \left(\frac{83}{13}\right)$  и по (10.4.2)  $\left(\frac{83}{13}\right) = \left(\frac{5}{13}\right)$ . Из (10.4.7) следует, что  $\left(\frac{5}{13}\right)\left(\frac{13}{5}\right) = +1$ , поэтому  $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right)$ . Теперь можно убедиться, что  $\left(\frac{3}{5}\right) = -1$ , либо непосредственным подсчетом, либо используя формулы (10.4.6) и (10.4.7):  $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ . Поэтому  $\left(\frac{13}{83}\right) = \left(\frac{83}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{3}{5}\right) = -1$ . Тогда  $\left(\frac{26}{83}\right) = (-1)(-1) = +1$  и уравнение  $x^2 \equiv 26 \pmod{83}$  имеет решение. Этот метод не позволяет, однако, найти само решение, которое находится путем перебора:  $x \equiv 21 \pmod{83}$ .

Для сравнений по модулю степеней простого числа  $p$  справедлива

**Теорема 10.4.3.** Пусть  $p$  — простое число, и пусть  $b = p^a b_1$ , где  $p$  не делит  $b_1$ . Тогда для произвольно высокой степени  $p^n$  числа  $p$  сравнение

$$x^2 \equiv b \pmod{p^n} \quad (10.4.8)$$

разрешимо в том и только в том случае, если: 1)  $a$  четно, 2)  $\left(\frac{b_1}{p}\right) = +1$ , если  $p$  нечетно, и  $b_1 \equiv 1 \pmod{8}$ , если  $p = 2$ .

В разделе 10.3 было дано необходимое условие (теорема Брука — Райзера — Човла) существования рациональной  $(v \times v)$ -матрицы  $A$ , удовлетворяющей условию

$$AA^T = B = (k - \lambda) I + \lambda J. \quad (10.4.9)$$

Оно состоит в следующем: 1) при  $v$  четном  $n = k - \lambda$  есть квадрат, 2) при  $v$  нечетном уравнение

$$nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2 = z^2 \quad (10.4.10)$$

имеет ненулевые решения в целых  $x, y, z$ . Эти условия также достаточны. Если  $n$  — квадрат, то мы находим, что

$$A = \sqrt{n} I + \frac{k - \sqrt{n}}{v} J \quad (10.4.11)$$

— рациональное решение для (10.4.9). Это охватывает все случаи с четным  $v$ . Доказательство достаточности (10.4.10) для нечетного  $v$  опирается на глубокую теорию квадратичных форм, принадлежащую Хассе и Минковскому. Если  $b$  и  $c$  — целые числа, то положим символ норменного вычета Гильберта  $(b, c)_p$  равным  $+1$  или  $-1$  в соответствии с тем, имеет или нет сравнение

$$bx^2 + cy^2 \equiv z^2 \pmod{p^m} \quad (10.4.12)$$

решение в целых числах  $x, y, z$ , не все из которых кратны  $p$ , для произвольно больших степеней  $p$ . Мы определим  $(b, c)_p$  и для  $p = \infty$ , считая, что  $(b, c)_{\infty} = +1$  или  $-1$  в соответствии с тем, имеет уравнение

$$bx^2 + cy^2 = z^2 \quad (10.4.13)$$

ненулевые решения в действительных числах  $x, y, z$  или нет. Таким образом,  $(b, c)_{\infty} = +1$ , если ни  $b$ , ни  $c$  не являются отрицательными. Более подробно об этой теории можно прочитать в книге Джонса [1, стр. 17—81].

**Теорема 10.4.4. Уравнение**

$$bx^2 + cy^2 = z^2 \quad (10.4.14)$$

имеет ненулевые решения в целых числах  $x, y, z$  тогда и только тогда, когда  $(b, c)_p = +1$  при всех простых  $p$ , включая  $p = \infty$ .

Мы отмечали, что матричное уравнение (10.4.9) эквивалентно уравнению

$$L_1^2 + \dots + L_v^2 = (k - \lambda)(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2. \quad (10.4.15)$$

Поэтому существование рациональной матрицы  $A$ , удовлетворяющей (10.4.9), в точности эквивалентно существованию рационального преобразования, переводящего форму  $x_1^2 + \dots + x_v^2$  в форму  $(k - \lambda)(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2$ . Теория Хассе — Минковского дает условия для рациональной эквивалентности любых двух рациональных квадратичных форм. Они выражаются посредством символа Хассе  $c_p(f)$ , определяемого для квадратичной формы

$$f = \sum_{i, j=1}^m b_{ij} x_i x_j, \quad b_{ij} = b_{ji},$$

и простых чисел  $p$ , включая  $p = \infty$ .

Если

$$f = \sum_{i, j=1}^m b_{ij} x_i x_j, \quad b_{ij} = b_{ji},$$

то определим при  $r = 1, \dots, m$  величину

$$D_r = \det(b_{ij}), \quad i, j = 1, \dots, r;$$

$D_r$  называется  $r$ -м ведущим главным минором матрицы  $B = (b_{ij})$ . Будем предполагать, что все  $b_{ij}$  — целые числа, а  $D_1, \dots, D_m$  все отличны от нуля. Более общая теория нам не понадобится.

Определим для  $f$  и каждого простого  $p$ , включая  $p = \infty$ , символ

$$c_p(f) = (-1, -D_m)_p \prod_{i=1}^{m-1} (D_i, -D_{i+1})_p. \quad (10.4.16)$$

Приведем основную теорему, на которую мы будем ссылаться.

**Теорема 10.4.5 (Хассе – Минковский).** Если  $f_1$  и  $f_2$  – целочисленные квадратичные формы от  $t$  переменных, ни у одной из которых ведущие главные миноры не обращаются в нуль, то необходимое и достаточное условие того, чтобы  $f_1$  и  $f_2$  были рационально эквивалентны, состоит в том, что  $c_p(f_1) = c_p(f_2)$  при всех нечетных простых  $p$  и  $p = \infty$ .

Следующая теорема дает основные свойства символа норменного вычета Гильберта  $(b, c)_p$ , используемые при подсчетах.

**Теорема 10.4.6.** Символ норменного вычета Гильберта обладает следующими свойствами ( $b, c, d, e$  – целые числа):

$$\prod (b, c)_p = 1, \quad \text{где произведение берется по всем простым числам, включая } p = \infty; \quad (10.4.17)$$

$$(b, c)_\infty = 1, \quad \text{если только } b \text{ и } c \text{ не являются оба отрицательными; } \quad (10.4.18)$$

$$(b, c)_p = (c, b)_p; \quad (10.4.19)$$

$$(b_1 b_2, c)_p = (b_1, c)_p (b_2, c)_p; \quad (10.4.20)$$

$$(bd^2, ce^2)_p = (b, c)_p; \quad (10.4.21)$$

$$(b, -b)_p = 1, \quad (b^2, c)_p = 1. \quad (10.4.22)$$

Если  $p$  – нечетное простое число, то

$$(b, c)_p = 1, \quad \text{если } b \text{ и } c \text{ взаимно просты с } p; \quad (10.4.23)$$

$$(b, p)_p = \left( \frac{b}{p} \right), \quad \text{если } b \not\equiv 0 \pmod{p}; \quad (10.4.24)$$

$$(p, p)_p = (-1, p)_p. \quad (10.4.25)$$

$$\text{Если } b_1 \equiv b_2 \not\equiv 0 \pmod{p}, \text{ то } (b_1, c)_p = (b_2, c)_p. \quad (10.4.26)$$

Посредством формулы (10.4.17) нам удалось исключить  $p = 2$  из рассмотрения в теореме 10.4.5, так как  $c_2(f_1) = c_2(f_2)$ , если  $c_p(f_1) = c_p(f_2)$  при всех нечетных простых  $p$  и  $p = \infty$ .

Задача, которой мы занимаемся, состоит в том, чтобы при нечетном  $v$  показать, что рациональное решение уравнения (10.4.15) эквивалентно существованию целых

$x, y, z$ , не равных одновременно нулю и удовлетворяющих (10.4.10). Рассмотрим рациональные формы

$$\begin{aligned}f_1 &= n(x_1^2 + \dots + x_v^2) + \lambda(x_1 + \dots + x_v)^2, \\f_2 &= x_1^2 + \dots + x_v^2.\end{aligned}$$

Имеем для  $f_1$

$$D_r = n^{r-1} [k + (r-1)\lambda], \quad r = 1, \dots, v,$$

а для  $f_2$

$$D_r = 1, \quad r = 1, \dots, v.$$

Для  $f_2$  без труда находим, что  $c_\infty(f_2) = -1$  и  $c_p(f_2) = +1$  при  $p$  конечном и нечетном. Так как для  $f_1$  все  $D_r$  положительны, то  $c_\infty(f_1) = -1$ . Следовательно, по теореме 10.4.5 формы  $f_1$  и  $f_2$  рационально эквивалентны тогда и только тогда, когда  $c_p(f_1) = +1$  для всех конечных нечетных простых чисел. Это равносильно требованию, чтобы для конечных нечетных  $p$

$$c_p(f_1) = (-1, -D_v)_p \prod_{i=1}^{v-1} (D_i, -D_{i+1})_p = 1, \quad (10.4.27)$$

$$D_i = n^{i-1} [k + (i-1)\lambda], \quad i = 1, \dots, v.$$

[ $D_i$  вычисляется совершенно аналогично  $\det B$  в (10.2.2).]

Детальный и довольно трудоемкий подсчет показывает, что при  $v$  нечетном формула (10.4.27) приводит к равенству

$$c_p(f_1) = \left( n, (-1)^{\frac{v-1}{2}} \lambda \right)_p = +1 \quad (10.4.28)$$

для конечных нечетных простых  $p$ . Так как  $n$  положительно, то

$$\left( n, (-1)^{\frac{v-1}{2}} \lambda \right)_\infty = +1. \quad (10.4.29)$$

Таким образом, используя (10.4.17), чтобы получить также равенство  $\left( n, (-1)^{\frac{v-1}{2}} \lambda \right)_2 = +1$ , мы можем обратиться к теореме 10.4.4 и заключить, что рациональная эквивалентность  $f_1$  и  $f_2$  для нечетного  $v$  эквивалентна существованию рациональных чисел  $x, y, z$ , не равных

одновременно нулю и удовлетворяющих уравнению

$$nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2 = z^2. \quad (10.4.30)$$

Тем самым условие (10.4.30) не только необходимо, но и достаточно для существования рационального решения (10.4.15) или, что эквивалентно, (10.4.9). Это доказывает теорему Брука — Райзера — Човла и рациональное обращение этой теоремы.

Остается лишь проделать трудоемкую работу, чтобы показать, что (10.4.27) сводится к (10.4.28) для нечетных простых  $p$ . Пусть

$$E_i = k + (i-1)\lambda, \quad i = 1, \dots, v,$$

и заметим, что  $E_v = k^2$ , так как  $k^2 - k = \lambda(v-1)$ . Поскольку  $v$  нечетно,  $n^{v-1}$  есть квадрат, поэтому для нечетных простых  $p$

$$(-1, -D_v)_p = (-1, -n^{v-1}k^2)_p = (-1, -1)_p = +1. \quad (10.4.31)$$

В последующих вычислениях мы для удобства опускаем индекс  $p$ . Используя (10.4.31), мы получаем

$$\begin{aligned} c(f_1) &= \prod_{i=1}^{v-1} (D_i, -D_{i+1}) = \\ &= \prod_{i=1}^{v-1} (n^{i-1}E_i, -n^iE_{i+1}) = \\ &= \prod_{i=1}^{v-1} (n^{i-1}, -n^i)(n^{i-1}, E_{i+1})(E_i, n^i)(E_i, -E_{i+1}). \end{aligned} \quad (10.4.32)$$

Если  $i$  четно, то  $(n^{i-1}, -n^i) = (n, -1)$ . Если  $i$  нечетно, то  $(n^{i-1}, -n^i) = (1, -n) = 1$ . Следовательно,

$$\prod_{i=1}^{v-1} (n^{i-1}, -n^i) = (n, -1)^{\frac{v-1}{2}}. \quad (10.4.33)$$

Далее,

$$\begin{aligned} \prod_{i=1}^{v-1} (n^{i-1}, E_{i+1}) &= \prod_{i=1}^{v-1} (n^2 \cdot n^{i-1}, E_{i+1}) = \\ &= \prod_{i=1}^{v-1} (n^{i+1}, E_{i+1}) = \\ &= (n^v, E_v) \prod_{j=2}^{v-1} (n^j, E_j) = \prod_{i=2}^{v-1} (n^i, E_i), \end{aligned} \quad (10.4.34)$$

так как  $E_v = k^2$ . Подставляя (10.4.33) и (10.4.34) в (10.4.32), приходим к равенству

$$\begin{aligned} c(f_1) &= (n, -1)^{\frac{v-1}{2}} (E_1, n) \prod_{i=2}^{v-1} (n^i, E_i)^2 \prod_{i=1}^{v-1} (E_i, -E_{i+1}) = \\ &= (n, -1)^{\frac{v-1}{2}} (k, n) \prod_{i=1}^{v-1} (E_i, -E_{i+1}). \end{aligned} \quad (10.4.35)$$

Докажем теперь, что

$$P = \prod_{i=1}^{v-1} (E_i, -E_{i+1}) = (k, n)(\lambda, n) \quad (10.4.36)$$

для каждого нечетного простого  $p$ . Если (10.4.36) верно, то подстановка его в (10.4.35) дает (10.4.28), что, как мы уже отмечали, доказывает теорему Брука — Райзера — Човла и ее рациональное обращение.

Пусть  $p^a$  (возможно,  $p^0 = 1$ ) — наибольшая степень  $p$ , делящая и  $k$ , и  $\lambda$ , так что  $k = p^a k_1$ ,  $\lambda = p^a \lambda_1$ ,  $p \nmid (k_1, \lambda_1)$ ,  $k_1 + (v-1)\lambda_1 = p^a k_1^2$ . Тогда

$$\begin{aligned} P &= \prod_{i=1}^{v-1} (p^a (k_1 + (i-1)\lambda_1), -p^a (k_1 + i\lambda_1)) = \\ &= \prod_{i=1}^{v-1} (p^a, -p^a) (p^a, k_1 + i\lambda_1) (k_1 + (i-1)\lambda_1, p^a) \times \\ &\quad \times (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1)) = \\ &= (k_1, p^a) (k_1 + (v-1)\lambda_1, p^a) \prod_{i=1}^{v-2} (p^a, k_1 + i\lambda_1)^2 \times \\ &\quad \times \prod_{i=1}^{v-1} ((k_1 + (i-1)\lambda_1), -(k_1 + i\lambda_1)). \end{aligned} \quad (10.4.37)$$

Очевидно,  $(k_1 + (v-1)\lambda_1, p^a) = (p^a k_1^2, p^a) = (p^a, p^a)$ .

Таким образом, из формулы (10.4.37) получаем

$$P = (k_1, p^a)(p^a, p^a) \prod_{i=1}^{v-1} (k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1)). \quad (10.4.38)$$

Предположим сначала, что  $p \mid \lambda_1$ . Из того, что  $k(k-1) = \lambda(v-1)$ , мы получаем, что  $k_1(p^a k_1 - 1) = \lambda_1(v-1)$ , следовательно, поскольку  $p \nmid k_1$ , должно быть  $a=0$  и  $k_1=k$ . Кроме того,  $p \nmid n = k-\lambda$ , и поэтому  $p \nmid k+i\lambda$  для всех  $i$ . Таким образом,  $P=1$  и

$$(k, n)(\lambda, n) = 1 \cdot (\lambda, k-\lambda) = (\lambda, k) = \\ = (\lambda, (k^2 - k) + k) = (\lambda, k^2) = 1,$$

так как  $k^2 - k \equiv 0 \pmod{p}$ . Следовательно, в этом случае  $P = (k, n)(\lambda, n)$ .

Пусть теперь  $p \nmid \lambda_1$ . Тогда самое большое одно из выражений  $k_1 + (i-1)\lambda_1$ ,  $k_1 + i\lambda_1$  делится на  $p$ , и если ни одно из них не делится на  $p$ , то  $(k_1 + (i-1)\lambda_1, -(k_1 + i\lambda_1)) = 1$ . Пусть  $r$  — целое число в отрезке  $0 \leq r \leq v-1$ , такое, что  $k_1 + r\lambda_1 \equiv 0 \pmod{p}$ . Если  $1 \leq r \leq v-2$ , то в произведении  $P$  есть точно два члена, содержащих  $k_1 + r\lambda_1$ , и их произведение равно

$$(k_1 + (r-1)\lambda_1, -(k_1 + r\lambda_1))(k_1 + r\lambda_1, -(k_1 + (r+1)\lambda_1)) = \\ = (-\lambda_1, -(k_1 + r\lambda_1))(k_1 + r\lambda_1, -\lambda_1) = \\ = (-\lambda_1, -(k_1 + r\lambda_1)^2) = \\ = (-\lambda_1, -1) = 1, \quad (10.4.39)$$

так как  $p \nmid \lambda_1$ . Следовательно,  $P = (k_1, p^a)(p^a, p^a)$ , если только ни одно из чисел  $k_1$  и  $k_1 + (v-1)\lambda_1$  не делится на  $p$ . Если  $a=0$ , то  $k_1=k$  и  $k_1 + (v-1)\lambda_1 = k^2$  и  $p$  не делит ни одно из них. В этом случае  $P=1$ , и поскольку  $p \nmid k$ ,  $p \nmid \lambda$ , то  $(k, n)(\lambda, n) = 1 \cdot 1$ , если  $p \nmid n = k-\lambda$ ; и если  $p \mid n = k-\lambda$ , то  $(k, n)(\lambda, n) = (k, n)^2 = 1$ . Таким образом, в случае  $a=0$  мы имеем  $P = (k, n)(\lambda, n)$ . Если

$$\begin{aligned}
 a > 0, \text{ то } k_1 + (v-1)\lambda_1 = p^a k_1^2 \text{ и} \\
 (k_1 + (v-2)\lambda_1, - (k_1 + (v-1)\lambda_1)) = \\
 = (-\lambda_1, -p^a k_1^2) = \\
 = (-\lambda_1, -p^a) = (-\lambda_1, -1)(-\lambda_1, p^a) = \\
 = (-1, p^a)(\lambda_1, p^a) = (p^a, p^a)(\lambda_1, p^a). \quad (10.4.40)
 \end{aligned}$$

Так как либо  $p | k_1$ , либо  $p \nmid k_1$ , то, используя (10.4.40), получаем

$$P = (k_1, p^a)(\lambda_1, p^a), \text{ если } p \nmid k_1, \quad (10.4.41)$$

$$P = (k_1, p^a)(\lambda_1, p^a)(k_1, -k_1 - \lambda_1), \text{ если } p | k_1. \quad (10.4.42)$$

С другой стороны, очевидно,

$$\begin{aligned}
 (k, n)(\lambda, n) &= (p^a k_1, p^a(k_1 - \lambda_1))(p^a \lambda_1, p^a(k_1 - \lambda_1)) = \\
 &= (k_1, p^a)(k_1, k_1 - \lambda_1)(\lambda_1, p^a)(\lambda_1, k_1 - \lambda_1). \quad (10.4.43)
 \end{aligned}$$

Если  $p \nmid k_1$ , то  $(k_1, k_1 - \lambda_1) = (\lambda_1, k_1 - \lambda_1)$ , так как если  $p \nmid k_1 - \lambda_1$ , то оба числа равны единице, а если  $p | k_1 - \lambda_1$ , то они равны между собой. Таким образом, ввиду (10.4.41) и (10.4.43) имеем  $P = (k, n)(\lambda, n)$ , если  $p \nmid k_1$ . Если же  $p | k_1$ , то

$$(k_1, -k_1 - \lambda_1) = (k_1, k_1 - \lambda_1)$$

и

$$(\lambda_1, k_1 - \lambda_1) = 1,$$

так как  $\lambda_1$  и  $k_1 - \lambda_1$  оба взаимно просты с  $p$ . Снова сравнивая формулы (10.4.42) и (10.4.43), находим, что  $P = (k, n)(\lambda, n)$ . Таким образом, мы доказали, что во всех случаях  $P = (k, n)(\lambda, n)$ .

Как было отмечено выше, подстановка полученного результата в (10.4.35) дает (10.4.28), откуда в свою очередь следует теорема Брука — Райзера — Човла и ее рациональное обращение.

Как приложение этой теоремы, рассмотрим вопрос о существовании блок-схемы с параметрами  $v = 29$ ,  $k = 8$ ,  $\lambda = 2$ . Здесь условие  $k^2 - k = \lambda(v-1)$  удовлетворяется. По теореме Брука — Райзера — Човла необходимым условием существования блок-схемы с этими параметрами является разрешимость в целых числах  $x, y, z$ , не равных

одновременно нулю, уравнения

$$6x^2 + 2y^2 = z^2. \quad (10.4.44)$$

Для разрешимости этого уравнения символ Гильберта  $(6,2)_p$  должен равняться  $+1$  при всех нечетных  $p$  и  $p = \infty$ . Это, конечно, верно для  $p = \infty$  и конечных простых  $p$ , не делящих 6 или 2, т. е. критическим случаем является  $p = 3$ . Но  $(6,2)_3 = (2,2)_3(3,2)_3 = (3,2)_3 = \left(\frac{2}{3}\right) = -1$  по теоремам 10.4.6 и 10.4.2, поэтому уравнение (10.4.44) не имеет решений в целых числах, не равных одновременно нулю, и схемы с параметрами  $v = 29$ ,  $k = 8$ ,  $\lambda = 2$  не существует.

# Разностные множества

---

## 11.1. Примеры и определения

**Определение.** Две блок-схемы  $B$  и  $B'$  называются *изоморфными*, если существует взаимно однозначное отображение  $\alpha$  элементов и блоков  $B$  на элементы и блоки  $B'$ , такое, что если  $x_i$  — элемент, а  $B_j$  — блок схемы  $B$  и

$$\alpha: x_i \rightarrow x'_i = (\alpha) x_i \text{ — элемент } B',$$

$$\alpha: B_j \rightarrow B'_j = (\alpha) B_j \text{ — блок } B',$$

то  $x_i \in B_j$  тогда и только тогда, когда  $(\alpha) x_i \in (\alpha) B_j$ .

Таким образом, две блок-схемы изоморфны, если они имеют одни и те же соотношения инцидентности, т. е. являются по существу одной и той же схемой. Если  $B' = B$ , то отображение  $\alpha$  называется *автоморфизмом* блок-схемы  $B$ . Автоморфизмы всякой блок-схемы  $B$  образуют группу, так как если  $a_1$  и  $a_2$  — два автоморфизма  $B$ , то их произведение  $a_1 a_2$  есть также автоморфизм и обратные отображения  $a_1^{-1}$  и  $a_2^{-1}$  — снова автоморфизмы.

Мы будем интересоваться здесь блок-схемами с автоморфизмами специального вида. В следующем примере  $B$  есть схема с вычетами  $0, 1, \dots, 12 \pmod{13}$  в качестве элементов и блоками  $B_i$ ,  $i = 0, \dots, 12 \pmod{13}$ :

$$\begin{aligned}
 B_0 &: 0, 1, 3, 9; \\
 B_1 &: 1, 2, 4, 10; \\
 B_2 &: 2, 3, 5, 11; \\
 B_3 &: 3, 4, 6, 12; \\
 B_4 &: 4, 5, 7, 0; \\
 B_5 &: 5, 6, 8, 1; \\
 B_6 &: 6, 7, 9, 2; \\
 B_7 &: 7, 8, 10, 3; \\
 B_8 &: 8, 9, 11, 4; \\
 B_9 &: 9, 10, 12, 5; \\
 B_{10} &: 10, 11, 0, 6; \\
 B_{11} &: 11, 12, 1, 7; \\
 B_{12} &: 12, 0, 2, 8.
 \end{aligned} \tag{11.1.1}$$

Здесь  $\alpha: i \rightarrow i+1$ ,  $B_i \rightarrow B_{i+1}$  есть автоморфизм схемы  $B$ , который переставляет как элементы, так и блоки по циклу длины 13. Вообще симметричная блок-схема  $B$  с параметрами  $v, k, \lambda$  ( $(v, k, \lambda)$ -блок-схема) называется  $B$ -циклической, если  $B$  имеет автоморфизм  $\alpha$ , который переставляет элементы и блоки по циклу длины  $v$ . Заметим, что циклический автоморфизм  $\alpha$  и множество элементов в отдельном блоке полностью определяют всю схему, как в случае схемы (11.1.1).

Произвольный блок в (11.1.1), например блок  $B_5 = \{5, 6, 8, 1\}$ , обладает тем свойством, что  $4 \cdot 3 = 12$  разностей различных элементов в этом блоке дают каждую разность  $(\bmod 13)$ , исключая 0, точно по одному разу. В самом деле,

$$\begin{array}{ll} 1 \equiv 6 - 5, & 7 \equiv 8 - 1, \\ 2 \equiv 8 - 6, & 8 \equiv 1 - 6, \\ 3 \equiv 8 - 5, & 9 \equiv 1 - 5, \\ 4 \equiv 5 - 1, & 10 \equiv 5 - 8, \quad (\bmod 13) \\ 5 \equiv 6 - 1, & 11 \equiv 6 - 8, \\ 6 \equiv 1 - 8, & 12 \equiv 5 - 6. \end{array} \quad (11.1.2)$$

**Определение.** Множество  $D$ , состоящее из  $k$  вычетов  $a_1, \dots, a_k$  по модулю  $v$ , называется  $(v, k, \lambda)$ -разностным множеством, если для каждого  $d \not\equiv 0 \pmod{v}$  существует точно  $\lambda$  упорядоченных пар  $(a_i, a_j)$ ,  $a_i, a_j \in D$ , таких, что  $a_i - a_j \equiv d \pmod{v}$ .

Таким образом,  $\{5, 6, 8, 1\}$  есть  $(13, 4, 1)$ -разностное множество по (11.1.2).

**Теорема 11.1.1.** Множество  $D$ , состоящее из  $k$  вычетов  $a_1, \dots, a_k$  по модулю  $v$ , есть  $(v, k, \lambda)$ -разностное множество тогда и только тогда, когда множества  $B_i = \{a_1 + i, \dots, a_k + i\}$  вычетов по модулю  $v$ ,  $i = 0, \dots, v-1$ , являются блоками циклической  $(v, k, \lambda)$ -блок-схемы  $B$ .

**Доказательство.** Предположим сначала, что множества  $B_i = \{a_1 + i, \dots, a_k + i\}$  вычетов по модулю  $v$  при  $i = 0, \dots, v-1$  образуют циклическую блок-схему  $B$ , где, очевидно,  $\alpha: i \rightarrow i+1$ ,  $B_i \rightarrow B_{i+1}$ ,  $i = 0, \dots, v-1$ , по модулю  $v$  — циклический автоморфизм. Тогда, если  $d \not\equiv 0 \pmod{v}$ , элементы  $0, d$  появляются вместе точно

в  $\lambda$  блоках, т. е. для  $\lambda$  наборов  $a_i, a_j \in D$  и  $t$  мы имеем

$$d \equiv a_i + t, \quad 0 \equiv a_j + t \pmod{v}, \quad (11.1.3)$$

следовательно, существует точно  $\lambda$  упорядоченных пар  $(a_i, a_j), a_i, a_j \in D$  с

$$a_i - a_j \equiv d \pmod{v}, \quad (11.1.4)$$

так как  $t \equiv -a_j$  однозначно определяется через  $a_j$ . Следовательно,  $D$  есть разностное множество. Обратно, пусть  $D = \{a_1, \dots, a_k\}$  есть  $(v, k, \lambda)$ -разностное множество. Тогда в множествах  $B_t = \{a_1 + t, \dots, a_k + t\}$  вычетов по модулю  $v$ ,  $i = 0, \dots, v-1$ , каждая пара различных вычетов  $r, s$  появляется вместе  $\lambda$  раз. В самом деле, пусть  $r - s \equiv d \not\equiv 0 \pmod{v}$ . Тогда точно для  $\lambda$  упорядоченных пар  $(a_i, a_j), a_i, a_j \in D$ ,

$$r - s \equiv a_i - a_j \pmod{v},$$

поэтому и  $r \equiv a_i + t$  и  $s \equiv a_j + t$  принадлежат  $B_t$ , где  $t$  определяется соотношением  $t \equiv r - a_i \equiv s - a_j \pmod{v}$ . Таким образом, множества  $B_t$  — блоки циклической  $(v, k, \lambda)$ -блок-схемы  $B$  и  $\alpha$ :  $i \rightarrow i+1$ ,  $B_i \rightarrow B_{i+1}$ , где элементы и индексы блоков берутся по модулю  $v$ , — соответствующий автоморфизм.

Брук [1] обобщил идею циклического разностного множества и определил групповое разностное множество  $D$ , которое может основываться на произвольной конечной группе  $G$ .

Пусть  $G$  — конечная группа порядка  $v$ , и пусть  $(v, k, \lambda)$ -блок-схема  $B$  допускает  $G$  в качестве регулярной группы автоморфизмов. Под этим подразумевается, что если  $x$  — какой-либо элемент, а  $B_0$  — какой-либо блок, то, когда  $g$  пробегает все элементы  $G$ ,  $(x)g$  и  $(B_0)g$  пробегают все элементы и блоки схемы  $B$ . Назовем тогда  $x$  базисной точкой. Если  $y = (x)g_1$  — другой элемент, то  $(x)g = (y)g_1^{-1}g$ . Таким образом, мы можем отождествить элементы схемы с элементами группы, и

при изменении базисной точки  $g$  заменяется на  $g_1^{-1}g$  для подходящего  $g_1$ .

Например, если  $G$  — абелева группа порядка 16, порожденная элементами  $a, b, c, d$ , где  $a^2 = b^2 = c^2 = d^2 = 1$ , то  $D = \{a, b, c, d, ab, cd\}$  есть групповое  $(16, 6, 2)$ -разностное множество, и если мы в качестве  $(B_0)$   $g$  возьмем множество  $\{ag, bg, cg, dg, abg, cdg\}$ , где  $g$  пробегает все 16 элементов группы  $G$ , то получим  $(16, 6, 2)$ -блок-схему, которая имеет  $G$  в качестве регулярной группы автоморфизмов. Для разностных множеств в группах, не обязательно абелевых, дадим следующее определение.

**Определение.** Множество  $D$ , состоящее из  $k$  различных элементов  $a_1, \dots, a_k$  группы  $G$  порядка  $v$ , называется *групповым  $(v, k, \lambda)$ -разностным множеством*, если выполняется одно из следующих условий:

1. Для всякого  $d \in G$ ,  $d \neq 1$ , существует точно  $\lambda$  упорядоченных пар  $(a_i, a_j)$ ,  $a_i, a_j \in D$ , таких, что  $a_i a_j^{-1} = d$ .

2. Для всякого  $d \in G$ ,  $d \neq 1$ , существует точно  $\lambda$  упорядоченных пар  $(a_i, a_j)$ ,  $a_i, a_j \in D$ , таких, что  $a_i^{-1} a_j = d$ .

Эти два условия эквивалентны очевидным образом, если группа  $G$  абелева, но мы увидим, что в действительности они эквивалентны для всякой конечной группы  $G$ . Заметим, что из определения непосредственно следует, что  $k(k-1) = \lambda(v-1)$ , так как существует всего  $k(k-1)$  упорядоченных пар, а должно быть  $\lambda$  представлений вида  $a_i a_j^{-1}$  или  $a_i^{-1} a_j$  для каждого из  $v-1$  элементов.

**Теорема 11.1.2.** *Свойства 1 и 2 группового разностного множества  $D$  эквивалентны. Если  $B$  есть  $(v, k, \lambda)$ -блок-схема, допускающая группу  $G$  порядка  $v$  в качестве регулярной группы автоморфизмов, и если  $(x) a_1, \dots, (x) a_k$  — элементы блока  $B_0$ , то  $D = \{a_1, \dots, a_k\}$  есть групповое  $(v, k, \lambda)$ -разностное множество. Обратно, если  $D = \{a_1, \dots, a_k\}$  — групповое  $(v, k, \lambda)$ -разностное множество элементов группы  $G$  порядка  $v$ , то множества  $B(g) = \{a_1 g, \dots, a_k g\}$ , где  $g$  пробегает  $G$ , образуют*

$(v, k, \lambda)$ -блок-схему, допускающую  $G$  в качестве регулярной группы автоморфизмов.

Доказательство. Предположим, что  $B$  есть  $(v, k, \lambda)$ -блок-схема, допускающая группу  $G$  порядка  $v$  в качестве регулярной группы автоморфизмов. Если  $x$  — произвольный элемент  $B$ , то, взяв  $x$  в качестве базисной точки, мы можем все элементы представить в виде  $(x)g$ ,  $g \in G$ , и отождествить  $(x)g$  с  $g$ . Тогда если  $a_1, \dots, a_k$  — элементы блока  $B_0$ , то  $(B_0)g$  содержит  $a_1g, \dots, a_kg$ . Если  $d$  — элемент группы  $G$  и  $d \neq 1$ , то существует точно  $\lambda$  блоков, содержащих  $d$  и  $1$ , т. е. существует точно  $\lambda$  упорядоченных пар  $(a_i, a_j)$ , таких, что для некоторого  $g$  имеем  $a_i g = d$ ,  $a_j g = 1$ , и, следовательно,  $a_i a_j^{-1} = d$ . Но здесь  $g = a_i^{-1}$  определяется элементом  $a_j$ . Следовательно,  $D = \{a_1, \dots, a_k\}$  есть  $(v, k, \lambda)$ -разностное множество, удовлетворяющее условию 1. Обратно, если  $D = \{a_1, \dots, a_k\}$  есть  $(v, k, \lambda)$ -разностное множество элементов группы  $G$  порядка  $v$ , удовлетворяющее свойству 1, то построим множества  $B(g) = \{a_1g, \dots, a_kg\}$ , где  $g$  пробегает элементы группы  $G$ . Если  $r, s$  — два различных элемента  $G$ , то полагаем  $rs^{-1} = d \neq 1$  и для любой из  $\lambda$  упорядоченных пар  $(a_i, a_j)$ , таких, что  $a_i a_j^{-1} = d$ , определим  $g$  соотношением  $a_i^{-1}r = a_j^{-1}s = g$ ; следовательно, как  $r = a_i g$ , так и  $s = a_j g$  принадлежат  $B(g)$ .

Таким образом, множества  $B(g)$  — это блоки схемы  $B$ , допускающей  $G$  в качестве регулярной группы автоморфизмов. Мы показали эквивалентность разностных множеств со свойством 1 блок-схемам  $B$ , которые допускают  $G$  в качестве регулярной группы автоморфизмов. Что же сказать о свойстве 2? Из раздела 10.2 мы знаем, что если  $d \neq 1$ , то блоки  $a_1, a_2, \dots, a_k$  и  $a_1d, a_2d, \dots, a_kd$  имеют точно  $\lambda$  общих элементов. Но это означает, что точно для  $\lambda$  упорядоченных пар  $(a_i, a_j)$  мы имеем  $a_i d = a_j$ , следовательно,  $d = a_i^{-1}a_j$ . Это свойство 2, и оно, таким образом, следует из свойства 1. Обратно, если нам дано свойство 2, то множества  $B(r) = \{a_1r, \dots, a_kr\}$  и  $B(s) = \{a_1s, \dots, a_ks\}$  имеют точно  $\lambda$  общих элементов, следовательно, в силу результатов раздела 10.2 они являются блоками  $(v, k, \lambda)$ -схемы.

## 11.2. Конечные поля

Поле  $F$  есть множество элементов с операциями сложения  $a + b$  и умножения  $ab$ , удовлетворяющими обычным аксиомам:

**A0.** Для  $a, b \in F$  существует, и притом единственный, элемент  $c \in F$ , такой, что  $a + b = c$ .

**A1.**  $(a + b) + c = a + (b + c)$ .

**A2.**  $b + a = a + b$ .

**A3.** Существует элемент  $0 \in F$ , такой, что  $a + 0 = 0 + a = a$  для всякого  $a \in F$ .

**A4.** Для всякого  $a \in F$  существует элемент  $-a \in F$ , такой, что  $a + (-a) = (-a) + a = 0$ .

**D.**  $a(b + c) = ab + ac$  и  $(a + b)c = ac + bc$ .

**M0.** Для  $a, b \in F$  существует, и притом единственный, элемент  $c \in F$ , такой, что  $ab = c$ .

**M1.**  $(ab)c = a(bc)$ .

**M2.**  $ba = ab$ .

**M3.** Существует элемент  $1 \in F$ , такой, что  $a1 = 1a = a$  для всякого  $a \in F$ .

**M4.** Для всякого  $a \neq 0$  из  $F$  существует элемент  $a^{-1} \in F$ , такой, что  $aa^{-1} = a^{-1}a = 1$ .

Наиболее известные поля — это поле рациональных чисел, поле действительных чисел и поле комплексных чисел. Но существуют и поля с конечным числом элементов. Например, четыре элемента  $0, 1, a, b$  образуют поле, если мы воспользуемся следующими таблицами сложения и умножения. Здесь  $x + y$  и  $xy$  даны в соответствующей таблице на пересечении строки с номером  $x$  и столбца с номером  $y$ .

| Сложение |     |     |     | Умножение |     |   |     |     |
|----------|-----|-----|-----|-----------|-----|---|-----|-----|
|          | 0   | 1   | $a$ |           | 0   | 1 | $a$ |     |
| 0        | 0   | 1   | $a$ | $b$       | 0   | 0 | 0   | 0   |
| 1        | 1   | 0   | $b$ | $a$       | 1   | 0 | $a$ | $b$ |
| $a$      | $a$ | $b$ | 0   | 1         | $a$ | 0 | $b$ | 1   |
| $b$      | $b$ | $a$ | 1   | 0         | $b$ | 0 | $b$ | $a$ |

(11.2.1)

Мы приведем некоторые основные факты из теории конечных полей, отсылая читателя за деталями и доказательствами к книгам Алберта [2] или Дина [1].

Сравнение рациональных чисел по модулю  $m$ , записанное в виде

$$x \equiv y \pmod{m}, \quad (11.2.2)$$

по определению эквивалентно равенству

$$x - y = tm \quad (11.2.3)$$

при некотором целом  $t$ . Аналогичным образом сравнение можно определить для полиномов  $A(x)$  над полем  $F$  (т. е. для полиномов с коэффициентами из  $F$ ):

$$A(x) \equiv B(x) \pmod{f(x)}, \quad (11.2.4)$$

что по определению эквивалентно равенству

$$A(x) - B(x) = t(x)f(x) \quad (11.2.5)$$

для некоторого полинома  $t(x)$ . Все целые числа  $x$ , такие, что  $x \equiv b \pmod{m}$  при фиксированном  $b$  образуют класс вычетов по модулю  $m$ , который можно обозначить через  $\{b\}$  или  $b \pmod{m}$ . Если  $x \equiv b \pmod{m}$ ,  $y \equiv c \pmod{m}$ , то  $x + y \equiv b + c \pmod{m}$  и  $xy \equiv bc \pmod{m}$ , и тем самым определены сложение и умножение классов вычетов по модулю  $m$ :

$$\{b\} + \{c\} = \{b + c\} \text{ и } \{b\}\{c\} = \{bc\}. \quad (11.2.6)$$

Те же рассуждения применимы и к классам вычетов полиномов над полем  $F$  по модулю  $f(x)$ . В обоих случаях легко проверить, что все аксиомы поля, исключая M4, удовлетворяются для сложения и умножения классов вычетов, заданных посредством (11.2.6). Однако M4, вообще говоря, не удовлетворяется. Обычно существуют делители нуля. Так,

$$4 \cdot 3 \equiv 0 \pmod{6}, \quad (11.2.7)$$

а для полиномов над рациональным полем

$$(3x + 3)(5x - 5) \equiv 0 \pmod{x^2 - 1}. \quad (11.2.8)$$

Очевидно, что если M4 выполнена и  $xy = 0$ ,  $x \neq 0$ , то  $y = x^{-1}(xy) = x^{-1}0 = 0$ .

Далее, пусть  $p$  — рациональное простое число; основным свойством простых чисел (доказательство опускаем) является то, что если  $p \mid xy$  ( $p$  делит  $xy$ ), то либо  $p \mid x$ , либо  $p \mid y$ . Следовательно, в терминах сравнений, если

$$xy \equiv 0 \pmod{p}, \quad (11.2.9)$$

то

$$x \equiv 0 \pmod{p} \text{ или } y \equiv 0 \pmod{p}. \quad (11.2.10)$$

Поэтому из определения (11.2.3) следует, что если

$$ax \equiv ay \pmod{p}, \quad a \not\equiv 0 \pmod{p}, \quad (11.2.11)$$

то

$$x \equiv y \pmod{p}. \quad (11.2.12)$$

Существует точно  $p$  классов вычетов по модулю  $p$ , и мы можем взять  $0, 1, \dots, p-1$  в качестве представителей этих классов. Тогда если  $a \not\equiv 0 \pmod{p}$ , то числа  $a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)$  все находятся в силу (11.2.11) и (11.2.12) в различных классах вычетов и все  $\not\equiv 0 \pmod{p}$ . Мы можем применить „принцип ящиков“: если конечное число  $n$  объектов размещено в  $n$  ящиках, причем ни один из ящиков не содержит двух объектов, то каждый ящик содержит точно один объект. Если сравнить  $a \cdot 1, a \cdot 2, \dots, a \cdot (p-1) \pmod{p}$  и  $1, 2, \dots, p-1 \pmod{p}$ , то принцип ящиков показывает, что это одни и те же классы вычетов с точностью до порядка. Это дает два ценных следствия: во-первых, для некоторого  $x = 1, \dots, p-1$  мы имеем

$$ax \equiv 1 \pmod{p}, \quad (11.2.13)$$

и, следовательно,  $x$  является обратным к  $a$  элементом в системе классов вычетов по модулю  $p$ , т. е. М4 удовлетворяется. Во-вторых, перемножая, получаем

$$(a \cdot 1)(a \cdot 2) \dots (a \cdot (p-1)) \equiv 1 \cdot 2 \dots (p-1) \pmod{p}, \quad (11.2.14)$$

и, разделив на  $(p-1)!$ , поскольку  $(p-1)! \not\equiv 0 \pmod{p}$ , приходим к формуле

$$a^{p-1} \equiv 1 \pmod{p}; \quad (11.2.15)$$

это знаменитая теорема Ферма. Таким образом, (11.2.15) удовлетворяется при  $a \not\equiv 0 \pmod{p}$ . Если умножим

(11.2.15) на  $a$ , то получим

$$a^p \equiv a \pmod{p}, \quad (11.2.16)$$

что справедливо при всяком целом  $a \pmod{p}$ . Таким образом, вычеты по модулю  $p$  образуют конечное поле с  $p$  элементами, которое мы обозначим через  $J_p$  или  $\text{GF}(p)$ . ( $\text{GF}$  означает Galois field — поле Галуа.)

Если мы рассматриваем полиномы над полем  $F$ , то аналогом простого числа является неприводимый полином. Мы скажем, что полином  $f(x)$  степени  $n \geq 1$  неприводим над полем  $F$ , если не существует таких двух полиномов  $g(x)$  и  $h(x)$  над  $F$ , каждый степени меньшей  $n$ , что  $f(x) = g(x)h(x)$ . Основное свойство неприводимых полиномов (доказательство опускаем) состоит в том, что если неприводимый полином  $f(x)$  делит произведение  $A(x)B(x)$ , то он либо делит  $A(x)$ , либо делит  $B(x)$ .

Предположим, что  $f(x)$  неприводим над  $J_p$ . Если для полинома  $A(x)$  имеем

$$A(x) = f(x)q(x) + r(x), \quad (11.2.17)$$

то

$$A(x) \equiv r(x) \pmod{f(x)}, \quad (11.2.18)$$

и если  $f(x)$  имеет степень  $n$ , то мы можем взять  $r(x)$  степени не выше  $n - 1$ . Следовательно, по модулю  $f(x)$  мы имеем в качестве представителей классов вычетов полиномы

$$A(x) \equiv a_0 + a_1x + \dots + a_{n-1}x^{n-1} \pmod{f(x)}, \quad (11.2.19)$$

где каждое из  $a_0, a_1, \dots, a_{n-1}$  может быть любым из  $p$  элементов поля  $J_p$ . Следовательно, существует  $p^n$  классов вычетов по модулю  $f(x)$  над  $J_p$ .

Обозначим  $q = p^n$ , и пусть  $u_0 = 0, u_1 = 1, u_2, \dots, u_{q-1}$  — представители различных классов вычетов по модулю  $f(x)$ . Если  $y \equiv u_i \not\equiv 0 \pmod{f(x)}$ , то рассмотрим  $yu_1, \dots, yu_{q-1} \pmod{f(x)}$ .

Если  $yu_i \equiv yu_k \pmod{f(x)}$ , то  $y(u_i - u_k)$  делится на  $f(x)$ , и в силу неприводимости  $f(x)$  это означает, что  $y \equiv 0 \pmod{f(x)}$  или  $u_i \equiv u_k \pmod{f(x)}$ , ни одно из которых не может выполняться. Следовательно,  $yu_i \not\equiv yu_k \pmod{f(x)}$  при  $i \neq k$ , и аналогично  $yu_i \not\equiv 0 \pmod{f(x)}$

при  $i \neq 0$ . Таким образом, как и в случае вычетов по модулю  $p$ , мы можем применить принцип ящиков и заключить, что  $yu_1, \dots, yu_{q-1} (\text{mod } f(x))$  — это классы вычетов  $u_1, \dots, u_{q-1} (\text{mod } f(x))$  с точностью до порядка. В частности, при некотором  $u_i$

$$yu_i \equiv u_1 \equiv 1 (\text{mod } f(x)), \quad (11.2.20)$$

и здесь  $u_i$  — обратный к  $y$  элемент в совокупности классов вычетов; таким образом, аксиома М4 выполняется, и  $q = p^n$  вычетов образуют конечное поле, обозначаемое через  $\text{GF}(p^n)$ . Как следствие получаем, что

$$(yu_1)(yu_2) \dots (yu_{q-1}) \equiv u_1 u_2 \dots u_{q-1} (\text{mod } f(x)), \quad (11.2.21)$$

и, разделив на  $u_1 u_2 \dots u_{q-1}$ , в силу основного свойства неприводимого полинома  $f(x)$  приходим к сравнению

$$y^{q-1} \equiv 1 (\text{mod } f(x)), \quad (11.2.22)$$

выполняющемуся для любого полинома  $y \not\equiv 0 (\text{mod } f(x))$ . Умножая (11.2.22) на  $y$ , получаем

$$y^q \equiv y (\text{mod } f(x)), \quad (11.2.23)$$

что справедливо для любого полинома  $y = A(x)$  над  $J_p$ .

В качестве примера рассмотрим полином  $f(x) = x^2 + x + 1$ . Он неприводим над  $J_2$ , так как полиномы степени 1 над  $J_2$  — это только  $x$  и  $x + 1$ , и ни один из них не делит  $x^2 + x + 1$ . Таким образом, вычеты 0, 1,  $x$ ,  $x + 1 (\text{mod } x^2 + x + 1)$  образуют конечное поле  $\text{GF}(2^2)$ . Эти вычеты соответствуют элементам 0, 1,  $a$ ,  $b$  из примера, данного в начале этого раздела, сложение и умножение которых определено таблицами (11.2.1).

Поля  $\text{GF}(p^n)$  — это фактически все конечные поля, и для всякой степени простого числа  $p^n$  существует поле  $\text{GF}(p^n)$ . Следующие теоремы дают основные свойства конечных полей. За доказательствами отсылаем читателя к книгам Алберта [2] или Дина [1]<sup>1)</sup>.

**Теорема 11.2.1.** Число элементов в конечном поле равно степени простого числа  $p^n$ . Для всякой степени

<sup>1)</sup> См. также З. И. Боревич, И. Р. Шафаревич, „Теория чисел“, М., 1964. — Прим. ред.

простого числа  $p^n$  существует конечное поле  $GF(p^n)$ , единственное с точностью до изоморфизма. Это поле  $GF(p^n)$  можно представить как множество всех классов вычетов по модулю произвольного полинома  $f(x)$  степени  $n$ , неприводимого над  $J_p$ .

**Теорема 11.2.2.** В поле  $GF(p^n)$   $p^n - 1$  элементов, отличных от 0, образуют циклическую группу по умножению. Образующий элемент этой мультипликативной группы называется примитивным корнем<sup>1)</sup> поля  $GF(p^n)$ .

**Теорема 11.2.3.** Автоморфизмы поля  $GF(p^n)$  образуют циклическую группу порядка  $n$ , которая порождается автоморфизмом  $a: x \rightarrow x^p$  для всякого  $x \in GF(p^n)$ .

**Теорема 11.2.4.** Подполе поля  $GF(p^n)$  — это в точности поля  $GF(p^m)$ , где  $m$  делит  $n$ . Для всякого  $m$ , делящего  $n$ , поле  $GF(p^n)$  имеет единственное подполе  $GF(p^m)$ , состоящее из элементов  $GF(p^n)$ , удовлетворяющих уравнению  $z^{p^m} = z$ . Примитивный корень  $x$  поля  $GF(p^n)$  удовлетворяет уравнению  $g(x) = 0$ , где  $g(x)$  — неприводимый над  $GF(p^m)$  полином степени  $n/m$ .

Проиллюстрируем содержание этих теорем несколькими примерами. Так как  $25 = 5^2$  есть степень простого числа, существует поле  $GF(5^2)$  с 25 элементами, и оно может быть представлено классами вычетов по модулю  $f(x)$ , где  $f(x)$  — неприводимый над  $J_5$  полином степени 2;  $f_1(x) = x^2 - 2$  и  $f_2(x) = x^2 + x + 1$  — два таких неприводимых полинома. Таким образом, мы имеем два поля,  $F_1$  и  $F_2$ , с 25 элементами. Теорема 11.2.1 утверждает, что  $F_1$  и  $F_2$  изоморфны. Элемент  $y \equiv 2x + 1 \pmod{x^2 + x + 1}$  удовлетворяет сравнению

$$y^2 \equiv 4x^2 + 4x + 1 \equiv -4 + 1 \equiv 2 \pmod{x^2 + x + 1}.$$

Отображение

$$ax + b \pmod{x^2 - 2} \rightarrow a(2x + 1) + b \pmod{x^2 + x + 1},$$

как легко проверить, есть изоморфизм между  $F_1$  и  $F_2$ . Полином  $f(x) = x^6 + x^5 + x^3 + x^2 + 1$  неприводим над  $J_2$ , поэтому вычеты  $A(x) \pmod{f(x)}$  образуют поле  $GF(2^6)$ .

<sup>1)</sup> Или первообразным элементом. — Прим. перев.

с 64 элементами. В этом поле  $x$  есть примитивный корень, а степени  $x$ , элементы  $1, x, x^2, \dots, x^{62}$ , дают 63 ненулевых элемента поля  $GF(2^6)$ . Подполями поля  $GF(2^6)$  являются  $GF(2)$ ,  $GF(2^2)$  и  $GF(2^3)$ . Поле  $GF(2)$  состоит из элементов  $0, 1$ ;  $GF(2^2)$  – из элементов  $0, 1, x^{21}, x^{42}$ ; они удовлетворяют уравнению  $z^4 = z$ . Поле  $GF(2^3)$  состоит из элементов  $0, 1, x^9, x^{18}, x^{27}, x^{36}, x^{45}, x^{54}$ ; они удовлетворяют уравнению  $z^8 = z$ . Автоморфизмы образуют циклическую группу порядка 6, которая порождается автоморфизмом  $\alpha$ :  $z \rightarrow z^2 = (z)\alpha$  для всякого  $z \in GF(2^6)$ . Например,

$$\begin{aligned} (x + x^2 + x^3)\alpha &= x^2 + x^4 + x^6 = \\ &= x^2 + x^4 + (x^5 + x^3 + x^2 + 1) = \\ &= x^5 + x^4 + x^3 + 1. \end{aligned}$$

Если мы возьмем  $w = x^{21} = x^4 + x^2 + x + 1$ , то  $x^3 + wx^2 + wx + w = 0$ , и полином  $F(x) = x^3 + wx^2 + wx + w$  неприводим над полем  $GF(2^2)$ , состоящим из элементов  $0, 1, w, w+1$ , где  $w^2 + w + 1 = 0$ . Мы можем проверить неприводимость  $F(x)$  над  $GF(2^2)$ , замечая, что если бы  $F(x)$  имел линейный множитель, то он должен был бы иметь корнем один из элементов  $0, 1, w$  или  $w+1$ , чего в действительности нет.

### 11.3. Теорема Зингера

Пусть  $F$  – произвольное поле. Пространство всех векторов  $(a_0, \dots, a_n)$ ,  $a_i \in F$ , называется *проективной геометрией* размерности  $n$  над  $F$  и обозначается через  $PG(n, F)$ . Нулевой вектор  $0 = (0, \dots, 0)$  есть пустое пространство, и мы скажем, что пустое пространство имеет размерность  $-1$ . Точка  $P$ , пространство размерности  $0$ , – это множество векторов

$$bx = (bx_0, \dots, bx_n),$$

где  $x = (x_0, \dots, x_n) \neq 0$ , а  $b$  пробегает все элементы поля  $F$ . Вообще если  $y_0, \dots, y_k$  – это  $k+1$  независимых векторов, то множество всех векторов

$$b_0y_0 + \dots + b_ky_k, \quad b_i \in F,$$

есть подпространство  $S_k$  размерности  $k$ . Подпространство размерности  $n - 1$  называется *гиперплоскостью*. Нетрудно показать, что точки, общие двум различным гиперплоскостям, образуют подпространство размерности  $n - 2$ . Если  $(c_0, \dots, c_n) \neq (0, \dots, 0)$ , то можно показать, что множество всех векторов  $(x_0, \dots, x_n)$ , удовлетворяющих равенству

$$c_0x_0 + \dots + c_nx_n = 0, \quad (11.3.1)$$

есть гиперплоскость, и, обратно, что каждая гиперплоскость может быть определена таким образом, причем  $(c_0, \dots, c_n)$  и  $(sc_0, \dots, sc_n)$ ,  $s \neq 0$ , определяют одну и ту же плоскость.

Если поле  $F$  есть конечное поле  $GF(p^r)$ , то существует  $q^{n+1}$  (здесь  $q = p^r$ ) векторов  $(x_0, \dots, x_n)$ ,  $x_i \in GF(p^r)$ . Каждый из  $q^{n+1} - 1$  векторов, отличных от 0, определяет точку, и, поскольку  $(x_0, \dots, x_n)$  и  $(bx_0, \dots, bx_n)$ ,  $b \neq 0$ , определяют одну и ту же точку, всего имеется  $v = (q^{n+1} - 1)/(q - 1)$  точек. Аналогично, поскольку  $(c_0, \dots, c_n) \neq (0, \dots, 0)$  и  $(sc_0, \dots, sc_n)$ ,  $s \neq 0$ , определяют одну и ту же гиперплоскость, существует  $v$  гиперплоскостей. Если  $y_0, \dots, y_t$  — это  $t + 1$  независимых векторов, то линейные комбинации  $b_0y_0 + \dots + b_ty_t$ ,  $b_i \in GF(p^r)$ , дают  $q^{t+1}$  различных векторов. Исключая нулевой вектор, имеем  $(q^{t+1} - 1)/(q - 1)$  различных точек в этом пространстве  $S_t$  размерности  $t$ . Таким образом, гиперплоскость имеет  $k = (q^n - 1)/(q - 1)$  различных точек, а пространство  $S_{n-2}$  имеет  $\lambda = (q^{n-1} - 1)/(q - 1)$  точек. Мы обозначим эту геометрию через  $PG(n, p^r)$ .

**Теорема 11.3.1 (теорема Зингера [1]). Гиперплоскости геометрии  $PG(n, p^r)$ ,  $q = p^r$ , взятые в качестве блоков, и точки, взятые в качестве элементов, образуют симметричную блок-схему с параметрами**

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^n - 1}{q - 1}, \quad \lambda = \frac{q^{n-1} - 1}{q - 1}.$$

*Эта схема является циклической, и точки в любой гиперплоскости определяют  $(v, k, \lambda)$ -разностное множество.*

**Доказательство.** Заметим, что при  $v, k, \lambda$ , данных в теореме,  $PG(n, p^r)$  имеет  $v$  точек и  $v$  гиперплоскостей.

скостей, каждая гиперплоскость содержит  $k$  точек, и две различные гиперплоскости пересекаются по подпространству  $S_{n-2}$ , которое имеет  $\lambda$  точек. Таким образом, гиперплоскости, взятые в качестве блоков, образуют  $(v, k, \lambda)$ -блок-схему. Это несложно. Основная часть теоремы состоит в доказательстве цикличности этой схемы.

Пусть  $x$  — примитивный корень поля  $GF(q^{n+1})$ . Тогда (по теореме 11.2.4)  $x$  есть корень полинома  $F(y)$  степени  $n+1$ , неприводимого над  $GF(q)$ . Пусть

$$F(y) = y^{n+1} + c_n y^n + \dots + c_1 y + c_0, \quad c_i \in GF(q). \quad (11.3.2)$$

Поскольку  $F(x) = 0$ , то  $x^{n+1} = -c_0 - c_1 x - \dots - c_n x^n$ . Отсюда следует, что для любой степени  $x$  мы можем записать

$$x^i = a_0 + a_1 x + \dots + a_n x^n, \quad a_j \in GF(q). \quad (11.3.3)$$

Тем самым устанавливается соответствие между  $x^i$  и вектором  $(a_0, \dots, a_n)$  над  $GF(q)$ . Все  $q^{n+1} - 1$  различных степеней  $x$  соответствуют  $q^{n+1} - 1$  различным векторам  $(a_0, \dots, a_n)$  над  $GF(q)$  за исключением нулевого вектора. Если мы положим  $v = (q^{n+1} - 1)/(q - 1)$ , то  $0, 1, x^v, \dots, x^{(q-2)v}$  дадут  $q$  решений уравнения  $z^q = z$ , и они будут образовывать подполе  $GF(q)$  поля  $GF(q^{n+1})$ . Если  $x^{sv} = t$ , то  $t \in GF(q)$ , и потому если (11.3.3) выполняется, то

$$x^{i+sv} = ta_0 + ta_1 x + \dots + ta_n x^n. \quad (11.3.4)$$

Следовательно,  $x^i$  и  $x^j$  соответствуют одной и той же точке из  $PG(n, q)$  тогда и только тогда, когда  $i \equiv j \pmod{v}$ . Таким образом, если задано отображение  $\alpha$  поля  $GF(q^{n+1})$ :

$$\begin{aligned} \alpha: 0 &\rightarrow 0, \\ \alpha: x^i &\rightarrow x^{i+1}, \end{aligned} \quad (11.3.5)$$

то ввиду (11.3.3) и (11.3.2) отображение векторов над  $GF(q)$  имеет вид

$$\begin{aligned} \alpha: (a_0, a_1, \dots, a_n) &\rightarrow \\ &\rightarrow (-a_n c_0, a_0 - a_n c_1, \dots, a_{n-1} - a_n c_n). \end{aligned} \quad (11.3.6)$$

Как показывает формула (11.3.6), стображение  $\alpha$  фактически есть отображение точек в точки и по существу пространств  $S_m$  на пространства  $S_m$ , так как если  $u_0, \dots, u_m$  — независимые векторы, то при  $b_0, \dots, b_m \in GF(q)$

$$(b_0 u_0 + \dots + b_m u_m) \alpha = b_0(u_0) \alpha + \dots + b_m(u_m) \alpha. \quad (11.3.7)$$

Поскольку  $x^{v(q-1)} = 1$ , отображение (11.3.5) является взаимно однозначным, и потому взаимно однозначно отображение (11.3.6). Далее, так как  $x^i$  и  $x^{i+v}$  соответствуют одной и той же точке, а  $1, x, \dots, x^{v-1}$  соответствуют различным точкам, отображение  $\alpha$  в (11.3.6) переставляет все  $v$  точек по единственному циклу. Заметим теперь, что поскольку  $v - qk = 1$ , то  $k$  и  $v$  взаимно просты. Если  $\alpha^j$  для некоторого  $j \neq 0$  переводит точки некоторой плоскости сами в себя, то  $\alpha^j$  переставляет их по циклам длины  $t$ , где  $t$  делит  $k$ . Но тогда, поскольку  $\alpha^v = 1$ ,  $t$  должно быть также делителем  $v$ , и, раз  $v - qk = 1$ , то имеем  $t = 1$  и  $\alpha^j = 1$ . Тогда, вследствие того, что никакая степень  $\alpha$ , исклучая  $\alpha^v = 1$ , не фиксирует гиперплоскость,  $\alpha$  должно переставлять гиперплоскости по циклу длины  $v$ . Это доказывает, что блок-схема  $B$  из  $v$  точек и  $v$  гиперплоскостей, где каждая из гиперплоскостей содержит  $k$  точек, есть циклическая блок-схема. Доказательство теоремы завершено.

Приведем пример на применение теоремы Зингера. Пусть  $q = 2^2$ ,  $n = 2$ . Здесь  $GF(q^{n+1}) = GF(2^6)$ . Тогда  $GF(q) = GF(2^2)$  можно взять как расширение поля  $J_2$  с элементами  $0, 1, w, w+1$ , где  $w^2 + w + 1 = 0$ . Как было замечено в разд. 11.2, примитивный корень  $x$  поля  $GF(2^6)$  удовлетворяет неприводимому уравнению  $x^3 + wx^2 + wx + w = 0$  над  $GF(2^2)$ . Это дает для  $1, x, \dots, x^{21}$  равенства

$$\begin{aligned} 1 &= 1, \\ x &= && x, \\ x^2 &= && x^2, \\ x^3 = w &+ && wx + wx^2, \\ x^4 = w + 1 &+ && x + x^2, \end{aligned}$$

$$\begin{aligned}
 x^5 &= w &+& x + (w+1)x^2, \\
 x^6 &= 1 &+& (w+1)x, \\
 x^7 &= && x + (w+1)x^2, \\
 x^8 &= 1 &+& x, \\
 x^9 &= && x + x^2, \\
 x^{10} &= w &+& wx + (w+1)x^2, \\
 x^{11} &= 1 &+& (w+1)x + (w+1)x^2, \\
 x^{12} &= 1 &+& w x^2, \\
 x^{13} &= w + 1 &+& wx + (w+1)x^2, \\
 x^{14} &= 1 &+& wx + (w+1)x^2, \\
 x^{15} &= 1 &+& (w+1)x^2, \\
 x^{16} &= 1 &+& x^2, \\
 x^{17} &= w &+& (w+1)x + wx^2, \\
 x^{18} &= w + 1 &+& x, \\
 x^{19} &= && (w+1)x + x^2, \\
 x^{20} &= w &+& wx + x^2, \\
 x^{21} &= w.
 \end{aligned} \tag{11.3.8}$$

Так как  $x^v = x^{21} = w \in GF(2^2)$ , отображение  $x^i \rightarrow x^{i+1}$  переставляет точки  $PG(2, 2^2)$  по циклу длины 21. Если  $x^i = a_0 + a_1x + a_2x^2$ , то точки  $(a_0, a_1, a_2)$  с  $a_2 = 0$  лежат в гиперплоскости („гиперплоскость“ – „прямая“ в плоскости). Если точки, соответствующие  $x^i$ ,  $i = 0, \dots, 20$ , заменить вычетами  $i \pmod{21}$ , то точки с  $a_2 = 0$  – это

$$0, 1, 6, 8, 18 \pmod{21}. \tag{11.3.9}$$

Эти вычеты образуют  $(21, 5, 1)$ -разностное множество, что легко показать непосредственно, и дают  $(21, 5, 1)$ -блок-схему с блоками

$$B_i = \{i, i+1, i+6, i+8, i+18\} \pmod{21}.$$

Аналогично тот же примитивный корень  $x$  поля  $GF(2^6)$  удовлетворяет над  $GF(2)$  уравнению

$$f(x) = x^6 + x^5 + x^3 + x^2 + 1 = 0, \tag{11.3.10}$$

и мы имеем

$$x^i = p_i + q_i x + r_i x^2 + s_i x^3 + t_i x^4 + u_i x^5. \tag{11.3.11}$$

Точки в  $PG(5, 2)$  с  $u_i = 0$  образуют гиперплоскость размерности 4. С помощью (11.3.10) мы можем проверить,

что для любого  $n$

$$u_{n+6} = u_{n+5} + u_{n+3} + u_{n+2} + u_n, \quad (11.3.12)$$

а из формулы (11.3.11) следует, что

$$u_0 = u_1 = u_2 = u_3 = u_4 = 0, \quad u_5 = 1. \quad (11.3.13)$$

При помощи (11.3.12) и (11.3.13) мы можем вычислить те индексы  $i$  по модулю  $63 = v$ , для которых  $u_i = 0$ . Существует  $k = 31$  таких индексов, а  $\lambda = 15$ . Таким образом, имеем следующее  $(61, 31, 15)$ -разностное множество:

$$\begin{aligned} 0, 1, 2, 3, 4, 8, 9, 10, 11, 13, 14, 16, 17, 18, 21, 24, 25, \\ 27, 30, 32, 36, 41, 42, 45, 46, 47, 49, 51, \\ 53, 54, 61 \pmod{63}. \end{aligned} \quad (11.3.14)$$

Для применения теоремы Зингера достаточно найти уравнение вида (11.3.10) для примитивного корня  $\text{GF}(q^{n+1})$  и подсчитать соответствующие  $u_i$  из рекуррентного соотношения, соответствующего формуле (11.3.12). Иметь примитивный корень поля  $\text{GF}(q^{n+1})$  необязательно, но нужно иметь элемент  $x$ , такой, что  $x^v$  есть первая из степеней  $x$ , принадлежащая  $\text{GF}(q)$ .

#### 11.4. Теорема о множителе

Разностное множество  $0, 1, 3, 9 \pmod{13}$  обладает следующим свойством: если его элементы умножить на 3, то в результате получим те же элементы, лишь в другом порядке. Умножение элементов  $0+i, 1+i, 3+i, 9+i \pmod{13}$  на 3 переводит эти вычеты в  $0+3i, 3+3i, 9+3i, 1+3i \pmod{13}$  или, что то же самое, блок  $B_i$  — в блок  $B_{3i}$ , где  $i = 0, \dots, 12 \pmod{13}$ , циклической блок-схемы, данной в (11.1.1). Это показывает, что отображение  $x \rightarrow 3x \pmod{13}$ ,  $B_i \rightarrow B_{3i}$  вычетов по модулю 13 и блоков порождает автоморфизм схемы. Конечно, это еще один автоморфизм схемы, в дополнение к циклическому автоморфизму  $i \rightarrow i+1$ ,  $B_i \rightarrow B_{i+1}$ , который определял саму схему по разностному множеству  $0, 1, 3, 9 \pmod{13}$ .

**Определение.** Целое число  $t$  называется **множителем** циклического разностного множества  $a_1, \dots, a_k \pmod{v}$ ,

если  $x \rightarrow xt \pmod{v}$  есть автоморфизм циклической блок-схемы.

Заметим, что  $t$  является множителем тогда и только тогда, когда  $x \rightarrow xt$  отображает разностное множество  $a_1, \dots, a_k$  на другой блок, т. е.  $ta_1, \dots, ta_k \pmod{v}$  — это  $a_1 + s, \dots, a_k + s \pmod{v}$  с точностью до порядка при подходящем  $s$ . Так как 1 должна появляться в качестве разности,  $1 = a_i - a_j$  и также  $1 \equiv ta_r - ta_s \pmod{v}$ , то, очевидно, множитель  $t$  должен быть взаимно прост с  $v$ . Отсюда следует, что множители образуют мультипликативную группу по модулю  $v$ . Так, например, 2 есть множитель разностного множества  $a_1, \dots, a_{31} \pmod{63}$ , указанного в (11.3.14), так как  $2a_1, \dots, 2a_{31} \pmod{63}$ , очевидно, является перестановкой вычетов  $a_1 + 18, a_2 + 18, \dots, a_{31} + 18 \pmod{63}$ .

Брук, распространивший идею разностного множества с циклического случая на случай групповых разностных множеств, заметил, что множитель  $t$  циклического разностного множества — это фактически автоморфизм  $x \rightarrow xt \pmod{v}$  группы, лежащей в основе схемы (здесь — циклической группы порядка  $v$ ), одновременно являющийся автоморфизмом блок-схемы. Точное определение множителя для общего случая таково:

**Определение.** Если  $x \rightarrow (x)\theta$  есть автоморфизм группы  $G$ , то  $\theta$  называется *множителем* группового разностного множества  $D = \{a_1, \dots, a_k\}$ , если  $D\theta = aDb$  при подходящих  $a, b \in G$ .

Например, если  $D = \{a, b, c, d, ab, cd\}$  — разностное множество в абелевой группе  $G$ , порожденной элементами  $a, b, c, d$ , где  $a^2 = b^2 = c^2 = d^2 = 1$ , то  $D\theta_i = D$  при

$$\theta_1: a \rightarrow b, b \rightarrow a, c \rightarrow d, d \rightarrow c,$$

$$\theta_2: a \rightarrow c, b \rightarrow d, c \rightarrow a, d \rightarrow b,$$

$$\theta_3: a \rightarrow d, b \rightarrow c, c \rightarrow b, d \rightarrow a,$$

$$\theta_4: a \rightarrow b, b \rightarrow a, c \rightarrow c, d \rightarrow d.$$

Знание множителя оказывает большую помощь при построении разностных множеств или доказательстве их несуществования. Замечателен факт, что неизвестно ни одного циклического разностного множества, не обла-

дающего некоторым нетривиальным множителем. Следующей теоремой, принадлежащей Холлу и Райзеру [1], устанавливается во многих случаях существование множителей.

**Теорема 11.4.1 (теорема о множителе).** *Если  $\{a_1, \dots, a_k\} \pmod v$  — циклическое разностное множество, где  $k(k-1) = \lambda(v-1)$ , и если  $p$  — простое число, делящее  $n = k - \lambda$ , такое, что  $(p, v) = 1$  и  $p > \lambda$ , то  $p$  — множитель указанного разностного множества.*

**Доказательство.** Рассмотрим кольцо  $R(x, x^{-1})$  полиномов от  $x$  и  $x^{-1}$  с целыми коэффициентами. Заметим, что в  $R$  имеем  $x^i \equiv x^j \pmod{x^v - 1}$  тогда и только тогда, когда  $i \equiv j \pmod{v}$ . Разностному множеству  $D = \{a_1, \dots, a_k\} \pmod v$  мы можем поставить в соответствие полином  $\theta(x) = x^{a_1} + x^{a_2} + \dots + x^{a_k}$ . Тогда, поскольку  $D$  — разностное множество, то

$$\theta(x)\theta(x^{-1}) \equiv k + \lambda(x + \dots + x^{v-1}) \pmod{x^v - 1}. \quad (11.4.1)$$

Действительно, левая часть равна

$$\sum_{i, j=1}^k x^{a_i - a_j},$$

и мы получаем 0 как разность  $a_i - a_j$  в  $k$  случаях и любое  $d \not\equiv 0 \pmod v$  как разность в  $\lambda$  случаях. Если обозначить  $n = k - \lambda$  и  $T(x) = 1 + x + \dots + x^{v-1}$ , то (11.4.1) примет вид

$$\theta(x)\theta(x^{-1}) \equiv n + \lambda T(x) \pmod{x^v - 1}. \quad (11.4.2)$$

Если  $t$  — множитель, то тот факт, что  $ta_1, \dots, ta_k \pmod v$  — это  $a_1 + s, \dots, a_k + s \pmod v$  при подходящем  $s$ , можно выразить в виде

$$\theta(x^t) \equiv x^s \theta(x) \pmod{x^v - 1}. \quad (11.4.3)$$

Так как  $x^v - 1 = (x - 1)T(x)$  и по предположению  $p \mid n$ , из (11.4.2) следует, что

$$\theta(x)\theta(x^{-1}) \equiv 0 \pmod{p, T(x)}, \quad (11.4.4)$$

где  $A(x) \equiv B(x) \pmod{p, T(x)}$  означает, что  $A(x) - B(x) = pU(x) + T(x)V(x)$  для подходящих полиномов  $U(x)$

и  $V(x)$ . Умножив (11.4.4) на  $\theta(x)^{p-1}$ , мы получим

$$\theta(x)^p \theta(x^{-1}) \equiv 0 \pmod{p, T(x)}. \quad (11.4.5)$$

Так как все биномиальные коэффициенты  $\binom{p}{i}$ ,  $i=1, \dots, p-1$ , кратны  $p$ , для любых полиномов  $A(x)$ ,  $B(x)$  имеем

$$(A(x) + B(x))^p \equiv A(x)^p + B(x)^p \pmod{p}, \quad (11.4.6)$$

и повторным применением этого правила находим, что

$$\theta(x)^p \equiv \theta(x^p) \pmod{p}. \quad (11.4.7)$$

Следовательно, подставляя выражение для  $\theta(x)^p$  в (11.4.5), получаем, что

$$\theta(x^p) \theta(x^{-1}) \equiv 0 \pmod{p, T(x)}. \quad (11.4.8)$$

Взяв этот результат по модулю  $x^v - 1$ , приходим к сравнению

$$\theta(x^p) \theta(x^{-1}) \equiv pR(x) + A(x)T(x) \pmod{x^v - 1}. \quad (11.4.9)$$

Так как  $x^v T(x) \equiv T(x) \pmod{x^v - 1}$ , то  $A(x)T(x) \equiv A(1)T(x) \pmod{x^v - 1}$  и, следовательно,

$$\theta(x^p) \theta(x^{-1}) \equiv pR(x) + A(1)T(x) \pmod{x^v - 1}. \quad (11.4.10)$$

Полагая в (11.4.10)  $x = 1$ , имеем

$$k^2 = pR(1) + A(1)v. \quad (11.4.11)$$

Но

$$k^2 = k - \lambda + \lambda v = n + \lambda v, \quad (11.4.12)$$

и поскольку  $p \nmid n$ , получаем

$$A(1)v \equiv \lambda v \pmod{p}, \quad (11.4.13)$$

а так как  $p \nmid v$ , то

$$A(1) \equiv \lambda \pmod{p}, \quad (11.4.14)$$

следовательно,  $A(1) = \lambda + pm$  при некотором целом  $m$ . Таким образом, (11.4.10) принимает вид

$$\theta(x^p) \theta(x^{-1}) \equiv pS(x) + \lambda T(x) \pmod{x^v - 1}, \quad (11.4.15)$$

где  $S(x) = R(x) + mT(x)$ .

Подставляя теперь в (11.4.15)  $x = 1$ , получаем

$$k^2 = pS(1) + \lambda v, \quad (11.4.16)$$

и в силу (11.4.12) отсюда следует, что

$$pS(1) = n. \quad (11.4.17)$$

В формуле (11.4.15) заменим  $x$  на  $x^{-1}$  и заметим, что модуль при этом не изменится, так как  $x^{-v} - 1 = -x^{-v}(x^v - 1)$ ,  $x^{-v} \equiv 1 \pmod{x^v - 1}$ , и что  $T(x^{-1}) \equiv T(x) \pmod{x^v - 1}$ . Таким образом, получается, что

$$\theta(x^{-p})\theta(x) \equiv pS(x^{-1}) + \lambda T(x) \pmod{x^v - 1}. \quad (11.4.18)$$

Имеем теперь четыре соотношения:

$$\begin{aligned} \theta(x)\theta(x^{-1}) &\equiv n + \lambda T(x) \pmod{x^v - 1}; \\ \theta(x^p)\theta(x^{-p}) &\equiv n + \lambda T(x) \pmod{x^v - 1}; \\ \theta(x^p)\theta(x^{-1}) &\equiv pS(x) + \lambda T(x) \pmod{x^v - 1}; \\ \theta(x^{-p})\theta(x) &\equiv pS(x^{-1}) + \lambda T(x) \pmod{x^v - 1}. \end{aligned} \quad (11.4.19)$$

Первое соотношение — это (11.4.2). Второе выражает тот факт, что  $\{pa_1, \dots, pa_k\} \pmod{v}$  наряду с  $\{a_1, \dots, a_k\} \pmod{v}$  также является разностным множеством, так как если  $a_i - a_j \equiv d \pmod{v}$ , то  $pa_i - pa_j \equiv pd$ , поэтому когда  $d$  пробегает все вычеты  $\not\equiv 0 \pmod{v}$ , то, поскольку  $(p, v) = 1$ ,  $pd$  также пробегает все вычеты  $\not\equiv 0 \pmod{v}$ . Произведение левых частей первых двух сравнений в (11.4.19) равно произведению левых частей третьего и четвертого сравнений. Следовательно, произведения соответствующих правых частей сравнимы, и мы имеем

$$\{pS(x) + \lambda T(x)\}\{pS(x^{-1}) + \lambda T(x)\} \equiv (n + \lambda T(x))^2 \pmod{x^v - 1}. \quad (11.4.20)$$

Так как  $pS(x)T(x) \equiv pS(1)T(x) \equiv nT(x) \pmod{x^v - 1}$ , (11.4.20) можно упростить:

$$p^2 S(x)S(x^{-1}) \equiv n^2 \pmod{x^v - 1}. \quad (11.4.21)$$

Далее, впервые воспользуемся условием  $p > \lambda$  из предположений теоремы. В (11.4.15) каждый коэффициент в  $\theta(x^p)\theta(x^{-1})$  — неотрицательное целое число, и это свойство не меняется при редукции по модулю  $x^v - 1$ .

Следовательно, если

$$\theta(x^p)\theta(x^{-1}) \equiv a_0 + a_1x + \dots + a_{v-1}x^{v-1} \pmod{x^v - 1}, \quad (11.4.22)$$

то  $a_i \geq 0$  при  $i = 0, \dots, v-1$ . Ввиду (11.4.15)

$$a_i \equiv \lambda \pmod{p}, \quad i = 0, \dots, v-1.$$

Поэтому из предположения  $p > \lambda$  вытекает, что  $a_i \geq \lambda$ , следовательно,

$$\theta(x^p)\theta(x^{-1}) - \lambda T(x) \equiv pS(x) \pmod{x^v - 1} \quad (11.4.23)$$

имеет неотрицательные коэффициенты и  $S(x)$  тоже имеет неотрицательные коэффициенты. Но если в

$$S(x) \equiv b_0 + b_1x + \dots + b_{v-1}x^{v-1} \pmod{x^v - 1}$$

хотя бы два коэффициента положительны, скажем,  $b_i > 0$  и  $b_j > 0$ , то в левой части (11.4.21) найдется член  $b_i b_j x^{i-j}$  с  $b_i b_j > 0$  и нет никакого отрицательного члена, сокращающегося с ним, а это противоречит тому, что в правой части коэффициент при  $x^{i-j}$  равен нулю. Следовательно,  $S(x)$  — одночлен (скажем,  $wx^s$ ) и

$$pS(x) \equiv pwx^s \equiv nx^s \pmod{x^v - 1}, \quad (11.4.24)$$

так как  $pS(1) = n$  в силу (11.4.17).

Подставляя теперь (11.4.24) в (11.4.15), получаем

$$\theta(x^p)\theta(x^{-1}) \equiv nx^s + \lambda T(x) \pmod{x^v - 1}. \quad (11.4.25)$$

Умножим (11.4.25) на  $\theta(x)$ :

$$\theta(x^p)\theta(x)\theta(x^{-1}) \equiv nx^s\theta(x) + \lambda\theta(x)T(x) \pmod{x^v - 1}. \quad (11.4.26)$$

Из (11.4.2) и сравнения

$$\theta(x)T(x) \equiv \theta(1)T(x) \equiv kT(x) \pmod{x^v - 1} \quad (11.4.27)$$

находим, что

$$\theta(x^p)(n + \lambda T(x)) \equiv nx^s\theta(x) + \lambda kT(x) \pmod{x^v - 1} \quad (11.4.28)$$

и, стало быть,

$$n\theta(x^p) \equiv nx^s\theta(x) \pmod{x^v - 1}. \quad (11.4.29)$$

Разделив на  $n$ , получим, что

$$\theta(x^p) \equiv x^s \theta(x) \pmod{x^v - 1}. \quad (11.4.30)$$

Сравнение с (11.4.3) показывает, что  $t = p$  — множитель.

Условие  $p > \lambda$ , которое использовалось для получения (11.4.24) из (11.4.15) и (11.4.21), по-видимому, необязательно. Для каждого известного разностного множества простое число  $p$  есть множитель, если  $p|n$  и  $(p, v) = 1$ . Но мы не можем заключить только из (11.4.21), что  $S(x)$  — одночлен по модулю  $x^v - 1$ , как это видно из следующего примера:

$$(-1 + 2x^a + 2x^{2a})(-1 + 2x^{-a} + 2x^{-2a}) \equiv 9 \pmod{x^{3a} - 1}. \quad (11.4.31)$$

## 11.5. Разностные множества в группах общего вида

Некоторые результаты теории циклических разностных множеств можно обобщить на теорию разностных множеств в любой конечной группе. Пусть  $D = \{a_1, \dots, a_k\}$  есть  $(v, k, \lambda)$ -разностное множество в группе  $G$  порядка  $v$ . Тогда некоторый элемент  $P$  можно выбрать в качестве базисной точки, и элементы схемы — это  $Pg$ ,  $g \in G$ , с базисной точкой  $P$ , представленной единицей группы  $G$ . Если в качестве базисной выбрана другая точка  $Q = Pg_1$ , то, поскольку  $Qg = Pg_1g$ , элемент, соответствующий  $g_1g$  при первом выборе базисной точки, соответствует  $g$  при втором выборе.

Таким образом, в нашей блок-схеме умножение всех элементов  $g$  группы слева на фиксированный элемент  $g_1$  соответствует просто изменению базисной точки. Аналогично  $D = \{a_1, \dots, a_k\}$  есть базисный блок нашей схемы, а  $Dg_2 = \{a_1g_2, \dots, a_kg_2\}$  — другой ее блок. Следовательно, при изменении базисной точки и замене одного базисного блока другим разностное множество  $D$  переходит в  $g_1Dg_2$ , где в качестве  $g_1$  и  $g_2$  мы можем взять любые два элемента группы  $G$ .

Как уже упоминалось, Брук [1] заметил, что множитель циклического разностного множества — это автоморфизм группы, являющийся также автоморфизмом блок-схемы. Пусть  $\alpha: g \rightarrow g^a$  — автоморфизм группы  $G$ .

Будем говорить, что  $a$  есть **множитель** разностного множества, если существуют элементы  $g_1, g_2$  группы  $G$ , такие, что

$$D^a = g_1 D g_2. \quad (11.5.1)$$

Назовем  $a$  **правым множителем**, если  $D^a = D g_2$ .

**Теорема 11.5.1** (Брук). *Пусть  $K$  — симметричная блок-схема, определенная разностным множеством  $D$  из  $k$  элементов группы  $G$  порядка  $v$ . Пусть  $N$  — нормализатор группы  $G$  в группе  $X$  всех автоморфизмов  $K$ . Тогда необходимым и достаточным условием того, чтобы отображение  $T$  схемы  $K$  на себя содержалось в  $N$ , является выполнение при всех  $x, y \in G$  равенств*

$$(Px)T = Pa^{-1}x^a, \quad (By)T = Bby^a, \quad (11.5.2)$$

где  $P$  — базисная точка,  $B$  — базисный блок,  $a$  — множитель  $D$ , такой, что  $D^a = aDb$ . Кроме того,  $N/G$  изоморфна группе правых множителей  $D$ .

**Доказательство.** Сначала предположим, что  $T$  определяется равенствами (11.5.2). Тогда  $T$  — взаимно однозначное отображение элементов и блоков  $K$  на себя. Если  $Px$  содержится в  $By$ , то  $xy^{-1} \in D$  и

$$(a^{-1}x^a)(by^a)^{-1} = a^{-1}(xy^{-1})^a b^{-1} \in a^{-1}D^a b^{-1} = D,$$

значит,  $(Px)T$  содержится в  $(By)T$ . Следовательно,  $T$  — автоморфизм  $K$ . Для любого  $z$  из  $G$  пусть  $z'$  определяется равенством  $(z')^a = z$ . Тогда

$$(Px)Tz = (Pxz')T, \quad (By)Tz = (Byz')T$$

при всех  $x, y, z \in G$ , а это означает, что  $T$  содержится в  $N$ .

Далее, предположим, что  $T$  содержится в  $N$  и  $PT = Pa^{-1}, BT = Bb$ . Определим  $a$  соотношением  $x^a = T^{-1}xT$ . Тогда  $a$  есть автоморфизм  $G$ , и равенства (11.5.2) получаются непосредственно. Для каждого  $d \in D$  элемент  $Pd$  содержится в  $B$ , поэтому  $Pa^{-1}d^a = (Pd)T$  содержитя в  $BT = Bb$  и, следовательно,  $a^{-1}d^a b^{-1} \in D$ ,  $D^a = aDb$ .

Наконец, поскольку группа  $G$  регулярна на элементах  $K$ , факторгруппа  $N/G$  изоморфна подгруппе группы  $N$ , оставляющей на месте  $P$ . Отсюда если  $PT = P$ , то  $a = 1$ , и для соответствующего множителя  $a$  имеем  $D^a = Db$ . Таким образом,  $N/G$  изоморфна группе правых множителей.

Для изучения разностных множеств в группах общего вида удобно использовать групповое кольцо  $G^*(R)$  группы  $G$  над кольцом коэффициентов  $R$ , в качестве которого обычно берется кольцо  $\mathbf{Z}$  рациональных целых чисел. Элементы  $G^*$  имеют вид

$$h = a_1x_1 + \dots + a_gx_g, \quad x_i \in G, \quad a_i \in R. \quad (11.5.3)$$

Сложение в  $G^*$  определяется правилом

$$(a_1x_1 + \dots + a_gx_g) + (b_1x_1 + \dots + b_gx_g) = \\ = (a_1 + b_1)x_1 + \dots + (a_g + b_g)x_g, \quad (11.5.4)$$

а умножение — правилом

$$(a_1x_1 + \dots + a_gx_g)(b_1x_1 + \dots + b_gx_g) = c_1x_1 + \dots + c_gx_g, \quad (11.5.5)$$

где

$$c_k = \sum_{i,j} a_i b_j \quad \text{для всех } i, j \text{ с } x_i x_j = x_k \text{ в } G. \quad (11.5.6)$$

Легко проверить, что  $G^*$  — ассоциативное кольцо. Если  $R$  имеет единицу, то  $G^*(R)$  также имеет единицу (обозначим ее через 1), которая является произведением единицы из  $R$  и единицы из  $G$ .

Предположим, что  $D$  — разностное множество из  $k$  элементов в группе  $G$  порядка  $v$ . В групповом кольце  $G^*(\mathbf{Z})$  положим

$$\theta(d) = d_1 + d_2 + \dots + d_k, \quad D = \{d_1, \dots, d_k\}. \quad (11.5.7)$$

Если  $t$  — любое целое число, то введем также обозначение

$$\theta(d^t) = d_1^t + d_2^t + \dots + d_k^t. \quad (11.5.8)$$

Запишем, кроме того,

$$T = \sum_{x \in G} x. \quad (11.5.9)$$

В этих обозначениях соотношение, выражающее тот факт, что  $D$  есть разностное множество над  $G$ , принимает вид

$$\theta(d)\theta(d^{-1}) = k - \lambda + \lambda T, \quad (11.5.10)$$

так как по свойствам разностного множества левая часть должна давать единицу  $k$  раз, а всякий другой элемент из  $G$   $\lambda$  раз. Теорему о множителе (теорема 11.4.1) можно обобщить на разностные множества в абелевой группе. Мы дадим здесь более общую теорему, а в следующем разделе — еще более общую теорему, доказательство которой опирается на теорию алгебраических чисел и групповых характеров. Оба обобщения были бы тривиальны, если бы мы могли исключить условие  $p > \lambda$  в предположениях теоремы 11.4.1.

**Теорема 11.5.2.** Пусть  $D$  — разностное множество из  $k$  элементов в абелевой группе  $G$  порядка  $v$ . Пусть  $n_1 = p_1 p_2 \dots p_s$  — делитель числа  $n = k - \lambda$ , где  $p_1, p_2, \dots, p_s$  — различные простые числа. Если  $(n_1, v) = 1$ ,  $n_1 > \lambda$ , и если  $t$  — целое число, такое, что  $t \equiv p_i^{e_i} \pmod{v}$  для некоторой подходящей степени  $p_i^{e_i}$ ,  $i = 1, \dots, s$ , то автоморфизм  $\alpha$  группы  $G$ , определяемый равенством  $x^\alpha = x^t$ , есть множитель разностного множества.

**Доказательство.** Если  $D = \{d_1, \dots, d_k\}$  — соответствующие элементы группового кольца  $G^*(\mathbf{Z})$  группы  $G$  над целыми числами, то поскольку  $G$  абелева и полиномиальные коэффициенты кратны  $p$ , когда  $p$  — простое число, мы имеем

$$\theta(d)^p = d_1^p + \dots + d_k^p + pW = \theta(d^p) + pW, \quad (11.5.11)$$

где  $W$  — элемент  $G^*(\mathbf{Z})$ .

Кроме того, так как

$$t \equiv p_i^{e_i} \pmod{v}, \quad i = 1, \dots, s, \quad (11.5.12)$$

то  $x^t = x^{p_i^{e_i}}$  при  $i = 1, \dots, s$  для любого  $x \in G$ . (Кстати, вместо  $v$  в этом сравнении мы могли бы использовать  $v^*$ , наименьшее общее кратное порядков элементов группы  $G$ .)

Таким образом,

$$\theta(d)^{p_i^{e_i}} = \theta(d^{p_i^{e_i}}) + p_i R_i = \theta(d^t) + p_i R_i, \quad i = 1, \dots, s. \quad (11.5.13)$$

Умножив соотношение

$$\theta(d) \theta(d^{-1}) = n + \lambda T \quad (11.5.14)$$

на  $\theta(d)^{q-1}$ , где  $q = p_i^{e_i}$ , получим

$$\theta(d)^q \theta(d^{-1}) = n \theta(d)^{q-1} + \lambda \theta(d)^{q-1} T. \quad (11.5.15)$$

Отсюда, поскольку  $xT = T$  для всякого  $x \in G$ , следует, что  $\theta(d)T = kT$ , и (11.5.15) принимает вид

$$\theta(d)^q \theta(d^{-1}) = n \theta(d)^{q-1} + \lambda(k^{q-1} - 1)T + \lambda T. \quad (11.5.16)$$

По условию  $p_i$  делит  $n = k - \lambda$ . Если  $p_i$  не делит  $k$ , то  $k^{q-1} - 1$  кратно  $p_i$ , а если  $p_i$  делит  $k$ , то  $p_i$  также делит  $\lambda$ . Следовательно, в любом случае формула (11.5.16) дает

$$\theta(d)^q \theta(d^{-1}) = p_i V_i + \lambda T. \quad (11.5.17)$$

Теперь, подставляя (11.5.13) в (11.5.17), приходим к равенству

$$(\theta(d^t) + p_i R_i) \theta(d^{-1}) = p_i V_i + \lambda T, \quad (11.5.18)$$

и

$$\theta(d^t) \theta(d^{-1}) = p_i S_i + \lambda T, \quad i = 1, \dots, s. \quad (11.5.19)$$

Но здесь, так как

$$\theta(d^t) \theta(d^{-1}) - \lambda T = p_i S_i, \quad i = 1, \dots, s, \quad (11.5.20)$$

правая часть должна быть кратной  $n_1 = p_1 p_2 \dots p_s$ . Таким образом,

$$\theta(d^t) \theta(d^{-1}) = n_1 S + \lambda T. \quad (11.5.21)$$

Если  $x_1, \dots, x_v$  — элементы группы  $G$ , то левая часть равенства (11.5.21) имеет вид  $a_1 x_1 + \dots + a_v x_v$ , где  $a_i$  — неотрицательные целые и  $\sum a_i = k^2$ . Сравнение с правой частью показывает, что  $a_i \equiv \lambda \pmod{n_1}$  при  $i = 1, \dots, v$ , и, поскольку  $n_1 > \lambda$ , отсюда следует, что  $a_i \geq \lambda$  при всяком  $i$ . Таким образом, если  $S = \sum s_i x_i$ , то  $n_1 s_i = a_i - \lambda \geq 0$ ,

$i = 1, \dots, v$ . Тогда  $\sum n_i s_i = \sum a_i - \lambda v = k^2 - \lambda v = k - \lambda = n$ . Таким образом,  $s_i$  — неотрицательные целые числа, такие, что  $\sum n_i s_i = n$ , следовательно,

$$n_1 ST = \sum_i n_i s_i T = nT. \quad (11.5.22)$$

Применяя автоморфизм  $x \rightarrow x^t$  группы  $G$  к (11.5.14) и  $x \rightarrow x^{-1}$  к (11.5.21), получаем

$$\theta(d^t) \theta(d^{-t}) = n + \lambda T \quad (11.5.23)$$

и

$$\theta(d) \theta(d^{-t}) = n_1 S^* + \lambda T, \quad (11.5.24)$$

где

$$S^* = \sum s_i x_i^{-1}.$$

Произведение левых частей (11.5.21) и (11.5.24) совпадает с произведением левых частей (11.5.23) и (11.5.14). Следовательно, для произведений соответствующих правых частей имеем

$$(n_1 S + \lambda T)(n_1 S^* + \lambda T) = (n + \lambda T)^2. \quad (11.5.25)$$

Используя (11.5.22) и соотношение

$$n_1 S^* T = \sum_i n_1 s_i T = nT, \quad (11.5.26)$$

упростим равенство (11.5.25):

$$n_1^2 S S^* = n^2, \quad (11.5.27)$$

или

$$n_1^2 \sum s_i x_i \sum s_i x_i^{-1} = n^2. \quad (11.5.28)$$

Так как  $s_i$  — неотрицательные целые числа, в левой части не может быть ненулевого члена  $s_i s_j x_i x_j^{-1}$  при  $i \neq j$ , поскольку только единица имеет ненулевой коэффициент в правой части. Следовательно,  $S$  состоит из единственного члена  $sg$  и  $n_1 S = n_1 sg = ng$ . Равенство (11.5.21) принимает теперь более простой вид

$$\theta(d^t) \theta(d^{-t}) = ng + \lambda T. \quad (11.5.29)$$

Умножая на  $\theta(d)$ , получаем

$$\theta(d^t)(n + \lambda T) = ng\theta(d) + \lambda\theta(d)T. \quad (11.5.30)$$

Но  $\theta(d^t)T = \theta(d)T = kT$ , и, стало быть,

$$n\theta(d^t) = ng\theta(d), \quad (11.5.31)$$

или, если разделить на  $n$ ,

$$\theta(d^t) = g\theta(d). \quad (11.5.32)$$

Но это означает, что автоморфизм  $x \rightarrow x^t$  группы  $G$  есть множитель разностного множества, и теорема доказана.

При построении разностного множества удобно строить блок, фиксируемый множителями (инвариантный относительно множителей), если мы можем быть уверены, что такой блок существует.

**Теорема 11.5.3.** Пусть  $D = \{d_1, \dots, d_k\}$  – разностное множество в абелевой группе  $G$  порядка  $v$ . Пусть  $x \rightarrow x^a$  – множитель схемы  $D(v, k, \lambda)$ , определяемой этим разностным множеством. Тогда существует блок, фиксируемый данным множителем. Если  $v$  и  $k$  взаимно просты, то существует блок, фиксируемый каждым множителем.

**Доказательство.** Первая часть этой теоремы принадлежит Манну, вторая – Джонсу, обе части объединены в одну формулировку автором.

Пусть  $A = (a_{ij})$  – матрица инцидентности блок-схемы  $D(v, k, \lambda)$ , определяемой  $D$ . Тогда множитель  $x \rightarrow x^a$  переставляет элементы. Будем сложение в  $G$  записывать аддитивно, и пусть  $g_1 = 0, g_2, \dots, g_v$  – элементы  $G$ . Рассмотрим матрицу  $P = (p_{rs})$ , где  $p_{rs} = 1$ , если  $g_r^a = g_s$ , и  $p_{rs} = 0$  в остальных случаях. Аналогично если  $B_1, \dots, B_v$  – блоки  $D(v, k, \lambda)$ , то  $x \rightarrow x^a$  переставляет  $B_i$ . Определим матрицу  $Q = (q_{mn})$ , где  $q_{mn} = 1$ , если  $B_m^a = B_n$ , и  $q_{mn} = 0$  в остальных случаях. Тогда утверждение, что  $x \rightarrow x^a$  индуцирует автоморфизм схемы  $D(v, k, \lambda)$ , выражается в матричной форме так:

$$P^{-1}AQ = A. \quad (11.5.33)$$

Поскольку  $A$  невырождена, отсюда получаем

$$Q = A^{-1}PA. \quad (11.5.34)$$

Значит, для следов  $P$  и  $Q$  имеем

$$\text{след } Q = \text{след } P. \quad (11.5.35)$$

Но, очевидно,  $g_1^a = 0^a = 0 = g_1$ , поэтому  $p_{11} = 1$  и след  $P > 0$ . Тогда по формуле (11.5.35) след  $Q > 0$ , а след  $Q$  равен числу блоков, фиксируемых множителем  $a$ . Эта часть принадлежит Манну и аналогична доказательству Паркера [1].

В блоке  $B_i = \{d_1 + g_i, d_2 + g_i, \dots, d_k + g_i\}$  сумма элементов равна  $(d_1 + d_2 + \dots + d_k) + kg_i$ . Следовательно, если  $(v, k) = 1$ , то существует в точности один элемент  $g_i$ , такой, что эта сумма равна нулевому элементу  $G$ . Очевидно, этот блок остается неподвижным при всяком множителе блок-схемы  $D(v, k, \lambda)$ .

## 11.6. Некоторые семейства разностных множеств

Известно несколько семейств разностных множеств. Мы сначала приведем их перечень с кратким описанием, а позже разберем их более детально. Эти семейства рассмотрены в работе М. Холла [1].

*Tun S* (зингеровы разностные множества). Это гиперплоскости в  $\text{PG}(n, q)$ ,  $q = p^r$ . Параметры:

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^n - 1}{q - 1}, \quad \lambda = \frac{q^{n-1} - 1}{q - 1}.$$

Доказательство существования и способ построения этих множеств даются теоремой 11.3.1.

*Tun Q* (квадратичные вычеты в  $\text{GF}(p^r)$ ,  $p^r \equiv 3 \pmod{4}$ ). Параметры:

$$v = p^r = 4t - 1, \quad k = 2t - 1, \quad \lambda = t - 1.$$

*Tun H<sub>6</sub>* ( $p$  — простое число вида  $p = 4x^2 + 27$ ). Существует примитивный корень  $r$  по модулю  $p$ , такой, что  $\text{Ind}_r(3) \equiv 1 \pmod{6}$ . Вычеты  $a_1, \dots, a_{\frac{p-1}{2}}$  ( $\pmod{p}$ ), такие, что  $\text{Ind}_r(a_i) \equiv 0, 1$  или  $3 \pmod{6}$ , образуют разностное множество с параметрами

$$v = p = 4t - 1, \quad k = 2t - 1, \quad \lambda = t - 1.$$

Заметим, что тип  $H_6$  имеет те же параметры, что и разностное множество типа  $Q$ .

*Typ T* (простые числа-близнецы). Предположим, что  $p$  и  $q = p + 2$  — простые числа. Среди  $(p - 1)(q - 1)$  вычетов по модулю  $pq$ , взаимно простых с  $pq$ , пусть  $a_1, \dots, a_m$ ,  $m = (p - 1)(q - 1)/2$ , — те вычеты, для которых  $\left(\frac{a_i}{p}\right) = \left(\frac{a_i}{q}\right)$ ; обозначим также  $0, q, 2q, \dots, (p-1)q$  через  $a_{m+1}, \dots, a_{m+p}$ . Тогда  $m + p = (pq - 1)/2 = k$ . Вычеты  $a_1, \dots, a_k$  образуют разностное множество по модулю  $v$  с параметрами  $v = pq$ ,  $k = (pq - 1)/2$ ,  $\lambda = (pq - 3)/4$ ; так как всегда  $pq \equiv -1 \pmod{4}$ , то

$$v = 4t - 1, \quad k = 2t - 1, \quad \lambda = t - 1.$$

Аналогично определяется разностное множество для  $GF(p^r)$  и  $GF(q^s)$ , если  $q^s = p^r + 2$ . Три типа:  $Q$ ,  $H_6$  и  $T$ , — это разностные множества типа Адамара, так как любая симметричная схема с параметрами  $v = 4t - 1$ ,  $k = 2t - 1$ ,  $\lambda = t - 1$  соответствует матрице Адамара порядка  $4t$ . Матрицы Адамара будут рассмотрены в гл. 14.

*Typ B* (биквадратичные вычеты простых чисел вида  $p = 4x^2 + 1$ ,  $x$  нечетно). Здесь

$$v = p = 4x^2 + 1, \quad k = x^2, \quad \lambda = \frac{x^2 - 1}{4}.$$

*Typ B<sub>0</sub>* (биквадратичные вычеты и нуль по модулю простых чисел вида  $p = 4x^2 + 9$ ,  $x$  нечетно). Здесь

$$v = 4x^2 + 9, \quad k = x^2 + 3, \quad \lambda = \frac{x^2 + 3}{4}.$$

*Typ O* (восьмеричные вычеты простых чисел вида  $p = 8a^2 + 1 = 64b^2 + 9$  с нечетными  $a, b$ ). Здесь

$$v = p, \quad k = a^2, \quad \lambda = b^2.$$

*Typ O<sub>0</sub>* (восьмеричные вычеты и нуль по модулю простых чисел вида  $p = 8a^2 + 49 = 64b^2 + 441$ ,  $a$  нечетно,  $b$  четно). Здесь

$$v = p, \quad k = a^2 + 6, \quad \lambda = b^2 + 7.$$

*Typ W<sub>4</sub>* (обобщение типа  $T$ , полученное Уитменом [1], использующее, однако, биквадратичные вычеты вместо

квадратичных). Здесь  $p$  и  $q$  — два простых числа, таких, что  $(p-1, q-1) = 4$ , и мы введем обозначение  $d = (p-1)(q-1)/4$ . Если взять число  $g$ , являющееся примитивным корнем как  $p$ , так и  $q$ , то разностное множество состоит из  $1, g, g^2, \dots, g^{d-1}, 0, q, 2q, \dots, (p-1)q$  по модулю  $pq$ , где  $v = pq$ ,  $k = (v-1)/4$ ,  $\lambda = (v-5)/16$ . Тогда должно выполняться равенство  $q = 3p + 2$ , а  $(v-1)/4$  должно быть нечетным квадратом.

Заметим, что если  $a_1, \dots, a_k$  — множество вычетов, образующих разностное множество по модулю нечетного  $v$ , то  $-a_1, \dots, -a_k$  не может быть тем же множеством, ибо если бы это было так, то  $d \equiv a_i - a_j \equiv (-a_j) - (-a_i) \pmod{v}$  и разность  $d$ , не имеющая вида  $2a_i$ , появлялась бы четное число раз, а разность вида  $2a_i$  появлялась бы нечетное число раз. Как следствие из этого замечания (при нечетном простом  $p$  вида  $ef + 1$ ) получаем: если множество вычетов по модулю  $p$  образует разностное множество, которое имеет вычеты степени  $e$  в качестве множителей, оставляющих это множество неподвижным, то  $f$  нечетно. Действительно, сравнение  $a \equiv b^e \pmod{p}$  эквивалентно сравнению  $a^f \equiv b^{ef} \equiv b^{p-1} \equiv 1 \pmod{p}$  и, когда  $f$  четно,  $(-1)^f \equiv 1 \pmod{p}$ , т. е.  $-1$  есть вычет степени  $e$  и, следовательно, множитель, фиксирующий данное множество, а это, как мы показали, невозможно.

Автоморфизм  $\alpha: g \rightarrow g^a = g^*$  группы  $G$  — взаимно однозначное отображение, поэтому отображение  $\alpha^{-1}: g^* \rightarrow g = g^{*a^{-1}}$  также взаимно однозначно и является автоморфизмом. Если даны два автоморфизма  $\alpha_1: g \rightarrow g^{a_1}$ ,  $\alpha_2: g \rightarrow g^{a_2}$ , то произведение  $\alpha_1\alpha_2: g = (g^{a_1})^{a_2} = g^{a_1a_2}$  снова является автоморфизмом. Таким образом, автоморфизмы группы  $G$  сами образуют группу  $A(G)$ . Мы можем объединить группу  $G$  и ее автоморфизмы  $A(G)$  в большую группу, которая называется *голоморфом* группы  $G$  и обозначается через  $H(G)$ . Для этого введем следующее правило:

$$(\alpha_1, g_1)(\alpha_2, g_2) = (\alpha_1\alpha_2, g_1^{a_2}g_2), \quad (11.6.1)$$

где  $\alpha_1, \alpha_2 \in A(G)$ ,  $g_1, g_2 \in G$ .

Легко проверить, что пары  $(\alpha, g)$  образуют группу  $H(G)$  относительно операции умножения (11.6.1). Здесь  $(\alpha, g)^{-1} = (\alpha^{-1}, g^{-\alpha^{-1}})$ . Если  $\alpha_1 = 1$  — тождественный автоморфизм, то  $(1, g_1)(1, g_2) = (1, g_1g_2)$  и элементы  $(1, g)$  группы  $H(G)$  образуют подгруппу, изоморфную  $G$ . Как легко проверить, группа  $G$  нормальна в  $H(G)$ , и  $H(G)/G$  изоморфна  $A(G)$ . В группе  $H(G)$  автоморфизм  $\alpha$  группы  $G$  индуцируется сопряжением при помощи  $(\alpha, 1)$ :

$$(\alpha^{-1}, 1)(1, g)(\alpha, 1) = (\alpha^{-1}, g)(\alpha, 1) = (1, g^\alpha). \quad (11.6.2)$$

Оба правила (11.6.1) и (11.6.2) применимы, если отображения  $\alpha$  образуют некоторую группу  $M$  автоморфизмов группы  $G$ , где  $M$  — любая подгруппа группы  $A(G)$ . В этом случае соответствующая группа обозначается через  $M(G)$ . Особый интерес для нас представляет тот случай, когда  $G$  — абелева группа порядка  $v$ , а  $M$  — группа множителей, о которой известно (по теореме 11.5.3 или по каким-либо другим соображениям), что она оставляет неподвижным некоторый блок разностного множества. Например, если  $v=43$ ,  $k=21$ ,  $\lambda=10$ , то  $n=k-\lambda=11$  есть множитель по теореме 11.4.1. Так как  $(v, k)=1$ , то по теореме 11.5.3 существует блок, фиксируемый всеми множителями, в частности, всеми степенями автоморфизма  $\alpha$ :  $x \rightarrow 11x \pmod{43}$ . Ниже перечислены классы сопряженных элементов группы  $G$  относительно степеней автоморфизма  $\alpha$ , причем сопряженность дается соотношением (11.6.2); вычет  $0 \pmod{43}$  обозначается через  $z$ :

| $z$                                | $z$ |  |
|------------------------------------|-----|--|
| $C_0$ : 1, 11, 35, 41, 21, 16, 4;  |     |  |
| $C_1$ : 3, 33, 19, 37, 20, 5, 12;  |     |  |
| $C_2$ : 9, 13, 14, 25, 17, 15, 36; |     |  |
| $C_3$ : 27, 39, 42, 32, 8, 2, 22;  |     |  |
| $C_4$ : 38, 31, 40, 10, 24, 6, 23; |     |  |
| $C_5$ : 28, 7, 34, 30, 29, 18, 26. |     |  |

Если операцию в  $G$  записывать в мультипликативной форме, то элементы  $G$  — это  $b=b^1, b^2, \dots, b^{42}, b^{43}=z=1$ ,

а числа в (11.6.3) — степени элемента  $b$ . В обозначениях (11.5.7) если существует разностное множество  $D = \{d_1, \dots, d_{21}\}$ , то  $\theta(d^{11}) = \theta(d) = d_1 + \dots + d_{21}$ . Следовательно,  $\theta(d)$  есть сумма классов. Аналогично, в обозначениях (11.5.10),  $\theta(d^{-1})$  есть также сумма классов. Таким образом, основное уравнение (11.5.10), т. е. уравнение

$$\theta(d)\theta(d^{-1}) = n + \lambda T, \quad (11.6.4)$$

получается с помощью умножения классов. Так как класс  $z$  имеет только один элемент, а классы  $C_0, \dots, C_5$  — по семь элементов, то ясно, что  $\theta(d)$  есть сумма трех из шести классов  $C_0, \dots, C_5$ .

Вообще пусть  $G$  — абелева группа, и пусть  $D = \{d_1, \dots, d_k\}$ ,  $\theta(d) = d_1 + \dots + d_k$ . Если  $a_1 = 1, a_2, \dots, a_s$  образуют группу  $M$  множителей, оставляющих неподвижным разностное множество  $D$ , то  $\theta(d^a) = d_1^a + \dots + d_k^a = \theta(d) = d_1 + \dots + d_k$  для всякого  $a = a_1, \dots, a_s$ . В этом случае  $\theta(d)$  есть сумма классов сопряженных элементов группы  $G$  в  $M(G)$ . Точно так же  $\theta(d^{-1})$  есть сумма классов элементов, обратных элементам  $\theta(d)$ . Поэтому если мы знаем таблицу умножения классов  $G$  в  $M(G)$ , то этого достаточно для того, чтобы вычислить  $\theta(d)\theta(d^{-1})$  и узнать, удовлетворяется или нет основное уравнение (11.6.4).

В произвольной группе  $G$  пусть  $K_1, K_2, \dots, K_r$  — классы сопряженных элементов и

$$C_i = \sum_{x \in K_i} x, \quad i = 1, \dots, r, \quad (11.6.5)$$

— элементы группового кольца  $G^*(\mathbf{Z})$ . Тогда существуют такие неотрицательные целые числа  $c_{ijk}$ , что

$$C_i C_j = \sum_{k=1}^r c_{ijk} C_k, \quad i, j = 1, \dots, r; \quad (11.6.6)$$

действительно, в  $C_i C_j$ , как легко проверить, сопряженные элементы из  $G$  появляются одинаково часто. Правила умножения классов из (11.6.3) даются следующими

формулами:

$$\begin{aligned}
 zC_i &= C_i z = C_i, \quad i = 0, \dots, 5, \\
 C_0^2 &= 2C_1 + 2C_2 + 3C_3, \\
 C_0C_1 = C_1C_0 &= 2C_0 + C_1 + C_2 + 2C_4 + C_5, \\
 C_0C_2 = C_2C_0 &= C_0 + C_1 + 2C_2 + C_4 + 2C_5, \\
 C_0C_3 = C_3C_0 &= 7z + 2C_1 + C_2 + 2C_4 + C_5, \\
 C_0C_4 = C_4C_0 &= 2C_0 + C_2 + 2C_3 + C_4 + C_5, \\
 C_0C_5 = C_5C_0 &= C_0 + C_1 + 2C_3 + C_4 + 2C_5.
 \end{aligned} \tag{11.6.7}$$

Кроме того, поскольку 3 — примитивный корень по модулю 43, отображение  $\beta: x \rightarrow 3x \pmod{43}$  является автоморфизмом группы  $G$ , причем  $\beta^{30} = \alpha$ . Поэтому  $\{\alpha, G\} = M(G)$  есть подгруппа группы  $\{\beta, G\} = H(G)$  индекса  $[H(G) : M(G)] = 6$ . Элемент  $\beta$  индуцирует на  $M(G)$  автоморфизм порядка 6, при котором  $C_i \rightarrow C_{i+1}$ ,  $i = 0, \dots, 5 \pmod{6}$ . Таким образом, из (11.6.7) мы можем вывести всю таблицу умножения для  $C_i$ . Класс  $C_i$  можно также описать как совокупность всех вычетов по модулю 43, индексы которых сравнимы с  $i$  по модулю 6. Так как  $-1 \equiv 42$  принадлежит  $C_3$ , то  $C_i$  и  $C_{i+3}$  состоят из взаимно обратных элементов для любого  $i$ . Поскольку  $\theta(d)$  есть сумма трех классов  $C_i$ , то если никакие два из них не являются последовательными, мы возьмем  $\theta(d) = C_0 + C_2 + C_4$ , и тогда разностное множество состоит из квадратичных вычетов по модулю 43. Если два класса  $C_i$  последовательны, то в качестве этих двух классов мы возьмем  $C_0, C_1$ . Находим, что

$$\begin{aligned}
 \theta(d) &= C_0 + C_2 + C_4, \\
 \theta(d)\theta(d^{-1}) &= 11 + 10T,
 \end{aligned} \tag{11.6.8}$$

$$T = z + C_0 + C_1 + C_2 + C_3 + C_4 + C_5.$$

Находим также [вычисления полностью приведены в (11.6.9)], что

$$\begin{aligned}
 \theta(d) &= C_0 + C_1 + C_3, \\
 \theta(d)\theta(d^{-1}) &= (C_0 + C_1 + C_3)(C_3 + C_4 + C_0), \\
 C_0C_3 = 7z &+ 2C_1 + C_2 + 2C_4 + C_5, \\
 C_0C_4 = & 2C_0 + C_2 + 2C_3 + C_4 + C_5,
 \end{aligned}$$

$$\begin{aligned}
 C_0^2 &= 2C_1 + 2C_2 + 3C_3, \\
 C_1C_3 &= 2C_0 + C_1 + C_2 + 2C_3 + C_5, \\
 C_1C_4 &= 7z + C_0 + 2C_2 + C_3 + 2C_5, \\
 C_1C_0 &= 2C_0 + C_1 + C_2 + 2C_4 + C_5, \\
 C_3^2 &= 3C_0 + 2C_4 + 2C_5, \\
 C_3C_4 &= 2C_1 + C_2 + 2C_3 + C_4 + C_5, \\
 C_3C_0 &= 7z + 2C_1 + C_2 + 2C_4 + C_5
 \end{aligned} \tag{11.6.9}$$

и

$$\begin{aligned}
 \theta(d)\theta(d^{-1}) &= 21z + 10C_0 + 10C_1 + 10C_2 + \\
 &\quad + 10C_3 + 10C_4 + 10C_5 = 11z + 10T.
 \end{aligned}$$

Таким образом, при  $v = 43$ ,  $k = 21$ ,  $\lambda = 10$  мы нашли, что существуют, с точностью до эквивалентности, два разностных множества, определяемые в (11.6.8) и (11.6.9): первое типа, который мы обозначили  $Q$ , а второе типа  $H_6$ . Никаких других разностных множеств не существует.

Большинство перечисленных выше типов можно классифицировать как разностные множества вычетов. При этом  $v = p$  — простое число,  $G$  — циклическая группа порядка  $p$ , а группа  $M$  множителей — циклическая группа порядка  $f$ , где  $p = ef + 1$ , состоящая из мультипликативной группы вычетов  $e$ -й степени по модулю  $p$ . Можно вообще рассматривать аддитивную группу  $G$  порядка  $p' = q$  в поле  $GF(p')$  и мультипликативную группу  $M$   $e$ -х степеней в  $GF(p')$ , где  $q = ef + 1$ . Как уже отмечалось,  $f$  не может быть четным при нечетном  $v$ , так как тогда число  $-1$  было бы множителем. Следовательно, нам нужно рассмотреть лишь случаи с четным  $e$  (если исключить возможность  $q = 2'$ ).

Пусть теперь  $M(G)$  — группа отображений группы  $GF(q)$  на себя:

$$x \rightarrow c^e x + d, \quad c \neq 0, \quad c, d \in GF(q), \tag{11.6.10}$$

где  $q = 1 + ef$ , и пусть  $G$  — аддитивная группа

$$A(b): x \rightarrow x + b, \tag{11.6.11}$$

а группа  $M$  множителей состоит из отображений

$$M(c^e): x \rightarrow c^e x, \quad c \neq 0. \tag{11.6.12}$$

Легко проверить, что

$$M(c^e)^{-1} A(b) M(c^e) = A(c^e b). \quad (11.6.13)$$

Следующее соответствие определяется соотношением (11.6.11):

$$b \in A(b): x \rightarrow x + b, \quad b \in GF(q); \quad (11.6.14)$$

при этом

$$A(b_1) A(b_2) = A(b_1 + b_2). \quad (11.6.15)$$

Когда это не приводит к двусмысленности, мы будем отождествлять элементы  $b$  и  $A(b)$ . Из (11.6.13) следует, что  $b$  и  $c^e b$  — сопряженные элементы в  $M(G)$ . Пусть  $g$  — примитивный корень  $GF(q)$ . Тогда из соотношения (11.6.13) следует, что  $g^u$  и  $g^v$  сопряжены в  $M(G)$  тогда и только тогда, когда существует такое  $e = g^l$ , что  $g^u = g^v c^e = g^v g^{je} = g^{v+je}$ , или, иначе говоря, тогда и только тогда, когда  $u \equiv v \pmod{e}$ , так как  $e$  есть делитель  $q - 1$ , т. е. порядка элемента  $g$ .

Следовательно, сопряженные классы группы  $G$  в  $M(G)$  — это нулевой элемент, который мы обозначим через  $z$ , и классы  $K_i$  элементов  $g^u$  с  $u \equiv i \pmod{e}$  при  $i = 0, 1, \dots, e - 1$ . Запишем это подробно следующим образом:

$$z; \quad K_i = \{g^u; u \equiv i \pmod{e}\}, \quad i = 0, \dots, e - 1. \quad (11.6.16)$$

Далее,  $M(G)$  — нормальная подгруппа группы  $L(G)$  — полной группы линейных преобразований:

$$x \rightarrow mx + b, \quad m \neq 0, \quad b \in GF(q). \quad (11.6.17)$$

В  $L(G)$  имеется преобразование  $\alpha(g)$  — умножение на примитивный корень  $g$ :

$$\alpha(g): x \rightarrow gx, \quad (11.6.18)$$

и мы видим, что

$$\alpha(g)^{-1} A(g^u) \alpha(g) = A(g^{u+1}). \quad (11.6.19)$$

Таким образом,  $\alpha = \alpha(g)$  индуцирует автоморфизм в  $M(G)$ , такой, что

$$\alpha^{-1} K_i \alpha = K_{i+1}, \quad i = 0, \dots, e - 1, \quad K_e = K_0. \quad (11.6.20)$$

Обратимся теперь к групповому кольцу  $M(\mathbf{Z})$  группы  $M(G)$  над целыми числами  $\mathbf{Z}$ . Элемент  $z$  — это единица в  $M(G)$  и, конечно, нулевой элемент  $G$ , если  $G$  записана аддитивно. В  $M(\mathbf{Z})$  представим элементы  $G$  в виде  $z, x_0, x_1, \dots, x_{q-2}$ , где

$$x_i = A(g^i). \quad (11.6.21)$$

Кроме того, пусть

$$C_i = \sum_{x \in K_i} x, \quad i = 0, \dots, e-1. \quad (11.6.22)$$

Суммы  $C_i$  элементов по классам и элемент  $z$  образуют базис некоторого подкольца кольца  $M(\mathbf{Z})$ , и мы имеем

$$C_i C_j = a_{ij} z + \sum_{k=0}^{e-1} c_{ijk} C_k, \quad i, j = 0, \dots, e-1, \quad (11.6.23)$$

где  $a_{ij}$  и  $c_{ijk}$  — неотрицательные целые числа. Здесь  $a_{ij}$  есть число решений уравнения

$$g^u + g^v = z = 0, \quad u \equiv i \pmod{e}, \quad v \equiv j \pmod{e}, \quad (11.6.24)$$

а  $c_{ijk}$  — число решений уравнения

$$g^u + g^v = g^w, \quad u \equiv i \pmod{e}, \quad v \equiv j \pmod{e}, \\ w \text{ фиксировано}, \quad w \equiv k \pmod{e}. \quad (11.6.25)$$

Соотношения (11.6.24) и (11.6.25) вытекают из того факта, что в любой конечной группе равенство  $ab = c$ ,  $a \in K_i$ ,  $b \in K_j$ ,  $c \in K_k$ , где  $K_i$  — классы сопряженных элементов, остается справедливым при сопряжении  $(x^{-1}ax)(x^{-1}bx) = x^{-1}cx$  для любого элемента  $x$ . Поэтому при фиксированных  $c$  и  $x^{-1}cx$  уравнения  $ab = c$  и  $a'b' = x^{-1}cx$  имеют одинаковое число решений с  $a$ ,  $a' \in K_i$ ,  $b, b' \in K_j$ . То же самое справедливо, если зафиксировать  $b$  или  $a$ .

Так как  $-1 = g^{\frac{q-1}{2}}$ , легко найти значение  $a_{ij}$ , числа решений (11.6.24). Заметим, что поскольку  $q-1 = ef$ , то  $-1 \in K_0$ , если  $f$  четно, и  $-1 \in K_{e/2}$ , если  $f$  нечетно. Тогда из

$$g^v = -g^u = g^{u+q(q-1)/2}$$

в (11.6.24) вытекает, что

$$\begin{aligned} a_{ii} &= f, \text{ если } f \text{ четно;} \\ a_{i, i+e/2} &= f, \text{ если } f \text{ нечетно;} \\ a_{ij} &= 0 \text{ в остальных случаях.} \end{aligned} \quad (11.6.26)$$

Если мы умножим (11.6.25) на  $g^{-u}$ , то получим

$$1 + g^{v-u} = g^{w-u}, \quad (11.6.27)$$

или

$$1 + g^{v'} = g^{w'}, \quad v' \equiv j - i, \quad w' \equiv k - i \pmod{e}. \quad (11.6.28)$$

Так как в каждом классе  $K_i$ ,  $i = 0, \dots, e-1$ , число  $f$  элементов одинаково, это дает основное соотношение

$$c_{ijk} = c_{0, j-i, k-i}. \quad (11.6.29)$$

В теории циклотомии число решений уравнения

$$1 + g^s = g^t, \quad s \equiv i, \quad t \equiv j \pmod{e}, \quad (11.6.30)$$

обозначается через  $(i, j)$ ; таким образом,

$$(i, j) = c_{0, i, j} = c_{s, i+s, j+s}. \quad (11.6.31)$$

Умножая (11.6.30) на  $g^{-s}$ , получаем

$$g^{-s} + 1 = g^{t-s}, \quad -s \equiv -i, \quad t - s \equiv j - i \pmod{e}. \quad (11.6.32)$$

С другой стороны,

$$g^s = -1 + g^t, \quad (11.6.33)$$

или

$$g^{s+\frac{q-1}{2}} = 1 + g^{t+\frac{q-1}{2}}. \quad (11.6.34)$$

Из (11.6.32) и (11.6.34) получаются соотношения

$$\begin{aligned} (i, j) &= (-i, j-i), \\ (j, i) &= (i, j), \text{ если } f \text{ четно,} \\ (j, i) &= \left(i + \frac{e}{2}, j + \frac{e}{2}\right), \text{ если } f \text{ нечетно.} \end{aligned} \quad (11.6.35)$$

Подсчитывая элементы в обеих частях (11.6.23), приходим к равенству

$$f^2 = a_{if} + f \sum_{k=0}^{e-1} c_{ijk}. \quad (11.6.36)$$

Мы можем (11.6.26) переписать в виде

$$a_{ij} = n_j - i f, \quad (11.6.37)$$

где

$$\begin{aligned} n_0 &= 1, \quad f \text{ четно}, \\ n_{e/2} &= 1, \quad f \text{ нечетно}, \\ n_i &= 0 \quad \text{в остальных случаях}. \end{aligned}$$

Заметив это, из (11.6.36) получим

$$\sum_{k=0}^{e-1} (j, k) = f - n_j, \quad j = 0, \dots, e-1. \quad (11.6.38)$$

Соотношений (11.6.35) и (11.6.38) достаточно, чтобы определить  $(i, j)$  при  $e = 2$ .

*Случай  $e = 2$ ,  $f$  нечетно.* Тогда

$$\begin{aligned} (0, 0) + (0, 1) &= f, \\ (1, 0) + (1, 1) &= f - 1, \\ (0, 0) &= (1, 1) = (1, 0). \end{aligned} \quad (11.6.39)$$

Следовательно,

$$(0, 0) = (1, 1) = (1, 0) = \frac{f-1}{2}, \quad (0, 1) = \frac{f+1}{2}. \quad (11.6.40)$$

Это дает разностные множества типа  $Q$ , ибо здесь, в обозначениях (11.5.14),  $\theta(d) = C_0$  — множеству квадратов в  $GF(q)$  (по модулю  $p$  — квадратичные вычеты), и  $\theta(d^{-1}) = C_1$ . Но соотношения (11.6.39) и (11.6.40) дают

$$\begin{aligned} \theta(d) \theta(d^{-1}) &= C_0 C_1 = fz + \frac{f-1}{2} (C_0 + C_1) = \\ &= \frac{f+1}{2} z + \frac{f-1}{2} T = (k - \lambda) z + \lambda T, \end{aligned} \quad (11.6.41)$$

где  $v = q = 4t - 1$ ,  $k = 2t - 1$ ,  $\lambda = t - 1$ .

*Случай  $e = 2$ ,  $f$  четно.* Тогда

$$\begin{aligned} (0, 0) + (0, 1) &= f - 1, \\ (1, 0) + (1, 1) &= f, \\ (1, 1) &= (1, 0) = (0, 1). \end{aligned} \quad (11.6.42)$$

Следовательно,

$$(1, 1) = (1, 0) = (0, 1) = \frac{f}{2}, \quad (0, 0) = \frac{f}{2} - 1. \quad (11.6.43)$$

Этот случай не приводит к разностным множествам.

*Случай e = 3.* Составим таблицу, помещая число  $(i, j)$  в строку  $i$  и столбец  $j$ . Эта таблица имеет вид

$$\begin{array}{ccc} (0, 0) & (0, 1) & (0, 2) \\ (0, 1) & (0, 2) & (1, 2) \\ (0, 2) & (1, 2) & (0, 1), \end{array} \quad (11.6.44)$$

так как

$$\begin{aligned} a &= (0, 0), \\ b &= (0, 1) = (1, 0) = (2, 2), \\ c &= (0, 2) = (2, 0) = (1, 1), \\ d &= (1, 2) = (2, 1) \end{aligned} \quad (11.6.45)$$

по (11.6.35).

При  $e = 3$  имеем  $q = 3f + 1$ , и  $(j, i) = (i, j)$  для четного  $f$ . Но если  $f$  нечетно, то  $q = 2^{2s}$ ; тогда  $-1$  и  $+1$  совпадают и (11.6.30) показывает, что  $(j, i) = (i, j)$ . Таблица (11.6.44) показывает, как перемножаются классы в  $G$ :

$$\begin{aligned} C_0^2 &= fz + aC_0 + bC_1 + cC_2, \\ C_0C_1 &= \quad bC_0 + cC_1 + dC_2, \\ C_0C_2 &= \quad cC_0 + dC_1 + bC_2. \end{aligned} \quad (11.6.46)$$

Из (11.6.38) мы получаем линейные соотношения

$$\begin{aligned} a + b + c &= f - 1, \\ b + c + d &= f. \end{aligned} \quad (11.6.47)$$

В силу (11.6.31) определены все произведения  $C_iC_j$ ; например,  $C_1C_2 = dC_0 + bC_1 + cC_2$ . Воспользовавшись законом ассоциативности умножения  $(C_0C_1)C_2 = C_0(C_1C_2)$ , находим

$$\begin{aligned} dfz + (bc + cd + bd)C_0 + (bd + bc + cd)C_1 + \\ + (b^2 + c^2 + ad)C_2 &= dfz + (ad + b^2 + c^2)C_0 + \\ + (bd + bc + cd)C_1 + (cd + bd + bc)C_2. \end{aligned} \quad (11.6.48)$$

Приравнивая коэффициенты, получаем, что

$$ad + b^2 + c^2 = bc + cd + bd;$$

подставляя сюда  $d = a + 1$ ,  $c = f - 1 - a - b$  [из (11.6.47)], приходим к соотношению

$$3a^2 + 3ab + 3b^2 - (3f - 5)a - (3f - 3)b = -f^2 + 3f - 2. \quad (11.6.49)$$

Умножив это равенство на 36 и перегруппировав члены, получим равенство

$$(9a - 3f + 7)^2 + 27(f - 1 - a - 2b)^2 = 12f + 4 = 4q. \quad (11.6.50)$$

Таким образом, числа из (11.6.44) определяются решением диофантова уравнения

$$L^2 + 27M^2 = 4q, \quad (11.6.51)$$

где знак  $L$  определяется сравнением  $L \equiv 1 \pmod{3}$ . Знак  $M$  будет зависеть от выбора примитивного корня. Мы находим:

$$\begin{aligned} 9a &= 9(0, 0) = q - 8 + L, \\ 18b &= 18(0, 1) = 2q - 4 - L - 9M, \\ 18c &= 18(0, 2) = 2q - 4 - L + 9M, \\ 9d &= 9(1, 2) = q + 1 + L. \end{aligned} \quad (11.6.52)$$

Чтобы получить разностное множество, мы должны иметь  $k = (q - 1)/3$  и  $a = b = c$  в первом из равенств (11.6.46). Но тогда  $M = 0$ ,  $L = 4$ ,  $q = 4 = v$  и, trivialно,  $k = 1$ .

Если  $q = p$  — простое число, то известно, что (11.6.51) определяет  $L$  и  $M$  с точностью до знака единственным образом. Если  $q = p^r$ ,  $p \equiv 2 \pmod{3}$ , то  $r$  должно быть четным,  $r = 2s$  и в (11.6.51) мы должны иметь  $M = 0$  и  $L = \pm 2q^s$ . Если  $q = p^r$ ,  $p \equiv 1 \pmod{3}$ ,  $r > 1$ , то решение (11.6.51) не единствено. В этом случае не ясно, какое из решений (11.6.51) может быть использовано в (11.6.52), но небольшой подсчет наводит на мысль, что если  $(u, v)$  — единственное решение уравнения  $4p = x^2 + 27y^2$ , то для  $q = p^r$  подходящее решение дается равенством

$$\frac{L + M \sqrt{-27}}{2} = \left( \frac{u + v \sqrt{-27}}{2} \right)^r.$$

Это решение характеризуется тем свойством, что  $L$  и  $M$  не кратны  $p$ . Это недавно было показано автором в работе [2] в предположении справедливости результатов работы Митчелла [1].

Соотношение

$$C_0^2 = fz + aC_0 + bC_1 + cC_2 \quad (11.6.53)$$

дает число решений уравнения

$$x + y = t_i, \quad x, y \in K_0, \quad t_i \in K_i, \quad t_i \text{ фиксировано.} \quad (11.6.54)$$

Если  $(x, y)$  — решение, то  $(y, x)$  — также решение, и совокупность решений распадается на такие пары, исключая случай  $y = x, 2x = t_i$ . Ясно, что тогда  $2 \in K_i$ , и, таким образом,  $2 \in K_0$ , если  $a$  нечетно,  $2 \in K_1$ , если  $b$  нечетно, и  $2 \in K_2$ , если  $c$  нечетно.

Аналогично

$$\begin{aligned} C_0^3 = afz + (a^2 + b^2 + c^2 + f)C_0 + (ab + bc + cd)C_1 + \\ + (ac + bd + bc)C_2 \end{aligned} \quad (11.6.55)$$

дает число решений уравнения

$$x + y + z = t_i, \quad x, y, z \in K_0, \quad t_i \in K_i, \quad t_i \text{ фиксировано.} \quad (11.6.56)$$

Переставляя  $x, y, z$  в (11.6.56), мы получаем шесть решений, если все три элемента  $x, y, z$  различны, три решения, если два из них равны, а третий отличен от них, и одно решение, если  $x = y = z$ ; в последнем случае  $3x = t_i$  и  $3 \in K_i$ . Таким образом, коэффициент при  $C_i$  в правой части (11.6.55) сравним с 1 по модулю 3 тогда и только тогда, когда  $3 \in K_i$ . Вычислим, учитывая соотношение  $4q = L^2 + 27M^2$ ,

$$\begin{aligned} A_0 &= a^2 + b^2 + c^2 + f = \frac{q^2 + 3q + 15 - 4L}{27}, \\ A_1 &= ab + bc + cd = \frac{2q^2 - 12q + 12 + L + 27M}{54}, \\ A_2 &= ac + bd + bc = \frac{2q^2 - 12q + 12 + L - 27M}{54}. \end{aligned} \quad (11.6.57)$$

Чтобы найти  $A_i \pmod{3}$ , нам нужны значения числителей в правой части по  $\pmod{81}$ . Здесь  $A_i \equiv 16A_i \pmod{3}$ . Поскольку  $L \equiv 1 \pmod{3}$ , полагаем  $L = 1 + 3t$ . Тогда справедливы сравнения по модулю 3 (используем  $4q = L^2 + 27M^2$ ):

$$\begin{aligned} A_0 &\equiv 16A_0 \equiv \frac{(L^2 + 27M^2)^2 + 12(L^2 + 27M^2) + 240 - 64L}{27} \equiv \\ &\equiv \frac{L^4 + 12L^2 - 64L + 240 + 54L^2M^2}{27} \equiv \frac{27 - 108(t - t^3) - 27M^2}{27} \equiv \\ &\equiv 1 - (t - t^3) - M^2 \pmod{3}. \end{aligned} \quad (11.6.58)$$

Но  $t - t^3 \equiv 0 \pmod{3}$  для всякого целого  $t$  и потому .

$$A_0 \equiv 1 - M^2 \pmod{3}. \quad (11.6.59)$$

Таким образом,  $A_0 \equiv 1 \pmod{3}$ , если  $M \equiv 0 \pmod{3}$ ; в противном случае  $A_0 \equiv 0 \pmod{3}$ . Следовательно, 3 есть кубичный вычет тогда и только тогда, когда  $M \equiv 0 \pmod{3}$ . Аналогично

$$\begin{aligned} A_1 \equiv 16A_1 &\equiv \frac{L^4 - 24L^2 + 8L + 96 + 54L^2M^2 + 216M}{27} \equiv \\ &\equiv -t + t^3 - M^2 - M \equiv -M^2 - M \pmod{3}. \end{aligned} \quad (11.6.60)$$

Следовательно, если  $M \equiv 0$  или  $2 \pmod{3}$ , то  $A_1 \equiv 0 \pmod{3}$ , а если  $M \equiv 1 \pmod{3}$ , то  $A_1 \equiv 1 \pmod{3}$ . Поэтому  $3 \in K_1$  тогда и только тогда, когда  $M \equiv 1 \pmod{3}$ . Точно так же

$$A_2 \equiv -M^2 + M \pmod{3}$$

и  $3 \in K_2$  тогда и только тогда, когда  $M \equiv 2 \pmod{3}$ . Объединим эти результаты о кубичном характере 2 и 3.

**Теорема 11.6.1.** Пусть  $q = p^r \equiv 1 \pmod{3}$ ,  $p$  — простое число,  $g$  — примитивный корень в  $\text{GF}(q)$ ;  $4q = L^2 + 27M^2$ , где  $L \equiv 1 \pmod{3}$  и  $M$  удовлетворяют соотношениям (11.6.52). Пусть, далее,  $g^m = 2$ ,  $g^{m'} = 3$ . Тогда  $m \equiv 0 \pmod{3}$ , если  $L \equiv 0 \pmod{2}$ ;  $m \equiv 1 \pmod{3}$ , если  $L + 9M \equiv 0 \pmod{4}$ ;  $m \equiv 2 \pmod{3}$ , если  $L - 9M \equiv 0 \pmod{4}$ ;  $m' \equiv M \pmod{3}$ .

Мы использовали ассоциативность умножения в групповом кольце  $G(\mathbf{Z})$ , чтобы получить соотношения для циклотомических коэффициентов  $(i, j)$  в уравнении (11.6.48). Существует другой, несколько более арифметический подход, основанный на групповом кольце  $G(\zeta)$ , где  $\zeta$  — первообразный корень уравнения  $x^{q-1} = 1$ . В  $G(\zeta)$  элементами базиса являются  $z$ , нулевой элемент группы и  $x_0, \dots, x_{q-2}$ , где  $x_i = A(g^i)$ , как в (11.6.21), а коэффициенты пробегают кольцо полиномов от  $\zeta$  над целыми числами. В  $G(\zeta)$

$$x_t x_{t+j} = A(g^t + g^{t+j}) + A(g^t(1 + g^j)).$$

Если теперь  $j = (q-1)/2$ , то  $1 + g^j = 1 - 1 = 0$  в  $\text{GF}(q)$ , и поэтому  $x_t x_{t+j} = z$ . Если  $j \neq (q-1)/2$ , то  $1 + g^j = g^s$

при подходящем  $s$ , и поэтому

$$x_t x_{t+j} = A(g^t g^s) = A(g^{t+s}) = x_{t+s}.$$

Полагаем  $T = z + x_0 + x_1 + \dots + x_{q-2}$ , тогда

$$\sum_{t=0}^{q-2} x_t x_{t+j} = \begin{cases} \sum_{t=0}^{q-2} z = (q-1)z, & \text{если } j = \frac{q-1}{2}, \\ \sum_{t=0}^{q-2} x_{t+s} = T - z, & \text{если } j \neq \frac{q-1}{2}. \end{cases} \quad (11.6.61)$$

Пусть  $\alpha \neq 1$  — корень уравнения  $x^{q-1} = 1$ . Определим функцию  $F(\alpha)$  следующим образом:

$$F(\alpha) = \sum_{k=0}^{q-2} \alpha^k x_k. \quad (11.6.62)$$

Тогда

$$F(\alpha) F(\alpha^{-1}) = \sum_{k=0}^{q-2} \alpha^k x_k \sum_{t=0}^{q-2} \alpha^{-t} x_t \quad (11.6.63)$$

и, полагая  $k - t = j$ ,

$$F(\alpha) F(\alpha^{-1}) = \sum_{j=0}^{q-2} \alpha^j \sum_{t=0}^{q-2} x_t x_{t+j}. \quad (11.6.64)$$

Используя (11.6.61), приводим это равенство к виду

$$F(\alpha) F(\alpha^{-1}) = \alpha^{\frac{q-1}{2}} (q-1)z + \sum_{j \neq \frac{q-1}{2}} \alpha^j (T - z). \quad (11.6.65)$$

Но так как

$$\sum_{j=0}^{q-2} \alpha^j = 0,$$

то (11.6.65) упрощается:

$$F(\alpha) F(\alpha^{-1}) = \alpha^{\frac{q-1}{2}} (q-1)z - \alpha^{\frac{q-1}{2}} (T - z) = \alpha^{\frac{q-1}{2}} (qz - T). \quad (11.6.66)$$

При  $q = 1 + ef$  классы  $K_i$  вычетов  $e$ -й степени в силу (11.6.22) таковы, что

$$C_i = \sum_{y \in K_i} y = \sum_j x_j, \quad j \equiv i \pmod{e}. \quad (11.6.67)$$

Следовательно, если  $\beta$  — такой корень уравнения  $x^{q-1} = 1$ , что  $\beta^e = 1$ , т. е.  $\beta^r = \beta^s$  для  $r \equiv s \pmod{e}$ , то при  $C_i$ , определенном соотношением (11.6.22),

$$F(\beta) = \sum_{k=0}^{q-2} \beta^k x_k = \sum_{i=0}^{e-1} \beta^i \sum_{j \equiv i \pmod{e}} x_j = \sum_{i=0}^{e-1} \beta^i C_i. \quad (11.6.68)$$

Пусть теперь  $\beta$  — первообразный корень степени  $e$  из единицы, а  $m, n$  — целые числа, причем  $m \not\equiv 0 \pmod{e}$ ,  $n \not\equiv 0 \pmod{e}$ . Предположим также, что  $m + n \not\equiv 0 \pmod{e}$ . Тогда

$$F(\beta^m) F(\beta^n) = \sum_{t=0}^{e-1} \sum_{j=0}^{e-1} \beta^{mj} \beta^{nt} C_j C_t, \quad (11.6.69)$$

и, полагая  $t = j + k$ , получаем

$$\begin{aligned} F(\beta^m) F(\beta^n) &= \sum_{k=0}^{e-1} \beta^{nk} \sum_{j=0}^{e-1} \beta^{(m+n)j} C_j C_{j+k} = \\ &= \sum_{k=0}^{e-1} \beta^{nk} \sum_{j=0}^{e-1} \beta^{(m+n)j} \sum_{h=0}^{e-1} [n_k f_z + (k, h) C_{j+h}], \end{aligned} \quad (11.6.70)$$

пользуясь правилами умножения (11.6.23) и (11.6.31), а также (11.6.37). Поскольку мы предположили, что  $m + n \not\equiv 0 \pmod{e}$ , то

$$\sum_{j=0}^{e-1} \beta^{(m+n)j} n_k f_z = 0. \quad (11.6.71)$$

Следовательно, (11.6.70) принимает вид

$$F(\beta^m) F(\beta^n) = \sum_{k=0}^{e-1} \sum_{h=0}^{e-1} \beta^{nk} \beta^{-(m+n)h} (k, h) \sum_{j=0}^{e-1} \beta^{(m+n)(j+h)} C_{j+h}. \quad (11.6.72)$$

Если определить функцию  $R(m, n)$ , которая принимает значения в области целых алгебраических чисел, посредством равенства

$$R(m, n) = \sum_{k=0}^{e-1} \sum_{h=0}^{e-1} \beta^{nk} \beta^{-(m+n)h} (k, h), \quad (11.6.73)$$

то (11.6.72) принимает вид

$$F(\beta^m) F(\beta^n) = R(m, n) F(\beta^{m+n}). \quad (11.6.74)$$

Исключенное значение  $m + n \equiv 0 \pmod{e}$  соответствует случаю  $m = -n$ , для которого мы можем вычислить  $F(\beta^m)F(\beta^{-m})$  из (11.6.66).

Сформулируем основные результаты в виде следующей теоремы.

**Теорема 11.6.2.** Пусть  $G$  — аддитивная группа  $A(q)$  поля  $\text{GF}(q)$ ,  $q = p^r$ , состоящего из нулевого элемента  $z$ , а также элементов  $x_0, \dots, x_{q-2}$ , где  $x_i = A(g^i)$ ,  $g$  — примитивный корень в  $\text{GF}(q)$ . Если  $a \neq 1$  есть корень уравнения  $x^{q-1} = 1$ , то полагаем

$$1) \quad F(a) = \sum_{k=0}^{q-2} a^k x_k.$$

Если обозначить  $T = z + x_0 + x_1 + \dots + x_{q-2}$ , то

$$2) \quad F(a)F(a^{-1}) = a^{\frac{q-1}{2}}(qz - T).$$

Если  $\beta$  — первообразный корень уравнения  $x^e = 1$  и  $m \not\equiv 0 \pmod{e}$ , где  $q = 1 + ef$ , то

$$3) \quad F(\beta^m) = \sum_{i=0}^{e-1} \beta^{mi} C_i,$$

где  $C_i$  — элемент из (11.6.22). Если определить  $R(m, n)$  по формуле

$$4) \quad R(m, n) = \sum_{k=0}^{e-1} \sum_{h=0}^{e-1} \beta^{nk} \beta^{-(m+n)h} (k, h),$$

где  $m, n, m+n \not\equiv 0 \pmod{e}$ , то

$$5) \quad F(\beta^m)F(\beta^n) = R(m, n)F(\beta^{m+n}).$$

Мы имеем также

$$6) \quad R(m, n)R(-m, -n) = q.$$

**Доказательство.** Все части этой теоремы, за исключением свойства 6, уже доказаны. Заменим в свойстве 5  $m$  и  $n$  на  $-m$  и  $-n$ . Это даст нам

$$F(\beta^{-m})F(\beta^{-n}) = R(-m, -n)F(\beta^{-m-n}). \quad (11.6.75)$$

Умножая это равенство на равенство из свойства 5 и замечая, что кольцо  $G(\xi)$  коммутативно, находим

$$\begin{aligned} F(\beta^m)F(\beta^{-m})F(\beta^n)F(\beta^{-n}) &= \\ &= R(m, n)R(-m, -n)F(\beta^{m+n})F(\beta^{-m-n}). \end{aligned} \quad (11.6.76)$$

Применим теперь свойство 2 с  $a = \beta^m$ ,  $\beta^n$  и  $\beta^{m+n}$  и получим

$$\begin{aligned} \beta^{m(q-1)/2}(qz-T)\beta^{n(q-1)/2}(qz-T) &= \\ &= R(m, n)R(-m, -n)\beta^{(m+n)(q-1)/2}(qz-T). \end{aligned} \quad (11.6.77)$$

Поскольку

$$\begin{aligned} (qz-T)^2 &= q^2z^2 - 2qzT + T^2 = \\ &= q^2z - 2qT + qT = \\ &= q(qz-T), \end{aligned} \quad (11.6.78)$$

то, сравнивая коэффициенты в (11.6.77), находим

$$R(m, n)R(-m, -n) = q. \quad (11.6.79)$$

**Теорема 11.6.3.** Если  $q = p^r$  нечетно и если  $m$  определяется равенством  $g^m = 2$ , то при  $a \neq 1$ ,  $a^{q-1} = 1$ ,

$$F(-1)F(a^2) = a^{2m}F(a)F(-a).$$

**Доказательство.** Следуя Диксону [1], мы покажем, что  $a^{2m+i}$  при всяком  $i = 0, \dots, q-2$  имеет один и тот же коэффициент в левой и правой частях равенства

$$F(-1)F(a^2) = a^{2m}F(a)F(-a). \quad (11.6.80)$$

В правой части коэффициент при  $a^{2m+i}$  равен

$$\sum_j (-1)^j x_j x_{i-j}. \quad (11.6.81)$$

Если  $i$  нечетно, то члены с  $j = J$  и  $j = i - J$  дают  $(-1)^J x_J x_{i-J} + (-1)^{i-J} x_{i-J} x_J = 0$ , и сумма равна нулю. Таким образом, при нечетном  $i$  коэффициент при  $a^{2m+i}$  в правой части равен нулю. Очевидно, левая часть также содержит лишь четные степени  $a$ . Пусть теперь  $i$  четно,  $i = 2t$ . В  $F(a^2)$  и  $x_{m+t}$ , и  $x_{m+t+(q-1)/2}$  имеют в качестве коэффициента  $a^{2m+2t}$ , и потому коэффициент при  $a^{2m+i} = a^{2m+2t}$  равен

$$F(-1)(x_{m+t} + x_{m+t+(q-1)/2}). \quad (11.6.82)$$

Но

$$x_{m+t} = A(g^{m+t}) = A(2g^t),$$

$$x_{m+t+(q-1)/2} = A(-2g^t).$$

Так как

$$F(-1) = \sum_{k=0}^{q-2} (-1)^k x_k,$$

(11.6.82) принимает вид

$$\sum_{k=0}^{q-2} (-1)^k (A(g^k + 2g^t) + A(g^k - 2g^t)), \quad (11.6.83)$$

а сумма (11.6.81) при  $i = 2t$  равна

$$\sum_{j=0}^{q-2} (-1)^j A(g^j + g^{2t-j}). \quad (11.6.84)$$

Покажем теперь, что  $A(c)$  при любом  $c$  появляется с одним и тем же коэффициентом в (11.6.83) и (11.6.84). Если  $c = +2g^t$ , то  $A(c)$  появляется при  $g^j = g^t$  в (11.6.84), при  $g^k = 4g^t$  — во второй сумме (11.6.83) и совсем не появляется в первой сумме. Здесь  $k$  и  $j$  имеют одну и ту же четность. Если  $c = -2g^t$ , то  $A(c)$  появляется при  $g^j = -g^t$  в (11.6.84), при  $g^k = -4g^t$  — в первой сумме (11.6.83), а  $j$  и  $k$  имеют одну и ту же четность. Если  $c \neq \pm 2g^t$  и  $c = g^j + g^{2t-j}$ , то в (11.6.84) два члена с  $j = J$  и  $j = 2t - J$ , оба одинаковой четности, дают  $A(c)$ , и мы замечаем, что

$$c^2 - 4g^{2t} = (g^j - g^{2t-j})^2 = \omega^2$$

есть ненулевой квадрат. С другой стороны,  $A(c)$  получается при  $g^k = g^{-j} (g^j - g^t)^2$  в первой сумме (11.6.83) и при  $g^k = g^{-j} (g^j + g^t)^2$  — во второй сумме, причем оба  $k$  той же четности, что и  $J$ . Если  $c$  не совпадает ни с каким значением, взятым в (11.6.84), то  $c^2 - 4g^{2t}$  не есть квадрат, и тогда для  $g^{k_1} + 2g^t = c$  и  $g^{k_2} - 2g^t = c$  в первой и во второй суммах (11.6.83) соответственно мы имеем

$$g^{k_1+k_2} = c^2 - 4g^{2t}.$$

Числа  $k_1$  и  $k_2$  — противоположной четности, и эти два члена сокращаются. Таким образом, при любой степени  $\alpha$

левая и правая части (11.6.80) имеют один и тот же коэффициент, и тождество доказано.

*Случай*  $e = 4$ . Здесь  $\beta = i$  и

$$R(1, 1) = (0, 0) - (0, 1) + (0, 2) - (0, 3) - (2, 0) + (2, 1) - \\ - (2, 2) + (2, 3) + 2i((1, 0) - (1, 1) + (1, 2) - (1, 3)). \quad (11.6.85)$$

*Подсуммай*  $e = 4$ ,  $f$  четно. Таблица для  $(i, j)$  с  $(i, j)$  в  $i$ -й строке и  $j$ -м столбце,  $i, j = 0, 1, 2, 3$ , имеет следующий вид:

|        |        |        |        |
|--------|--------|--------|--------|
| (0, 0) | (0, 1) | (0, 2) | (0, 3) |
| (0, 1) | (0, 3) | (1, 2) | (1, 2) |
| (0, 2) | (1, 2) | (0, 2) | (1, 2) |
| (0, 3) | (1, 2) | (1, 2) | (0, 1) |

(11.6.86)

Линейные соотношения (11.6.38) в нашем случае таковы:

$$(0, 0) + (0, 1) + (0, 2) + (0, 3) = f - 1, \\ (0, 1) + (0, 3) + 2(1, 2) = f, \quad (11.6.87) \\ (0, 2) + (1, 2) = \frac{f}{2}.$$

Подстановкой в (11.6.85) находим, что

$$R(1, 1) = -x + 2iy, \\ x = 2f + 1 - 8(1, 2), \quad (11.6.88) \\ y = (0, 1) - (0, 3).$$

Тогда по (11.6.79)

$$q = x^2 + 4y^2, \quad (11.6.89)$$

и знак для  $x$  выбирается так, чтобы  $x \equiv 1 \pmod{4}$ . Вместе с (11.6.87) это дает

$$16(0, 0) = q - 11 - 6x, \\ 16(0, 1) = q - 3 + 2x + 8y, \\ 16(0, 2) = q - 3 + 2x, \quad (11.6.90) \\ 16(0, 3) = q - 3 + 2x - 8y, \\ 16(1, 2) = q + 1 - 2x.$$

Подслучай  $e = 4$ ,  $f$  нечетно. Таблица для  $(i, j)$  имеет вид

$$\begin{array}{cccc} (0, 0) & (0, 1) & (0, 2) & (0, 3) \\ (1, 0) & (1, 0) & (0, 3) & (0, 1) \\ (0, 0) & (1, 0) & (0, 0) & (1, 0) \\ (1, 0) & (0, 3) & (0, 1) & (1, 0) \end{array} \quad (11.6.91)$$

причем выполняются [по (11.6.38)] следующие линейные соотношения:

$$\begin{aligned} (0, 0) + (0, 1) + (0, 2) + (0, 3) &= f, \\ 2(1, 0) + (0, 3) + (0, 1) &= f, \\ (0, 0) + (1, 0) &= \frac{f-1}{2}. \end{aligned} \quad (11.6.92)$$

Отсюда

$$\begin{aligned} R(1, 1) &= -x + 2iy, \\ x &= 2f - 1 - 8(1, 0), \\ y &= (0, 3) - (0, 1) \end{aligned} \quad (11.6.93)$$

и по (11.6.79)

$$q = x^2 + 4y^2. \quad (11.6.94)$$

Знак для  $x$  выбирается так, чтобы  $x \equiv 1 \pmod{4}$ , и мы получаем

$$\begin{aligned} 16(0, 0) &= q - 7 + 2x, \\ 16(0, 1) &= q + 1 + 2x - 8y, \\ 16(0, 2) &= q + 1 - 6x, \\ 16(0, 3) &= q + 1 + 2x + 8y, \\ 16(1, 0) &= q - 3 - 2x. \end{aligned} \quad (11.6.95)$$

*Произвольное*  $e$ . Если

$$C_0^2 = n_0 fz + (0, 0) C_0 + (0, 1) C_1 + \dots + (0, e-1) C_{e-1}, \quad (11.6.96)$$

то число  $(0, 0)$  дает число решений уравнения  $u + v = 1$  в  $\text{GF}(q)$  с  $u, v \in K_0$ , и это число четно, если в  $K_0$  нет элемента  $u$  со свойством  $2u = 1$ . Если же в  $K_0$  такой элемент есть, то  $2 \in K_0$ . Мы заметили это при доказательстве теоремы 11.6.1.

Соотношения (11.6.40) и (11.6.43) показывают, что 2 есть квадратичный вычет в  $\text{GF}(q)$ , если  $q \equiv 1, 7 \pmod{8}$ , и 2 есть квадратичный невычет, если  $q \equiv 3, 5 \pmod{8}$ . Выясним теперь, для какого  $q \equiv 1 \pmod{4}$  2 есть четверичный вычет. Если  $q \equiv 5 \pmod{8}$ , то 2, будучи квадратичным невычетом, не является, конечно, четверичным вычетом. Но если  $q \equiv 1 \pmod{8}$ , то можем применить (11.6.90). Таким образом, 2 есть четверичный вычет для  $q \equiv 1 \pmod{8}$  тогда и только тогда, когда

$$q - 11 - 6x \equiv 16 \pmod{32}, \quad x \equiv 1 \pmod{4}. \quad (11.6.97)$$

Полагая  $x = 1 + 4t$  и  $q = x^2 + 4y^2$ , мы приводим (11.6.97) к виду

$$1 + 8t + 16t^2 + 4y^2 - 11 - 6 - 24t \equiv 16 \pmod{32}, \quad (11.6.98)$$

и, поскольку  $t + t^2 \equiv 0 \pmod{2}$  для любого  $t$ , получаем, что

$$4y^2 \equiv 0 \pmod{32}, \quad (11.6.99)$$

или

$$y \equiv 0 \pmod{4} \quad (11.6.100)$$

— необходимое и достаточное условие того, что 2 есть четверичный вычет для  $q \equiv 1 \pmod{8}$ . Сформулируем полученные результаты в виде теоремы.

**Теорема 11.6.4.** Пусть  $q = p' = 1 + 4f$ , и пусть  $q = x^2 + 4y^2$ , где знак  $x$  выбран так, что  $x \equiv 1 \pmod{4}$ . Тогда для четного  $f$  циклотомические числа  $(i, j)$  даются соотношениями (11.6.90) и (11.6.86), а для нечетного  $f$  — соотношениями (11.6.91) и (11.6.95). В общем случае, число 2 является квадратичным вычетом для  $q = p'$ , если  $q \equiv 1, 7 \pmod{8}$ , и квадратичным невычетом, если  $q \equiv 3, 5 \pmod{8}$ . Если  $q \equiv 1 \pmod{8}$ , то 2 является четверичным вычетом в том и только в том случае, когда  $y \equiv 0 \pmod{4}$  в равенстве  $q = x^2 + 4y^2$ .

**Замечание.** Если  $q$  простое, представление  $q = x^2 + 4y^2$ , как известно, единственno. Если  $q = p'$ ,  $p \equiv 3 \pmod{4}$ , то  $r$  четно,  $r = 2s$ , и единственное решение есть  $x = \pm p^s$ ,  $y = 0$ . Если  $q = p'$ ,  $r > 1$ ,  $p \equiv 1 \pmod{4}$ , то представление не единственno, и поэтому значения в (11.6.90) и (11.6.95) не вполне определены теоремой.

Разностное множество  $D$  с четверичными вычетами в качестве множителей должно состоять из одного или более классов  $z, K_0, K_1, K_2, K_3$ . Поскольку  $-1$  не может быть множителем,  $f$  должно быть нечетным.

**Теорема 11.6.5.** *Пусть  $q = p' \equiv 5 \pmod{8}$ . Четверичные вычеты в  $\text{GF}(q)$  образуют разностное множество, если  $q$  имеет вид  $q = 1 + 4y^2$ ; четверичные вычеты и нуль образуют разностное множество, если  $q$  имеет вид  $q = 9 + 4y^2$ . Эти разностные множества принадлежат соответственно типам В и  $B_0$ , указанным в начале этого параграфа. Никакие другие комбинации четверичных вычетов, по существу отличающиеся от указанных, не образуют разностного множества.*

**Доказательство.** Так как  $f$  нечетно, воспользуемся значениями  $(i, j)$  в (11.6.91) и (11.6.95). Если  $D$  состоит из одного класса, то в качестве  $D$  можно взять  $K_0$ . Таким образом,  $\theta(d) = C_0, \theta(d^{-1}) = C_2$  и (11.6.91) показывает, что

$$\begin{aligned} \theta(d)\theta(d^{-1}) &= C_0C_2 = fz + aC_0 + bC_1 + aC_2 + bC_3, \\ 16a &= 16(0, 0) = q - 7 + 2x, \\ 16b &= 16(1, 0) = q - 3 - 2x. \end{aligned} \quad (11.6.101)$$

Разностное множество получается в том и только в том случае, когда  $\theta(d)\theta(d^{-1}) = (k - \lambda)z + \lambda T$ , и это условие соблюдено в (11.6.101) тогда и только тогда, когда  $a = b$ , т. е. тогда и только тогда, когда  $x = 1$ . В этом случае  $q$  имеет вид  $q = 1 + 4y^2$ . Если  $D$  состоит из одного ненулевого класса и нуля, то мы можем взять  $\theta(d) = z + C_0$ . В этом случае

$$\begin{aligned} \theta(d)\theta(d^{-1}) &= (C_0 + z)(C_2 + z) = \\ &= (f + 1)z + (a + 1)C_0 + bC_1 + (a + 1)C_2 + bC_3. \end{aligned} \quad (11.6.102)$$

Разностное множество получается тогда и только тогда, когда  $a + 1 = b$  или  $x = -3$ , и в этом случае  $q = 9 + 4y^2$ . При  $q = p = 1 + 4y^2$  мы имеем тип В, а при  $q = p = 9 + 4y^2$  — тип  $B_0$ . Требование нечетности  $y$  необходимо для того, чтобы  $f$  было нечетно. Типы В и  $B_0$  не случайно были указаны только для простых чисел. Для

степеней  $q = p^r$  простых чисел  $r$  должно быть нечетным и  $p \equiv 1 \pmod{4}$ . Можно показать, что  $p^r = 1 + 4y^2$  и  $p^r = 9 + 4y^2$  в самом деле не имеют решений при нечетном  $r$ , большем 1.

**Теорема 11.6.6.** *Если ни одно из чисел  $m, n, m+n$  не делится на  $e$ , то*

$$R(m, n) = R(n, m) = (-1)^{nf} R(-m-n, n).$$

**Доказательство.** В силу теоремы 11.6.2 если ни одно из чисел  $m, n, m+n$  не делится на  $e$ , то

$$F(\beta^m) F(\beta^n) = R(m, n) F(\beta^{m+n}). \quad (11.6.103)$$

Отсюда непосредственно следует, что  $R(n, m) = R(m, n)$ . Умножив на  $F(\beta^{-m-n})$  и применив (11.6.66), получим

$$\begin{aligned} F(\beta^m) F(\beta^{-m-n}) F(\beta^n) &= \\ &= R(m, n) \beta^{(m+n)(q-1)/2} (qz - T). \end{aligned} \quad (11.6.104)$$

Теперь к левой части применима формула (11.6.103) с  $-m-n$  вместо  $m$ , и мы получаем

$$F(\beta^m) R(-m-n, n) F(\beta^{-m}) = R(m, n) \beta^{(m+n)(q-1)/2} (qz - T). \quad (11.6.105)$$

Далее по (11.6.66)

$$\beta^{m(q-1)/2} (qz - T) R(-m-n, n) = R(m, n) \beta^{(m+n)(q-1)/2} (qz - T). \quad (11.6.106)$$

Сравнивая коэффициенты, получаем

$$R(m, n) = \beta^{-n(q-1)/2} R(-m-n, n). \quad (11.6.107)$$

Так как  $\beta$  — первообразный корень степени  $e$  из единицы и  $q-1 = ef$ , справедливо равенство  $\beta^{(q-1)/2} = (-1)^f$ , поскольку если  $e$  четно, то  $\beta^{e/2} = -1$ , а если  $e$  нечетно, то  $f$  четно и  $\beta^{(q-1)/2} = 1 = (-1)^f$ . Соотношение теоремы установлено.

**Случай  $e = 6$ .** Здесь рассмотрения зависят от кубичного характера числа 2, и соотношение  $F(-1) F(a^2) = a^{2m} F(a) F(-a)$ , где  $g^m = 2$  в  $GF(q)$ , установленное в теореме 11.6.3, показывает, каким образом он влияет на

значения  $R(m, n)$ . В качестве первообразного корня степени 6 из 1 мы берем  $\beta = (1 + \sqrt{-3})/2$ .

Вообще при замене  $\beta$  на  $\beta^j$ , где  $j$  взаимно просто с  $e$ ,  $R(m, n)$  переходит в сопряженное число  $R(jm, jn)$ . Равенство (11.6.73) приводит к тому же самому выражению через  $(h, k)$  для  $R(m, n)$  и сопряженных с ним. Поэтому Диксон вводит термин „приведенный“ для минимального множества значений  $R(m, n)$ , таких, что все другие могут быть получены из этих с помощью соотношений теоремы 11.6.6 и сопряжения. При  $e = 6$  множество приведенных  $R(m, n)$  состоит из  $R(1, 1)$ ,  $R(1, 2)$  и  $R(2, 2)$ .

При  $\alpha = \beta$ , поскольку  $\beta^3 = -1$ , (11.6.80) дает

$$F(\beta^3) F(\beta^2) = \beta^{2m} F(\beta) F(\beta^4), \quad (11.6.108)$$

или

$$R(3, 2) F(\beta^5) = \beta^{2m} R(1, 4) F(\beta^5). \quad (11.6.109)$$

Следовательно,

$$R(3, 2) = \beta^{2m} R(1, 4). \quad (11.6.110)$$

Вычислим

$$[F(\beta^2) F(\beta^2)] F(\beta) = F(\beta^2) [F(\beta^2) F(\beta)],$$

$$R(2, 2) F(\beta^4) F(\beta) = F(\beta^2) R(2, 1) F(\beta^3), \quad (11.6.111)$$

$$R(2, 2) R(4, 1) F(\beta^5) = R(2, 1) R(2, 3) F(\beta^5).$$

Отсюда

$$R(2, 2) R(4, 1) = R(2, 1) R(2, 3). \quad (11.6.112)$$

По теореме 11.6.6

$$R(2, 3) = R(3, 2) = R(1, 2), \quad R(2, 1) = R(1, 2), \quad (11.6.113)$$

$$R(4, 1) = R(1, 4), \quad R(1, 1) = (-1)^f R(4, 1).$$

Используя (11.6.113), представим (11.6.110) в виде

$$R(1, 2) = \beta^{2m} (-1)^f R(1, 1), \quad (11.6.114)$$

а (11.6.112) — в виде

$$R(2, 2) (-1)^f R(1, 1) = R(1, 2)^2. \quad (11.6.115)$$

Комбинируя эти два соотношения, имеем

$$R(1, 1) = (-1)^f \beta^{2m} R(2, 2), \quad (11.6.116)$$

$$R(1, 2) = \beta^{4m} R(2, 2).$$

Диксон ошибочно утверждает, что второе из этих соотношений может быть получено, если в (11.6.80) взять  $a = \beta$ . Далее,  $R(2, 2)$  первоначально было определено в (11.6.74) из соотношения

$$F(\beta^2)F(\beta^2) = R(2, 2)F(\beta^4). \quad (11.6.117)$$

Но  $\beta^2 = \omega$  — первообразный кубический корень из единицы. Обозначив  $R(2, 2)$  через  $R_6(2, 2)$ , чтобы указать, что  $e = 6$ , и заменив в (11.6.117)  $\beta^2$  на  $\omega$ , получим

$$R_6(2, 2) = R_3(1, 1). \quad (11.6.118)$$

Но при  $a, b, c, d$ , взятых из соотношений (11.6.46),

$$R_3(1, 1) = (a + 2d) + 3b\omega + 3c\omega^2. \quad (11.6.119)$$

Поскольку  $\omega = (-1 + \sqrt{-3})/2$ ,

$$\begin{aligned} R_6(2, 2) = R_3(1, 1) &= \frac{(2a + 4d - 3b - 3c) + 3\sqrt{-3}(b - c)}{2} = \\ &= \frac{(L - 3\sqrt{-3}M)}{2}, \end{aligned} \quad (11.6.120)$$

где  $L$  и  $M$  — те же, что в (11.6.51) и (11.6.52).

Мы теперь обладаем достаточной информацией, чтобы определить циклотомические числа для  $e = 6$ . Для разностных множеств нам нужны лишь значения  $q$  с нечетным  $f$ .

*Подслучай*  $e = 6$ ,  $f$  нечетно. Таблица чисел  $(i, j)$  имеет вид

$$\begin{aligned} (0, 0) &(0, 1) (0, 2) (0, 3) (0, 4) (0, 5) \\ (1, 0) &(2, 0) (1, 2) (0, 4) (0, 2) (1, 2) \\ (2, 0) &(2, 1) (1, 0) (0, 5) (1, 2) (0, 1) \\ (0, 0) &(1, 0) (2, 0) (0, 0) (1, 0) (2, 0) \\ (1, 0) &(0, 5) (1, 2) (0, 1) (2, 0) (2, 1) \\ (2, 0) &(1, 2) (0, 4) (0, 2) (1, 2) (1, 0) \end{aligned} \quad (11.6.121)$$

Если ввести обозначения

$$R(2, 2) = \frac{L - 3M\sqrt{-3}}{2},$$

$$R(1, 1) = \frac{E + F\sqrt{-3}}{2}, \quad (11.6.122)$$

$$R(1, 2) = -A + B\sqrt{-3},$$

то выполняются следующие линейные соотношения:

$$\begin{aligned}
 & (0, 0) + (0, 1) + (0, 2) + (0, 3) + (0, 4) + (0, 5) = f, \\
 & (1, 0) + (2, 0) + (1, 2) + (0, 4) + (0, 2) + (1, 2) = f, \\
 & (2, 0) + (2, 1) + (1, 0) + (0, 5) + (1, 2) + (0, 1) = f, \\
 & (0, 0) + (1, 0) + (2, 0) = (f - 1)/2, \\
 & (1, 0) - (2, 0) + (0, 2) - (0, 4) = B, \\
 & (0, 1) + (0, 4) - (0, 2) - (0, 5) + \\
 & \quad + 2(1, 0) - 2(2, 0) = -M, \\
 & (0, 4) - (0, 2) + 3(0, 5) - 3(0, 1) + \\
 & \quad + 2(1, 0) - 2(2, 0) = F, \quad (11.6.123) \\
 & (0, 0) + (0, 2) - (0, 3) + (0, 4) - (1, 0) - (2, 0) - \\
 & \quad - (1, 2) + (2, 1) = -A, \\
 & 6(0, 0) - 3(0, 1) - 3(0, 2) + 2(0, 3) - 3(0, 4) - \\
 & \quad - 3(0, 5) - 6(1, 0) - 6(2, 0) + \\
 & \quad + 12(1, 2) + 4(2, 1) = L, \\
 & 2(0, 0) + 3(0, 1) - (0, 2) - 2(0, 3) - \\
 & \quad - (0, 4) + 3(0, 5) - 2(1, 0) - 2(2, 0) + \\
 & \quad + 4(1, 2) - 4(2, 1) = -E.
 \end{aligned}$$

Первые четыре из этих соотношений получаются из (11.6.38), а остальные — из определения  $R(m, n)$  в (11.6.73) с использованием обозначений (11.6.122). Решение зависит от кубичного характера числа 2 по модулю  $q$ , который определяет соотношения (11.6.116).

Имеем

$$q = A^2 + 3B^2, \quad 4q = L^2 + 27M^2 = E^2 + 3F^2, \quad g^m = 2. \quad (11.6.124)$$

Возможны три случая, зависящие от значения  $m$  по модулю 3 (см. таблицу на стр. 224).

**Теорема 11.6.7.** При  $q = p^r \equiv 7 \pmod{12}$  квадратичные вычеты образуют разностное множество с  $v = q = 4t - 1$ ,  $k = 2t - 1$ ,  $\lambda = t - 1$ . Если  $q = A^2 + 27$ , то кубичные вычеты и класс, состоящий из элементов  $a_i$  с  $\text{Ind}_g(a_i) \equiv 1 \pmod{6}$  и включающий вычет 3, образуют разностное множество с теми же параметрами, принадлежащее типу  $H_6$ .

*Разностное множество, которое имеет вычеты степени 6 в качестве множителей, эквивалентно одному из этих типов.*

*Доказательство.* Если  $D$  – разностное множество в  $\text{GF}(q)$ , которое имеет вычеты 6-й степени в качестве множителей, то  $\theta(d)$  есть сумма одного или более

|          | Два – кубичный вычет<br>$L = -2A$ ,<br>$-3M = 2B$ ,<br>$E = 2A$ , $F = -2B$ | $m \equiv 1 \pmod{3}$<br>$L = A - 3B$<br>$3M = A + B$<br>$E = -A - 3B$<br>$F = -A + B$ | $m \equiv 2 \pmod{3}$<br>$L = A - 3B$<br>$3M = -A + B$<br>$E = -A + 3B$<br>$F = A + B$ |
|----------|---|--|--|
| 36 (0,0) | $q - 11 - 8A$   | $q - 11 - 2A$  | $q - 11 - 2A$  |
| 36 (0,1) | $q + 1 - 2A + 12B$  | $q + 1 + 4A$   | $q + 1 - 2A - 12B$   |
| 36 (0,2) | $q + 1 - 2A + 12B$  | $q + 1 - 2A + 12B$   | $q + 1 - 8A + 12B$   |
| 36 (0,3) | $q + 1 + 16A$   | $q + 1 + 10A - 12B$  | $q + 1 + 10A + 12B$  |
| 36 (0,4) | $q + 1 - 2A - 12B$  | $q + 1 - 8A - 12B$   | $q + 1 - 2A - 12B$   |
| 36 (0,5) | $q + 1 - 2A - 12B$  | $q + 1 - 2A + 12B$   | $q + 1 + 4A$   |
| 36 (1,0) | $q - 5 + 4A + 6B$   | $q - 5 - 2A + 6B$  | $q - 5 + 4A + 6B$  |
| 36 (2,0) | $q - 5 + 4A - 6B$   | $q - 5 + 4A - 6B$  | $q - 5 - 2A - 6B$  |
| 36 (1,2) | $q + 1 - 2A$  | $q + 1 + 4A$   | $q + 1 + 4A$   |
| 36 (2,1) | $q + 1 - 2A$  | $q + 1 - 8A - 12B$   | $q + 1 - 8A + 12B$   |

элементов  $C_i$  и, быть может,  $z$ . Если в  $D$  входит только один класс, то мы можем принять  $\theta(d) = C_0$ . Тогда  $\theta(d^{-1}) = C_3$ , и

$$\begin{aligned} \theta(d)\theta(d^{-1}) &= f + (0, 0)C_0 + (1, 0)C_1 + (2, 0)C_2 + \\ &\quad + (0, 0)C_3 + (1, 0)C_4 + (2, 0)C_5, \end{aligned} \quad (11.6.125)$$

где  $(0, 0) = (1, 0) = (2, 0)$ , если  $\theta(d)$  – разностное множество. Отсюда вытекает, что если 2 – кубичный вычет, то  $B = 0$ ,  $12A = -6$ , а это невозможно. При  $m \equiv 1 \pmod{3}$  должно быть  $A = -2$ ,  $B = -1$ , следовательно,  $q = 7$ , и „разностное множество“ состоит из одного единственного вычета. Аналогично при  $m \equiv 2 \pmod{3}$  мы находим  $A = -2$ ,  $B = 1$  и  $q = 7$ . Случай  $\theta(d) = z + C_0$  приводит к соотношению  $(0, 0) + 1 = (1, 0) = (2, 0)$ . Если 2 – кубичный вычет, отсюда следует, что  $B = 0$ ,  $12A = 30$ , а это

невозможно. При  $m \equiv \pm 1 \pmod{3}$  мы находим  $A = 10$ ,  $B = \pm 5$ ,  $q = 175$ , что снова невозможно.

Для  $\theta(d) = C_0 + C_1 + C_3$

$$\begin{aligned} \theta(d)\theta(d^{-1}) &= 3f + RC_0 + SC_1 + TC_2 + \\ &\quad + RC_3 + SC_4 + TC_5, \end{aligned} \quad (11.6.126)$$

откуда в зависимости от значения  $m$  по модулю 3

$$\begin{array}{lll} m \equiv 0 & m \equiv 1 & m \equiv 2 \\ 36R = 9q - 45 + 6B, & 9q - 45 - 18B, & 9q - 45 + 6A - 6B, \\ 36S = 9q - 27, & 9q - 27 - 6A + 12B, & 9q - 27 - 6A - 12B, \\ 36T = 9q - 9 - 6B, & 9q - 9 + 6A + 6B, & 9q - 9 + 18B. \end{array} \quad (11.6.127)$$

Для того чтобы получить разностное множество, мы должны иметь  $R = S = T$ . Если 2 — кубический вычет и  $m \equiv 0 \pmod{3}$ , то  $B = 3$ . При  $m \equiv 1 \pmod{3}$  получаем  $A = -2$ ,  $B = -1$  и, следовательно,  $q = 7$ . При  $m \equiv 2 \pmod{3}$  находим  $A = 2$ ,  $B = -1$  и  $q = 7$ . Когда  $q = 7$ , вычеты 1, 5, 6 образуют разностное множество, эквивалентное множеству квадратичных вычетов 1, 2, 4. В первом случае при  $B = 3$  мы имеем  $q = A^2 + 27$ . Это приводит к типу  $H_6$ . Здесь  $4q = (2A)^2 + 27(2^2)$ , и из этого представления по теореме 11.6.1 получаем, что 2 есть кубический вычет, если  $q = p$  — простое число, а также если это подходящее представление  $q$ , степени простого числа. Поскольку  $-3M = 2B$ , если 2 — кубический вычет,  $B = 3$  влечет за собой  $M = -2$ , и по теореме 11.6.1 индекс вычета 3 сравним с 1 по модулю 3. Для  $q \equiv 7 \pmod{12}$  число 3 есть квадратичный невычет. Следовательно, вычет 3 находится в классе  $K_1 = \{g^u; u \equiv 1 \pmod{6}\}$  при надлежащем выборе первообразного корня, дающего значения в (11.6.73). Таким образом, наше разностное множество  $D$  состоит из кубических вычетов и класса, состоящего из элементов  $a_i$  с  $\text{Ind}_g(a_i) \equiv 1 \pmod{6}$  и включающего вычет 3. Разумеется, квадратичные вычеты дают разностное множество типа Q. Никакие другие комбинации, для которых вычеты 6-й степени являются множителями, не дают иных разностных множеств, хотя, конечно, при замене

первообразного корня и  $B = -3$  мы снова получим разностное множество  $D$  типа  $H_6$  с  $\theta(d) = C_0 + C_3 + C_5$ .

*Случай  $e = 8$ , f нечетно.* Здесь

$$q = x^2 + 4y^2 = a^2 + 2b^2, \quad x \equiv a \equiv 1 \pmod{4}. \quad (11.6.128)$$

Таблица для  $(i, j)$  имеет вид

|        |        |        |        |        |        |        |        |
|--------|--------|--------|--------|--------|--------|--------|--------|
| (0, 0) | (0, 1) | (0, 2) | (0, 3) | (0, 4) | (0, 5) | (0, 6) | (0, 7) |
| (1, 0) | (1, 1) | (1, 2) | (1, 3) | (0, 5) | (1, 3) | (0, 3) | (1, 7) |
| (2, 0) | (2, 1) | (2, 0) | (1, 7) | (0, 6) | (1, 3) | (0, 2) | (1, 2) |
| (1, 1) | (2, 1) | (2, 1) | (1, 0) | (0, 7) | (1, 7) | (1, 2) | (0, 1) |
| (0, 0) | (1, 0) | (2, 0) | (1, 1) | (0, 0) | (1, 0) | (2, 0) | (1, 1) |
| (1, 0) | (0, 7) | (1, 7) | (1, 2) | (0, 1) | (1, 1) | (2, 1) | (2, 1) |
| (2, 0) | (1, 7) | (0, 6) | (1, 3) | (0, 2) | (1, 2) | (2, 0) | (2, 1) |
| (1, 1) | (1, 2) | (1, 3) | (0, 5) | (0, 3) | (0, 3) | (1, 3) | (1, 0) |

и входящие в нее числа принимают следующие значения:

| Если 2 — четверичный вычет             | Если 2 — четверичный невычет |
|--|------------------------------|
| $64(0, 0) \quad q - 15 - 2x$           | $q - 15 - 10x - 8a$          |
| $64(0, 1) \quad q + 1 + 2x - 4a + 16y$ | $q + 1 + 2x - 4a - 16b$      |
| $64(0, 2) \quad q + 1 + 6x + 8a - 16y$ | $q + 1 - 2x + 16y$           |
| $64(0, 3) \quad q + 1 + 2x - 4a - 16y$ | $q + 1 + 2x - 4a - 16b$      |
| $64(0, 4) \quad q + 1 - 18x$           | $q + 1 + 6x + 24a$           |
| $64(0, 5) \quad q + 1 + 2x - 4a + 16y$ | $q + 1 + 2x - 4a + 16b$      |
| $64(0, 6) \quad q + 1 + 6x + 8a + 16y$ | $q + 1 - 2x - 16y$           |
| $64(0, 7) \quad q + 1 + 2x - 4a - 16y$ | $q + 1 + 2x - 4a + 16b$      |
| $64(1, 0) \quad q - 7 + 2x + 4a$       | $q - 7 + 2x + 4a + 16y$      |
| $64(1, 1) \quad q - 7 + 2x + 4a$       | $q - 7 + 2x + 4a - 16y$      |
| $64(1, 2) \quad q + 1 - 6x + 4a + 16b$ | $q + 1 + 2x - 4a$            |
| $64(1, 3) \quad q + 1 + 2x - 4a$       | $q + 1 - 6x + 4a$            |
| $64(1, 7) \quad q + 1 - 6x + 4a - 16b$ | $q + 1 + 2x - 4a$            |
| $64(2, 0) \quad q - 7 - 2x - 8a$       | $q - 7 + 6x$                 |
| $64(2, 1) \quad q + 1 + 2x - 4a$       | $q + 1 - 6x + 4a$            |

При этих значениях мы находим, что множество  $D$  с  $\theta(d) = C_0$  — разностное множество, если  $x = 1$ ,  $a = -3$ , и это приводит к разностным множествам типа  $O$ . Множество  $D$  с  $\theta(d) = C_0 + z$  — также разностное множество, если  $x = +21$ ,  $a = -7$ , — множество типа  $O_0$ .

Мы продолжим, переходя к разностным множествам типа  $T$ . Пусть  $p^r$  и  $q^s$  — степени простых чисел, такие, что  $p^r + 2 = q^s$ . (Это включает случай  $5^2 + 2 = 3^3$ , но автор не знает никакого другого примера, когда  $r > 1$  и  $s > 1$ .) Рассмотрим систему  $(a, b)$  упорядоченных пар  $a \in GF(p^r)$ ,  $b \in GF(q^s)$ , оперируя с ними по правилам

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{и} \quad (a, b)(c, d) = (ac, bd).$$

Эта система называется *прямой суммой*  $GF(p^r)$  и  $GF(q^s)$  и обозначается через

$$S = GF(p^r) \oplus GF(q^s).$$

Если  $p$  и  $q$  — простые числа, то  $GF(p) \oplus GF(q)$  есть система вычетов по модулю  $pq$ , где  $e \equiv (1, 0)$  и  $f \equiv (0, 1)$  есть такие вычеты по модулю  $pq$ , что

$$e \equiv 1 \pmod{p}, \quad e \equiv 0 \pmod{q} \quad \text{и} \quad f \equiv 0 \pmod{p}, \quad f \equiv 1 \pmod{q}.$$

Образуем в  $S$  множество  $D$  из следующих пар:

- 1)  $(c, d)$ , где  $c$  и  $d$  — ненулевые квадраты;
- 2)  $(g, h)$ , где  $g$  и  $h$  — не квадраты;
- 3) пары  $(u, 0)$ .

Так как (за исключением  $p^r = 2$ ,  $q^s = 4$ )  $p^r$  и  $q^s$  оба нечетны, существует

$$(p^r - 1)(q^s - 1)/4$$

пар типа 1 и такое же число пар типа 2, а также  $p^r$  пар типа 3. Тогда  $D$  содержит  $k = [(p^r q^s - p^r - q^s + 1)/2] + p^r$  элементов, и при  $v = p^r q^s$ , замечая, что  $q^s = p^r + 2$ , мы получаем  $k = (v - 1)/2$ . Так как  $p^r$  и  $q^s$  нечетны и отличаются на 2, одно из них сравнимо с 1 по модулю 4, а другое — с 3 по модулю 4.

Поэтому  $v = p^r q^s \equiv -1 \pmod{4}$ , и если  $v = 4t - 1$ , то  $k = 2t - 1$ . Множество  $D$  — такая система в  $S$ , что совокупность  $M$  всех пар типа 1 и 2 можно рассматривать как множители системы.

Далее,  $(-1, -1)$  не содержится в  $D$ , так как  $-1$  есть квадратичный вычет в одном из полей  $\text{GF}(p')$ ,  $\text{GF}(q^s)$  и невычет — в другом.

Если  $(x, y) - (z, w) = (a, b)$ , где  $(x, y), (z, w) \in D$ , и  $(m_1, m_2) \in M$ , то, умножая на  $(m_1, m_2)$ , получаем

$$(m_1x, m_2y) - (m_1z, m_2w) = (m_1a, m_2b).$$

Следовательно, элементы  $(a, b)$  и  $(m_1a, m_2b)$  появляются одинаково часто как разности элементов множества  $D$ . Элементы  $S$  можно подразделить на классы эквивалентности относительно умножения на пары из  $M$  следующим образом:

- $(a, b)$ ,  $a, b$  — одного и того же квадратичного типа <sup>1)</sup>;
- $(c, d)$ ,  $c, d$  — противоположных квадратичных типов <sup>2)</sup>;
- $(e, 0)$ ,  $e \neq 0$ ;
- $(0, f)$ ,  $f \neq 0$ ;
- $(0, 0)$ .

Если  $(x, y) - (z, w) = (a, b)$  с  $(x, y), (z, w) \in D$ , то

$$(z, w) - (x, y) = (-a, -b).$$

Поскольку  $(-1, -1)$  не содержится в  $D$ , то если  $a, b$  — одного и того же квадратичного типа,  $-a, -b$  будут противоположных квадратичных типов. Поэтому все элементы  $(a, b)$ ,  $a \neq 0, b \neq 0$ , системы  $S$  появляются одно и то же число раз (скажем,  $\lambda_1$ ) в качестве разностей элементов множества  $D$ . Пусть пара вида  $(e, 0)$ ,  $e \neq 0$ , задана в виде разности

$$(a_1, b) - (a_2, b) = (a_1 - a_2, 0), \quad b \neq 0,$$

для каждого из  $q^s - 1$  значений  $b$  ( $b$  фиксировано) с различными элементами  $a_1$  и  $a_2$ , квадратичный тип которых тот же, что и у  $b$ .

Таких разностей всего  $(q^s - 1)(p' - 1)(p' - 3)/4$ . Для элементов типа  $(u, 0)$  в  $D$

$$(u_1, 0) - (u_2, 0) = (u_1 - u_2, 0),$$

<sup>1)</sup> То есть либо и  $a$ , и  $b$  — квадратичные вычеты, либо оба — квадратичные невычеты. — Прим. перев.

<sup>2)</sup> То есть одно из чисел  $a$  и  $b$  — квадратичный вычет, а другое — квадратичный невычет. — Прим. перев.

и таких разностей с  $u_1 \neq u_2$  всего  $p^r(p^r - 1)$ . Так как для каждого  $e \neq 0$  пара  $(e, 0)$  представляется в виде разности пар одинаковое число раз, то для каждого из  $p^r - 1$  элементов  $(e, 0)$ ,  $e \neq 0$ , будет

$$\lambda = \frac{(q^s - 1)(p^r - 3)}{4} + p^r = \frac{p^r q^s - 3}{4}$$

таких представлений. Так как  $q^s = p^r + 2$  и  $v = p^r q^s = 4t - 1$ , мы находим, что  $\lambda = (v - 3)/4 = t - 1$ .

Пары вида  $(0, f)$ ,  $f \neq 0$ , получаются в виде разностей пар из  $D$  тремя способами:  $(a, b_1) - (a, b_2) = (0, b_1 - b_2)$ ,

$$(a, b) - (a, 0) = (0, b), \quad (a, 0) - (a, b) = (0, -b).$$

В первом случае мы имеем  $(p^r - 1)(q^s - 1)(q^s - 3)/4$  таких разностей, а в двух других — всего  $2(p^r - 1)(q^s - 1)/2$  разностей. Поэтому для каждого из  $q^s - 1$  значений  $f$ ,  $f \neq 0$ , число таких представлений пары  $(0, f)$  равно

$$\frac{(p^r - 1)(q^s - 3)}{4} + p^r - 1 = \frac{p^r q^s - 3}{4} = \frac{v - 3}{4} = t - 1,$$

если учесть, что  $q^s = p^r + 2$ .

Пары  $(e, 0)$ ,  $e \neq 0$ , и  $(0, f)$ ,  $f \neq 0$ , представляются  $\lambda = t - 1$  раз в виде разности двух пар из  $D$ , а общее число ненулевых разностей элементов из  $D$  равно  $k(k - 1)$ . Таким образом, поскольку каждый из  $(p^r - 1) \times (q^s - 1)$  элементов  $(a, b)$ ,  $a \neq 0$ ,  $b \neq 0$ , появляется  $\lambda_1$  раз, мы имеем

$$k(k - 1) = (p^r - 1)(q^s - 1)\lambda_1 + (p^r - 1)(t - 1) + (q^s - 1)(t - 1).$$

Так как  $k = 2t - 1$ ,  $v = p^r q^s = 4t - 1$ , получаем

$$\begin{aligned} (p^r - 1)(q^s - 1)\lambda_1 &= (t - 1)(4t - 2 - p^r - q^s + 2) = \\ &= (t - 1)(p^r q^s - p^r - q^s + 1); \end{aligned}$$

следовательно,  $\lambda_1 = t - 1$ .

Таким образом, каждая ненулевая пара  $(a, b)$  в  $S$  представляется  $\lambda = t - 1$  раз в виде разности элементов из  $D$ , и  $D$  дает разностное множество типа Т с

$$v = p^r q^s = 4t - 1, \quad q^s = p^r + 2, \quad k = 2t - 1, \quad \lambda = t - 1.$$

Вывод для типа  $W_4$  по существу аналогичен выводу для типа Т. За доказательствами читатель отсылается к работе Уитмена [1].

# Конечные геометрии

---

## 12.1. Основания

С точки зрения настоящей книги, геометрия есть частный вид системы инцидентности, в которой неопределяемые элементы суть „точки“ и „прямые“, а основное отношение — отношение инцидентности  $P \equiv L$ , которое гласит: „точка  $P$  лежит на прямой  $L$ “ или „прямая  $L$  содержит (проходит через) точку  $P$ “. Веблен и Юнг [1] рассматривают точки как неопределяемые элементы, а прямые — как некоторые выделенные подмножества точек. Согласно аксиомам, две различные прямые не могут содержать одни и те же точки. Таким образом, различие между этими точками зрения небольшое. *Конечной геометрией* называется геометрия, в которой число точек конечно.

**Аксиомы проективной геометрии:**

**PG1.** Существует одна и только одна прямая, проходящая через две различные точки.

**PG2.** Если  $A, B, C$  — три точки, не лежащие на одной прямой,  $D \neq A$  — точка на прямой, проходящей через  $A$  и  $B$ , и  $E \neq A$  — точка на прямой, проходящей через  $A$  и  $C$ , то существует точка  $F$ , лежащая как на прямой, проходящей через  $D$  и  $E$ , так и на прямой, проходящей через  $B$  и  $C$ .

**PG3.** Каждая прямая содержит не меньше трех различных точек.

Веблен и Юнг [1] определяют „размерность“ проективного пространства индуктивно: точка есть пространство размерности нуль, прямая — размерности 1; и по индукции, если  $X_{n-1}$  есть пространство размерности  $n-1$ ,  $P$  — точка, не содержащаяся в  $X_{n-1}$ , то множество всех точек на всех прямых  $PB$ , где  $B$  — точка из  $X_{n-1}$ , есть пространство  $X_n$  размерности  $n$ . В духе этого опре-

деления целесообразно принять  $-1$  за размерность пустого пространства, которое не содержит ни одной точки. Доказывается, что пространство  $X_n$  определяется любым пространством  $X_{n-1}$  и точкой  $P \notin X_{n-1}$ , где  $X_{n-1}$  и  $P$  содержатся в  $X_n$ . Подпространства проективного пространства  $X$  образуют структуру, в которой, если  $A$  и  $B$  — подпространства  $X$ , то пересечение  $A \cap B$  — подпространство всех точек, принадлежащих и  $A$ , и  $B$ , а объединение  $A \cup B$  состоит из всех точек, лежащих на прямых, соединяющих какую-либо точку  $P$  из  $A$  с какой-либо точкой  $Q$  из  $B$ . Можно показать, что в силу этого определения  $A \cup B$  есть подпространство. Размерность  $d(A)$  подпространств удовлетворяет следующему соотношению:

$$d(A \cup B) + d(A \cap B) = d(A) + d(B). \quad (12.1.1)$$

Отсюда и из свойства: если  $R \subseteq S$  и  $d(R) = d(S)$ , то  $R = S$ , получаем свойство модулярности для подпространств.

**Свойство модулярности.** Если  $A \supseteq B$ , то

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

**Конфигурацией** называется конечное множество точек и прямых с инцидентностями специального вида. С конфигурациями связаны две важные теоремы.

**Теорема 12.1.1 (теорема Дезарга).** Если  $O, A_1, B_1, C_1, A_2, B_2, C_2$  — различные точки и если  $OA_1A_2, OB_1B_2, OC_1C_2$  — различные прямые, причем  $A_1B_1$  и  $A_2B_2$  пересекаются в некоторой точке  $C_3$ ,  $A_1C_1$  и  $A_2C_2$  пересекаются в некоторой точке  $B_3$ ,  $B_1C_1$  и  $B_2C_2$  пересекаются в некоторой точке  $A_3$ , то точки  $A_3, B_3, C_3$  лежат на одной прямой (рис. 12.1).

**Теорема 12.1.2 (теорема Паппа).** Если  $A_1, B_1, C_1$  — точки некоторой прямой, а  $A_2, B_2, C_2$  — точки другой прямой, лежащей в той же плоскости, и если  $A_1B_2$  и  $A_2B_1$  пересекаются в точке  $C_3$ ,  $A_1C_2$  и  $A_2C_1$  пересекаются в точке  $B_3$ , а  $B_1C_2$  и  $B_2C_1$  пересекаются в точке  $A_3$ , то  $A_3, B_3, C_3$  лежат на одной прямой (рис. 12.2).

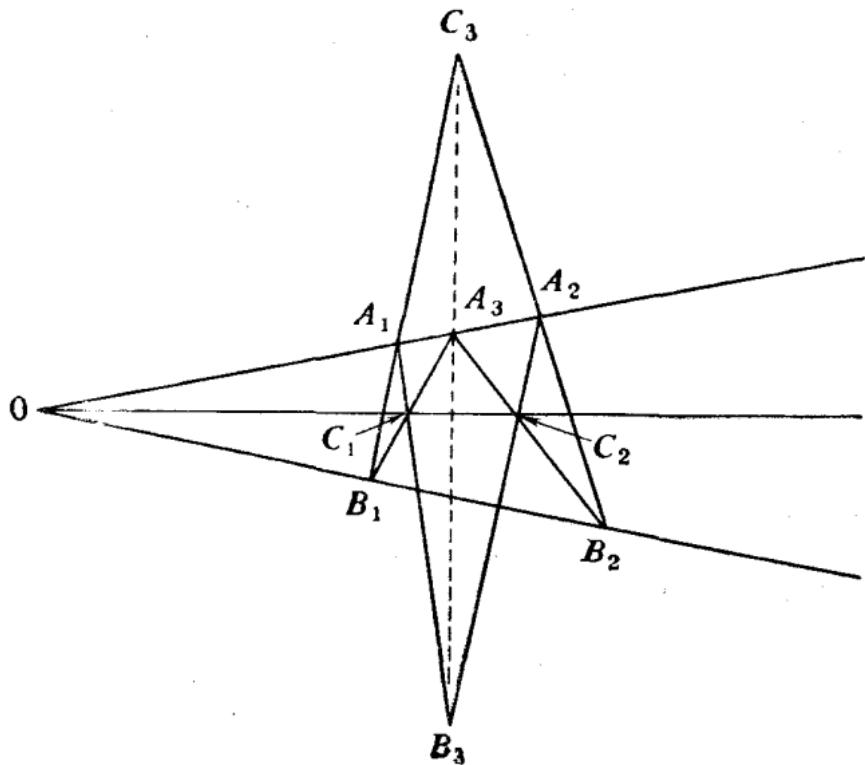


Рис. 12.1. Теорема Дезарга.

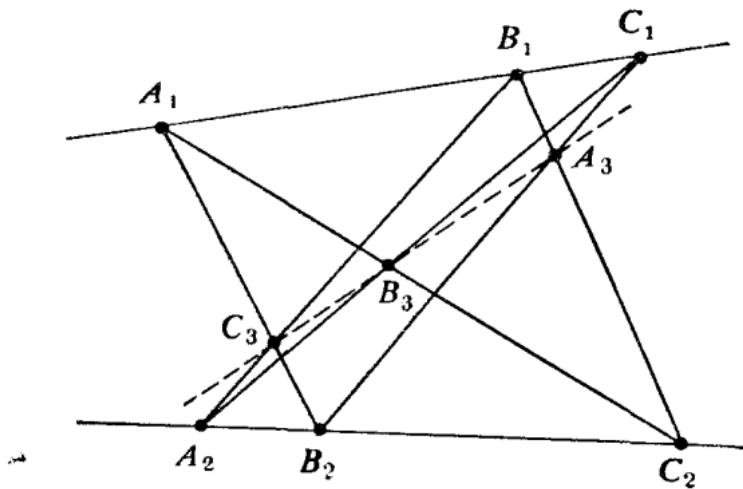


Рис. 12.2. Теорема Паппа.

Мы не будем здесь доказывать теорем 12.1.1 и 12.1.2. Читатель может найти доказательства в книге Веблена и Юнга [1] или в более современной книге Блюменталя [1]<sup>1</sup>).

**Теорема 12.1.3.** *Теорема Дезарга справедлива в любом проективном пространстве размерности 3 и выше. Если теорема Дезарга справедлива в проективной плоскости  $\pi$ , то  $\pi$  может быть вложена в проективное пространство  $S_n$  любой конечной размерности  $n \geq 3$ , и при данном  $n$  пространство  $S_n$  единственно с точностью до изоморфизма.*

Существуют проективные плоскости, в которых теорема Дезарга не выполняется. Мы будем говорить о *дезарговой* или *недезарговой* плоскостях в зависимости от того, справедлива или нет в данной плоскости теорема Дезарга.

**Теорема 12.1.4** (введение координат). *В дезарговой плоскости  $S_2$  или в проективном пространстве  $S_n$ ,  $n \geq 3$ , можно ввести координаты так, чтобы точка  $P$  представлялась левыми скалярными кратными  $(n+1)$ -мерного ненулевого вектора над некоторым телом  $R$ :*

$$P = u(x_1, \dots, x_{n+1}) = (ux_1, \dots, ux_{n+1}), \\ (x_1, \dots, x_{n+1}) \neq (0, \dots, 0).$$

Если  $P_1 = u_1(x_1, \dots, x_{n+1})$  и  $P_2 = u_2(y_1, \dots, y_{n+1})$  — различные точки, то ненулевые векторы вида

$$uQ = u_1P_1 + u_2P_2 = (u_1x_1 + u_2y_1, \dots, u_1x_{n+1} + u_2y_{n+1})$$

представляют точки на прямой, соединяющей  $P_1$  и  $P_2$ . Тело  $R$  определяется единственным образом пространством  $S_n$ . Векторы  $(1, 0, \dots, 0)$ ,  $(0, 1, \dots, 0)$ ,  $\dots$ ,  $(0, 0, \dots, 1)$  и  $(1, 1, \dots, 1)$  могут быть взяты за координаты любых  $n+2$  точек  $P_1, \dots, P_{n+2}$ , таких, что никакое подмножество из  $n+1$  этих точек не лежит ни в каком  $S_{n-1}$ . Тогда координаты всех других точек определяются однозначно. Обратно, если дано произ-

<sup>1</sup>) См. также статью: Л. А. Скорняков, Проективные плоскости, УМН, 6:6 (46) (1951), 112–154. — Прим. перев.

сольное тело  $R$ , то точки и прямые, указанные выше, образуют дезаргово проективное пространство  $S_n$ .

**Теорема 12.1.5.** Из теоремы Паппа следует теорема Дезарга, а также коммутативность умножения в  $R$ ; следовательно, тело координат  $R$  есть поле  $F$ . Обратно, в проективном пространстве с координатами из поля  $F$  справедлива теорема Паппа.

В силу теоремы 12.1.4 число точек на прямой бесконечно, если тело  $R$  бесконечно. Поэтому в случае конечной геометрии тело  $R$  конечно. По теореме Веддербёрна (см. ниже) отсюда следует, что в конечной дезарговой геометрии справедлива также теорема Паппа.

**Теорема 12.1.6 (Веддербёрн).** Конечное тело есть конечное поле.

Очень краткое доказательство теоремы Веддербёрна дано Виттом [1].

В проективном пространстве  $S_n$  с координатами из тела  $R$  множество ненулевых точек  $P = u(x_1, \dots, x_{n+1})$ , удовлетворяющих линейному уравнению

$$x_1a_1 + x_2a_2 + \dots + x_{n+1}a_{n+1} = 0, \quad (12.1.2)$$

есть  $S_{n-1}$ . Это подпространство называется *гиперплоскостью*. Каждое  $S_{n-1}$  в  $S_n$  может быть определено таким образом. Следовательно, гиперплоскости можно сопоставить с векторами  $[a_1, \dots, a_{n+1}] \neq 0$  и их правыми кратными  $[a_1v, \dots, a_{n+1}v]$ . Иногда удобно считать проективную геометрию определяемой точками  $P = u(x_1, \dots, x_{n+1})$  и гиперплоскостями  $S_{n-1} = [a_1, \dots, a_{n+1}] v$  с отношением инцидентности  $P \in S_{n-1}$  в том и только в том случае, когда выполняется (12.1.2).

Мы можем образовать тело  $R^*$ , *двойственное* к  $R$ , если возьмем элементы  $R$  в качестве элементов  $R^*$ , сохраним ту же операцию сложения, но определим умножение  $x \circ y$  в  $R^*$  правилом

$$x \circ y = yx \text{ в } R. \quad (12.1.3)$$

Это дает соответствие

$$\begin{aligned} [a_1, \dots, a_{n+1}] v &\rightarrow v \circ (a_1, \dots, a_{n+1}), \\ u(x_1, \dots, x_{n+1}) &\rightarrow [x_1, \dots, x_{n+1}] \circ u, \end{aligned} \quad (12.1.4)$$

или

$$P \rightarrow P^*, \quad K \rightarrow K^*, \quad (12.1.5)$$

где  $P$  — точка,  $K$  — гиперплоскость в  $S_n(R)$ , а  $P^*$  — гиперплоскость,  $K^*$  — точка в  $S_n(R^*)$  и

$$K^* \equiv P^* \text{ тогда и только тогда, когда } P \equiv K. \quad (12.1.6)$$

Если гиперплоскости рассматривать как блоки схемы, а точки — как элементы, то эта двойственность — не что иное, как двойственность, рассмотренная ранее [см. (10.2.13)].

Точками *аффинного* пространства  $A_n$  размерности  $n$  над телом  $R$  будут

$$P = (x_1, \dots, x_n), \quad x_i \in R, \quad (12.1.7)$$

и если  $P, Q = (y_1, \dots, y_n)$  — различные точки, то прямая, соединяющая  $P$  и  $Q$ , состоит из всех точек  $T$ , таких, что

$$T = t(x_1, \dots, x_n) + (1 - t)(y_1, \dots, y_n), \quad t \in R. \quad (12.1.8)$$

Аффинное пространство  $A_n$  может быть получено из проективного пространства  $S_n$  удалением некоторой гиперплоскости, которая рассматривается затем как бесконечно удаленная. Это легко можно описать в терминах координат: из совокупности всех точек проективного пространства  $P = u(x_1, \dots, x_n, x_{n+1})$  мы удаляем точки с  $x_{n+1} = 0$  (т. е. гиперплоскость  $x_{n+1} = 0$ ) и фиксируем множитель  $u$ , полагая  $ux_{n+1} = 1$ . Тогда  $P = (y_1, \dots, y_n, 1)$ , или, в аффинной форме,  $(y_1, \dots, y_n)$ .

## 12.2. Конечные геометрии как блок-схемы

Пусть задана проективная геометрия  $S_n$  размерности  $n$  над конечным полем  $F_q = GF(q)$  с  $q = p^m$  элементами, где  $p$  — простое число. Мы будем иногда обозначать это через  $S_n = PG(n, q)$ . Из теоремы 12.1.4 следует, что все  $q^{n+1} - 1$  векторов

$$(x_1, \dots, x_{n+1}) \neq 0, \quad x_i \in GF(q),$$

распадаются на множества из  $q - 1$  векторов, каждое из которых представляет точку. Следовательно,  $S_n$  содержит  $(q^{n+1} - 1)/(q - 1)$  точек. Гиперплоскость  $S_{n-1}$  в  $S_n$  содержит  $(q^n - 1)/(q - 1)$  точек. Поскольку  $S_n$  является объединением любых двух различных гиперплоскостей  $S_{n-1}$ , из соотношения для размерностей (12.1.1) следует, что пересечение любых двух гиперплоскостей есть  $S_{n-2}$  с  $(q^{n-1} - 1)/(q - 1)$  точками. Следовательно, гиперплоскости в  $S_n$  образуют симметричную блок-схему с

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^n - 1}{q - 1}, \quad \lambda = \frac{q^{n-1} - 1}{q - 1}. \quad (12.2.1)$$

По теореме Зингера (теорема 11.3.1) эта схема обладает циклическим автоморфизмом порядка  $v$  и может быть представлена разностным множеством. Полная группа автоморфизмов этой схемы имеет значительно больший порядок, так как она является полной группой коллинеаций пространства  $S_n$ . Порядок полной группы коллинеаций равен

$$m (q^{n+1} - 1)(q^{n+1} - q) \dots (q^{n+1} - q^n)/(q - 1).$$

Эта группа представляет собой проективную группу всех невырожденных матриц порядка  $n + 1$  над  $\text{GF}(p^m)$ , объединенную с группой автоморфизмов  $\text{GF}(p^m)$ . При этом матрицы, отличающиеся скалярным множителем (таких множителей  $q - 1$ ), определяют одну и ту же коллинеацию, а группа автоморфизмов поля  $\text{GF}(p^m)$  — циклическая порядка  $m$ .

Из  $\text{PG}(n, q)$  можно образовать несимметричные схемы, взяв точки в качестве элементов и пространства  $S_s$ ,  $1 \leq s \leq n - 1$ , в качестве блоков. В  $S_n$  имеется всего  $(q^{n+1} - 1)/(q - 1)$  точек, и для определения  $S_s$  мы можем выбрать  $s + 1$  независимых представителей точек  $(q^{n+1} - 1)(q^{n+1} - q)(q^{n+1} - q^2) \dots (q^{n+1} - q^s)$  способами. Но внутри  $S_s$  эти  $s + 1$  независимых представителей могут быть выбраны  $(q^{s+1} - 1)(q^{s+1} - q) \dots (q^{s+1} - q^s)$  способами. Таким образом, число  $b$  блоков, т. е. число различных подпространств  $S_s$ , есть частное этих двух величин.

Поэтому для такой схемы

$$\begin{aligned} b &= \frac{(q^{n+1}-1)(q^{n+1}-q)\dots(q^{n+1}-q^s)}{(q^{s+1}-1)(q^{s+1}-q)\dots(q^{s+1}-q^s)}, \\ v &= \frac{q^{n+1}-1}{q-1}, \\ r &= \frac{(q^{n+1}-q)(q^{n+1}-q^2)\dots(q^{n+1}-q^s)}{(q^{s+1}-q)(q^{s+1}-q^2)\dots(q^{s+1}-q^s)}, \quad (12.2.2) \\ k &= \frac{q^{s+1}-1}{q-1}, \\ \lambda &= \frac{(q^{n+1}-q^2)\dots(q^{n+1}-q^s)}{(q^{s+1}-q^2)\dots(q^{s+1}-q^s)}. \end{aligned}$$

Аналогично подпространства данной размерности аффинного пространства образуют блок-схему. Аффинное пространство  $A_n$  размерности  $n$  над конечным полем  $\text{GF}(q)$ ,  $q = p^r$ , содержит  $q^n$  точек. Взяв точки в качестве элементов и подпространства  $A_s$ ,  $1 \leq s \leq n-1$ , в качестве блоков, мы получим блок-схему с параметрами

$$\begin{aligned} b &= \frac{q^n(q^n-1)\dots(q^n-q^{s-1})}{q^s(q^s-1)\dots(q^s-q^{s-1})}, \\ v &= q^n, \\ r &= \frac{(q^n-1)(q^n-q)\dots(q^n-q^{s-1})}{(q^s-1)(q^s-q)\dots(q^s-q^{s-1})}, \quad (12.2.3) \\ k &= q^s, \\ \lambda &= \frac{(q^n-q)\dots(q^n-q^{s-1})}{(q^s-q)\dots(q^s-q^{s-1})}. \end{aligned}$$

Заметим, что блок-схема (даже симметричная) с параметрами, соответствующими какой-либо геометрии, не обязательно является геометрией.

Например, при  $v=31$ ,  $k=15$ ,  $\lambda=7$  существуют два разностных множества:

$$\begin{aligned} B_0 &= \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\} \\ &\quad (\text{mod } 31), \\ B'_0 &= \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\} \\ &\quad (\text{mod } 31). \end{aligned} \quad (12.2.4)$$

Из них первое состоит из гиперплоскостей четырехмерного пространства  $\text{PG}(4, 2)$ . Второе состоит из квадратичных вычетов по модулю 31. В нем блоки  $B'_0$ ,  $B'_1$  и  $B'_2$  имеют три общих элемента: 9, 10 и 20, в то время как  $B'_0$ ,  $B'_1$  и  $B'_4$  имеют четыре общих элемента: 5, 8, 10, 19. Но над  $\text{GF}(2)$  проективная прямая имеет три точки, а плоскость — семь точек. Следовательно, вторая схема не есть  $\text{PG}(4, 2)$ .

### 12.3. Конечные плоскости

Для проективных плоскостей аксиомы разд. 12.1 могут быть сформулированы в более простой форме.

Аксиомы для проективных плоскостей:

PP1. Существует одна и только одна прямая, проходящая через две различные точки.

PP2. Существует одна и только одна точка, общая двум различным прямым.

PP3. Существуют четыре точки, из которых никакие три не лежат на одной прямой.

Аксиома PG2 может быть интерпретирована так: две прямые в одной и той же плоскости имеют точку пересечения. Тогда аксиома PP2 означает, что все прямые лежат в одной и той же плоскости. Из аксиомы PP3 легко получается аксиома PG3. Первые две аксиомы, PP1 и PP2, очевидно, устанавливают двойственность между точками и прямыми, и нетрудно показать, что аксиома PP3 эквивалентна двойственной аксиоме

PP3'. Существуют четыре прямые, никакие три из которых не проходят через одну и ту же точку.

Имеется мало общих результатов, полученных для конечных проективных плоскостей. Один несложный результат дает следующая

Теорема 12.3.1. Пусть  $n \geq 2$  — целое число. В проективной плоскости  $\pi$  любое из следующих свойств влечет все остальные:

1. Некоторая прямая содержит точно  $n + 1$  точек.
2. Некоторая точка лежит точно на  $n + 1$  прямых.

3. Каждая прямая содержит точно  $n+1$  точек.
4. Каждая точка лежит точно на  $n+1$  прямых.
5. В  $\pi$  существует точно  $n^2+n+1$  точек.
6. В  $\pi$  существует точно  $n^2+n+1$  прямых.

**Доказательство.** Пусть  $A, B, C, D$  — четыре точки, из которых никакие три не лежат на одной прямой. Существование таких точек обеспечено аксиомой РРЗ. Тогда мы имеем прямые  $L_1, \dots, L_6$ , содержащие  $A, B, C, D$  и еще три точки  $X, Y, Z$ :

$$\begin{aligned} L_1: & A, B, X, \dots, \\ L_2: & A, C, Y, \dots, \\ L_3: & A, D, Z, \dots, \\ L_4: & B, C, Z, \dots, \\ L_5: & B, D, Y, \dots, \\ L_6: & C, D, X, \dots, \end{aligned} \quad (12.3.1)$$

где  $X, Y, Z$  — точки пересечения пар прямых  $L_1, L_6$ ;  $L_2, L_5$  и  $L_3, L_4$ . Из аксиом 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 инциденций 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  $L_4$ .

Обратимся теперь к доказательству теоремы и допустим, что выполняется свойство 1. 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 (12.3.1) 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  $n + 1$  точек, 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  $n + 1$  точек, т. е. каждая прямая, исключая, быть может,  $L_1 = ABX$ , содержит точно  $n + 1$  точек. Тогда  $L_2 = ACY$  содержит точно  $n + 1$  точек, и точка  $Z$ , не лежащая на  $L_2$ , лежит точно на  $n + 1$  прямых; следовательно,  $L_1$  которая не содержит  $Z$ , также должна содержать  $n + 1$  точек. Таким образом, свойство 1 влечет за собой свойство 3.

Но для любой точки  $P$  мы можем найти прямую, не проходящую через нее, и потому, так же, как и выше, существует точно  $n + 1$  прямых, проходящих через  $P$ , чем доказаны свойства 2 и 4. Пусть теперь  $P_0$  — некоторая точка, и пусть  $n + 1$  прямых  $L_1, \dots, L_{n+1}$  проходят 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  $\pi$ , общее число точек в  $\pi$  равно  $1 + (n + 1)n = n^2 + n + 1$ , тем самым доказано свойство 5. Аналогично если  $L_0$  — прямая, содержащая точки  $P_1, \dots, P_{n+1}$ , каждая из которых лежит точно на  $n$  других прямых, то в  $\pi$  будет  $1 + (n + 1)n = n^2 + n + 1$  прямых, и свойство 6 также доказано.

Мы показали, что свойство 1 влечет за собой остальные пять свойств, поэтому свойство 3 также влечет за собой все остальные. Аналогично в силу двойственности, поменяв ролями „точки“ и „прямые“, мы видим, что свойство 2 и свойство 4 влекут за собой остальные. Если выполняется свойство 5, то прямая  $L_1$  из (12.3.1) содержит  $m + 1$  точек при некотором целом  $m \geq 2$ , и поэтому, как показано выше,  $\pi$  содержит  $m^2 + m + 1$  точек. Но из равенства  $m^2 + m + 1 = n^2 + n + 1$  для це-

лых положительных  $m$  и  $n$  следует, что  $m = n$ , и свойство 5 влечет за собой свойство 1, а потому и все остальные свойства. Аналогичным образом из свойства 6 вытекает свойство 2, а значит, и все другие. Теорема полностью доказана.

**Определение.** Конечная проективная плоскость имеет *порядок*  $n$ , если некоторая ее прямая содержит точно  $n + 1$  точек.

Заметим, что плоскость имеет порядок  $n$ , если она обладает любым из шести свойств теоремы 12.3.1. Если мы возьмем точки в качестве элементов, а прямые примем за блоки, то конечная проективная плоскость есть симметричная блок-схема с параметрами

$$v = n^2 + n + 1, \quad k = n + 1, \quad \lambda = 1. \quad (12.3.2)$$

Обратно, блок-схема с такими параметрами есть конечная проективная плоскость, так как, очевидно, все аксиомы выполняются. Конечная проективная плоскость, в которой можно ввести координаты из поля  $GF(q)$ ,  $q = p^r$ , как в разд. 12.1, имеет порядок  $n = p^r$ . Это де-зарговы плоскости, и они существуют для любого порядка, являющегося степенью простого числа. Все конечные плоскости, известные в настоящее время, имеют порядок, равный степени простого числа, причем недезарговы плоскости существуют для всех порядков, равных  $p^r$ , где  $p$  — простое число и  $r \geq 2$ , исключая 4 и 8.

Применение теоремы 10.3.1 дает необходимое условие существования конечной проективной плоскости.

**Теорема 12.3.2 (Брук — Райзер).** Для существования конечной проективной плоскости порядка  $n$  необходимо, чтобы при  $n \equiv 1, 2 \pmod{4}$  существовали целые  $x, y$ , удовлетворяющие равенству  $n = x^2 + y^2$ .

**Доказательство.** Имеем  $v = n^2 + n + 1$ ,  $k = n + 1$ ,  $\lambda = 1$  и  $k - \lambda = n$ , следовательно, обозначение  $n$  для порядка плоскости согласуется с обозначением  $n = k - \lambda$ , использованным в теореме 10.3.1. Так как  $n(n+1) \equiv 0 \pmod{2}$ , то  $v$ , очевидно, нечетно, и по теореме 10.3.1 должны существовать такие целые  $x, y, z$ , не равные

одновременно нулю, что

$$z^2 = nx^2 + (-1)^{\frac{v-1}{2}} y^2. \quad (12.3.3)$$

Так как  $v = n^2 + n + 1$ , то  $(v-1)/2$  четно, если  $n \equiv 0, 3 \pmod{4}$ , и мы имеем

$$z^2 - y^2 = nx^2. \quad (12.3.4)$$

Если  $n \equiv 3 \pmod{4}$ , то, полагая  $x = 1$ ,  $y = (n-1)/2$ ,  $z = (n+1)/2$ , получаем решение (12.3.4); если  $n \equiv 0 \pmod{4}$ , то берем  $x = 1$ ,  $y = (n-4)/4$ ,  $z = (n+4)/4$ . Если  $n \equiv 1, 2 \pmod{4}$ , то  $(v-1)/2$  нечетно, и (12.3.3) принимает вид

$$z^2 + y^2 = nx^2. \quad (12.3.5)$$

Хорошо известно (см., например, Харди и Райт [1], стр. 299), что при выполнении (12.3.5) существуют такие целые числа  $a$ ,  $b$ , что  $n = a^2 + b^2$ , и теорема доказана. Она показывает, что существует бесконечно много чисел  $n$ , которые не могут быть порядками проективных плоскостей; первые такие числа  $n = 6, 14, 21, 22, \dots$ . Поскольку для степени простого  $p^r$  всегда существует проективная плоскость порядка  $p^r$ , то первым сомнительным случаем является  $n = 10$ .

Если  $v = n^2 + n + 1$ ,  $k = n + 1$ ,  $\lambda = 1$  — параметры конечной проективной плоскости, рассматриваемой как блок-схема, то остаточная схема, определенная в разд. 10.1, есть аффинная плоскость, и параметры этой схемы суть

$$b = n^2 + n, \quad v = n^2, \quad k = n, \quad r = n + 1, \quad \lambda = 1. \quad (12.3.6)$$

Если дана схема с такими параметрами, то ее всегда можно вложить в симметричную схему. Мы докажем это, используя процесс, эквивалентный присоединению бесконечно удаленной прямой к аффинной евклидовой плоскости.

**Теорема 12.3.3.** *Если дана блок-схема  $D^*$  с параметрами  $b^* = n^2 + n$ ,  $v^* = n^2$ ,  $r^* = n + 1$ ,  $k^* = n$ ,  $\lambda^* = 1$ , то мы можем присоединить к ней, причем единственным способом, еще один блок с  $n + 1$  новыми элементами и добавить один из новых элементов к каждому из данных первоначально блоков так, чтобы получилась*

симметричной схемы  $D$  с параметрами  $v = b = n^2 + n + 1$ ,  $r = k = n + 1$ ,  $\lambda = 1$ .

**Доказательство.** Пусть дана блок-схема  $D^*$ . Рассмотрим некоторый блок  $B^*$  с элементами  $a_1, \dots, a_n$ . Пусть  $x$  — какой-либо элемент, отличный от них. Тогда  $n$  блоков  $B_i = \{x, a_i, \dots\}$ ,  $i = 1, \dots, n$ , определены единственным образом, так как  $\lambda = 1$ , и все различны, поскольку  $x \notin B^*$  и никакой блок, кроме  $B^*$ , не содержит более одного элемента  $a_i$ ,  $i = 1, 2, \dots, n$ . Таким образом, получены  $n$  блоков из  $n+1$ , содержащих элемент  $x$ . Поэтому существует точно один блок  $B_0 = \{x, \dots\}$ , содержащий  $x$  и не содержащий ни одного из элементов блока  $B^*$ . Мы назовем блок  $B_0$  „параллельным“ блоку  $B^*$  и содержащим  $x$ . Мы доказали тем самым постулат Евклида о параллельных для  $D^*$ . Следовательно, для любого данного блока  $B^*$  и любого элемента  $x$ , не принадлежащего  $B^*$ , существует единственный блок, параллельный  $B^*$  и содержащий  $x$ . Два различных блока  $B_u$  и  $B_v$ , параллельные блоку  $B^*$ , параллельны и между собой, так как если бы они имели общий элемент  $y$ , это противоречило бы единственности блока, параллельного  $B^*$  и содержащего  $y$ . Следовательно, если дан некоторый блок  $B_1$ , то не принадлежащие  $B_1$   $n^2 - n$  элементов содержатся в параллельных блоках  $B_2, \dots, B_n$ , т. е.  $B_1, B_2, \dots, B_n$  — семейство  $n$  параллельных блоков, которые в совокупности содержат каждый из  $n^2$  элементов точно один раз. Таким образом,  $b = n^2 + n$  блоков схемы  $D^*$  могут быть разделены, и притом единственным способом, на  $n+1$  семейства  $F_1, \dots, F_{n+1}$  параллельных блоков так, что каждое  $F_i$  содержит  $n$  блоков и каждый элемент из  $D^*$  встречается точно один раз в некотором блоке семейства  $F_i$ . Возьмем теперь новые элементы  $y_1, \dots, y_{n+1}$  и новый блок  $B_\infty$ , состоящий из  $y_1, \dots, y_{n+1}$ , а также присоединим элемент  $y_i$  к каждому блоку семейства  $F_i$ . Теперь видно непосредственно, что новый блок  $B_\infty$  и блоки схемы  $D^*$  с присоединенными к ним  $y_i$  образуют блоки симметричной схемы с  $v = b = n^2 + n + 1$ ,  $r = k = n + 1$ ,  $\lambda = 1$ .

Блок-схема из второго примера разд. 10.1 имеет параметры  $b = 12$ ,  $v = 9$ ,  $r = 4$ ,  $k = 3$ ,  $\lambda = 1$ , и 12 блоков

распадаются на четыре семейства:

$$\begin{aligned} F_1: & B_1, B_2, B_3; \quad F_2: B_4, B_5, B_6; \\ F_3: & B_7, B_8, B_9; \quad F_4: B_{10}, B_{11}, B_{12}. \end{aligned}$$

Мы можем взять новые элементы 10, 11, 12, 13 в качестве элементов блока  $B_{13}$ , добавить 10 к блокам из  $F_1$ , 11 — к блокам из  $F_2$ , 12 — к блокам из  $F_3$ , 13 — к блокам из  $F_4$  и получить симметричную схему с  $v = b = 13$ ,  $r = k = 4$ ,  $\lambda = 1$ , т. е. конечную проективную плоскость порядка 3.

По теореме 12.3.3 аффинная плоскость порядка  $n$  существует тогда и только тогда, когда существует проективная плоскость порядка  $n$ , и аффинная плоскость есть остаточная схема проективной плоскости. Но если мы возьмем проективную плоскость, то аффинные плоскости, полученные удалением двух различных прямых, будут изоморфны в том и только том случае, когда существует автоморфизм проективной плоскости, переводящий одну из этих прямых в другую. В самом деле, доказательство теоремы 12.3.3 показывает, что изоморфизм между аффинными плоскостями единственным образом можно распространить на изоморфизм между проективными плоскостями, в которые они вложены.

Аффинная форма конечной плоскости порядка  $n$  приводит к представлению этой плоскости семейством попарно ортогональных латинских квадратов порядка  $n$ . Два латинских квадрата порядка  $n$ , содержащие числа от 1 до  $n$  (по одному разу в каждой строке и в каждом столбце), называются *ортогональными*, если при наложении одного из них на другой  $n^2$  полученных при этом ячеек (ячейка состоит из упорядоченной пары  $(i, j)$ , где  $i$  берется из первого квадрата, а  $j$  — из второго) все различны, т. е. получается квадрат, состоящий из всех пар  $(u, v)$ ,  $u, v = 1, \dots, n$ , где каждая пара встречается точно один раз. Несколько латинских квадратов называются *попарно ортогональными*, если любые два из них ортогональны.

Пусть дана аффинная плоскость порядка  $n$ . Ее прямые (т. е. блоки) разделяются на  $n + 1$  семейств параллельных прямых. Обозначим какие-либо два из этих

семейств через  $F_r$  и  $F_c$  и назовем их семейством строк и семейством столбцов, а остальные семейства обозначим через  $F_1, \dots, F_{n-1}$ . Каждый из  $n^2$  элементов есть точка. Перенумеруем произвольным образом прямые каждого семейства от 1 до  $n$ . Нумерацию в  $F_r$  будем считать нумерацией строк квадрата, а нумерацию в  $F_c$  — нумерацией столбцов квадрата. Любая точка  $P$  лежит на одной прямой из  $F_r$  и на одной прямой из  $F_c$ , и потому ее можно сопоставить с определенной ячейкой квадрата.

Таким образом, точку  $P$  из  $i$ -й строки и  $j$ -го столбца мы можем обозначить через  $P = (i, j)$ . Семейства  $F_r$  и  $F_c$  просто соответствуют строкам и столбцам. Для каждого из  $F_1, \dots, F_{n-1}$  построим латинский  $n \times n$ -квадрат следующим образом. Пусть  $F_u$  — одно из этих семейств, состоящее из прямых  $L_1^u, \dots, L_n^u$ , где нумерация нижних индексов произвольна. Построим квадрат  $S_u$  из  $F_u$ . Возьмем  $n \times n$ -квадрат и поместим число  $v$  в ячейку на пересечении  $i$ -й строки и  $j$ -го столбца, если точка  $P = (i, j)$  лежит на  $v$ -й прямой  $L_v^u$  семейства  $F_u$ . Так как каждая точка лежит точно на одной прямой из  $F_u$ , то мы поместили в точности одно число в каждую ячейку квадрата  $S_u$ . Прямая из  $F_r$  (или  $F_c$ ) пересекает каждую прямую из  $F_u$  точно по одному разу, и потому строка (или столбец) квадрата  $S_u$  содержит каждое из чисел  $1, \dots, n$  точно по одному разу. Следовательно,  $S_u$  — латинский квадрат.

Рассмотрим теперь два квадрата  $S_u$  и  $S_w$ ,  $w \neq u$ . Пусть  $a(i, j)$  — число в ячейке  $(i, j)$  квадрата  $S_u$ , а  $b(i, j)$  — число в ячейке  $(i, j)$  квадрата  $S_w$ . Если бы мы имели

$$a = a(i_1, j_1) = a(i_2, j_2) \quad \text{и} \quad b = b(i_1, j_1) = b(i_2, j_2),$$

то точки  $P_1 = (i_1, j_1)$  и  $P_2 = (i_2, j_2)$  обе лежали бы на прямой  $L_a^u$  из  $F_u$  и на прямой  $L_b^w$  из  $F_w$ , что противоречит условию  $\lambda = 1$ , т. е. тому, что через две различные точки проходит одна и только одна прямая. Следовательно, упорядоченные пары  $(a(i, j), b(i, j))$ ,  $i, j = 1, \dots, n$ , все различны, и квадраты  $S_u$  и  $S_w$  ортогональны.

Таким образом, конечная плоскость порядка  $n$  приводит к семейству  $n - 1$  попарно ортогональных латинских квадратов порядка  $n$ .

Пусть мы имеем семейство из  $m$  попарно ортогональных латинских квадратов. Свойство ортогональности не нарушается, если произвести подстановку над числами любого квадрата. Следовательно, можно предполагать, что первая строка каждого квадрата — это  $1, 2, \dots, n$ . Поэтому число, появляющееся во второй строке и первом столбце каждого квадрата, есть одно из  $n - 1$  чисел  $2, \dots, n$ . Если бы число  $i$  появилось на этом месте дважды, то при наложении этих двух квадратов пара  $(i, i)$  появилась бы в ячейке  $(2, 1)$  и в ячейке  $(1, i)$ , что противоречит предположению ортогональности. Следовательно, в ячейке  $(2, 1)$  числа не могут повторяться и потому существует не более  $n - 1$  попарно ортогональных квадратов порядка  $n$ . Пусть  $m = n - 1$ . Рассмотрим теперь каждую ячейку  $(i, j)$  как точку  $P(i, j)$  и образуем семейства прямых  $F_r, F_c, F_1, \dots, F_{n-1}$ :  $P(i, j)$  находится на  $i$ -й прямой из  $F_r$ ,  $j$ -й прямой из  $F_c$  и на  $v$ -й прямой из  $F_u$ ,  $u = 1, \dots, n - 1$ , если число в ячейке  $(i, j)$  квадрата  $S_u$  есть  $v$ . Это дает нам  $n + 1$  семейств из  $n$  прямых, каждая из которых содержит  $n$  точек. Общее число точек равно  $n^2$ . Свойство быть латинским квадратом и свойство ортогональности квадратов  $S_1, \dots, S_{n-1}$  гарантирует нам, что через две различные точки нельзя провести двух различных прямых. Привольная точка  $P_0$  находится на  $n + 1$  прямых, каждая из которых содержит еще  $n - 1$  других точек, поэтому  $P_0$  соединена точно один раз с каждой другой точкой, и мы имеем  $\lambda = 1$ . Таким образом, мы показали, что семейство из  $n - 1$  попарно ортогональных латинских квадратов эквивалентно конечной плоскости порядка  $n$ .

В качестве примера такой эквивалентности рассмотрим блок-схему с параметрами  $v = 21$ ,  $k = 5$ ,  $\lambda = 1$  (плоскость порядка 4), которую мы можем считать определенной разностным множеством  $B_0 = \{3, 6, 7, 12, 14 \pmod{21}\}$ . Примем  $B_0$  за бесконечно удаленную прямую и вычеркнем ее точки из других прямых. Пучки проективных прямых, проходящие через 3, 6, 7, 12, 14, становятся семействами аффинных параллельных прямых  $F_r, F_c$ ,

$F_1$ ,  $F_2$ ,  $F_3$  соответственно. Таким образом, если  $B_i = \{3+i, 6+i, 7+i, 12+i, 14+i \pmod{21}\}$  и  $B_i^*$  — это  $B_i$ , из которого вычеркнуто число 3, 6, 7, 12 или 14, то мы имеем:

 $F_r(3)$ 

- |                                |                                |
|--------------------------------|--------------------------------|
| 1: $B_{10}^*$ : 13, 16, 17, 1. | 1: $B_3^*$ : 9, 10, 15, 17.    |
| 2: $B_{12}^*$ : 15, 18, 19, 5. | 2: $B_{13}^*$ : 16, 19, 20, 4. |
| 3: $B_{17}^*$ : 20, 2, 8, 10.  | 3: $B_{15}^*$ : 18, 0, 1, 8.   |
| 4: $B_{18}^*$ : 0, 4, 9, 11.   | 4: $B_{20}^*$ : 2, 5, 11, 13.  |

 $F_1(7)$ 

- |                               |                                      |
|-------------------------------|--------------------------------------|
| 4: $B_1^*$ : 4, 8, 13, 15.    | 1: $B_5^*$ : 8, 11, 17, 19.          |
| 2: $B_4^*$ : 10, 11, 16, 18.  | 4: $B_6^*$ : 9, 13, 18, 20. (12.3.7) |
| 1: $B_{14}^*$ : 17, 20, 0, 5. | 2: $B_9^*$ : 15, 16, 0, 2.           |
| 3: $B_{16}^*$ : 19, 1, 2, 9.  | 3: $B_{19}^*$ : 1, 4, 5, 10.         |

 $F_3(14)$ 

- |                               |
|-------------------------------|
| 2: $B_2^*$ : 5, 8, 9, 16.     |
| 4: $B_7^*$ : 10, 13, 19, 0.   |
| 3: $B_8^*$ : 11, 15, 20, 1.   |
| 1: $B_{11}^*$ : 17, 18, 2, 4. |

В терминах координат ячеек из  $F_r$  и  $F_e$

$$\begin{array}{llll} 17 = (1,1); & 16 = (1,2); & 1 = (1,3); & 13 = (1,4); \\ 15 = (2,1); & 19 = (2,2); & 18 = (2,3); & 5 = (2,4); \\ 10 = (3,1); & 20 = (3,2); & 8 = (3,3); & 2 = (3,4); \\ 9 = (4,1); & 4 = (4,2); & 0 = (4,3); & 11 = (4,4). \end{array} \quad (12.3.8)$$

Мы перенумеровали прямые семейств  $F_1$ ,  $F_2$ ,  $F_3$  так, что в квадратах  $S_1$ ,  $S_2$ ,  $S_3$  первая строка — это 1, 2, 3, 4.

Следуя описанному построению, получим

$$\begin{array}{c}
 S_1 \qquad S_2 \qquad S_3 \\
 \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{array} \\
 \end{array} \quad (12.3.9)$$

## 12.4. Некоторые типы конечных плоскостей

В любой проективной плоскости можно ввести систему координат. Для конечных плоскостей это легче всего осуществить, если воспользоваться разделением аффинной плоскости на семейства параллельных прямых

$$F_r, F_c, F_l, \dots, F_{n-1}.$$

Координаты будем обозначать  $n$  символами  $a_0, a_1, \dots, a_{n-1}$ , среди которых два играют роль нуля и единицы и обозначаются  $a_0 = 0, a_1 = 1$ .

Если  $P_0, P_1, \dots, P_{n-1}$  — точки на первой прямой семейства  $F_1$  (в некотором фиксированном порядке), то пусть

$$P_0 = (0, 0), P_1 = (1, 1), \dots, P_i = (a_i, a_i), \dots$$

$$\dots, P_{n-1} = (a_{n-1}, a_{n-1}). \quad (12.4.1)$$

Прямую из  $F_r$ , содержащую  $P_i$ , мы обозначим через  $x = a_i$ , а прямую из  $F_c$ , содержащую  $P_j$ , обозначим через  $y = a_j$ . Точку пересечения  $x = a_i$  и  $y = a_j$  представим упорядоченной парой  $(a_i, a_j)$ ; заметим, что это представление согласуется с (12.4.1). В любом семействе  $F_a$  существует единственная прямая, проходящая через  $P_0 = (0, 0)$ , и пересечение этой прямой с  $x = 1$  есть точка  $(1, w)$ . Мы воспользуемся этим, чтобы перенумеровать семейства, полагая  $F_u = F_w$ . Тогда семейству  $F_1$  приписывается „номер“  $a_1 = 1$  [по (12.4.1)], семейству  $F_c$  — „номер“  $a_0 = 0$ , но семейству  $F_r$  не приписывается никакого „номера“. Нумеруя семейство, мы как бы задаем угловой коэффициент для параллельных прямых, входящих

в него, и прямым  $x = c$  из  $F_r$ , мы можем приписать угловой коэффициент  $\infty$ , отличный от  $a_0, a_1, \dots, a_{n-1}$ .

Определим теперь тернарную операцию  $x \cdot m \circ b$  на элементах  $a_0, a_1, \dots, a_{n-1}$ .

*Тернарная операция:*  $y = x \cdot m \circ b$ , если точка  $(x, y)$  лежит на прямой из  $F_m$ , проходящей через точку  $(0, b)$ .

Легко проверить, что эта операция определена для любых  $x, m$  и  $b$ , выбранных из  $a_0, a_1, \dots, a_{n-1}$ .

Определим умножение  $xm$  и сложение  $x + b$  как частные случаи тернарной операции следующим образом:

$$xm = x \cdot m \circ 0, \quad x + b = x \cdot 1 \circ b. \quad (12.4.2)$$

Для тернарной операции выполнены следующие свойства:

$$\text{T1. } 0 \cdot m \circ c = a \cdot 0 \circ c = c.$$

$$\text{T2. } 1 \cdot m \circ 0 = m \cdot 1 \circ 0 = m.$$

Т3. Для данных  $a, m, c$  существует единственное  $z$ , такое, что  $a \cdot m \circ z = c$ .

Т4. Для данных  $m_1 \neq m_2, b_1, b_2$  существует единственное  $x$ , такое, что  $x \cdot m_1 \circ b_1 = x \cdot m_2 \circ b_2$ .

Т5. Для данных  $a_1 \neq a_2, c_1, c_2$  существует единственная пара  $m, b$ , такая, что

$$a_1 \cdot m \circ b = c_1 \text{ и } a_2 \cdot m \circ b = c_2^1).$$

Свойства Т1 и Т2 непосредственно вытекают из определений; Т3 означает, что в семействе  $F_m$  есть прямая, проходящая через точку  $(a, c)$ ; Т4 означает, что непараллельные прямые имеют единственную точку пересечения; Т5 означает, что две точки, не лежащие на прямой  $x = a$  семейства  $F_\infty$ , лежат на единственной прямой одного из остальных семейств. Эти свойства не являются независимыми, но их достаточно, чтобы определить проективную плоскость. Доказательство этого следует непосредственно из определений, и мы его здесь не приводим.

Координаты и тернар были определены для аффинной плоскости. Чтобы распространить их на проективную

<sup>1)</sup> Множество с тернарной операцией, для которой выполняются свойства Т1 – Т5, будем называть *тернаром*. См. статью Л. А. Скорнякова „Проективные плоскости“, упомянутую выше в примечании на стр. 223. — Прим. ред.

плоскость, мы введем бесконечно удаленные точки  $(0)$ ,  $(1)$ ,  $\dots$ ,  $(a_{n-1})$  и  $(\infty)$ , лежащие все на единственной бесконечно удаленной прямой  $L_\infty$ , и присоединим  $(\infty)$  к прямым из  $F_r$ , а  $(a_i)$  — к прямым из  $F_{a_i}$ ,  $i = 0, \dots, n-1$ .

Может оказаться, что тернарная операция выражается через умножение и сложение:

$$x \cdot m \circ b = xm + b. \quad (12.4.3)$$

Можно показать, что алгебраическое соотношение (12.4.3) эквивалентно в некоторых случаях выполнимости теоремы Дезарга с  $L_\infty$ , взятой за ось перспективы и точкой  $(\infty)$  в качестве центра перспективы<sup>1)</sup>.

Один важный тип тернара называется *системой Веблена — Веддербёрна*. В этой системе определены сложение  $a + b$  и умножение  $ab$  и выделены элементы  $0$  и  $1$ , причем выполняются свойства:

VW1. Система есть абелева группа по сложению.

VW2. Уравнение  $xy = z$  однозначно разрешимо, если даны два элемента из  $x, y, z$ , отличные от нуля, при этом решение также отлично от нуля.

VW3.  $1x = x1 = x$ ,  $0x = x0 = 0$ ,  $x + 0 = 0 + x = x$ .

VW4.  $(a + b)m = am + bm$ .

VW5. Если  $r \neq s$ , то  $xr = xs + t$  однозначно разрешимо относительно  $x$ .

VW6.  $x \cdot m \circ b = xm + b$ .

Если свойства VW1—5 выполняются, то, используя тернарную операцию VW6, можно определить плоскость.

В конечной системе VW5 является следствием остальных свойств, ибо если  $r \neq s$  и  $x_1, x_2$  — решения уравнения  $xr = xs + t$ , то  $x_1r - x_1s = x_2r - x_2s$  и в силу VW4  $(x_1 - x_2)r = (x_1 - x_2)s$ ; элемент  $(x_1 - x_2)r$  обозначим через  $w$ . Так как хотя бы одно из  $r, s$  отлично от нуля, то при  $x_1 - x_2 \neq 0$  по VW2 имеем  $w \neq 0$  и  $r = s$ . Значит, когда  $x$  пробегает все  $n$  элементов конечной системы, то  $xr - xs$  также все различны и, значит, существует единственное  $x$ , для которого  $xr - xs = t$ . Конечно, каждое тело,

<sup>1)</sup> См. М. Холл, Теория групп, М., ИЛ, 1952, гл. 20. — Прим. ред.

и, в частности, конечное поле, есть система Веблена — Веддербёрна.

Системы Веблена — Веддербёрна (сокращенно VW-системы) одного частного вида известны под названием систем Холла.

Пусть  $F$  — поле и  $f(x) = x^2 - rx - s$  — многочлен второго порядка, неприводимый над  $F$ . За элементы VW-системы  $S$  примем всевозможные выражения  $a + bu$ , где  $a, b \in F$ , а  $u$  неизвестное. Вместо введения неизвестного можно, конечно, оперировать с упорядоченными парами  $(a, b)$ . Сложение в  $S$  определяется правилом

$$A. (a_1 + b_1 u) + (a_2 + b_2 u) = (a_1 + a_2) + (b_1 + b_2) u.$$

При умножении мы пользуемся двумя правилами:

M1. При  $a \in F$  полагаем  $(e + fu)a = ae + afu$ .

M2. При  $z = a + bu$ ,  $b \neq 0$ , и  $w = e + fu$  полагаем

$$wz = (e + fu)(a + bu) =$$

$$= (ae - b^{-1}a^2f + b^{-1}raf + b^{-1}sf) + (be - af + rf)u.$$

Правила умножения легче понять в следующем виде

M1\*. При  $c \in F$  пусть

$$c(a + bu) = (a + bu)c = ac + bcu.$$

M2\*.  $(x + y)z = xz + yz$ .

M3\*. При  $z \notin F$  пусть  $z^2 = rz + s$ .

Если  $F$  — конечное поле  $GF(q)$ ,  $q = p^r$ , то система Холла определяет конечную плоскость порядка  $q^2$ . Помимо случая  $q^2 = 4$ , плоскость, определенная таким образом, отлична от дезарговой плоскости порядка  $q^2$  с координатами из  $GF(q^2)$ . Для конечного  $F$ , поскольку VW5 есть следствие свойств VW1—4, все свойства VW-систем, кроме VW2, легко следуют из определения системы  $S$ .

Чтобы доказать VW2, нужно установить, что если в уравнении  $wz = v$  заданы и отличны от нуля любые два из элементов  $w, v, z$ , то третий определяется однозначно и отличен от нуля. Пусть

$$w = e + fu, \quad z = a + bu, \quad v = c + du,$$

где  $a, b, c, d, e, f \in F$ . Если даны  $w$  и  $z$  и  $b = 0$ , то мы используем для определения  $v$  правило M1, а если  $b \neq 0$ , то правило M2. Если  $b = 0, w = 0, z = a \neq 0$ , то, очевидно,  $v = 0$ . Поэтому, если даны  $z = a \neq 0$  и  $v = c + du \neq 0$ , то  $w = e + fu \neq 0$  и однозначно определяется из соотношений  $ae = c, af = d$ . Пусть теперь  $z = a + bu, b \neq 0$ , тогда применимо M2, и мы имеем

$$ae + (-b^{-1}a^2 + b^{-1}ra + b^{-1}s)f = c, \quad be + (-a + r)f = d. \quad (12.4.4)$$

Рассмотрим эти равенства как систему линейных уравнений относительно  $e$  и  $f$  с определителем, равным  $-s$ . Так как  $x^2 - rx - s$  неприводим над  $F, s \neq 0$ . Это показывает, что когда  $b \neq 0$ , а значит, и  $z = a + bu \neq 0$ , то при  $w = e + fu \neq 0$  имеем  $v = c + du \neq 0$ . Отсюда также следует, что если даны  $z$  и  $v$ , то  $w$  существует и единственно. Наиболее труден случай, когда даны  $w = e + fu$  и  $v = c + du$ . Во-первых, если  $ed - fc = 0$ , то уравнения  $ae = c, af = d$  разрешимы, следовательно, используя M1\*, получаем решение  $z = a$ . С другой стороны, если существует решение вида  $z = a$ , то должно быть  $ed - fc = 0$ .

Предположим теперь, что  $ed - fc \neq 0$ . Нам теперь даны  $e, f, c, d$ , и мы хотим решить (12.4.4) относительно  $a$  и  $b$ . Если  $f = 0$ , то  $e \neq 0$ , и (12.4.4) сводится к системе  $ae = c, be = d$ , из которой определяются  $a$  и  $b$ . Пусть  $f \neq 0$ . Решаем второе уравнение относительно  $a$ :

$$a = bef^{-1} - df^{-1} + r. \quad (12.4.5)$$

Подстановка этого значения  $a$  в первое уравнение дает

$$def^{-1} - b^{-1}d^2f^{-1} + b^{-1}dr + b^{-1}sf = c. \quad (12.4.6)$$

Умножая на  $f$  и перенося первый член в правую часть, получаем

$$-b^{-1}(d^2 - rdf - sf^2) = cf - de. \quad (12.4.7)$$

Из неприводимости многочлена  $x^2 - rx - s$  следует, что  $d^2 - rdf - sf^2 \neq 0$ , если  $d$  и  $f$  не равны одновременно нулю, что выполняется в силу  $cf - de \neq 0$ . Поэтому из (12.4.7) однозначно определяется  $b^{-1} \neq 0$  и, значит,

$b \neq 0$ , а затем (12.4.5) однозначно определяет  $a$ . Тем самым доказано, что для  $S$  выполняется VW2.

Если умножение в VW-системе ассоциативно, то ее элементы, отличные от 0, образуют группу, и VW-система называется тогда *почти-полям*. Все конечные почти- поля были определены Цассенхаузом [1]. Естественно, сюда входят и конечные поля  $GF(p')$ .

Помимо семи особых случаев, конечные почти- поля (не совпадающие с полями) описываются так.

Пусть  $q = p^h$  — степень простого числа  $p$  и  $v > 1$  — целое число, все простые делители которого делят  $q - 1$ , и мы требуем также, чтобы  $v \not\equiv 0 \pmod{4}$ , если  $q \equiv 3 \pmod{4}$ . Тогда при  $hv = r$  мы можем построить почти- поле  $K$  с  $n = p^r$  элементами из конечного поля  $GF(p')$  следующим образом.

1. Элементы  $K$  — те же, что и у  $GF(p')$ .

2. Сложение в  $K$  — та же операция сложения, что и в  $GF(p')$ .

3. Произведение  $w \circ u$  в  $K$  можно выразить в терминах произведения  $xu$  в  $GF(p')$  следующим образом. Пусть  $z$  — фиксированный первообразный элемент  $GF(p')$ ; если теперь  $u = z^{tv+1}$ , то целое  $i$  однозначно определено по модулю  $v$  сравнением

$$q^i \equiv 1 + j(q - 1) \pmod{v(q - 1)}.$$

Тогда  $w \circ u$  определяется равенством

$$w \circ u = w^{q^i} u. \quad (12.4.8)$$

Во всех семи особых случаях порядок системы  $K$  равен  $n = p^2$  для подходящего нечетного простого  $p$ , элементы  $K$  имеют вид  $a + bu$ ,  $a, b \in GF(p)$  и выполнены соотношения

$$(a_1 + b_1 u) + (a_2 + b_2 u) = (a_1 + a_2) + (b_1 + b_2) u, \quad (12.4.9)$$

$$(x + y)z = xz + yz, \quad (xy)z = x(yz), \quad 1z = z, \quad (12.4.10)$$

где  $x, y, z \in K$ ,

$$u^2 = -1. \quad (12.4.11)$$

В каждом из семи случаев имеют место также дополнительные соотношения:

$$\text{Случай I. } n = 5^2, \quad u(1 - 2u) = -1 - 2u.$$

$$\text{Случай II. } n = 11^2, \quad u(1 + 5u) = -5 - 2u, \quad u(4) = 4u.$$

$$\text{Случай III. } n = 7^2, \quad u(1 + 3u) = -1 - 2u.$$

$$\text{Случай IV. } n = 23^2, \quad u(1 - 6u) = 12 - 2u, \quad u(2) = 2u.$$

$$\text{Случай V. } n = 11^2, \quad u(2 + 4u) = 1 - 3u.$$

$$\text{Случай VI. } n = 29^2, \quad u(1 - 7u) = -12 - 2u, \quad u(16) = 16u.$$

$$\text{Случай VII. } n = 59^2, \quad u(9 + 15u) = -10 - 10u, \quad u(4) = 4u.$$

Хотя это и не очевидно, но указанные соотношения определяют полностью семь особых случаев.

VW-система, в которой выполняются оба дистрибутивных закона, называется *полуполем*, или, что то же, неассоциативным телом. Алберт [1] дал метод построения полуполей порядка  $p^r$ , где  $p$  — простое нечетное число,  $r$  — нечетное и  $r > 1$ . В  $\mathrm{GF}(p^r)$  определим новое произведение  $(x, y)$ :

$$(x, y) = \frac{1}{2} (xy^p + x^py). \quad (12.4.12)$$

Равенство нулю произведения  $(x, y)$  при  $x \neq 0, y \neq 0$  привело бы к соотношению

$$y^{p-1} = -x^{p-1}. \quad (12.4.13)$$

Так как  $r$  и  $p$  оба нечетны,  $m = (p^r - 1)/(p - 1)$  также нечетно. Возведя обе части (12.4.13) в  $m$ -ю степень, получим

$$1 = y^{p^r-1} = -x^{p^r-1} = -1, \quad (12.4.14)$$

что противоречит предположению  $p \neq 2$ .

Таким образом, произведение, определенное (12.4.12), не приводит к делителям нуля. Следовательно, для  $x \neq 0$  существует единственное  $u \neq 0$ , такое, что

$$x = (u, 1) = \frac{1}{2} (u + u^p). \quad (12.4.15)$$

Можно определить взаимно однозначное отображение  $\alpha$ :

$$u = x\alpha, \quad (12.4.16)$$

если  $u$  и  $x$  удовлетворяют (12.4.15). Мы можем, далее, получить полуполе  $K$ , если определим произведение  $x \circ y$

формулой

$$x \circ y = (xa, ya). \quad (12.4.17)$$

Полуполе  $K$ , образованное таким способом, не может быть изоморфно полю  $GF(p^r)$ , и, следовательно, соответствующая плоскость является недезарговой. Два построения, (12.4.8) и (12.4.17), дают недезарговы плоскости всех порядков  $n = p^r$  для нечетного  $p$  и  $r \geq 2$  и для  $p = 2$ , четного  $r$ ,  $r \geq 4$ . Полуполя порядков  $2^m$  с нечетным  $m$  были построены Дональдом Киутом. При  $m \geq 5$  они не являются полями и потому приводят к недезарговым плоскостям. Дадим их построение.

Пусть  $m$  нечетно, и пусть  $x$  — такой элемент в  $GF(2^m)$ , что  $1, x, x^2, \dots, x^{m-1}$  образуют базис над  $GF(2)$ . Построим полуполе  $K(2^m)$ , элементы и операция сложения которого те же, что элементы и операция сложения в  $GF(2^m)$ . Для умножения в  $K(2^m)$  считаем выполненными оба закона дистрибутивности, и определим произведение  $y \circ z$  в  $K(2^m)$  через умножение  $yz$  в  $GF(2^m)$  посредством следующих правил перемножения базисных элементов:

$$\begin{aligned} x^i \circ x^j &= x^i x^j, \quad i, j = 0, 1, \dots, m-2, \\ x^i \circ x^{m-1} &= x^{m-1} \circ x^i = \\ &= x^{m-1} x^i + x^{2i} + x^i, \quad i = 0, \dots, m-2, \\ x^{m-1} \circ x^{m-1} &= x^{2m-2} + 1. \end{aligned} \quad (12.4.18)$$

Если  $y, z$  — элементы в аддитивной системе  $S$  с базисом  $1, x, \dots, x^{m-2}$ , то отсюда получается

$$\begin{aligned} y \circ z &= y \cdot z, \\ (x^{m-1} + y) \circ z &= z \circ (x^{m-1} + y) = z(x^{m-1} + z + 1 + y), \\ (x^{m-1} + y) \circ (x^{m-1} + z) &= x^{2m-2} + 1 + \\ &\quad + z(x^{m-1} + z + 1) + y(x^{m-1} + y + 1) + yz = \\ &= (x^{m-1} + y + 1)^2 + (x^{m-1} + y + 1)(y + z) + (y + z)^2. \end{aligned} \quad (12.4.19)$$

Так как дистрибутивные законы выполняются и, очевидно,  $1$  есть единица, то  $K$  есть полуполе, если в нем нет делителей нуля. Если произведение находим по первому из правил (12.4.19), то  $yz \neq 0$  при  $y \neq 0$  и  $z \neq 0$  в силу отсутствия делителей нуля в  $GF(2^m)$ , если же

находим произведение по второму правилу, то из  $z(x^{m-1} + z + 1 + y) = 0$  и  $z \neq 0$  следует, что  $x^{m-1} + z + 1 + y = 0$  и, поскольку  $y, z, 1$  принадлежат  $S$ ,  $x^{m-1} \in S$ , а это противоречит тому, что  $1, x, \dots, x^{m-2}$  — базис в  $S$ . В третьем случае, если произведение

$$(x^{m-1} + y) \circ (x^{m-1} + z)$$

равно нулю, то имеем

$$u^2 + uv + v^2 = 0, \quad (12.4.20)$$

где  $u = x^{m-1} + y + 1 \neq 0$ ,  $v = y + z$ . Отсюда  $w = v/u$  удовлетворяет уравнению

$$w^2 + w + 1 = 0.$$

Но тогда  $0, 1, w, w + 1$  образуют подполе порядка  $2^2$  поля  $GF(2^m)$ , что невозможно, если  $m$  нечетно. Следовательно,  $K$  не имеет делителей нуля и является полуполем. Если  $m \geq 5$ , то

$$\begin{aligned} x^m &= (x \circ x^{(m-1)/2}) \circ (x^{(m-1)/2}) \neq x \circ (x^{(m-1)/2} \circ x^{(m-1)/2}) = \\ &= x^m + x^2 + x \end{aligned}$$

и  $K$  не является полем.

При  $m = 3$  в  $GF(2^3)$  элемент  $x$  должен удовлетворять одному из уравнений  $f(x) = x^3 + x + 1 = 0$  или  $f(x) = x^3 + x^2 + 1 = 0$ . Произведение  $\circ$ , определенное одним из этих многочленов  $f(x)$ , дает обычное произведение, определенное другим  $f(x)$ . Следовательно, при  $m = 3$  имеем  $K(2^3) = GF(2^3)$ . Исчерпывающим исследованием на ЭВМ было установлено, что для порядка 8 вообще не существует недезарговой конечной плоскости.

Можно использовать почти-поле для совершенно иного метода построения недезарговой плоскости. Первый пример такого рода для порядка 9 был построен Вебленом и Веддербёрном [1], общее построение было указано Хьюзом [1].

Пусть  $F$  — поле порядка  $q = p^h$  и  $K$  — почти-поле порядка  $q^2$ , содержащее  $F$  в качестве своего центра. Здесь  $K$  может быть одним из особых почти-полей или одним из регулярных почти-полей с  $v = 2$ . Рассмотрим сначала дезаргову плоскость  $\pi_0$  порядка  $q$  с координатами из  $F$ . Точки  $\pi_0$  представим как тройки  $(x, y, z)$ ,

$x, y, z \in F$  и  $(x, y, z) \neq (0, 0, 0)$ , причем  $(x, y, z) = (xu, yu, zu)$ , если  $u \in F$ ,  $u \neq 0$ . Если  $a, b, c$  не равны одновременно нулю и являются элементами  $F$ , то точки  $P = (x, y, z)$ , удовлетворяющие равенству  $ax + by + cz = 0$ , лежат на одной прямой, и каждая прямая в  $\pi_0$  определяется таким уравнением. По теореме Зингера (теорема 11.3.1)  $\pi_0$  имеет коллинеацию  $\alpha$  порядка  $q^2 + q + 1$ , которая переставляет точки  $\pi_0$ , равно как и ее прямые, по единственному циклу. Эту коллинеацию  $\alpha$  можно представить как линейное преобразование с коэффициентами из  $F$ . Таким образом, при  $P = (x, y, z)$  и  $P \rightarrow P\alpha$  имеем

$$\begin{aligned} P\alpha &= (x, y, z)\alpha = (x, y, z)A, \\ A &= (a_{ij}), \quad i, j = 1, 2, 3, \quad a_{ij} \in F, \end{aligned} \quad (12.4.21)$$

для некоторой  $(3 \times 3)$ -матрицы  $A$ . Здесь  $A^m = cI$ ,  $c \in F$ , при  $m = q^2 + q + 1$  и ни при каком  $m < q^2 + q + 1$ .

Мы попытаемся построить плоскость  $\pi$  порядка  $q^2$  с координатами из  $K$ , предполагая, что мы сможем использовать матрицу  $A$ , чтобы определить коллинеацию в этой большей плоскости. К счастью, все это проходит.

За точки плоскости  $\pi$  примем тройки  $(x, y, z) \neq (0, 0, 0)$ ,  $x, y, z \in K$ , причем будем считать  $(x, y, z) = (xu, yu, zu)$ , если  $u \neq 0$ ,  $u \in K$ . Рассмотрим уравнение

$$x + ty + z = 0, \quad (12.4.22)$$

где либо  $t = 1$ , либо  $t$  есть один из  $q^2 - q$  элементов почти- поля  $K$ , не принадлежащих  $F$ . Мы определим „базисные прямые“  $L_t$  следующим условием:  $P = (x, y, z)$  лежит на  $L_t$  тогда и только тогда, когда  $x, y, z$  удовлетворяют (12.4.22). В силу правого закона дистрибутивности  $(a + b)c = ac + bc$  и ассоциативности умножения из (12.4.22) следует, что

$$\begin{aligned} (x + ty + z)u &= 0, \\ xu + (ty)u + zu &= 0, \\ xu + t(yu) + zu &= 0. \end{aligned} \quad (12.4.23)$$

Поэтому если  $(x, y, z)$  удовлетворяет (12.4.22), то этому уравнению удовлетворяет также  $(xu, yu, zu)$ ,  $u \neq 0$ ,

и посредством (12.4.22) отношение инцидентности точки  $P$  и прямой  $L_t$  вполне определено. Мы имеем теперь  $q^2 - q + 1$  базисных прямых  $L_t$ . Легко показать, что каждая из них содержит  $q^2 + 1$  точек. Определим далее прямые  $L_t^{(i)}$ ,  $i = 0, 1, \dots, q^2 + q$ , по следующему правилу.

*Правило.* Если  $(x, y, z) \in L_t$ , то  $(x, y, z) A^i \in L_t^{(i)}$  и  $L_t^{(i)}$  не содержит никаких других точек.

Заметим, что  $L_t^{(0)} = L_t$ . Таким образом, мы построили

$$(q^2 - q + 1)(q^2 + q + 1) = q^4 + q^2 + 1$$

прямых, каждая из которых содержит  $q^2 + 1$  точек. Теперь основная трудность состоит в том, чтобы показать, что если  $L_t^{(i)}$  и  $L_s^{(j)}$  различны, то они имеют в точности одну общую точку.

Рассмотрим множества точек  $L_t^{(i)}$ ,  $i = 0, 1, \dots, q^2 + q$ . Независимо от того, образуют ли они прямые в плоскости, это — множества точек, которые переводятся одно в другое какой-либо степенью линейного преобразования  $A$ . Таким образом,  $L_t^{(g)}$  и  $L_s^{(h)}$  имеют общую точку тогда и только тогда, когда  $L_t^{(g-h)}$  и  $L_s^0 = L_s$  имеют общую точку. Пусть  $L_t^{(g-h)}$  и  $L_s^0 = L_s$  имеют общую точку  $(x, y, z)$ . Тогда  $(x, y, z)$  принадлежит  $L_s$ , а  $(x, y, z) A^{h-g}$  есть точка прямой  $L_t^0 = L_t$ . Если  $A^{h-g} = (a_{ij})$ ,  $i, j = 1, 2, 3$ , то

$$(x, y, z) A^{h-g} = (a_{11}x + a_{21}y + a_{31}z, a_{12}x + a_{22}y + a_{32}z, a_{13}x + a_{23}y + a_{33}z). \quad (12.4.24)$$

Так как  $(x, y, z)$  лежит на  $L_s$ , а точка прямой (12.4.24) лежит на  $L_t$ , то мы имеем два соотношения:

$$(a_{11}x + a_{21}y + a_{31}z) + t(a_{12}x + a_{22}y + a_{32}z) + (a_{13}x + a_{23}y + a_{33}z) = 0, \quad (12.4.25)$$

$$x + sy + z = 0. \quad (12.4.26)$$

Решая (12.4.26) относительно  $x$  и подставляя решение в (12.4.25), находим

$$uy + az + t(vy + bz) = 0, \quad (12.4.27)$$

где

$$\begin{aligned} u &= a_{21} + a_{23} - (a_{11} + a_{13})s, & v &= a_{22} - a_{12}s, \\ a &= a_{31} + a_{33} - (a_{11} + a_{13}), & b &= a_{32} - a_{12}. \end{aligned} \quad (12.4.28)$$

Заметим, что  $a$  и  $b$  принадлежат  $F$ , центру  $K$ . Далее доказательство разбивается на три случая.

*Случай 1:*  $b \neq 0$ . Перепишем (12.4.27) в виде

$$(u - ab^{-1}v)y + (ab^{-1} + t)(vy + bz) = 0. \quad (12.4.29)$$

Если  $t = 1$ , то (12.4.25) принимает вид

$$b_1x + b_2y + b_3z = 0, \quad b_i \in F, \quad (12.4.30)$$

и это уравнение имеет лишь одно решение, удовлетворяющее (12.4.26), — точку  $(x, y, z)$ , если исключить случай  $s = 1$  и  $b_1 = b_2 = b_3 \neq 0$ , когда (12.4.30) и (12.4.26) — это одно и то же уравнение  $x + y + z = 0$ . Но  $A$  представляет прямые подплоскости  $\pi_0$  по циклу длины  $q^2 + q + 1$ , и эта исключительная ситуация может быть достигнута только тогда, когда  $s = t = 1$  и  $g = h$ , т. е. когда две данные прямые совпадают. Если  $t \neq 1$ , то  $t \notin F$ , и поэтому  $w = ab^{-1} + t \neq 0$ . Умножим (12.4.29) слева на  $w^{-1}$  и, используя ассоциативность и правый дистрибутивный закон, получим

$$[w^{-1}(u - ab^{-1}v) + v]y + bz = 0. \quad (12.4.31)$$

Поскольку  $b \neq 0$ , точка  $(x, y, z)$  — единственное (с точностью до множителя) решение системы уравнений (12.4.31) и (12.4.26), т. е. единственная точка, общая двум нашим прямым.

*Случай 2:*  $b = 0, a \neq 0$ . Здесь (12.4.27) принимает вид:

$$(u + tv)y + az = 0, \quad (12.4.32)$$

и поскольку  $a \neq 0$ , (12.4.32) совместно с (12.4.26) определяют единственную точку  $(x, y, z)$ .

*Случай 3:*  $b = 0, a = 0$ . Теперь

$$a_{31} + a_{33} = a_{11} + a_{13} \text{ и } a_{32} = a_{12}.$$

Следовательно, из (12.4.24) получаем

$$(1, 0, -1) A^{h-g} = (a_{11} - a_{31})(1, 0, -1). \quad (12.4.33)$$

Здесь  $a_{11} - a_{31} \neq 0$ , так как  $A$  невырождена и  $A^{h-g}$  оставляет на месте точку  $(1, 0-1)$  подплоскости  $\pi_0$ . Следовательно,  $h-g \equiv 0 \pmod{q^2+q+1}$ , и так как мы выбираем  $g$ ,  $h$  среди  $0, \dots, q^2+q$ , то  $h=g$  и уравнения (12.4.25) и (12.4.26) принимают вид  $x+ty+z=0$  и  $x+sy+z=0$ . Поскольку наши прямые не совпадают,  $t \neq s$ , и эти уравнения имеют единственную общую точку  $(1, 0-1)$ , что и требовалось доказать.

Итак, мы имеем  $N = q^4 + q^2 + 1$  прямых, каждая из которых содержит  $q^2 + 1$  точек. Так как существует не более одной прямой, проходящей через две различные точки, то точка  $P_i$ , лежащая на  $m_i$  прямых, соединена с  $m_i q^2$  другими точками. Так как общее число точек равно  $q^4 + q^2 + 1$ , то  $m_i \leq q^2 + 1$  для каждой точки  $P_i$ . Общее число упорядоченных пар точек на наших  $N = q^4 + q^2 + 1$  прямых равно  $N(q^2 + 1)q^2$ . Поэтому

$$\sum_{i=1}^N m_i q^2 = N(q^2 + 1)q^2$$

и  $m_i = q^2 + 1$  для любого  $i = 1, 2, \dots, N$ , следовательно, каждая точка лежит на  $q^2 + 1$  прямых и соединена с  $q^4 + q^2$  другими точками, т. е. со всякой другой точкой. Таким образом, мы действительно имеем плоскость.

В первоначальном примере Веблена и Веддербёрна недезаргова плоскость имеет порядок 9. В этом случае порядок коллинеации равен 13, и коллинеация отображает индексы  $i \rightarrow i + 1 \pmod{13}$  как точек, так и прямых. Семь базисных прямых — это

$$\begin{aligned} L_0: & A_0 A_1 A_3 A_9 B_0 C_0 D_0 E_0 F_0 G_0, \\ M_0: & A_0 B_1 B_8 D_3 D_{11} E_2 E_5 E_6 G_7 G_9, \\ N_0: & A_0 C_1 C_8 E_7 E_9 F_3 F_{11} G_2 G_5 G_6, \\ P_0: & A_0 B_7 B_9 D_1 D_8 F_2 F_5 F_6 G_3 G_{11}, \\ Q_0: & A_0 B_2 B_5 B_6 C_3 C_{11} E_1 E_8 F_7 F_9, \\ R_0: & A_0 C_7 C_9 D_2 D_5 D_6 E_3 E_{11} F_1 F_8, \\ S_0: & A_0 B_3 B_{11} C_2 C_5 C_6 D_7 D_9 G_1 G_8. \end{aligned} \quad (12.4.34)$$

# Ортогональные латинские квадраты

---

## 13.1. Ортогональность и ортогональные таблицы

Дональд Кнут и Боуз заметили, что свойство быть латинским квадратом можно выразить как некоторое отношение ортогональности. Рассмотрим две ( $n \times n$ )-матрицы  $A = (a_{ij})$  и  $B = (b_{ij})$ , элементы которых — числа  $1, \dots, n$ . Скажем, что  $A$  ортогональна к  $B$  (в обозначениях  $A \perp B$ ), если для каждой упорядоченной пары чисел  $(a, b)$  существует не менее одной пары индексов  $(i, j)$ , такой, что  $a_{ij} = a$ ,  $b_{ij} = b$ . Так как всего имеется  $n^2$  ячеек и  $n^2$  упорядоченных пар  $(a, b)$ , мы можем заменить выражение „не менее“ выражениями „не более“ или „точно“. Следующие две матрицы

$$R = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 2 & 2 & \dots & 2 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ n & n & \dots & n \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & \dots & n \end{bmatrix}, \quad (13.1.1)$$

очевидно, ортогональны. Множество матриц называется множеством попарно ортогональных матриц, если любые две матрицы в этом множестве ортогональны. Отношение ортогональности не изменяется 1) при любой подстановке  $P$  над числами  $1, \dots, n$  в одной из матриц, если в этой матрице  $i$  всюду заменяется на  $P(i)$ , и 2) при любой одинаковой перестановке  $n^2$  ячеек во всех матрицах одновременно. Если  $A \perp B$ , то каждая из матриц  $A, B$  должна содержать каждое из чисел  $1, \dots, n$  точно  $n$  раз, и потому подходящей перестановкой ячеек мы можем одновременно преобразовать  $A$  в  $R$  и  $B$  в  $C$ .

Из приведенных выше рассмотрений следует, что  $(n \times n)$ -матрица  $L$  — латинский квадрат относительно  $1, \dots, n$  тогда и только тогда, когда  $L \perp R$  и  $L \perp C$ . Обратно, если  $E, F, G$  — три попарно ортогональные матрицы, то мы можем переставить ячейки так, что две из этих матриц становятся матрицами  $R$  и  $C$ , а третья — латинским квадратом  $L$ . Таким образом, свойство быть латинским квадратом можно полностью определить через свойство ортогональности. Существование  $k+2$  попарно ортогональных матриц в точности эквивалентно существованию  $k$  попарно ортогональных латинских квадратов. Кроме того, любая из этих матриц может быть преобразована в  $R$  и любая другая — в  $C$ .

Это соответствует выбору пучков параллельных прямых в главе 12 для введения системы координат в конечной плоскости.

Вопросы существования и построения попарно ортогональных латинских квадратов сведены, таким образом, к изучению отношения ортогональности. Этому подходу хорошо соответствует конструкция, называемая ортогональной таблицей. Скажем, что два вектора-строки  $v_1$  и  $v_2$  длины  $n^2$ ,

$$v_1 = (x_1, \dots, x_{n^2}) \quad \text{и} \quad v_2 = (y_1, \dots, y_{n^2}),$$

ортогональны, если среди упорядоченных пар  $(x_i, y_i)$ ,  $i = 1, \dots, n^2$ , каждая пара  $(a, b)$  встречается точно один раз,  $a, b$  — числа  $1, \dots, n$ .

**Определение.** *Ортогональной таблицей*  $\text{OA}(n, s)$  порядка  $n$  и высоты  $s$  называется матрица с  $s$  строками и  $n^2$  столбцами, элементы которой — числа  $1, \dots, n$ , а каждая пара строк ортогональна.

Мы можем поставить в соответствие столбцам  $\text{OA}(n, s)$ , взятым в произвольном порядке,  $n^2$  ячеек  $(n \times n)$ -матрицы и затем построить  $s$  матриц  $A_1, A_2, \dots, A_s$ , используя  $i$ -ю строку  $\text{OA}(n, s)$  для заполнения ячеек  $A_i$  в порядке, определенном соответствием столбцов с ячейками. Ортогональность матриц  $A_i$  и  $A_j$  в точности эквивалентна ортогональности  $i$ -й и  $j$ -й строк  $\text{OA}(n, s)$ . Обратно, если даны попарно ортогональные матрицы  $A_1, \dots, A_s$  по-

рядка  $n$ , то мы можем обращением этого процесса построить  $\text{OA}(n, s)$ .

Перестановка строк или столбцов ортогональной таблицы  $\text{OA}(n, s)$  снова дает  $\text{OA}(n, s)$ . Аналогично выполнение подстановки над числами  $1, \dots, n$  некоторой строки  $\text{OA}(n, s)$  дает другую ортогональную таблицу  $\text{OA}(n, s)$ . Две ортогональные таблицы, которые можно таким образом получить одну из другой, называются эквивалентными. Если исключить некоторую строку из  $\text{OA}(n, s)$ , то остающаяся таблица есть  $\text{OA}(n, s - 1)$ .

### 13.2. Основные теоремы

В гл. 12 было показано, что существует конечная плоскость порядка  $n$ , если  $n$  — степень простого числа,  $n = p^r$ , и что это эквивалентно существованию  $n - 1$  попарно ортогональных латинских квадратов порядка  $n$ , или, что то же самое,  $n + 1$  ортогональных матриц. Соответствующая ортогональная таблица — это  $\text{OA}(n, n + 1)$ . Легко видеть, что эквивалентные ортогональные таблицы определяют одну и ту же плоскость. Мы можем вообще считать, что  $\text{OA}(n, s)$  определяет  $s$  пучков параллельных прямых, где столбцы — это точки, и точка (столбец)  $j$  лежит на  $i$ -й прямой  $i$ -го пучка, если в  $\text{OA}(n, s)$   $a_{ij} = i$ . Таким образом, эквивалентность ортогональных таблиц заключается в том, что одна получается из другой перенумерованием точек и прямых, сохраняющим неизменными инцидентности.

**Теорема 13.2.1** (Макнейш [1]). *Если существуют  $\text{OA}(n_1, s)$  и  $\text{OA}(n_2, s)$ , то существует  $\text{OA}(n_1 n_2, s)$ .*

**Доказательство.** Пусть  $\text{OA}(n_1, s)$  — матрица

$$A = (a_{ij}), \quad i = 1, \dots, s, \quad j = 1, \dots, n_1^2,$$

а  $\text{OA}(n_2, s)$  — матрица

$$B = (b_{ij}), \quad i = 1, \dots, s, \quad j = 1, \dots, n_2^2.$$

Образуем новую матрицу

$$D = (d_{ij}), \quad i = 1, \dots, s, \quad j = 1, \dots, n_1^2 n_2^2,$$

заменяя в  $A$  элемент  $a_{ij}$  вектором-строкой

$$(b_{i1} + m_{ij}, b_{i2} + m_{ij}, \dots, b_{in_2^2} + m_{ij}), \quad m_{ij} = (a_{ij} - 1)n_2$$

для любой пары  $i, j$ .

Так как числа  $a_{ij}$  принимают значения от 1 до  $n_1$ , а числа  $b_{ij}$  — от 1 до  $n_2$ , то числа  $b_{it} + m_{ij}$  принимают значения от 1 до  $n_1 n_2$ , следовательно,  $d_{ij}$  есть одно из чисел 1, ...,  $n_1 n_2$ . Рассмотрим  $h$ -ю и  $i$ -ю строки  $D$ , и пусть  $u, v$  — любые два из чисел 1, ...,  $n_1 n_2$ . Тогда мы можем написать

$$u = u_1 + (u_2 - 1)n_2, \quad v = v_1 + (v_2 - 1)n_2,$$

где  $1 \leq u_1, v_1 \leq n_2$ ,  $1 \leq u_2, v_2 \leq n_1$  и  $u_1, v_1, u_2, v_2$  определяются однозначно. Обозначим в  $A$  через  $j$  номер столбца, в котором  $a_{hj} = u_2$ ,  $a_{ij} = v_2$ . В  $B$  обозначим через  $t$  номер столбца, в котором  $b_{ht} = u_1$  и  $b_{it} = v_1$ . Тогда в  $D$ , в столбце  $g = t + n_2(j - 1)$ , получим

$$d_{hg} = b_{ht} + (a_{hj} - 1)n_2 = u_1 + (u_2 - 1)n_2 = u$$

и

$$d_{ig} = b_{it} + (a_{ij} - 1)n_2 = v_1 + (v_2 - 1)n_2 = v,$$

что означает ортогональность  $h$ -й и  $i$ -й строк  $D$  и, таким образом, доказывает, что  $D$  — ортогональная таблица.

Можно привести доказательство этой теоремы в другой форме. Пусть  $A_1, \dots, A_s$  — попарно ортогональные матрицы порядка  $n_1$ , где вместо чисел 1, ...,  $n_1$  стоят неизвестные  $x_u$ ,  $u = 1, \dots, n_1$ ; и аналогично  $B_1, \dots, B_s$  — попарно ортогональные матрицы порядка  $n_2$ , элементы которых — неизвестные  $y_v$ ,  $v = 1, \dots, n_2$ . Тогда прямые произведения

$$A_1 \times B_1, A_2 \times B_2, \dots, A_s \times B_s,$$

рассматриваемые как матрицы с  $n_1 n_2$  неизвестными

$$z_{uv} = x_u y_v, \quad u = 1, \dots, n_1, \quad v = 1, \dots, n_2,$$

в качестве элементов, попарно ортогональны. Для двух данных индексов  $h, i$  из множества  $\{1, \dots, s\}$  и для  $z_{u_1 v_1}$  и  $z_{u_2 v_2}$  существует ячейка, в которой в  $A_h$  стоит  $x_{u_1}$ ,

а в  $A_i$  стоит  $x_{u_2}$ , а также ячейка, в которой в  $B_h$  стоит  $y_{v_1}$ , а в  $B_i$  стоит  $y_{v_2}$ . Соответствующая ячейка в  $A_h \times B_h$  содержит  $z_{u_1 v_1}$ , а в  $A_i \times B_i$  содержит  $z_{u_2 v_2}$ .

Следующая теорема по существу является следствием теоремы 13.2.1.

**Теорема 13.2.2.** *Если  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  есть представление целого числа в виде произведения степеней различных простых чисел  $p_1, \dots, p_r$ , то существует не меньше  $N(n)$  попарно ортогональных латинских квадратов порядка  $n$ , где*

$$N(n) \geq \min(p_i^{e_i} - 1), \quad i = 1, \dots, r.$$

**Доказательство.** Из существования конечной плоскости порядка  $n_i = p_i^{e_i}$ ,  $i = 1, \dots, r$ , следует существование ОА( $n_i, n_i + 1$ ),  $i = 1, \dots, r$ . Поэтому если  $s$  — минимум  $n_i + 1$ , то существует ОА( $n_i, s$ ). Повторное применение теоремы 13.2.1 дает доказательство существования ОА( $n, s$ ), т. е. существования  $s - 2 = \min(n_i - 1)$  попарно ортогональных латинских квадратов порядка  $n$ , что и составляет утверждение теоремы.

Если через  $N(n)$  обозначить максимальное число попарно ортогональных латинских квадратов, то эта теорема дает нижнюю границу для  $N(n)$ . В частности, если  $n$  имеет вид  $n = 4t + 2$ , то утверждение теоремы тривиально:  $N(n) \geq 1$ . Эйлер в 1782 г. предположил, что для  $n = 4t + 2$  не существует пары ортогональных латинских квадратов: „Я не колеблясь готов утверждать, что невозможно построить какой-либо полный квадрат из 36 элементов, и эта невозможность распространяется на все случаи  $n = 10, n = 14$  и вообще для всех нечетных четных чисел“. Макнейш в 1922 г. пришел к предположению, что

$$N(n) = \min(p_i^{e_i} - 1), \quad i = 1, \dots, r \quad \text{для } n = p_1^{e_1} \dots p_r^{e_r},$$

и опубликовал ошибочное доказательство того, что  $N(4t + 2) = 1$ , используя некоторый топологический метод. Как мы увидим, оба предположения, Эйлера и Макнейша, были, наконец, опровергнуты в 1959 г.

В действительности Эйлер был прав только в случаях  $n = 2$  и  $n = 6$ . В случае  $n = 6$  это было подтверждено в 1900 г. Терри [1] путем перебора всех возможностей.

Не для каждого латинского квадрата существует другой латинский квадрат, ортогональный данному, или, как мы будем говорить, *ортогональный соквадрат*<sup>1)</sup>. Одно необходимое условие для существования ортогонального соквадрата было установлено Манном [1].

Пусть  $n$  чисел разделены на два множества  $A$  и  $B$ , где  $A$  содержит  $k$  чисел, а  $B$  содержит  $n - k$  чисел. Потребуем, кроме того, чтобы  $k$  было нечетным. Столбцы таблицы ОА( $n, 3$ ), соответствующей латинскому квадрату порядка  $n$ , могут быть разделены на восемь типов в соответствии с тем, числа какого множества появляются в каждой строке. Напишем

| $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $x_7$ | $x_8$ |
|-------|-------|-------|-------|-------|-------|-------|-------|
| $A$   | $A$   | $A$   | $A$   | $B$   | $B$   | $B$   | $B$   |
| $A$   | $A$   | $B$   | $B$   | $A$   | $A$   | $B$   | $B$   |
| $A$   | $B$   | $A$   | $B$   | $A$   | $B$   | $A$   | $B$   |

(13.2.1)

где  $x_i$  обозначает число столбцов данного типа. Ортогональность строк дает несколько соотношений для  $x_i$ . Заметим, что в любых двух строках имеется  $k^2$  комбинаций вида  $AA$ ,  $k(n-k)$  — вида  $BA$ ,  $k(n-k)$  — вида  $AB$  и  $(n-k)^2$  — вида  $BB$ . Это приводит к следующим (наряду с другими) соотношениям:

$$\begin{aligned} x_1 + x_2 &= k^2, & x_2 + x_4 &= k(n-k), & x_7 + x_8 &= (n-k)^2, \\ x_1 + x_3 &= k^2, & x_5 + x_6 &= k(n-k), \\ x_1 + x_5 &= k^2, & x_5 + x_7 &= k(n-k). \end{aligned} \quad (13.2.2)$$

Отсюда

$$\begin{aligned} x_2 &= k^2 - x_1, & x_6 &= nk - 2k^2 + x_1, \\ x_3 &= k^2 - x_1, & x_7 &= nk - 2k^2 + x_1, \\ x_4 &= nk - 2k^2 + x_1, & x_8 &= n^2 - 3nk + 3k^2 - x_1. \\ x_5 &= k^2 - x_1, \end{aligned} \quad (13.2.3)$$

<sup>1)</sup> В оригинале *orthogonal mate*. — Прим. перев.

Назовем нечетными те столбцы, которые содержат  $A$  нечетное число раз, а именно столбцы типов  $x_1, x_4, x_6$  и  $x_7$ . Общее число нечетных столбцов равно  $4x_1 + 3nk - 6k^2$ . Предположим, что

$$4x_1 + 3nk - 6k^2 < n. \quad (13.2.4)$$

Тогда, если можно добавить четвертую строку так, чтобы получилась ортогональная таблица  $OA(n, 4)$ , то, поскольку существует менее  $n$  нечетных столбцов, должно существовать число (скажем,  $u$ ) в четвертой строке, появляющееся только в четных столбцах:

$$\begin{array}{cccc} y_2 & y_3 & y_5 & y_8 \\ A & A & B & B \\ A & B & A & B \\ B & A & A & B \\ u & u & u & u \end{array} \quad (13.2.5)$$

Здесь  $y_i$  — число таких столбцов каждого вида. Так как в (13.2.5) учтены все появления  $u$ , то

$$\begin{aligned} y_2 + y_3 + y_5 + y_8 &= n, \\ y_2 + y_3 &= k, \quad y_3 + y_5 = k, \\ y_2 + y_5 &= k, \end{aligned} \quad (13.2.6)$$

где в первой сумме учитывается общее число появлений  $u$ , а в остальных — число парных комбинаций  $u$  с числами  $A$  для первой, второй и третьей строк соответственно. Но отсюда

$$2(y_2 + y_3 + y_5) = 3k, \quad (13.2.7)$$

что противоречит нашему предположению о нечетности  $k$ . Следовательно, если  $k$  нечетно, условие (13.2.4) ведет к противоречию. Возможность такого выбора  $k, n$  и  $x$ , чтобы удовлетворялось (13.2.4), обеспечивается условиями следующей теоремы.

**Теорема 13.2.3 (Манн).** Пусть  $L$  — латинский квадрат порядка  $4t + 2$  (соответственно  $4t + 1$ ) с подквадратом порядка  $2t + 1$  ( $2t$ ), все ячейки которого, за исключением  $t$  (соответственно  $[(t - 1)/2]$ ) или меньшего

числа ячеек, заполнены элементами из множества  $2t+1$  (соответственно  $2t$ ) чисел. Тогда не существует латинского квадрата, ортогонального к  $L$ .

**Доказательство.** В первом случае возьмем  $k = 2t+1$ . Условие (13.2.4) сводится к  $4x_1 < 4t+2$ , или  $x_1 \leq t$ . Оно выполняется, так как в подквадрате порядка  $2t+1$ , соответствующем столбцам из (13.2.1), помеченным  $x_1$  и  $x_2$ , все элементы принадлежат  $B$ , за исключением не более  $t$  букв из  $A$ .

Во втором случае при  $n = 4t+1$ ,  $k = 2t+1$  условие (13.2.4) сводится к  $4x_1 < 10t+4$ . Подквадрат порядка  $2t$  из столбцов двух типов  $x_7$  и  $x_8$  содержит  $x_7 = x_1 - 2t - 1$  элементов из  $A$ . Условие (13.2.4) в нашем случае эквивалентно неравенству

$$x_7 < \frac{t}{2}, \quad \text{или} \quad x_7 \leq \left[ \frac{t-1}{2} \right],$$

и справедливость его вытекает из условий теоремы. Для  $n$  вида  $4t$  или  $4t+3$  результата, аналогичного теореме 13.2.3, нет.

Островский и Ван Дюрен при помощи вычислительной машины нашли пару ортогональных латинских квадратов порядка 10, в которой один из квадратов имел подквадрат порядка 5, все ячейки которого, за исключением трех, были заняты числами от 0 до 4. Таким образом, неравенство Манна неулучшаемо. Эти квадраты таковы:

|           |           |           |                    |
|-----------|-----------|-----------|--------------------|
| 0 1 2 3 4 | 5 6 7 8 9 | 0 1 9 2 3 | 8 4 6 5 7          |
| 3 4 0 1 2 | 7 9 8 6 5 | 6 7 8 9 5 | 2 3 1 0 4          |
| 4 3 1 2 0 | 9 7 6 5 8 | 9 3 7 4 6 | 5 8 2 1 0          |
| 1 2 4 0 7 | 8 5 3 9 6 | 3 8 2 5 4 | 7 9 0 6 1          |
| 2 0 3 7 5 | 6 8 9 4 1 | 1 4 5 0 7 | 3 6 9 8 2          |
| 5 7 6 9 8 | 3 4 1 2 0 | 2 5 6 1 9 | 4 0 8 7 3 (13.2.8) |
| 8 9 7 5 6 | 1 2 0 3 4 | 4 0 1 3 8 | 6 2 7 9 5          |
| 6 5 9 8 1 | 4 3 2 0 7 | 5 6 4 8 0 | 1 7 3 2 9          |
| 9 8 5 6 3 | 0 1 4 7 2 | 8 2 0 7 1 | 9 5 4 3 6          |
| 7 6 8 4 9 | 2 0 5 1 3 | 7 9 3 6 2 | 0 1 5 4 8          |

### 13.3. Построение ортогональных квадратов

Мы начнем с построения, которое докажет неравенство  $N(12t + 10) \geq 2$ . Пусть  $m$  — такое число, что существует пара ортогональных латинских квадратов порядка  $m$ . Определим следующие векторы длины  $m$ , составленные из вычетов по модулю  $2m + 1$  для  $i = 0, 1, \dots, 2m$ :

$$\begin{aligned} a_i &= (i, i, i, \dots), \\ b_i &= (i+1, i+2, \dots, i+m), \\ c_i &= (i-1, i-2, \dots, i-m). \end{aligned} \quad (13.3.1)$$

Образуем разности этих векторов:

$$\begin{aligned} d_1 &= a_i - b_i = (2m, 2m-1, \dots, m+1), \\ d'_1 &= b_i - a_i = (1, 2, \dots, m), \\ d_2 &= a_i - c_i = (1, 2, \dots, m), \\ d'_2 &= c_i - a_i = (2m, 2m-1, \dots, m+1), \\ d_3 &= b_i - c_i = (2, 4, \dots, 2m), \\ d'_3 &= c_i - b_i = (2m-1, 2m-3, \dots, 1). \end{aligned} \quad (13.3.2)$$

При любом  $j$ ,  $j = 1, 2, 3$ ,  $d_j$  и  $d'_j$ , взятые вместе, содержат все ненулевые вычеты по модулю  $2m + 1$ . Построим теперь векторы длины  $m(2m + 1)$ :

$$\begin{aligned} A &= (a_0, a_1, a_2, \dots, a_{2m}), \\ B &= (b_0, b_1, b_2, \dots, b_{2m}), \\ C &= (c_0, c_1, c_2, \dots, c_{2m}). \end{aligned} \quad (13.3.3)$$

Возьмем  $m$  новых букв  $x_1, \dots, x_m$  и образуем вектор  $X$  длины  $m(2m + 1)$ :

$$X = (x_1, \dots, x_m, x_1, \dots, x_m, \dots, x_1, \dots, x_m), \quad (13.3.4)$$

а затем  $[4 \times 4m(2m + 1)]$ -матрицу  $D$ :

$$D = \begin{bmatrix} A & B & C & X \\ B & A & X & C \\ C & X & A & B \\ X & C & B & A \end{bmatrix}. \quad (13.3.5)$$

Рассмотрим любые две строки этой матрицы. Они содержат одну из подматриц:  $\begin{bmatrix} A & B \\ B & A \end{bmatrix}$ ,  $\begin{bmatrix} A & C \\ C & A \end{bmatrix}$  или  $\begin{bmatrix} B & C \\ C & B \end{bmatrix}$ . Тогда, если  $u$ ,  $v$  — различные вычеты по модулю  $2m+1$ , то вычет

$$e \equiv u - v \pmod{2m+1}$$

появляется в соответствующем  $d_j$  или  $d'_j$ :

$$e \equiv (i+g) - (i+h) \equiv g - h \equiv u - v \pmod{2m+1},$$

где  $(i+g) - (i+h)$  есть разность из  $d_j$  или  $d'_j$ . Определим  $i$  сравнением  $i + h \equiv v \pmod{2m+1}$ , тогда

$$i + g \equiv (i + h) + u - v \equiv u \pmod{2m+1},$$

следовательно, пара  $\begin{pmatrix} u \\ v \end{pmatrix}$  появляется как столбец в этих двух строках. Аналогично в любых двух строках из (13.3.5) появляется одна из подматриц  $\begin{bmatrix} AX \\ XA \end{bmatrix}$ ,  $\begin{bmatrix} BX \\ XB \end{bmatrix}$  или  $\begin{bmatrix} CX \\ XC \end{bmatrix}$ , и отсюда мы получаем все столбцы  $\begin{pmatrix} x_j \\ u \end{pmatrix}$  и  $\begin{pmatrix} u \\ x_j \end{pmatrix}$ ,

где  $u$  — любой вычет по модулю  $2m+1$ , а  $x_j$  — любое из  $x_1, \dots, x_m$ . Если мы предполагаем, что существует пара ортогональных квадратов порядка  $m$ , то существует  $OA(m, 4) = E$  с элементами  $x_1, \dots, x_m$ , т. е. матрица размера  $4 \times m^2$ , строки которой ортогональны относительно  $x_i$ . Образуем теперь матрицу  $F$ :

$$F = \begin{bmatrix} 0 & 1 & 2 & \dots & 2m \\ 0 & 1 & 2 & \dots & 2m \\ 0 & 1 & 2 & \dots & 2m \\ 0 & 1 & 2 & \dots & 2m \end{bmatrix} DE. \quad (13.3.6)$$

Здесь  $F$  имеет четыре строки и  $2m+1+4m(2m+1)+m^2 = (3m+1)^2$  столбцов. В любых двух строках матрицы  $F$  мы получаем столбцы  $\begin{pmatrix} u \\ u \end{pmatrix}$ , где  $u$  — вычет по модулю  $2m+1$ , из первых  $2m+1$  столбцов, столбцы  $\begin{pmatrix} x_i \\ x_j \end{pmatrix}$  — из  $E$  и все остальные — из  $D$ . Следовательно,  $F$  есть

ОА( $3m + 1$ , 4). Сформулируем наш результат в виде теоремы.

**Теорема 13.3.1.** *Если  $N(m) \geq 2$ , то  $N(3m + 1) \geq 2$ . В частности, так как  $N(4t + 3) \geq 2$ , отсюда следует, что  $N(12t + 10) \geq 2$ .*

Основная теорема о построении ортогональных квадратов представляет собой рекурсивное построение, основанное на существовании уравновешенной относительно пар блок-схемы. Уравновешенной относительно пар (элементов) блок-схемой BIB( $v, k_1, \dots, k_m, \lambda$ )<sup>1)</sup> называется такое размещение  $v$  элементов по  $b$  блокам, что: 1) каждый блок содержит  $k_i < v$  различных элементов при некотором  $i = 1, \dots, m$ ; 2) каждая пара элементов появляется вместе точно в  $\lambda$  блоках. Пусть  $b_i$  — число блоков с  $k_i$  элементами. Тогда

$$\sum b_i = b, \quad \lambda v(v - 1) = \sum b_i k_i (k_i - 1). \quad (13.3.7)$$

Эти  $b_i$  блоков с  $k_i$  элементами будем называть  $i$ -й равноблочной компонентой. Свободным множеством назовем множество всех блоков нескольких равноблочных компонент, в котором никакие два блока не имеют общего элемента. Будем писать

$$\text{BIB}(v, k_1, \dots, k_r, \dots, k_m, \lambda),$$

если первые  $r$  равноблочных компонент образуют свободное множество. В наших построениях мы будем использовать только уравновешенные относительно пар блок-схемы с  $\lambda = 1$ .

Следующая теорема, но в более слабой форме, впервые была получена Паркером [2], позднее обобщена Боузом и Шрикханде [1], а затем еще более обобщена всеми тремя авторами совместно [1].

**Теорема 13.3.2** (основная теорема). *Если существует уравновешенная относительно пар блок-схема*

$$\text{BIB}(v, k_1, \dots, k_r, \dots, k_m, 1),$$

<sup>1)</sup> Обозначение идет от сокращения термина balanced incomplete block design. — Прим. перев.

то

$$N(v) \geq \min(N(k_1), \dots, N(k_r), N(k_{r+1}) - 1, \dots, N(k_m) - 1).$$

**Доказательство.** Свободное множество будет рассматриваться иначе, чем остальные блоки схемы, что отражается в формулировке теоремы. Свободное множество, грубо говоря, аналогично параллельным прямым в аффинной плоскости, несвободное множество — прямым в проективной плоскости.

Полагаем

$$c = \min(N(k_1) + 2, \dots, N(k_r) + 2, N(k_{r+1}) + 1, \dots, N(k_m) + 1),$$

и для  $i = 1, \dots, r$  пусть  $A_i = \text{OA}(k_i, c)$ . Для  $i = r+1, \dots, n$  существует

$$\text{OA}(k_i, c+1) = D_i.$$

В  $D_i$ , матрице с элементами  $1, \dots, k_i$ , переставим  $k_i$  столбцов с 1 в первой строке в левую часть матрицы и перенумеруем элементы в остальных строках так, чтобы первые  $k_i$  столбцов матрицы  $D_i$  приняли вид

$$\left[ \begin{array}{cccc} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & k_i \\ 1 & 2 & \dots & k_i \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 1 & 2 & \dots & k_i \end{array} \right]. \quad (13.3.8)$$

Затем для  $i = r+1, \dots, m$  образуем матрицу  $A_i$  вычеркиванием первой строки и первых  $k_i$  столбцов из  $D_i$ . Матрица  $A_i$  есть  $[c \times (k_i^2 - k_i)]$ -матрица, имеющая во всякой паре строк все столбцы  $\binom{u}{w}$  с  $u \neq w$ ,  $u, w = 1, \dots$

$\dots, k_i$ , но не имеющая столбцов вида  $\binom{u}{u}$ . Пусть  $S_1, S_2, \dots, S_b$  — это  $b$  блоков данной уравновешенной схемы.

Если  $S_j$  имеет  $k_i$  элементов, то образуем из  $A_i$  таблицу  $B_j$ , заменяя числа  $1, \dots, k_i$  матрицы  $A_i$  элементами из  $S_j$ . Наконец, образуем таблицу

$$C = (B_1, B_2, \dots, B_b, E), \quad (13.3.9)$$

где  $E$  — такое дополнительное множество столбцов, что каждый столбец в  $E$  состоит из одного и того же числа, повторенного  $c$  раз, и в  $E$  имеется один столбец для каждого элемента, не появляющегося в блоках свободного множества.

Мы утверждаем, что таблица  $C$  из (13.3.9) есть ОА( $v, c$ ). Выберем в  $C$  две строки. Если  $u \neq w$  — два различных элемента из  $v$  элементов нашей уравновешенной схемы, то существует точно один блок  $S_j$ , содержащий оба элемента, и в соответствующем  $B_j$  в этих двух строках найдется столбец  $\begin{pmatrix} u \\ w \end{pmatrix}$ . Кроме того,  $u$  и  $w$  не появляются вместе ни в каком другом блоке  $B$ , они не могут появиться и в столбце множества  $E$ . Если  $u$  — элемент блока  $S_j$  свободного множества, то матрица  $B_j$  содержит столбец  $\begin{pmatrix} u \\ u \end{pmatrix}$  в двух выбранных строках. Если  $u$  не есть элемент блока свободного множества, то в  $E$  найдется столбец  $\begin{pmatrix} u \\ u \end{pmatrix}$ . Таким образом, две строки ортогональны, и  $C$  есть ОА( $v, c$ ). Следовательно, существует не менее  $c - 2$  попарно ортогональных квадратов порядка  $v$  и  $N(v) \geq c - 2$ , т. е. утверждение теоремы доказано.

Конечная плоскость порядка 4 — это ВИВ(21,5,1), и применение к ней теоремы 13.3.2 дает неравенство  $N(21) \geq N(5) - 1 = 3$ , что улучшает значение Макнейша,  $N(21) = 2$ . Это неравенство приведено в работе Паркера и было первым опровержением предположения Макнейша. Следующие две теоремы получаются почти непосредственно как приложения основной теоремы.

**Теорема 13.3.3.** Если существует ВИВ( $v, k, 1$ ), то

$$(1) \quad N(v - 1) \geq \min(N(k - 1), N(k) - 1)$$

**и**

$$(2) \quad N(v-x) \geqslant \min(N(k-x), N(k-1)-1, N(k)-1)$$

при любом  $x$ , таком, что  $1 \leqslant x \leqslant k$ .

В дальнейшем условимся, что  $N(0) = N(1) = \infty$ .

**Доказательство.** Вычеркнем  $x$  элементов некоторого блока из этого и всех остальных блоков. Если  $x=1$ , то блоки, из которых был вычеркнут этот элемент, образуют свободное множество блоков с  $k-1$  элементами, и мы имеем  $\text{BIB}(v-1, k-1, k, 1)$ . Применение теоремы 13.3.2 дает (1). Если  $x > 1$ , то блок с  $k-x$  элементами является свободным множеством, а все другие блоки имеют  $k-1$  или  $k$  элементов. Применение теоремы 13.3.2 дает (2).

**Теорема 13.3.4.** *Если существует  $\text{BIB}(v, k, 1)$ , то*

$$N(v-3) \geqslant \min(N(k-2), N(k-1)-1, N(k)-1).$$

**Доказательство.** Вычеркнем из  $\text{BIB}(v, k, 1)$  три элемента, не принадлежащие одному и тому же блоку. Получим

$$\text{BIB}(v-3, k-2, k-1, k, 1),$$

так как три блока, из которых были вычеркнуты два элемента, образуют свободное множество, а все остальные блоки имеют либо  $k-1$ , либо  $k$  элементов. Применение основной теоремы дает требуемый результат. В частности, из существования  $\text{BIB}(21, 5, 1)$  следует

$$N(18) \geqslant \min(N(3), N(4)-1, N(5)-1) = \min(2, 2, 3) = 2,$$

что доказывает существование пары ортогональных квадратов порядка 18.

Схема называется *разрешимой*, если блоки могут быть разделены на  $r$  множеств (дубликатов) так, что в блоках каждого из этих множеств каждый элемент встретится точно один раз. Например, прямые аффинной плоскости порядка  $n$ , разделенные на  $n+1$  множеств параллельных прямых, образуют разрешимую схему.

**Теорема 13.3.5.** Если существует разрешимая BIB( $v, k, 1$ ) с  $r$  дубликатами, то

- 1)  $N(v+x) \geq \min(N(x), N(k)-1, N(k+1)-1)$   
при  $1 \leq x < r-1$ ,
- 2)  $N(v+r-1) \geq \min(N(r-1), N(k), N(k+1)-1)$ ,
- 3)  $N(v+r) \geq \min(N(r), N(k+1)-1)$ .

**Доказательство.** Пусть  $1 \leq x \leq r$ . К каждому блоку  $i$ -го дубликата добавим новый элемент  $Y_i$ ,  $1 \leq i \leq x$ . Затем к блокам схемы добавим блок  $Y_1, \dots, Y_x$ . Если  $1 \leq x < r-1$ , то получается BIB( $v+x, x, k, k+1, 1$ ); если  $x = r-1$ , то имеем BIB( $v+r-1, r-1, k, k+1, 1$ ); если  $x = r$ , то имеем BIB( $v+r, r, k+1, 1$ ). Утверждения теоремы следуют теперь из основной теоремы 13.3.2. Рассмотрим в качестве примера применение доказанной теоремы к аффинной плоскости порядка 7, которая есть BIB(49, 7, 1). При  $x = 1$  находим, что  $N(50) \geq 5$ , а при  $x = 5$  имеем  $N(54) \geq 4$ .

Другой вид схем, тесно связанных с ортогональными таблицами, — это *схемы с делительностью на группы* (group divisible design) GD( $v; k, m; \lambda_1, \lambda_2$ )<sup>1</sup>. Так называются схемы, в которых элементы разделены на  $v/m$  групп, с  $m$  элементами в каждой из групп, причем 1) каждый блок содержит  $k$  элементов, 2) любые два элемента одной и той же группы появляются вместе в  $\lambda_1$  блоках, в то время как любые два элемента разных групп появляются вместе в  $\lambda_2$  блоках. Нам нужен лишь тот случай, когда  $\lambda_1 = 0, \lambda_2 = 1$ .

**Теорема 13.3.6.** Если  $k \leq N(m) + 1$ , то существует разрешимая<sup>2</sup> схема GD( $km; k, m; 0, 1$ ).

**Доказательство.** Построим ОА( $m, k+1$ ). Расположим в ней столбцы так, чтобы последняя строка имела вид

$$1, \dots, 1, 2, \dots, 2, 3, \dots, 3, \dots, m, \dots, m. \quad (13.3.10)$$

<sup>1</sup>) Схема GD( $v; k, m; \lambda_1, \lambda_2$ ) — это частный случай так называемых частично уравновешенных блок-схем (PBIB-схем). — Прим. перев.

<sup>2</sup>) С  $m$  дубликатами. — Прим. ред.

Тогда столбцы разделятся на  $m$  множеств по  $m$  столбцов в каждом:  $i$ -е множество — то, для которого элементы в последней строке равны  $i$ . В результате первые  $k$  строк разделятся на  $m$  частей. Выбросим теперь последнюю строку и заменим каждое число  $i$  в  $j$ -й строке упорядоченной парой  $(i, j)$ , в результате чего получим  $km$  новых элементов. Столбцы полученной таким образом таблицы будем рассматривать как блоки новой схемы. Элементы с одинаковой второй координатой никогда не повторяются в одном и том же блоке, а элементы, у которых вторые координаты различны, появляются в одном блоке точно один раз. Кроме того, схема разрешима, так как ортогональность  $(k+1)$ -й строки остальным в исходной таблице гарантирует нам, что в каждой из  $m$  частей каждая из  $km$  пар  $(i, j)$  встретится точно один раз.

Теоремы 13.3.5 и 13.3.6 указывают на связь между ортогональными таблицами и разрешимыми схемами, так что при помощи таблиц мы можем строить схемы, и наоборот.

**Теорема 13.3.7.** *Если существует разрешимая схема  $\text{GD}(v; k, m; 0, 1)$  с  $r$  дубликатами, то*

- 1)  $N(v+x) \geq \min(N(m), N(x), N(k)-1, N(k+1)-1)$   
при  $1 \leq x < r$ ,
- 2)  $N(v+r) \geq \min(N(m), N(r), N(k+1)-1)$ ,
- 3)  $N(v+r) \geq \min(N(k), N(r), N(k+1)-1, N(m+1)-1)$ ,
- 4)  $N(v+r+1) \geq \min(N(r+1), N(k+1)-1, N(m+1)-1)$ .

**Доказательство.** Для каждой группы элементов образуем блок, состоящий из всех  $m$  элементов группы и присоединим к  $\text{GD}(v; k, m; 0, 1)$  эти  $v/m$  блоков. Тогда получим  $\text{BIB}(v, m, k, 1)$ . Затем присоединим к каждому блоку  $i$ -го дубликата исходной схемы,  $i = 1, \dots, x$ , новый элемент  $Y_i$  и образуем также новый блок  $Y_1, \dots, Y_x$ . При  $x < r$  получаем

$$\text{BIB}(v+x, x, m, k, k+1, 1).$$

При  $x = r$  имеем

$$\text{BIB}(v+r, r, m, k+1, 1).$$

Первые два утверждения нашей теоремы следуют из основной теоремы. Для доказательства третьего утверждения возьмем  $x = r - 1$ ; оставив последний дубликат свободным, присоединим  $Y_0$  к каждому из блоков, составленных из элементов некоторой группы, и образуем также блок  $Y_0, Y_1, \dots, Y_{r-1}$ ; тогда получим

$$\text{BIB}(v + r, k, r, k + 1, m + 1, 1).$$

Чтобы доказать последнее утверждение теоремы, добавим  $Y_i$ ,  $i = 1, \dots, r$ , к блокам  $i$ -го дубликата,  $Y_0$  — ко всем блокам, составленным из элементов некоторой группы, и образуем также  $Y_0, Y_1, \dots, Y_r$ . Тогда получаем

$$\text{BIB}(v + r + 1, r + 1, k + 1, m + 1, 1),$$

и теорема доказана.

Теоремы 13.3.6 и 13.3.7 можно объединить в одну и получить следующий важный результат.

**Теорема 13.3.8.** *Если  $k \leq N(m) + 1$ , то при  $1 \leq x < m$  имеем*

$$N(km + x) \geq \min(N(m), N(x), N(k) - 1, N(k + 1) - 1).$$

**Доказательство.** Доказательство получается из теоремы 13.3.6 и первого неравенства теоремы 13.3.7 с  $v = km$ .

### 13.4. Опровержение предположения Эйлера

Предположение Эйлера о том, что не существует пары ортогональных латинских квадратов порядка  $n$ , когда  $n = 4t + 2$ , оказывается верным для  $n = 2$  и  $n = 6$ , но не верно ни в каком другом случае. Данный раздел посвящен доказательству этого факта и, следовательно, полному опровержению предположения.

**Теорема 13.4.1.** *Для всякого  $n > 6$  существует пара ортогональных латинских квадратов порядка  $n$ .*

**Доказательство.** Требуется доказать, что  $N(n) \geq 2$  при  $n > 6$ . В силу теоремы 13.2.2 достаточно доказать это для  $n = 4t + 2$ . Следующая лемма сводит доказательство к конечному числу значений  $n$ .

**Лемма 13.4.1.** Если  $N(4t+2) \geq 2$  для  $10 \leq 4t+2 \leq 726$ , то  $N(v) \geq 2$  для всех  $v > 6$ .

**Доказательство.** Пусть  $v = 4t+2$ ,  $v \geq 730$ . Тогда  $v-10 \geq 720$  и мы можем написать

$$v-10 = 144g + 4u, \quad g \geq 5, \quad 0 \leq u \leq 35. \quad (13.4.1)$$

Отсюда

$$v = 4(36g) + 4u + 10, \quad g \geq 5, \quad 0 \leq u \leq 35. \quad (13.4.2)$$

Обратимся теперь к теореме 13.3.8 при  $k=4$ ,  $m=36g$  и  $x=4u+10$ . Имеем  $N(4)=3$ ,  $N(5)=4$ . При  $m=36g$  наименьшая степень простого числа, делящая  $m$ , не меньше 4, поэтому  $N(m) \geq 3$ , и условие  $k \leq N(m)+1$  удовлетворяется при  $k=4$ . Поскольку  $0 \leq u \leq 35$ , мы имеем  $10 \leq x \leq 150$ ; так как  $g \geq 54$ ,  $m \geq 180$ , условие  $1 \leq x < m$  удовлетворяется. Таким образом, из теоремы 13.3.8 следует, что

$$N(v) \geq \min(N(m), N(x), 2, 3) = \min(N(x), 2),$$

и если  $N(x) \geq 2$ , то  $N(v) \geq 2$ . Это показывает, что если  $N(x) \geq 2$  при  $10 \leq x \leq 726$ , то

$$N(v) = N(4t+2) \geq 2 \quad \text{для всех } v = 4t+2 \geq 730,$$

что и требовалось доказать.

Начнем с трех частных примеров.

**Пример 1.** Пусть  $n=14$ . Рассмотрим матрицу

$$P_0 = \begin{bmatrix} 0 & x_1 & x_2 & x_3 \\ 1 & 0 & 0 & 0 \\ 4 & 4 & 6 & 9 \\ 6 & 1 & 2 & 8 \end{bmatrix},$$

где  $x_1, x_2, x_3$  — неизвестные, а остальные элементы рассматриваются как вычеты по модулю 11. Пусть  $P_1, P_2, P_3$  получены из  $P_0$  циклической перестановкой строк. Полагаем  $A_0 = (P_0, P_1, P_2, P_3)$ , и пусть  $A_i$  получается из  $A_0$  прибавлением  $i^1)$  по модулю 11 к каждому вы-

<sup>1)</sup>  $i=1, \dots, 10$ . — Прим. перев.

чтету в  $A_0$ . Если  $A^*$  есть ОА (3, 4) относительно  $x_1, x_2, x_3$ , а  $E$  есть  $(4 \times 11)$ -матрица,  $i$ -й столбец которой содержит на каждом месте  $i$ , то матрица<sup>1)</sup>

$$D = (E, A, A^*)$$

— матрица порядка  $4 \times 196$ , и можно проверить, что она является ОА (14, 4); следовательно,  $N(14) \geq 2$ .

Пример 2. Исходя из матрицы

$$P_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & x_1 & x_2 & x_3 \\ 3 & 6 & 2 & 1 & 0 & 0 & 0 \\ 8 & 20 & 12 & 16 & 20 & 17 & 8 \\ 12 & 16 & 7 & 2 & 19 & 6 & 21 \end{bmatrix}$$

с вычетами по модулю 23, мы можем, как в примере 1, построить некоторую матрицу и показать, что она является ОА (26, 4); следовательно,  $N(26) \geq 2$ .

Пример 3. Если взять вычеты по модулю 41 в качестве элементов, то можно построить схему с параметрами  $v = 41$ ,  $b = 82$ ,  $r = 10$ ,  $k = 5$ ,  $\lambda = 1$  и блоками

$$A_i = \{i, i + 1, i + 4, i + 11, i + 29\},$$

$$B_i = \{i + 1, i + 10, i + 16, i + 18, i + 37\},$$

$$i = 0, \dots, 40 \pmod{41}.$$

Мы можем проверить это, заметив, что два множества вычетов по модулю 41:  $\{0, 1, 4, 11, 29\}$  и  $\{1, 10, 16, 18, 37\}$ , имеют то свойство, что каждый ненулевой вычет  $d$  по модулю 41 можно представить в точности одним способом в виде

$$d \equiv x_i - x_j \pmod{41},$$

где  $x_i$  и  $x_j$  принадлежат или оба первому, или оба второму множеству. Если теперь  $u$  и  $v$  — два различных вычета по модулю 41, то определим  $x_i$  и  $x_j$  сравнением  $u - v \equiv x_i - x_j \pmod{41}$ . Полагая  $t \equiv u - x_i \pmod{41}$ ,

<sup>1)</sup>  $A = (A_0, A_1, \dots, A_{10})$ . — Прим. перев.

имеем

$$u \equiv x_i + t \pmod{41}, \quad v \equiv x_j + t \pmod{41},$$

и  $u$  и  $v$  находятся вместе либо в  $A_t$ , либо в  $B_t$ . Таким образом, каждая пара различных элементов появляется вместе в одном блоке, и так как имеется 82 блока, содержащих каждый по пять элементов, то этого достаточно, чтобы установить, что мы имеем схему с

$$b = 82, \quad v = 41, \quad k = 5, \quad r = 10, \quad \lambda = 1,$$

т. е. BIB (41, 5, 1). Применяя теорему 13.3.4, получаем

$$N(38) \geq \min(N(3), N(4) - 1, N(5) - 1) = 2,$$

т. е. существует пара ортогональных квадратов порядка 38.

Мы теперь в состоянии показать, что  $N(n) \geq 2$  для всех  $n = 4t + 2$  в пределах  $10 \leq 4t + 2 \leq 726$ . Три рассмотренных примера, теоремы 13.2.2, 13.3.1 и 13.3.8 и еще одно приложение теоремы 13.3.4 исчерпывают все случаи. В следующем ниже перечне вид, в котором представлено число, указывает, какая из теорем применяется. Так,  $50 = 5 \cdot 10$  означает, что по теореме 13.2.2

$$N(50) \geq \min(N(5), N(10)) \geq 2.$$

Аналогично  $34 \equiv 10 \pmod{12}$  означает, что применяется теорема 13.3.1 и  $N(34) \geq 2$ . Представление  $n = 4m + x$  означает, что применяется теорема 13.3.8 с  $k = 4$ . Для этого необходимо, чтобы  $N(m) \geq 3$  и  $1 \leq x < m$ , что легко проверяется в каждом случае.

$$10 \equiv 10 \pmod{12}.$$

$$50 = 5 \cdot 10.$$

$$14 \text{ Пример 1.}$$

$$54 = 3 \cdot 18.$$

$$18 = 21 - 3. \text{ [Теорема}$$

$$58 \equiv 10 \pmod{12}.$$

$$13.3.4 \text{ приме-}$$

$$62 = 4 \cdot 13 + 10.$$

$$\text{nется к BIB}$$

$$66 = 3 \cdot 22.$$

$$(21, 5, 1).]$$

$$70 \equiv 10 \pmod{12}.$$

$$22 \equiv 10 \pmod{12}.$$

$$74 = 4 \cdot 16 + 10.$$

$$26 \text{ Пример 2.}$$

$$78 = 3 \cdot 26.$$

$$30 = 3 \cdot 10.$$

$$82 \equiv 10 \pmod{12}.$$

$$34 \equiv 10 \pmod{12}.$$

$$86 = 4 \cdot 19 + 10.$$

$$38 \text{ Пример 3.}$$

$$90 = 4 \cdot 19 + 14.$$

$$42 = 3 \cdot 14.$$

$$94 = 4 \cdot 19 + 18.$$

$$46 \equiv 10 \pmod{12}.$$

$$98 = 7 \cdot 14.$$

Чтобы доказать, что  $N(n) \geq 2$  для значений  $n$ , больших 100, достаточно в каждом случае применить теорему 13.3.8 с  $k = 4$ ,  $n = 4m + x$ . В следующей ниже таблице для каждого данного  $m$   $x$  имеет вид  $4t + 2$  и может принимать значения из указанной области; это дает соответствующую область изменения  $n = 4m + x$ .

| $m$ | Значения $x$ | Значения $n = 4m + x$ |
|-----|--------------|-----------------------|
| 23  | 10—22        | 102—114               |
| 27  | 10—26        | 118—134               |
| 31  | 14—30        | 138—154               |
| 37  | 10—34        | 158—182               |
| 44  | 10—42        | 186—218               |
| 53  | 10—50        | 222—262               |
| 64  | 10—62        | 266—318               |
| 77  | 14—74        | 322—382               |
| 92  | 18—90        | 386—458               |
| 113 | 10—110       | 462—562               |
| 139 | 10—138       | 566—694               |
| 172 | 10—38        | 698—726               |

Нет оснований полагать, что найденные результаты близки к наилучшим. Например,  $N(12) \geq 2$  — это все, что мы доказали. Но непосредственным построением Дюльмаж, Джонсон и Мендельсон [1] нашли пять попарно ортогональных латинских квадратов порядка 12. Они исходили из абелевой группы порядка 12, являющейся прямым произведением циклических групп порядков 6 и 2. Пусть  $a$  и  $b$  с  $a^6 = 1$  и  $b^2 = 1$  — ее образующие элементы.

Обозначим

$$a_i = a^i, \quad i = 0, \dots, 5, \quad b_i = ba^i, \quad i = 0, \dots, 5.$$

Построим пять строк:

$$\begin{array}{ccccccccc} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & b_0 & b_1 & b_2 \\ a_0 & b_0 & b_2 & a_2 & b_1 & a_1 & b_3 & b_5 & a_4 \\ a_0 & a_3 & b_0 & a_1 & b_3 & b_5 & a_2 & b_2 & a_5 \\ a_0 & b_2 & a_1 & b_5 & a_5 & b_3 & a_3 & b_4 & a_1 \\ a_0 & a_4 & b_5 & b_4 & a_2 & b_1 & b_2 & b_0 & a_3 \end{array}$$

$$\begin{array}{ccccccccc} b_5 & b_3 & b_4 & b_1 & b_0 & b_2 & a_4 & a_5 & a_3 \\ a_5 & a_3 & a_1 & a_4 & a_2 & a_5 & b_1 & b_4 & b_0 \\ a_3 & a_1 & a_5 & a_2 & a_4 & a_0 & b_4 & b_0 & b_5 \\ a_1 & a_5 & a_3 & a_0 & a_2 & a_4 & b_1 & b_3 & b_2 \\ a_4 & a_2 & a_0 & a_5 & a_1 & a_3 & b_0 & b_5 & b_3 \end{array}$$

Возьмем эти строки в качестве первых строк пяти квадратов. Строки со второй по двенадцатую образуются умножением первых строк соответственно на  $a_1, \dots, a_5, b_0, \dots, b_5$ . Нет никакого другого квадрата порядка 12, ортогонального ко всем этим квадратам, и не было найдено никакого множества из шести попарно ортогональных квадратов порядка 12.

Следующая теорема доказана Човла, Эрдёшем и Страусом [1].

**Теорема 13.4.2.** *Существует число  $v_0$ , такое, что  $N(v) \geq \frac{1}{3} v^{1/91}$  для всех  $v > v_0$ .*

Доказательство основано на теореме 13.3.8 и на некоторых сложных арифметических соображениях.

# Матрицы Адамара

---

## 14.1. Конструкции Пэли

Матрицей Адамара порядка  $m$  называется  $(m \times m)$ -матрица  $H$ , элементами которой являются  $+1$  и  $-1$ , такая, что

$$HH^T = mI. \quad (14.1.1)$$

Это равенство эквивалентно утверждению, что любые две строки  $H$  ортогональны. Очевидно, что перестановка строк или столбцов  $H$ , равно как и умножение строк или столбцов  $H$  на  $-1$ , сохраняют это свойство. Будем считать  $H_1$  и  $H_2$  эквивалентными матрицами Адамара, если

$$H_2 = PH_1Q, \quad (14.1.2)$$

где  $P$  и  $Q$  – мономиальные матрицы перестановки с элементами  $+1$  и  $-1$ . Это означает, что  $P$  и  $Q$  имеют точно 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 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 нормализованности матрицы, но, вообще говоря, могут существовать эквивалентные нормализованные матрицы, которые не получаются одна из другой простой перестановкой строк и столбцов.

Будем называть матрицу Адамара сокращенно  *$H$ -матрицей*. Существуют  $H$ -матрицы порядков 1 и 2:

$$H_1 = [1], \quad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (14.1.3)$$

Пусть  $H$  есть нормализованная  $H$ -матрица порядка  $m > 2$ , тогда ее первая строка целиком состоит из единиц. Поэтому три строки  $H$  могут быть представлены в виде

$$\begin{array}{c|ccccc|ccccc} 1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 \\ 1 & \dots & 1 & 1 & \dots & 1 & -1 & \dots & -1 \\ 1 & \dots & 1 & -1 & \dots & -1 & 1 & \dots & 1 \end{array} \quad (14.1.4)$$

Пусть число столбцов каждого типа равно соответственно  $x, y, z, w$ . Тогда

$$\begin{aligned} x + y + z + w &= m, \\ x + y - z - w &= 0, \\ x - y + z - w &= 0, \\ x - y - z + w &= 0. \end{aligned} \quad (14.1.5)$$

В первом из этих уравнений учитывается общее число столбцов. Остальные три выражают соответственно ортогональность первых двух строк, первой и третьей строк, второй и третьей строк. Мы можем легко решить уравнения (14.1.5) и найти

$$x = y = z = w = \frac{m}{4}. \quad (14.1.6)$$

Отсюда заключаем, что если  $H$  — матрица Адамара порядка  $m > 2$ , то  $m$  кратно 4.

Из нормализованной  $H$ -матрицы порядка  $m = 4t$  мы можем построить симметричную блок-схему  $D$  с параметрами  $v = 4t - 1$ ,  $k = 2t - 1$ ,  $\lambda = t - 1$ , и, обратно, из такой схемы  $D$  мы можем построить нормализованную  $H$ -матрицу. Предположим сначала, что дана нормализованная  $H$ -матрица порядка  $4t$ . Пронумеруем строки и столбцы  $H$  числами  $0, 1, \dots, 4t - 1$  так, что строка и столбец с нулевым номером состоят целиком из +1. Остальным строкам сопоставим элементы  $a_i$ ,  $i = 1, \dots, 4t - 1$ , а остальным столбцам сопоставим блоки  $B_j$ ,  $j = 1, \dots, 4t - 1$ . Полагаем  $a_i \in B_j$ , если  $b_{ij} = +1$  в  $H$ , и  $a_i \notin B_j$ , если  $b_{ij} = -1$ .

Таким образом, мы построим систему инцидентности из  $v = 4t - 1$  элементов и  $v$  блоков с матрицей инцидентности

$$A = (a_{ij}), \quad i, j = 1, \dots, v,$$

где  $a_{ij} = +1$ , если  $b_{ij} = +1$ , и  $a_{ij} = 0$ , если  $b_{ij} = -1$ . В (14.1.4), (14.1.5) и (14.1.6) было показано, что в нормализованной матрице Адамара каждая строка, кроме нулевой, содержит  $2t$  положительных единиц, и две таких строки имеют  $t$  общих положительных единиц. После исключения нулевого столбца эти значения становятся равными  $2t - 1$  и  $t - 1$  соответственно. Таким образом,  $A$  удовлетворяет равенствам

$$AA^T = tI + (t - 1)J, \quad AJ = (2t - 1)J. \quad (14.1.7)$$

В силу теоремы 10.2.3 отсюда следует, что  $A$  удовлетворяет также равенствам

$$A^TA = tI + (t - 1)J, \quad JA = (2t - 1)J, \quad (14.1.8)$$

и потому  $A$ , будучи матрицей инцидентности, является матрицей инцидентности симметричной схемы  $D$  с  $v = 4t - 1$ ,  $k = 2t - 1$ ,  $\lambda = t - 1$ . Обратно, если дана симметричная схема  $D$  с  $v = 4t - 1$ ,  $k = 2t - 1$ ,  $\lambda = t - 1$ , то ее матрица инцидентности удовлетворяет (14.1.7) и (14.1.8). Мы построим теперь матрицу  $H = (b_{ij})$ ,  $i, j = 0, \dots, 4t - 1$ , полагая  $b_{0j} = b_{i0} = +1$  и для  $i, j = 1, \dots, 4t - 1$

$$b_{ij} = +1, \quad \text{если } a_{ij} = +1, \quad b_{ij} = -1, \quad \text{если } a_{ij} = 0.$$

Из того факта, что  $A$  удовлетворяет (14.1.7), следует теперь, что  $H$  удовлетворяет (14.1.1) и потому является матрицей Адамара.

Таким образом, построение нормализованной матрицы Адамара эквивалентно построению симметричной схемы с  $v = 4t - 1$ ,  $k = 2t - 1$ ,  $\lambda = t - 1$ . Но следует заметить, что неэквивалентные схемы могут давать эквивалентные матрицы, поскольку матрица Адамара может быть нормализована многими способами. Условие Брука — Райзера — Човла (теорема 10.3.1) для схем с указанными параметрами состоит в том, чтобы существовали решения в целых  $x, y, z$ , не равных одновременно нулю, уравнения

$$z^2 = tx^2 - (t - 1)y^2. \quad (14.1.9)$$

Очевидно, что  $x = y = z = 1$  есть решение, и, значит, можно предполагать, что матрица Адамара порядка  $t$

существует для каждого  $m$ , кратного 4. Так это или нет, остается нерешенной проблемой.

Можно строить матрицы Адамара из схем другим путем. Предположим, что  $H_m$  не нормализована и что +1 во всех столбцах определяют принадлежность элементов блокам. Тогда  $v = m = 4t$ , и мы должны иметь  $k$  положительных единиц и  $v - k$  отрицательных единиц в каждом столбце, а так же в каждой строке. Из условия

$$H_m H_m^T = H_m^T H_m = mI \quad (14.1.10)$$

следует, что скалярное произведение двух различных строк равно

$$\lambda - (k - \lambda) - (k - \lambda) + (v - 2k + \lambda) = 0, \quad (14.1.11)$$

где слагаемые равны числу столбцов вида  $\begin{pmatrix} +1 \\ +1 \end{pmatrix}$ ,  $\begin{pmatrix} +1 \\ -1 \end{pmatrix}$ ,  $\begin{pmatrix} -1 \\ +1 \end{pmatrix}$  и  $\begin{pmatrix} -1 \\ -1 \end{pmatrix}$  соответственно в этих двух строках. Поскольку  $v$  четно,  $k - \lambda$  должно быть квадратом (теорема 10.3.1). Таким образом, необходимо, чтобы выполнялись равенства

$$k - \lambda = u^2, \quad (14.1.12)$$

(14.1.11) и основное равенство

$$k(k - 1) = \lambda(v - 1). \quad (14.1.13)$$

Из этих соотношений, взяв, если это необходимо,  $-H_m$  вместо  $H_m$ , чтобы  $k$  было меньше половины  $v$ , имеем

$$v = 4u^2, \quad k = 2u^2 - u, \quad \lambda = u^2 - u. \quad (14.1.14)$$

Такие схемы существуют; пример при  $v = 16$ ,  $k = 6$ ,  $\lambda = 2$  был построен в начале разд. 11.4. Рассмотрим элементарную абелеву группу  $A$  порядка 16 с образующими элементами  $a, b, c, d$  порядка 2 и групповое разностное множество  $a, b, c, d, ab, cd$ . Если мы выпишем элементы группы  $A$  в следующем порядке: 1,  $a, b, c, d, ab, ac, ad, bc, bd, cd, abc, abd, acd, bcd, abcd$ , пронумеровав их от 1 до 16, то блок-схема, соответствующая

положительным единицам, имеет вид

$$\begin{array}{ll}
 B_1: 2, 3, 4, 5, 6, 11; & B_9: 3, 4, 7, 10, 12, 15; \\
 B_2: 1, 3, 6, 7, 8, 14; & B_{10}: 3, 5, 8, 9, 13, 15; \\
 B_3: 1, 2, 6, 9, 10, 15; & B_{11}: 1, 4, 5, 14, 15, 16; \\
 B_4: 1, 5, 7, 9, 11, 12; & B_{12}: 4, 6, 7, 9, 13, 16; \\
 B_5: 1, 4, 8, 10, 11, 13; & B_{13}: 5, 6, 8, 10, 12, 16; \\
 B_6: 1, 2, 3, 12, 13, 16; & B_{14}: 2, 7, 8, 11, 15, 16; \\
 B_7: 2, 4, 8, 9, 12, 14; & B_{15}: 3, 9, 10, 11, 14, 16; \\
 B_8: 2, 5, 7, 10, 13, 14; & B_{16}: 6, 11, 12, 13, 14, 15. \\
 \end{array} \tag{14.1.15}$$

Соответствующая  $H$ -матрица симметрична, так как  $i \in B_j$ , тогда и только тогда, когда  $j \in B_i$ .

Существует несколько методов для построения матриц Адамара. Можно построить матрицы Адамара следующих порядков  $N$  (в приводимом перечне  $p$  — нечетное простое число):

- I.  $N = 2^r$ .
- II.  $N = p^r + 1 \equiv 0 \pmod{4}$ .
- III.  $N = h(p^r + 1)$ , где  $h \geq 2$  — порядок матрицы Адамара.
- IV.  $N = h(h - 1)$ , где  $h$  — произведение чисел вида I и II.
- V.  $N = 92, 116, 172$ .
- VI.  $N = h(h + 3)$ , где  $h$  и  $h + 4$  — произведения чисел вида I и II.
- VII.  $N = h_1 h_2 (p^r + 1) p^r$ , где  $h_1 > 1$  и  $h_2 > 1$  — порядки матриц Адамара.
- VIII.  $N = h_1 h_2 s(s + 3)$ , где  $h_1 > 1$ ,  $h_2 > 1$  — порядки матриц Адамара, а  $s$  и  $s + 4$  имеют вид  $p^r + 1$ .
- IX.  $N = q(q + 2) + 1$ , где  $q$  и  $q + 2$  — степени простых чисел.
- X.  $N$  — произведение чисел вида I — IX.

В разделе 11.6 разностные множества типа Q дают тип II, разностные множества типа  $H_6$  существуют лишь для таких значений параметров, для которых существуют Q, и также дают тип II, а разностные множества Т дают тип IX. Остальные случаи в том виде, как они представлены здесь, изучены Уильямсоном [1], [2],

который обобщил ранее известные методы, главным образом методы Пэли [1].

Эти построения используют прямое (или кронекерово) произведение двух матриц. Если  $A = (a_{ij})$  есть  $(m \times m)$ -матрица и  $B = (b_{rs})$  есть  $(n \times n)$ -матрица, то прямым произведением  $A \times B$  называется  $(mn \times mn)$ -матрица:

$$A \times B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1}B & a_{i2}B & \dots & a_{im}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mm}B \end{bmatrix}. \quad (14.1.16)$$

Легко видеть, что

$$A \times B = (A \times I_n)(I_m \times B) = (I_m \times B)(A \times I_n). \quad (14.1.17)$$

Очевидно, что  $(A \times B) \times C = A \times (B \times C)$  во всех случаях. Матрицу  $B \times A$  можно получить из  $A \times B$  подходящей перестановкой строк и столбцов. Прямое произведение обладает полезными свойствами:

$$\begin{aligned} a(A \times B) &= (aA) \times B = A \times (aB), \quad a - \text{скаляр}, \\ (A_1 + A_2) \times B &= A_1 \times B + A_2 \times B, \\ A \times (B_1 + B_2) &= A \times B_1 + A \times B_2, \\ (A \times B)(C \times D) &= AC \times BD, \\ (A \times B)^T &= A^T \times B^T. \end{aligned} \quad (14.1.18)$$

Здесь  $A, A_1, A_2, C - (m \times m)$ -матрицы, а  $B, B_1, B_2, D - (n \times n)$ -матрицы.

**Теорема 14.1.1.** *Если существуют  $H$ -матрицы порядков  $m$  и  $n$ , то их прямое произведение есть  $H$ -матрица порядка  $mn$ .*

**Доказательство.** Пусть  $H_m$  и  $H_n$  — две  $H$ -матрицы порядков  $m$  и  $n$  соответственно. Тогда

$$\begin{aligned} (H_m \times H_n)(H_m \times H_n)^T &= (H_m \times H_n)(H_m^T \times H_n^T) = \\ &= H_m H_m^T \times H_n H_n^T = m I_m \times n I_n = mn I_{mn}. \end{aligned} \quad (14.1.19)$$

Для некоторых методов требуется  $H$ -матрицы с дополнительными специальными свойствами. Мы начнем с некоторого построения, основанного на свойствах конечных полей  $GF(p^r)$ , где  $p$  — нечетное простое число. Пусть  $\chi(x)$  — характер, определенный на  $F = GF(p^r)$ :

$$\chi(0) = 0, \quad \chi(x) = +1,$$

если  $x$  — квадрат, и  $\chi(x) = -1$ , если  $x$  — не квадрат. Тогда из свойств конечного поля  $\chi(xy) = \chi(x)\chi(y)$  для всех  $x, y$ .

**Лемма 14.1.1.**  $\sum_b \chi(b)\chi(b+c) = -1$ , если  $c \neq 0$ .

**Доказательство.** Ясно, что  $\chi(0)\chi(0+c) = 0$ . Для  $b \neq 0$  существует единственный  $z \neq 0$ , такой, что  $b+c = bz$ . Если  $b$  пробегает все ненулевые элементы  $F$ , то  $z$  пробегает все элементы  $F$ , исключая 1. (При  $b = -c$  имеем  $z = 0$ .) Следовательно,

$$\begin{aligned} \sum_b \chi(b)\chi(b+c) &= \sum_{b \neq 0} \chi(b)\chi(b+c) = \\ &= \sum_{b \neq 0} \chi(b)^2 \chi(z) = \sum_{z \neq 1} \chi(z) = \\ &= \sum_z \chi(z) - \chi(1) = 0 - 1 = -1. \end{aligned} \quad (14.1.20)$$

Для  $q = p^r$  пусть  $a_0 = 0, a_1, \dots, a_{q-1}$  — элементы поля  $F$ , пронумерованные так, что  $a_0 = 0, a_{q-i} = -a_i, i = 1, \dots, q-1$ . Полагаем теперь

$$Q = (q_{ij}), \quad q_{ij} = \chi(a_i - a_j). \quad (14.1.21)$$

Тогда

$$q_{ji} = \chi(a_j - a_i) = \chi(-1)\chi(a_i - a_j),$$

и так как  $-1$  есть квадрат, если  $q \equiv 1 \pmod{4}$ , и не квадрат, если  $q \equiv 3 \pmod{4}$ , получаем, что  $Q$  — симметрическая матрица, если  $q \equiv 1 \pmod{4}$ , и кососимметрическая матрица, если  $q \equiv 3 \pmod{4}$ .

**Лемма 14.1.2.**  $QQ^T = qI_q - J$ ,  $QJ = JQ = 0$ , где  $J$  (как обычно) — матрица, целиком состоящая из единиц.

Если  $QQ^T = B = (b_{ij})$ , то

$$\begin{aligned} b_{ii} &= \sum_t \chi(a_i - a_t) \chi(a_i - a_t) = \\ &= \begin{cases} q-1, & \text{если } i=j, \\ -1, & \text{если } i \neq j. \end{cases} \quad (14.1.22) \end{aligned}$$

Последнее соотношение получается из леммы 14.1.1 при  $b = a_i - a_t$ ,  $c = a_i - a_i$ . Эти соотношения доказывают первую часть леммы 14.1.2. Соотношения  $QJ = JQ = 0$  следуют из того, что  $\sum_z \chi(z) = 0$ . Пусть  $e = e_q = (1, \dots, 1)$  есть  $q$ -мерный вектор из единиц. Тогда если  $q = p^r \equiv -1 \pmod{4}$ , то матрица

$$S = \begin{bmatrix} 0 & e \\ -e^T & Q \end{bmatrix} \quad (14.1.23)$$

обладает свойствами

$$S^T = -S, \quad SS^T = qI_{q+1}. \quad (14.1.24)$$

Поэтому матрица

$$H_{q+1} = (I_{q+1} + S) \quad (14.1.25)$$

есть  $H$ -матрица порядка  $q+1$ , так как каждый элемент в  $H$  равен  $\pm 1$  и

$$\begin{aligned} HH^T &= (I + S)(I + S^T) = I + S + S^T + SS^T = \\ &= I + qI = (q+1)I. \quad (14.1.26) \end{aligned}$$

Скажем, что  $H$ -матрица есть матрица *кососимметрического типа*, если она имеет вид

$$H_m = I_m + S_m, \quad S_m^T = -S_m. \quad (14.1.27)$$

Уильямсон [1] называет такую  $H$ -матрицу матрицей „типа I“. Ей доказана следующая полезная лемма.

**Лемма 14.1.3.** Пусть  $S$  — матрица порядка  $n$ , такая, что  $S^T = \varepsilon S$ ,  $\varepsilon = \pm 1$ ,  $SST = (n-1)I_n$ . Пусть далее  $A$  и  $B$  — матрицы порядка  $m$ , удовлетворяющие условиям

$$AA^T = BB^T = mI_m \quad \text{и} \quad AB^T = -\varepsilon BA^T.$$

Тогда матрица  $K = A \times I_n + B \times S$  удовлетворяет условию  $KK^T = mnI_{mn}$ .

**Доказательство.** Вычислим

$$\begin{aligned}
 KK^T &= (A \times I_n + B \times S)(A^T \times I_n + B^T \times S^T) = \\
 &= AA^T \times I_n + AB^T \times S^T + BA^T \times S + BB^T \times SS^T = \\
 &= mI_m \times I_n + (-\epsilon BA^T) \times (\epsilon S) + BA^T \times S + \\
 &\quad + mI_m \times (n-1)I_n = \\
 &= mI_{mn} + m(n-1)I_{mn} = mnI_{mn}.
 \end{aligned} \tag{14.1.28}$$

Если  $q = p' \equiv 1 \pmod{4}$ , то при  $n = q+1$  рассмотрим матрицу

$$S_n = \begin{bmatrix} 0 & e \\ e^T & Q \end{bmatrix}, \quad e = e_{n-1}, \tag{14.1.29}$$

где матрица  $Q$  берется из (14.1.21) и является симметрической. В силу леммы 14.1.2 матрица  $S_n$  удовлетворяет соотношениям

$$S_n^T = S_n, \quad S_n S_n^T = (n-1)I_n. \tag{14.1.30}$$

Пусть теперь  $A$  есть любая  $H$ -матрица порядка  $m > 1$ . Здесь  $m$  четно, и мы можем построить матрицу  $U_m$ , которая имеет  $m/2$  матриц  $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$  вдоль главной диагонали, или

$$U_m = I_{m/2} \times \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{14.1.31}$$

Определим теперь  $B$  равенством

$$B = U_m A. \tag{14.1.32}$$

Тогда находим

$$\begin{aligned}
 BB^T &= U_m A A^T U_m^T = U_m m I_m U_m^T = m I_m, \\
 AB^T &= A A^T U_m^T = m I_m U_m^T = -m U_m, \\
 BA^T &= U_m A A^T = U_m (m I_m) = m U_m.
 \end{aligned} \tag{14.1.33}$$

Таким образом, матрица  $S_n$ , определенная соотношением (14.1.29), и матрицы  $A$  и  $B$  удовлетворяют условиям леммы 14.1.3. Заметим, что  $S_n$  имеет 0 на главной диагонали и  $\pm 1$  на остальных местах. Следовательно, матрица  $K$  из леммы имеет на всех местах  $\pm 1$  и

является  $H$ -матрицей порядка  $tn$ . Сформулируем доказанное в виде теоремы.

**Теорема 14.1.2.** *Если  $p' \equiv 1 \pmod{4}$ ,  $p$  простое, и  $h > 1$  — порядок некоторой  $H$ -матрицы, то существует  $H$ -матрица порядка  $h(p' + 1)$ .*

В результате мы получили случай III из приведенного выше перечня для порядков  $N$ , так как если  $p' \equiv -1 \pmod{4}$ , то существует  $H$ -матрица порядка  $p' + 1$  и можно применить теорему 14.1.1. Эта теорема Уильямсона (теорема 14.1.2) обобщает результат Пэли [1], доказавшего, что существует  $H$ -матрица порядка  $2(p' + 1)$ , если  $p' \equiv 1 \pmod{4}$ . Построение Пэли эквивалентно образованию

$$H_{2n} = S_n \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} + I_n \times \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}, \quad (14.1.34)$$

где  $S_n$  берется из (14.1.29). Из (14.1.30) легко следует, что  $H_{2n}$  — симметрическая  $H$ -матрица.

**Лемма 14.1.4.** *Если  $n$  имеет вид  $n = 2^t k_1 \dots k_s$ , где либо  $k_i = p_i^{r_i} + 1 \equiv 0 \pmod{4}$ , либо  $k_i = 2(p_i^{u_i} + 1)$ ,  $p_i^{u_i} \equiv 1 \pmod{4}$ , то существует симметрическая  $H$ -матрица порядка  $n$ .*

**Доказательство.** Прямое произведение симметрических  $H$ -матриц есть симметрическая  $H$ -матрица. Существует симметрическая  $H$ -матрица порядка 2, а в (14.1.34) мы имеем симметрическую  $H$ -матрицу порядка  $2(p' + 1)$ , где  $p' \equiv 1 \pmod{4}$ . Остается показать, что если  $n = p' + 1 \equiv 0 \pmod{4}$ , то существует симметрическая  $H$ -матрица порядка  $n$ . Существует  $H$ -матрица  $A$  порядка  $n$  кососимметрического типа (см. (14.1.25)):

$$A = I_n + S = I_n + \begin{bmatrix} 0 & e \\ -e^T & Q \end{bmatrix}. \quad (14.1.35)$$

Пусть  $U$  — матрица порядка  $n - 1 = p' = q$ , где

$$\begin{aligned} U &= (u_{ij}), \quad i, j = 0, \dots, q - 1, \\ u_{00} &= 1, \\ u_{i, q-i} &= 1, \quad i = 1, \dots, q - 1, \\ u_{ij} &= 0 \text{ в остальных случаях.} \end{aligned} \quad (14.1.36)$$

Определим теперь матрицу  $B$  равенством

$$B = \begin{bmatrix} -1 & 0 \\ 0 & U \end{bmatrix} A = \begin{bmatrix} -1 & 0 \\ 0 & U \end{bmatrix} + \begin{bmatrix} 0 & -e \\ -e^T & UQ \end{bmatrix}. \quad (14.1.37)$$

Так как

$$Q = (b_{ij}), \quad i, j = 0, \dots, q-1, \quad \text{и} \quad b_{ij} = \chi(a_i - a_j),$$

то, полагая  $UQ = (c_{ij})$ , имеем  $c_{0j} = \chi(0 - a_j)$  и

$$c_{ij} = \chi(a_{q-i} - a_j) = \chi(-a_i - a_j), \quad i = 1, \dots, q-1.$$

Отсюда во всех случаях  $c_{ij} = \chi(-a_i - a_j)$ , поэтому  $UQ$  — симметрическая и  $B$  — также симметрическая матрица:

$$B^T = B. \quad (14.1.38)$$

Замечая, далее, что  $U$  симметрична и  $U^2 = I$ , мы получаем

$$BB^T = \begin{bmatrix} -1 & 0 \\ 0 & U \end{bmatrix} AA^T \begin{bmatrix} -1 & 0 \\ 0 & U \end{bmatrix} = nI_n. \quad (14.1.39)$$

Матрица  $B$  — симметрическая  $H$ -матрица порядка  $n = p' + 1$ , и лемма доказана.

**Лемма 14.1.5.** *Если существует  $H$ -матрица порядка  $n$  кососимметрического типа и если  $p' + 1 \equiv 0 \pmod{4}$ ,  $p$  — простое, то существует  $H$ -матрица порядка  $n(p' + 1)$  кососимметрического типа.*

**Доказательство.** По предположению  $H_n = I_n + S$ , где  $S^T = -S$ , и

$$H_n H_n^T = (I_n + S)(I_n - S) = nI_n, \quad (14.1.40)$$

откуда

$$SS^T = -S^2 = (n-1)I_n. \quad (14.1.41)$$

Если  $A$  и  $B$  определены формулами (14.1.35) и (14.1.37) соответственно, то при  $m = p' + 1$  имеем

$$AA^T = BB^T = mI_m,$$

$$AB^T = mI_m \begin{bmatrix} -1 & 0 \\ 0 & U \end{bmatrix} = BA^T. \quad (14.1.42)$$

Таким образом,  $A$ ,  $B$ ,  $S$  удовлетворяют требованиям леммы 14.1.3 с  $\epsilon = +1$ . Следовательно,

$$K = A \times I_n + B \times S \quad (14.1.43)$$

есть  $H$ -матрица порядка  $mn$ , и поскольку  $A = I_m + C$ , где  $C = \begin{bmatrix} 0 & e \\ -e^T & Q \end{bmatrix}$  и  $C^T = -C$ , мы имеем

$$\begin{aligned} (K - I_{mn})^T &= (C \times I_n + B \times S)^T = \\ &= (-C) \times I_n + B \times (-S) = -(K - I_{mn}). \end{aligned} \quad (14.1.44)$$

Таким образом,  $K$  есть матрица кососимметрического типа, и наша лемма доказана.

**Лемма 14.1.6.** *Существует  $H$ -матрица кососимметрического типа порядка  $n$ , где  $n = 2^t k_1 \dots k_s$  и каждое  $k_i$  имеет вид  $p^r + 1 \equiv 0 \pmod{4}$ .*

Матрица  $H_{q+1}$  из (14.1.25) порядка  $q+1 = p^r + 1 \equiv 0 \pmod{4}$  удовлетворяет условиям леммы. Кроме того, если  $H$  кососимметрического типа и порядка  $n$  (включая матрицу [!] порядка 1), то

$$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \times H$$

есть снова  $H$ -матрица кососимметрического типа порядка  $2n$ . Вместе с леммой 14.1.5 это позволяет получить все значения  $n$  в лемме.

**Теорема 14.1.3.** *Если существует  $H$ -матрица кососимметрического типа порядка  $n$ , то существует  $H$ -матрица порядка  $n(n-1)$ .*

**Доказательство.** Пусть  $H = (b_{ij})$ ,  $i, j = 1, \dots, n$ . Так как  $H$  кососимметрического типа,  $b_{ii} = +1$ ,  $i = 1, \dots, n$ . Если мы умножим  $r$ -ю строку и  $r$ -й столбец на  $-1$ , то кососимметричность сохранится. Следовательно, мы можем положить  $b_{1j} = +1$ ,  $j = 2, \dots, n$ , без ограничения общности. Таким образом,

$$H = I_n + S, \quad S^T = -S,$$

$$H = \begin{bmatrix} 1 & e \\ -e^T & D \end{bmatrix}. \quad (14.1.45)$$

Так как  $HH^T = nI_n$ , мы имеем

$$SS^T = (n-1)I_n, \quad (14.1.46)$$

а также

$$\begin{aligned} DD^T &= nI_{n-1} - J_{n-1}, \quad (D - I_{n-1})^T = -(D - I_{n-1}), \\ eD^T &= e, \quad De^T = e^T, \quad e^Te = J_{n-1}, \\ J_{n-1}D^T &= e^T(eD^T) = e^Te = J_{n-1}. \end{aligned} \quad (14.1.47)$$

Если мы положим

$$K = J_{n-1} \times I_n + D \times S, \quad (14.1.48)$$

то получим

$$\begin{aligned} KK^T &= (J_{n-1} \times I_n + D \times S)(J_{n-1}^T \times I_n + D^T \times S^T) = \\ &= J_{n-1}^2 \times I_n + J_{n-1}D^T \times (-S) + J_{n-1}D \times S + \\ &\quad + (nI_{n-1} - J_{n-1}) \times ((n-1)I_n) = \\ &= (n-1)J_{n-1} \times I_n + J_{n-1} \times (-S) + J_{n-1}(2I_{n-1} - D^T) \times S + \\ &\quad + n(n-1)I_{n-1} \times I_n - (n-1)J_{n-1} \times I_n = \\ &= -J_{n-1} \times S + (2J_{n-1} - J_{n-1}) \times S + n(n-1)I_{n-1} \times I_n = \\ &= n(n-1)I_{n(n-1)}. \end{aligned} \quad (14.1.49)$$

Значит,  $K$  есть  $H$ -матрица порядка  $n(n-1)$ , что и требовалось доказать. Эта теорема Уильямсона обобщает результат Скарписа [1], который показал для  $p \equiv 3 \pmod{4}$  существование  $H$ -матрицы порядка  $p(p+1)$ . Вместе с леммой 14.1.6 теорема 14.1.3 дает случай IV.

**Теорема 14.1.4.** *Если существует  $H$ -матрица порядка  $n$  кососимметрического типа и симметрическая  $H$ -матрица порядка  $m = n+4$ , то существует  $H$ -матрица порядка  $n(n+3)$ .*

**Доказательство.** Пусть  $H_m$  — симметрическая матрица,  $H_n$  — матрица кососимметрического типа. Тогда, заменяя, если это необходимо,  $H_m$  на  $-H_m$  и умножая, если это необходимо, строку и столбец с одинаковым номером на  $-1$ , получаем

$$H_m = \begin{bmatrix} 1 & e \\ e^T & D \end{bmatrix}, \quad e = e_{m-1}, \quad H_n = I_n + S_n. \quad (14.1.50)$$

Поскольку  $mI_m = H_m H_m^T = H_m^2$ , имеем

$$\begin{bmatrix} m & e + eD \\ e^T + De^T & e^T e + D^2 \end{bmatrix} = \begin{bmatrix} m & 0 \\ 0 & mI_{m-1} \end{bmatrix} \quad (14.1.51)$$

и

$$D^T = D, \quad eD = -e, \quad De^T = -e^T, \quad D^2 = mI_{m-1} - J_{m-1}. \quad (14.1.52)$$

Так как  $e^T e = J_{m-1}$ , находим, что

$$J_{m-1} D = -J_{m-1} = DJ_{m-1}. \quad (14.1.53)$$

Положим теперь  $F_{m-1} = 2I_{m-1} - J_{m-1}$ . Тогда

$$F_{m-1} D = DF_{m-1}, \quad F_{m-1}^2 = 4I_{m-1} + (m-5)J_{m-1}. \quad (14.1.54)$$

Поскольку  $H_n$  кососимметрического типа,

$$S_n^T = -S_n, \quad S_n S_n^T = (n-1)I_n. \quad (14.1.55)$$

Определим теперь  $W$  равенством

$$W = F_{m-1} \times I_n + D \times S_n \quad (14.1.56)$$

и заметим, что каждый элемент  $W$  равен  $\pm 1$ . Тогда

$$\begin{aligned} WW^T &= (F_{m-1} \times I_n + D \times S_n)(F_{m-1} \times I_n - D \times S_n) = \\ &= F_{m-1}^2 \times I_n - D^2 \times S_n^2 = (4I_{m-1} + (m-5)J_{m-1}) \times I_n + \\ &\quad + (mI_{m-1} - J_{m-1}) \times ((n-1)I_n) = \\ &= (mn - m + 4)I_{m-1} \times I_n + (m-n-4)J_{m-1} \times I_n. \end{aligned} \quad (14.1.57)$$

Следовательно, при  $m = n + 4$   $W$  есть  $H$ -матрица порядка  $n(n+3)$ , и наша теорема доказана. Эта теорема вместе с леммами 14.1.4 и 14.1.6 даёт случай VI и даже несколько более сильное утверждение.

**Лемма 14.1.7.** *Если существует  $H$ -матрица  $A$  порядка  $n > 1$ , то существуют две  $H$ -матрицы  $B$  и  $C$  порядка  $n$ , такие, что*

$$AB^T = -BA^T, \quad AC^T = CA^T, \quad BC^T = CB^T.$$

**Доказательство.** По условию  $n$  четно,  $n = 2m$ . Полагаем

$$X = I_m \times \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad Y = I_m \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (14.1.58)$$

и проверяем непосредственно, что  $B = XA$ ,  $C = YA$  удовлетворяют условиям леммы.

Допустим теперь, что  $p' \equiv 1 \pmod{4}$ ,  $p$  простое, и обозначим  $m = p' + 1$ . Тогда  $Q$  из (14.1.21) — симметрическая матрица, и в силу леммы 14.1.2

$$QQ^T = Q^2 = (m-1)I_{m-1} - J_{m-1}, \quad QJ_{m-1} = J_{m-1}Q = 0. \quad (14.1.59)$$

Пусть  $A_1$  и  $B_1$  — две  $H$ -матрицы порядка  $n$ , как в лемме 14.1.7, так что

$$A_1B_1^T = -B_1A_1^T. \quad (14.1.60)$$

Определим матрицу  $K$  порядка  $(m-1)n_1$  соотношением

$$K = A_1 \times I_{m-1} + B_1 \times Q. \quad (14.1.61)$$

Тогда всякий элемент из  $K$  равен  $\pm 1$  и

$$\begin{aligned} KK^T &= A_1A_1^T \times I_{m-1} + B_1B_1^T \times Q^2 = \\ &= n_1I_{n_1} \times (mI_{m-1} - J_{m-1}). \end{aligned} \quad (14.1.62)$$

Если  $M = A_1 \times J_{m-1}$ , то

$$MM^T = n_1I_{n_1} \times (m-1)J_{m-1}. \quad (14.1.63)$$

Пусть теперь  $A_2$  и  $B_2$  —  $H$ -матрицы порядка  $n_2$ , удовлетворяющие условию

$$A_2B_2^T = -B_2A_2^T. \quad (14.1.64)$$

Определим  $W$  соотношением

$$W = (A_2 \times M) \times I_m + (B_2 \times K) \times S, \quad (14.1.65)$$

где

$$S = \begin{bmatrix} 0 & e \\ e^T & Q \end{bmatrix}, \quad S^2 = (m-1)I_m. \quad (14.1.66)$$

Тогда

$$\begin{aligned} WW^T &= (A_2A_2^T \times MM^T) \times I_m + (B_2B_2^T \times KK^T) \times S^2 = \\ &= [n_2I_{n_2} \times (n_1I_{n_1} \times (m-1)J_{m-1}) + \\ &\quad + (m-1)n_2I_{n_2} \times (n_1I_{n_1} \times (mI_{m-1} - J_{m-1}))] \times I_m = \\ &= [n_2I_{n_2} \times n_1I_{n_1} \times ((m-1)J_{m-1} + (m-1)mI_{m-1} - \\ &\quad - (m-1)J_{m-1})] \times I_m = NI_N, \end{aligned} \quad (14.1.67)$$

где  $N = n_1n_2m(m-1)$ .

Мы доказали следующую теорему.

**Теорема 14.1.5.** *Если существуют  $H$ -матрицы порядков  $n_1$  и  $n_2$ ,  $n_1 > 1$ ,  $n_2 > 1$ , и  $p$  — простое число, такое, что  $p^r \equiv 1 \pmod{4}$ , то существует  $H$ -матрица порядка  $n_1 n_2 (p^r + 1) p^r$ .*

Если  $p^r \equiv 3 \pmod{4}$ , то существует  $H$ -матрица порядка  $(p^r + 1) p^r$  (случай (IV)). Этим замечанием вместе с доказанной теоремой устанавливается случай VII.

Доказательство случая VIII почти аналогично доказательству случая VII. Пусть  $A_1, B_1, C_1$  —  $H$ -матрицы порядка  $n_1$ , удовлетворяющие соотношениям леммы 14.1.7, и  $A_2, B_2, C_2$  — аналогичные матрицы порядка  $n_2$  ( $C_2$  нам не понадобится).

Полагаем

$$\begin{aligned} U &= C_1 \times (2I_{m-1} - J_{m-1}), \\ V &= A_1 \times I_{m-1} + B_1 \times Q_1, \end{aligned} \quad (14.1.68)$$

где  $Q_1$  совпадает с матрицей  $Q$  порядка  $m-1 = p_1^r$ ,  $p_1$  простое,  $p_1^r \equiv 1 \pmod{4}$  в (14.1.59). Аналогично пусть  $S_n$  — матрица из (14.1.29) порядка  $n = p_2^s + 1$ ,  $p_2$  простое,  $p_2^s \equiv 1 \pmod{4}$ . Наконец, положим

$$W = (A_2 \times U) \times I_n + (B_2 \times V) \times S_n. \quad (14.1.69)$$

Тогда

$$\begin{aligned} UU^T &= n_1 I_{n_1} \times (4I_{m-1} + (m-5)J_{m-1}), \\ VV^T &= n_1 I_{n_1} \times (mI_{m-1} - J_{m-1}), \\ UV^T &= C_1 A_1^T \times (2I_{m-1} - J_{m-1}) + C_1 B_1^T \times 2Q_1. \end{aligned} \quad (14.1.70)$$

Так как  $A_1, B_1, C_1$  удовлетворяют условиям леммы 14.1.7, то  $UV^T$  — симметрическая матрица,

$$UV^T = VU^T. \quad (14.1.71)$$

Следовательно,

$$\begin{aligned} WW^T &= n_2 I_{n_2} \times (UU^T \times I_n + VV^T \times S_n^2) = \\ &= n_1 n_2 I_{n_1 n_2} \times [(4I_{m-1} + (m-5)J_{m-1}) \times I_n + \\ &\quad + (mI_{m-1} - J_{m-1}) \times (n-1)I_n] = \\ &= n_1 n_2 I_{n_1 n_2} \times [(4 + mn - m)I_{m-1} + (m-4-n)J_{m-1}] \times I_n. \end{aligned} \quad (14.1.72)$$

Поэтому при  $m = n + 4$

$$WW^T = NI_N, \quad N = n_1 n_2 n(n+3), \quad (14.1.73)$$

и  $W$  есть  $N$ -матрица порядка  $N$ . Тем самым доказана

**Теорема 14.1.6.** *Если  $n$  и  $n + 4$  — числа вида  $p^r + 1$ ,  $p$  простое, и  $n_1 > 1$ ,  $n_2 > 1$  — порядки  $H$ -матриц, то существует  $H$ -матрица порядка  $n_1 n_2 n(n+3)$ .*

Заметим, что если  $n \equiv 0 \pmod{4}$ , то эта теорема является следствием случая VI. Предыдущее доказательство охватывает значения  $n \equiv 2 \pmod{4}$ . Тем самым случай VIII доказан.

## 14.2. Метод Уильямсона

Уильямсону принадлежит также и другой метод для построения  $H$ -матриц. Этот метод был с успехом применен в ряде случаев, в частности для порядков 92, 116 и 172 случая V.

Рассмотрим матрицу

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}. \quad (14.2.1)$$

Если  $A, B, C, D$  — числа, то

$$HH^T = (A^2 + B^2 + C^2 + D^2) \times I_4. \quad (14.2.2)$$

При некоторых условиях равенство (14.2.2) справедливо, если  $A, B, C, D$  — матрицы порядка  $n$ . Для этого достаточно, чтобы  $A, B, C, D$  были симметричны и перестановочны друг с другом. Будем предполагать, что это имеет место.

Пусть  $U$  — матрица порядка  $n$ , соответствующая циклической перестановке порядка  $n$ :

$$U = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}, \quad U^n = I. \quad (14.2.3)$$

Если  $A, B, C, D$  — полиномы относительно  $U$ , то они перестановочны друг с другом. Полагаем

$$\begin{aligned} A &= a_0I + a_1U + \dots + a_{n-1}U^{n-1}, \\ B &= b_0I + b_1U + \dots + b_{n-1}U^{n-1}, \\ C &= c_0I + c_1U + \dots + c_{n-1}U^{n-1}, \\ D &= d_0I + d_1U + \dots + d_{n-1}U^{n-1}. \end{aligned} \quad (14.2.4)$$

Так как  $U^T = U^{-1}$ , матрицы  $A, B, C, D$  будут симметрическими, если

$$\begin{aligned} a_{n-i} &= a_i, \quad b_{n-i} = b_i, \quad c_{n-i} = c_i, \quad d_{n-i} = d_i, \\ i &= 1, \dots, n-1. \end{aligned} \quad (14.2.5)$$

Если каждый из коэффициентов  $a, b, c, d$  равен  $\pm 1$ , то элементы  $H$  равны  $\pm 1$  и

$$HH^T = 4nI_{4n}, \quad (14.2.6)$$

если

$$A^2 + B^2 + C^2 + D^2 = 4nI_n. \quad (14.2.7)$$

Таким образом,  $H$  из (14.2.1) при выполнении (14.2.7) будет  $H$ -матрицей порядка  $4n$ , если  $A, B, C, D$  имеют вид (14.2.4) с коэффициентами  $\pm 1$ , подчиненными условиям (14.2.5). Например, если  $n = 3$ , мы можем взять

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad B = C = D = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}. \quad (14.2.8)$$

Из (14.2.8)

$$A^2 + B^2 + C^2 + D^2 = 12I_3, \quad (14.2.9)$$

и матрица  $H$  вида (14.2.1) есть  $H$ -матрица порядка 12.

В дальнейшем будем считать  $n$  нечетным и, если это необходимо, менять знаки у  $A, B, C, D$  так, чтобы

$$a_0 = b_0 = c_0 = d_0 = +1. \quad (14.2.10)$$

Можно рассматривать (14.2.4) и (14.2.7) как соотношения между элементами группового кольца  $R(G)$  над целыми числами, где  $G$  — циклическая группа с элемен-

тами  $1, u, \dots, u^{n-1}, u^n = 1$ ;  $u$  соответствует  $U$ . Таким образом,

$$A = a_0 + a_1 u + \dots + a_{n-1} u^{n-1}, \quad (14.2.11)$$

и аналогично запишем  $B, C$  и  $D$ . Полагаем

$$A = P_1 - N_1, \quad (14.2.12)$$

где  $P_1$  — сумма положительных членов в  $A$ , а  $-N_1$  — сумма отрицательных членов в  $A$ :

$$P_1 = \sum_j a_j u^j, \quad a_j = +1, \quad -N_1 = \sum_j a_j u^j, \quad a_j = -1. \quad (14.2.13)$$

Запишем также

$$B = P_2 - N_2, \quad C = P_3 - N_3, \quad D = P_4 - N_4. \quad (14.2.14)$$

Так как  $a_0 = +1$  и в силу (14.2.5)  $a_{n-i} = a_i$ ,  $i = 1, \dots, n-1$ , положительные члены, кроме  $a_0$ , появляются дважды, то число  $p_1$  членов в  $P_1$  нечетно. Числа  $p_2, p_3, p_4$  также нечетны. Полагаем

$$T = 1 + u + u^2 + \dots + u^{n-1}. \quad (14.2.15)$$

Тогда

$$P_i + N_i = T, \quad i = 1, 2, 3, 4. \quad (14.2.16)$$

В силу формул (14.2.12), (14.2.13) и (14.2.14) соотношение

$$A^2 + B^2 + C^2 + D^2 = 4n, \quad (14.2.17)$$

соответствующее (14.2.7), принимает вид

$$(2P_1 - T)^2 + (2P_2 - T)^2 + (2P_3 - T)^2 + (2P_4 - T)^2 = 4n. \quad (14.2.18)$$

Так как  $u^j T = T$  для всех  $j$ , то  $P_i T = p_i T$  и  $T^2 = nT$ , а (14.2.18) принимает вид

$$\begin{aligned} 4(P_1^2 + P_2^2 + P_3^2 + P_4^2) - \\ - 4(p_1 + p_2 + p_3 + p_4)T + 4nT = 4n. \end{aligned} \quad (14.2.19)$$

Разделив на 4, получаем

$$P_1^2 + P_2^2 + P_3^2 + P_4^2 = (p_1 + p_2 + p_3 + p_4 - n)T + n. \quad (14.2.20)$$

Так как каждое  $p_i$  нечетно и  $n$  нечетно, мы видим, что каждый член  $u^j$ ,  $j \neq 0$ , должен появляться нечетное

число раз (а именно  $p_1 + p_2 + p_3 + p_4 - n$  раз) в левой части (14.2.20). Для каждого  $t = 1, \dots, n-1$  существует единственное  $s$ , такое, что  $(u^s)^2 = u^t$ . Из  $P_i^2 = (\sum u^k)^2$ , где  $k$  пробегает элементы некоторого подмножества из  $\{0, 1, \dots, n-1\}$ , имеем  $P_i^2 \equiv \sum u^{2k} \pmod{2}$ . Следовательно, каждое  $u^t = (u^s)^2$ , чтобы появиться с нечетным коэффициентом в левой части (14.2.20), должно входить точно в одну или в три суммы  $P_1^2, P_2^2, P_3^2, P_4^2$ . Соответствующее  $u^s$  появляется точно в одном или в трех из  $P_1, P_2, P_3, P_4$ .

**Лемма 14.2.1.** *Если  $n$  нечетно и если матрицы  $A, B, C, D$  из (14.2.4) выбраны с такими знаками, что  $a_0 = b_0 = c_0 = d_0 = 1$ , и удовлетворяют условию  $A^2 + B^2 + C^2 + D^2 = 4nI_n$ , то для каждого  $i = 1, \dots, n-1$  из  $a_i, b_i, c_i, d_i$  точно три имеют один и тот же знак.*

**Доказательство.** Полагаем  $A = P_1 - N_1, B = P_2 - N_2, C = P_3 - N_3, D = P_4 - N_4$ . Как было показано, член  $u^i$  появляется либо в одном, либо в трех из  $P_1, P_2, P_3, P_4$  и потому либо  $u^i$  появляется точно в трех из  $A, B, C, D$ , либо  $-u^i$  появляется точно в трех из них.

Определим теперь  $W_1, W_2, W_3, W_4$  равенствами

$$\begin{aligned} 2W_1 &= A + B + C - D, & 2W_2 &= A + B - C + D, \\ 2W_3 &= A - B + C + D, & 2W_4 &= -A + B + C + D. \end{aligned} \quad (14.2.21)$$

Подставляя в (14.2.17), находим

$$W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4n, \quad (14.2.22)$$

и в силу леммы 14.2.1 каждое  $W_i$  имеет целые коэффициенты и

$$W_i = 1 \pm 2u^j \pm \dots \pm 2u^k, \quad (14.2.23)$$

где для каждого  $j = 1, \dots, n-1$  член  $\pm 2u^j$  присутствует точно в одном из  $W_i$ . Например, если  $u^i$  появляется с коэффициентом  $-1$  в  $A, B$  и  $C$  и с коэффициентом  $+1$  в  $D$ , то мы имеем  $-2u^i$  в  $W_1$ , и члена с  $u^i$  не будет ни в  $W_2$ , ни в  $W_3$ , ни в  $W_4$ . Поскольку  $u^i$  и  $u^{n-i}$  имеют один и тот же коэффициент в каждом из полиномов  $A, B, C, D$ , то и в  $W_i$  коэффициенты при  $u^i$  и  $u^{n-i}$  одинаковы. Обратно, если  $W_i$  имеют вид (14.2.23), причем

коэффициенты при  $u^i$  и  $u^{n-i}$  равны и удовлетворяют условию (14.2.22), то следующие  $A, B, C, D$ :

$$2A = W_1 + W_2 + W_3 - W_4, \quad 2C = W_1 - W_2 + W_3 + W_4, \quad (14.2.24)$$

$$2B = W_1 + W_2 - W_3 + W_4, \quad 2D = -W_1 + W_2 + W_3 + W_4,$$

удовлетворяют условиям леммы 14.2.1 и дают  $H$ -матрицу в (14.2.1). Так как (14.2.22) должно выполняться для элементов группового кольца  $R(G)$  циклической группы  $\{u\}$  с  $u^n = 1$ , то это соотношение должно быть справедливо, когда  $u$  заменяется на любой корень  $n$ -й степени из единицы, в частности когда мы берем  $u = 1$ . В этом случае каждое из  $W_i$  есть нечетное целое число. По теореме Лагранжа (Харди и Райт [1]) каждое целое число может быть представлено в виде суммы четырех квадратов целых чисел. Верно также и то, что если  $n$  нечетно, то  $4n$  можно представить в виде суммы четырех квадратов нечетных целых чисел. Если  $n = 23$ , то существует два таких представления:

$$92 = 9^2 + 3^2 + 1^2 + 1^2 = 7^2 + 5^2 + 3^2 + 3^2. \quad (14.2.25)$$

Обозначая  $v_i = u^i + u^{n-i}$ ,  $i = 1, \dots, \frac{n-1}{2}$ , имеем

$$W_j = W_j(u) = 1 \pm 2v_1 \pm \dots \pm 2v_k, \quad j = 1, 2, 3, 4. \quad (14.2.26)$$

При  $u = 1$  имеем  $v_i = 2$  для всех  $i$ , и знак у  $W_j(1)$  выбираем так, чтобы выполнялось сравнение  $W_j(1) \equiv 1 \pmod{4}$ . Тогда из первого разложения 92 в (14.2.25) получаем

$$\begin{aligned} 92 &= (1 + 2v_a + 2v_b + \dots)^2 + \\ &\quad + (1 - 2v_c + \dots)^2 + (1 + \dots)^2 + (1 + \dots)^2, \end{aligned} \quad (14.2.27)$$

где на месте многоточий стоят суммы слагаемых вида

$$2v_d - 2v_e, \quad 2v_f - 2v_g, \quad 2v_h - 2v_i, \quad 2v_j - 2v_k,$$

а  $a, b, \dots, k$  — числа  $1, \dots, 11$ , взятые в некотором порядке. В этой форме задача поддается исследованию на ЭВМ. Бомер, Голомб и Холл [1] нашли следующее

решение:

$$92 = (1 + 2v_2 + 2v_6)^2 + (1 - 2v_3 + 2v_1 - 2v_{10})^2 + \\ + (1 + 2v_5 - 2v_7)^2 + (1 + 2v_{11} - 2v_8 + 2v_9 - 2v_4)^2. \quad (14.2.28)$$

Таким образом, существует  $H$ -матрица порядка 92 вида (14.2.1), которую можно построить исходя из (14.2.28) и используя (14.2.24). Другое представление,  $92 = 7^2 + 5^2 + 3^2 + 3^2$ , не приводит к  $H$ -матрице. Тем же путем Уильямсон нашел для  $4n = 172$ , что если взять

$$a_j = v_{3j} + v_{3j+1} + v_{3j+2}, \quad (14.2.29)$$

то получим

$$172 = (1 + 2a_0 - 2a_2)^2 + (1 + 2a_3 - 2a_1)^2 + \\ + (1 + 2a_4 - 2a_6)^2 + (1 + 2a_5)^2. \quad (14.2.30)$$

Это дает второе значение, 172, в V. В работе [1] Уильямсон дал несколько решений для (14.2.22), в том числе (14.2.29), но не указал решения для  $4n = 92$ , и оно не было найдено до 1962 г. Бомер [1] нашел все решения для (14.2.22) при нечетном  $n$ ,  $n = 3, \dots, 23$ , а также решения в случаях  $n = 25$  и  $n = 27$ . Путем машинного исследования Бомер недавно обнаружил решение при  $4n = 116$ :

$$116 = (1 + 2w_{12} + 2w_6 + 2w_2 - 2w_{11} - 2w_9 - 2w_4)^2 + \\ + (1 + 2w_{10} + 2w_7 - 2w_8 - 2w_3 - 2w_5)^2 + \\ + (1 + 2w_1)^2 + (1 + 2w_{13} + 2w_{14})^2. \quad (14.2.31)$$

Существует парадокс, связанный с изложенным в этом разделе методом Уильямсона. При всех тех нечетных  $n$ , для которых удалось провести полное исследование, найдены  $H$ -матрицы такого типа порядка  $4n$ , однако бесконечного класса  $H$ -матриц этого типа не найдено. Доказательство того, что этот метод всегда будет успешным, решило бы, разумеется, основную проблему об  $H$ -матрицах, так как если существует  $H_{4n}$  для нечетного  $n$ , то существует  $H_{2^j n}$  для  $j > 2$  и, значит, существует  $H_m$  для  $m \equiv 0 \pmod{4}$ .

### 14.3. Три новых метода

Можно добавить к уже описанным еще два метода для построения матриц Адамара. Если  $A, B, C, D$  — симметрические циркулянтные матрицы порядка  $n$ , такие, что  $H$  вида (14.2.1) является  $H$ -матрицей порядка  $4n$ , то существует следующая  $H$ -матрица порядка  $12n$ :

$$H_{12n} = \begin{bmatrix} A & A & A & B - B & C - C - D & B & C - D - D \\ A - A & B - A - B - D & D - C - B - D - C - C \\ A - B - A & A - D & D - B & B - C - D & C - C \\ B & A - A - A & D & D & D & C & C - B - B - C \\ B - D & D & D & A & A & C - C & B - C & B \\ B & C - D & D & A - A & C - A - D & C & B - B \\ D - C & B - B & A - C - A & A & B & C & D - D \\ -C - D - C - D & C & A - A - A - D & B - B - B \\ D - C - B - B - B & C & C - D & A & A & A & D \\ -D - B & C & C & C & B & B - D & A - A & D - A \\ C - B - C & C & C & D - B - D - B & A - D - A & A \\ -C - D - D & C - C - B & B & B & D & A - A - A \end{bmatrix} \quad (14.3.1)$$

ибо мы можем непосредственно проверить, что

$$H_{12n} H_{12n}^T = (3A^2 + 3B^2 + 3C^2 + 3D^2) \times I_{12} = 12nI_{12n}. \quad (14.3.2)$$

Это построение было осуществлено Бомером и автором [1]. Оно привело к  $H$ -матрице порядка 156. Возможно, матрица (14.3.1) — пример нового типа композиции.

Второй из методов принадлежит Голлбергу. Если  $H$  — матрица Адамара кососимметрического типа порядка  $n$  вида (14.1.45), то  $D$  имеет порядок  $n-1$  и  $D - I_{n-1} = D_1$ , где  $D_1^T = -D_1$ . Определим матрицу  $A$  формулой

$$A = \frac{1}{2}(D + J_{n-1}) - I_{n-1}. \quad (14.3.3)$$

Тогда элемент в  $A$  равен 1, если соответствующий элемент в  $D_1$  равен 1; все остальные элементы в  $A$  равны

нулю. Далее,

$$D = I_{n-1} + A - A^T, \quad A + A^T = J_{n-1} - I_{n-1}. \quad (14.3.4)$$

Из других соотношений в (14.1.47) получаем, что

$$e_{n-1}A = e_{n-1}A^T, \quad A^TA = AA^T = \left(\frac{n}{4}\right)I_{n-1} + \frac{(n-4)}{4}J_{n-1}. \quad (14.3.5)$$

Обозначив через  $(X, Y, Z)$  прямое произведение матриц  $X, Y, Z$ , определим матрицу

$$\begin{aligned} A_{(n-1)^3} &= (I, A, J) + (J, I, A) + (A, J, I) + \\ &+ (A, A, A) + (A, A^T, A^T) + (A^T, A, A^T) + (A^T, A^T, A). \end{aligned} \quad (14.3.6)$$

Тогда  $A_{(n-1)^3}$  есть матрица из нулей и единиц порядка  $(n-1)^3$ , удовлетворяющая тем же соотношениям, что и  $A$ , если  $n$  заменить на  $(n-1)^3 + 1$ . Отсюда следует, что если существует  $H$ -матрица порядка  $n$  кососимметрического типа, то существует и  $H$ -матрица порядка  $(n-1)^3 + 1$  кососимметрического типа.

Третий метод принадлежит Элиху [1].

**Теорема 14.3.1.** *Если существует  $H$ -матрица порядка  $n+1$  кососимметрического типа и если  $n-2 = m = p^s \equiv 1 \pmod{4}$ ,  $p$  простое, то существует  $H$ -матрица порядка  $(n-1)^2$ .*

**Доказательство.** Нам дана матрица  $H^*$  порядка  $n+1$ ,

$$H^* = \begin{bmatrix} 1 & e_n \\ -e_n^T & I_n + G \end{bmatrix}, \quad G^T = -G, \quad (14.3.7)$$

и  $H^*H^{*T} = (n+1)I_{n+1}$ .

При  $m = p^s \equiv 1 \pmod{4}$  существует матрица  $Q$  порядка  $m$ , такая, что

$$\begin{aligned} Q &= [q_{ij}], \quad q_{ii} = 0, \quad q_{ij} = \pm 1, \quad j \neq i, \\ QQ^T &= Q^2 = mI_m - J_m \end{aligned} \quad (14.3.8)$$

[см. (14.1.21) и лемму 14.1.2].

Элих строит матрицу

$$K = Q \times G - I_m \times (J_n - I_n) + J_m \times I_n, \quad (14.3.9)$$

и матрица

$$H = \begin{bmatrix} 1 & e_{mn} \\ e_{mn}^T & K \end{bmatrix} \quad (14.3.10)$$

состоит из  $\pm 1$ . Предыдущие соотношения дают

$$HH^T = (mn + 1) I_{mn+1}, \quad mn + 1 = (n - 1)^2, \quad (14.3.11)$$

и теорема доказана.

# Общие методы построения блок-схем

---

## 15.1. Методы построения

Известные методы построения блок-схем делятся в основном на два типа — прямые и рекурсивные. Прямой метод позволяет построить схему с параметрами частного вида, обычно с использованием конечных полей или сравнений. Рекурсивный метод — способ построения блок-схемы из схем меньшего размера<sup>1)</sup>. При построении ортогональных латинских квадратов в гл. 13 были использованы оба эти метода. Прямые методы приводят обычно к более легкому построению, но применимы только для частных значений параметров, быть может, лишь тогда, когда число элементов  $v$  есть степень простого числа.

Раздел 15.2 содержит основные рекурсивные теоремы Ханани. В разд. 15.3 дается несколько способов прямого построения, большинство из которых принадлежит Боузу [1]. В разд. 15.4 детально рассмотрены системы троек — блок-схемы с  $k = 3$ . Раздел 15.5 посвящен схемам с  $k > 3$ , и в нем некоторые результаты скорее просто сформулированы, нежели полностью доказаны.

## 15.2. Основные определения. Теоремы Ханани

Уравновешенная неполная блок-схема была определена в разд. 10.1 как размещение  $v$  различных элементов в  $b$  блоках, такое, что каждый блок содержит точно  $k$  различных элементов, каждый элемент появляется точно в  $r$  различных блоках и всякая (неупорядоченная) пара различных элементов появляется точно в  $\lambda$  блоках. Была показана справедливость следующих

<sup>1)</sup> То есть с меньшими параметрами. — Прим. перев.

соотношений:

$$bk = vr, \quad (15.2.1)$$

$$r(k-1) = \lambda(v-1). \quad (15.2.2)$$

Мы будем считать, что  $k \geq 3$ , поскольку случаи  $k=1$  и  $k=2$  тривиальны.

Будут рассматриваться также блок-схемы более общего вида, в которых число элементов может изменяться от блока к блоку. Пусть  $K = (k_1, \dots, k_n)$  — конечное множество целых чисел  $k_i$ , где  $k_i \geq 3$ ,  $i = 1, \dots, n$ . Блок-схема  $B[K, \lambda, v]$  есть такое размещение  $v$  различных элементов в  $b$  блоках  $B_1, \dots, B_b$ , что каждый блок  $B_i$  содержит  $k_i$  элементов для некоторого  $k_i$ ,  $i = 1, \dots, n$ , и всякая (неупорядоченная) пара различных элементов появляется точно в  $\lambda$  блоках. Если  $K$  состоит из единственного числа  $k$ , то мы пишем  $B[K, \lambda, v] = B[k, \lambda, v]$ . Здесь всякий раз, когда некоторый элемент появляется в блоке, он появляется в паре с  $k-1$  остальными элементами. Поскольку он должен встречаться в паре с каждым из  $v-1$  элементов точно  $\lambda$  раз, этот элемент входит в  $\lambda(v-1)/(k-1)$  блоков. Таким образом, число появлений некоторого элемента в блоках одинаково для каждого элемента, и  $B[k, \lambda, v]$  есть неполная уравновешенная блок-схема. Класс значений  $v$ , для которых  $B[K, \lambda, v]$  существует, обозначим через  $B(K, \lambda)$ .

Ханани в работе [1] ввел трансверсальные системы, или  $T$ -системы. Это по существу то же самое, что ортогональные таблицы.

**Определение.** Пусть дан класс  $m$  попарно непересекающихся множеств  $w_i$ ,  $i = 0, \dots, m-1$ , каждое из которых состоит из  $t$  элементов.  $T$ -система  $T_0(m, t)$  состоит из  $t^2$  множеств  $Y_j$ ,  $j = 1, \dots, t^2$ , содержащих каждое  $m$  элементов и таких, что: (1) каждое  $Y_j$  имеет точно один элемент, общий с каждым из  $w_i$ , и (2) если  $j \neq k$ , то  $Y_j$  и  $Y_k$  имеют не более одного общего элемента.

Предположим, что мы имеем ортогональную таблицу  $OA(t, m)$ , строки которой мы перенумеруем от 0 до  $m-1$ . Числом  $1, \dots, t$  в  $i$ -й строке поставим в соответствие

некоторые символы  $a_{i1}, \dots, a_{it}$ ; множество  $\{a_{i1}, a_{i2}, \dots, a_{it}\}$  обозначим через  $w_i$ ,  $i = 0, \dots, m - 1$ . Множества  $Y_j$ ,  $j = 1, \dots, t^2$ , образуем из  $t^2$  столбцов ортогональной таблицы ОА  $(t, m)$ : если  $j$ -й столбец ОА  $(t, m)$  содержит число  $u$  в  $i$ -й строке, то мы поместим в  $Y_j$  элемент  $a_{iu}$ . Таким образом, каждое  $Y_j$  содержит  $m$  элементов, по одному из каждого  $w_i$ . Утверждение, что если  $j \neq k$ , то  $Y_j$  и  $Y_k$  имеют не более одного общего элемента, эквивалентно ортогональности строк таблицы ОА  $(t, m)$ , означающей, что в подматрице, образованной любыми двумя строками, столбец  $\begin{pmatrix} u \\ v \end{pmatrix}$  не может появиться более одного раза. Обратно, если мы имеем непересекающиеся множества  $w_i$ ,  $i = 0, \dots, m$ , из  $t$  элементов каждое и систему  $T_0(m, t)$ , то заменим  $t$  элементов множества  $w_i$  числами  $1, 2, \dots, t$ . Образуем теперь из множеств  $Y_j$  столбцы матрицы: для  $j$ -го столбца мы поместим в  $i$ -ю строку число  $u$ , если  $Y_j$  содержит элемент из  $w_i$ , соответствующий числу  $u$ . Условие (2) для  $Y_j$  обеспечивает ортогональность строк полученной матрицы, которая является, следовательно, ОА  $(t, m)$ .

Класс чисел  $t$ , для которых существует система  $T_0(m, t)$ , обозначим через  $T_0(m)$ . Множество из  $t$  трансверсалей  $Y_j$  в  $T_0(m, t)$  назовем параллельным множеством, если никакие две из них не имеют общего элемента. Таким образом, для данного элемента существует точно одна трансверсаль параллельного множества, содержащая его. Если система  $T_0(m, t)$  содержит  $e$  (или более) параллельных множеств трансверсалей, то мы обозначим ее через  $T_e(m, t)$ , а класс чисел  $t$ , для которых существует  $T_e(m, t)$ , обозначим через  $T_e(m)$ .

**Теорема 15.2.1.** *Если существует  $T_d(m, s)$  и  $T_e(m, t)$ , то существует и  $T_{de}(m, st)$ .*

**Доказательство.** Нам даны  $s$ -множества

$$v_i = \{a_{i1}, \dots, a_{is}\}, \quad i = 0, \dots, m - 1,$$

и  $s^2$  трансверсалей  $X_j$ ,  $j = 1, \dots, s^2$ , а также  $t$ -множества

$$w_i = \{b_{i1}, \dots, b_{it}\}, \quad i = 0, \dots, m - 1,$$

и  $t^2$  трансверсалей  $Y_k$ ,  $k = 1, \dots, t^2$ , причем имеется  $d$  параллельных множеств трансверсалей  $X_j$  и  $e$  параллельных множеств трансверсалей  $Y_k$ . Определим элементы  $c_{i,g,h} = (a_{ig}, b_{ih})$ ,  $g = 1, \dots, s$ ;  $h = 1, \dots, t$ , как упорядоченные пары из  $a_{ig}$  и  $b_{ih}$ , и пусть

$$u_i = \{c_{i,1,1}, \dots, c_{i,g,h}, \dots\}, \quad i = 0, \dots, m-1.$$

Получаем  $m$  множеств  $u_i$ , каждое из которых содержит  $st$  элементов. В качестве трансверсалей возьмем множества  $Z_{jk}$ ,  $j = 1, \dots, s^2$ ;  $k = 1, \dots, t^2$ ;  $c_{i,g,h} \in Z_{jk}$  тогда и только тогда, когда  $a_{ig} \in X_j$ ,  $b_{ih} \in Y_k$ . Легко проверить, что  $Z_{jk}$  образуют множество  $T_{de}(m, st)$ , если заметить, что, когда  $j$  пробегает индексы некоторого параллельного множества из  $T_d(m, s)$ , а  $k$  — индексы некоторого параллельного множества из  $T_e(m, t)$ , соответствующие  $Z_{jk}$  образуют параллельное множество.

**Теорема 15.2.2.** Система  $T_t(m-1, t)$  существует тогда и только тогда, когда существует система  $T_0(m, t)$ .

**Доказательство.** Пусть существует система  $T_0(m, t)$  трансверсалей к  $w_0, w_1, \dots, w_{m-2}, w_{m-1}$ ;  $t$  трансверсалей, содержащих какой-либо элемент из  $w_{m-1}$ <sup>1)</sup>, не имеют других общих элементов. Следовательно, если мы отбросим  $w_{m-1}$  и его элементы, мы получим  $t$  множеств параллельных трансверсалей к  $w_0, \dots, w_{m-2}$ , каждое из которых соответствует некоторому элементу из  $w_{m-1}$ , т. е. систему  $T_t(m-1, t)$ . Обратно, если мы имеем систему  $T_t(m-1, t)$  трансверсалей к  $w_0, \dots, w_{m-2}$ , то мы можем к каждой трансверсали в параллельном множестве добавить новый элемент и образовать из этих  $t$  новых элементов множество  $w_{m-1}$ . Тогда получается система  $T_0(m, t)$ .

<sup>1)</sup> Очевидно, любой элемент каждого из множеств  $w_i$  содержится ровно в  $t$  трансверсалах. Действительно, если бы какой-либо элемент  $a_{ij} \in w_i$  принадлежал трансверсалам  $X_1, X_2, \dots, X_{t_1}$ ,  $t_1 > t$ , то для любого  $k$ ,  $k \neq i$ ,  $k = 0, \dots, m-1$ , можно было бы найти два множества  $X_{t_1}, X_{t_2}$ , которые содержали бы некоторый элемент  $a_{kh}$  из  $w_k$  (так как все  $w_k$  состоят из  $t$  элементов), и в пересечении  $X_{t_1} \cap X_{t_2}$  содержалось бы более одного элемента. — Прим. ред.

**Теорема 15.2.3.** Если  $t = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$ , где  $p_i$  — простые числа, и если  $m = \min(p_1^{e_1}, \dots, p_r^{e_r})$ , то существует  $T_t(m, t)$ .

**Доказательство.** По теореме 13.2.2 для степени простого числа  $p^e$  существует полное множество  $p^e - 1$  ортогональных латинских квадратов и ортогональная таблица  $\text{OA}(p^e, p^e + 1)$ , а значит, и  $\text{OA}(p^e, m + 1)$ , что эквивалентно существованию системы  $T_0(m + 1, p^e)$ . По теореме 15.2.2 мы имеем тогда систему  $T_{p^e}(m, p^e)$  и потому, применяя несколько раз теорему 15.2.1, можем построить систему  $T_t(m, t)$ .

Некоторые блок-схемы  $B[K, \lambda, v]$  обладают свойством, похожим в известной степени на разрешимость. Это свойство используется Ханани. Мы будем называть его центральной разрешимостью.

**Определение.** Пусть дана система  $B[K, \lambda, v]$  на элементах некоторого множества  $E$ . Если существуют элемент  $A \subseteq E$  и число  $m \in K$ , такие, что  $m - 1$  делит  $v - 1$ , и множество  $E - A$  может быть разбито на  $(v - 1)/(m - 1)$  попарно не пересекающихся подмножеств  $E_i$ ,  $i = 1, \dots, (v - 1)/(m - 1)$ , состоящих каждого из  $m - 1$  элементов, таким образом, что каждое из множеств  $E_i \cup A$ ,  $i = 1, \dots, (v - 1)/(m - 1)$ , появляется ровно  $\lambda$  раз в качестве блока системы  $B[K, \lambda, v]$ , то мы назовем эту систему *центрально разрешимой* и обозначим ее через  $B_m[K, \lambda, v]$ . Класс всех чисел  $v$ , для которых существуют системы  $B_m[K, \lambda, v]$ , обозначим через  $B_m(K, \lambda)$ . Назовем  $A$  *центром*, а  $E_i \cup A$  — *выделенными блоками*.

Мы можем теперь доказать две основные рекурсивные теоремы Ханани, используемые для построения блок-схем. Первая из них очень похожа на теорему 13.3.2.

**Теорема 15.2.4.** Если  $v = (m - 1)u + 1$ , где  $u \in B(K', \lambda')$ , и если для каждого  $k' \in K'$  имеем  $(m - 1)k' + 1 \in B_m(K, \lambda'')$ , то  $v \in B_m(K, \lambda)$ , где  $\lambda = \lambda'\lambda''$ .

**Доказательство.** Множество элементов  $E$  образуем из точки  $A$  и точек

$$(x, y), \quad 0 \leq x \leq u - 1, \quad 0 \leq y \leq m - 2.$$

Это дает  $1 + (m - 1)u = v$  элементов. Возьмем далее подмножества

$$(A, i) = \{A, (i, y), \quad 0 \leq y \leq m - 2\}, \quad i = 0, \dots, n - 1.$$

Пусть в системе  $B[K', \lambda', u]$  элементы — это числа  $0, 1, \dots, u - 1$ . Если  $B'_j$  — блок из  $B[K', \lambda', u]$ , то пусть его элементы суть  $a_1, \dots, a_r$ , где, конечно,  $r \in K'$ . Возьмем теперь множество  $E'_j$  из  $(m - 1)r + 1$  элементов:

$$E'_j = \{A, (a_i, y), \quad i = 1, \dots, r, \quad y = 0, \dots, m - 2\}.$$

По предположению, существует система  $B_m[K, \lambda'', (m - 1)r + 1]$ . Построим систему

$$B'_{mj} = B_m[K, \lambda'', (m - 1)r + 1]$$

с центром  $A$  и выделенными блоками  $(A, a_i)$ ,  $i = 1, \dots, r$ , на элементах из  $E'_j$ . Удалим из  $B'_{mj}$  выделенные блоки  $(A, a_i)$  и оставшееся множество блоков обозначим через  $\bar{B}'_{mj}$ . Пусть теперь  $B'_j$  пробегает все блоки из  $B[K', \lambda', u]$ . Рассмотрим совокупность всех блоков из всех множеств  $\bar{B}'_{mj}$ , а также множества  $(A, i)$ , взятые в качестве блоков каждое  $\lambda$  раз. Мы утверждаем, что это множество блоков на  $v$  элементах множества  $E$  есть система  $B_m[K, \lambda, v]$ . Конечно,  $m \in K$ , и число элементов в каждом блоке, построенном в каждом из  $B'_{mj}$ , является числом из  $K$ . Точка  $A$  появляется только в выделенных блоках  $(A, i)$  и потому встречается в паре с каждым другим элементом точно  $\lambda$  раз. Далее, точки  $(i, y_1)$  и  $(i, y_2)$  появляются вместе только в выделенных блоках из  $B'_{mj}$  и потому только в выделенных блоках  $(A, i)$  полученной нами системы. Рассмотрим две точки  $(s, y_1)$  и  $(t, y_2)$ , где  $s \neq t$ , а  $y_1$  и  $y_2$  могут быть равны;  $s$  и  $t$  появляются вместе в  $\lambda'$  блоках  $B'_j$  из  $B[K', \lambda', u]$ . При каждом таком появлении точки  $(s, y_1)$  и  $(t, y_2)$  встречаются вместе в  $\lambda''$  блоках соответствующего множества  $\bar{B}'_{mj}$ . Следовательно,  $(s, y_1)$  и  $(t, y_2)$  появляются вместе точно в  $\lambda'\lambda''$  блоках нашей системы, которая является, следовательно, системой  $B_m[K, \lambda, v]$ , т. е. центрально разрешимой с центром  $A$  и выделенными блоками  $(A, i)$ .

Проиллюстрируем теорему 15.2.4 на простом примере. Для  $K' = \{4, 3\}$  мы имеем следующие блоки схемы  $B[K', 1, 10]$ , определенной на числах  $0, \dots, 9$ :

$$\begin{array}{ll} B'_0: 0, 1, 2, 3; & B'_6: 2, 4, 8; \\ B'_1: 0, 4, 5, 6; & B'_7: 2, 5, 9; \\ B'_2: 0, 7, 8, 9; & B'_8: 2, 6, 7; \\ B'_3: 1, 4, 7; & B'_9: 3, 4, 9; \\ B'_4: 1, 5, 8; & B'_{10}: 3, 5, 7; \\ B'_5: 1, 6, 9; & B'_{11}: 3, 6, 8. \end{array} \quad (15.2.3)$$

Возьмем  $m = 3$ . На множествах из  $1 + (3 - 1)3 = 7$  и  $1 + (3 - 1)4 = 9$  элементов существуют центрально разрешимые схемы  $B_3[3, 1, 7]$  и  $B_3[3, 1, 9]$ . Для  $B_3[3, 1, 7]$  на элементах  $A, 1, \dots, 6$  мы имеем:

$$\begin{array}{lll} C_1: A, 1, 2; & C_4: 1, 3, 5; & C_6: 2, 3, 6; \\ C_2: A, 3, 4; & C_5: 1, 4, 6; & C_7: 2, 4, 5. \\ C_3: A, 5, 6; & & \end{array} \quad (15.2.4)$$

Для  $B_3(3, 1, 9)$  на элементах  $A, 1, \dots, 8$  имеем

$$\begin{array}{lll} D_1: A, 1, 2; & D_5: 1, 3, 5; & D_8: 2, 3, 8; \\ D_2: A, 3, 4; & D_6: 1, 4, 7; & D_9: 2, 4, 6; \\ D_3: A, 5, 6; & D_7: 1, 6, 8; & D_{10}: 2, 5, 7; \\ D_4: A, 7, 8; & & \end{array} \quad (15.2.5)$$

Теорема утверждает существование  $B_3[3, 1, 21]$ , где  $21 = 1 + (3 - 1)10$ ; 21 элемент множества  $E$  — это  $A$  и точки  $(x, y)$ ,  $x = 0, \dots, 9$ ,  $y = 0, 1$ . Выделенными блоками будут

$$(A, i) = \{A, (i, 0), (i, 1)\}, \quad i = 0, \dots, 9. \quad (15.2.6)$$

Упростим обозначения. Пусть

$$(i, 0) = i, \quad (i, 1) = 1i, \quad i = 0, \dots, 9, \quad (15.2.7)$$

и множество  $E$  состоит из точки  $A$  и чисел  $0, 1, \dots, 19$ . По блоку  $B'_0 = \{0, 1, 2, 3\}$  в (15.2.3) строится множество

$E'_0 = \{A, 0, 1, 2, 3, 10, 11, 12, 13\}$  и на нем схема  $B'_{03}[3, 1, 9]$  с выделенными блоками  $(A, i)$ ,  $i = 0, 1, 2, 3$  (см. (15.2.6)).

В обозначениях (15.2.7) схема  $B'_{03}$  состоит из блоков

$$A, 1, 10; \quad 0, 1, 2; \quad 10, 1, 13; \quad 1, 12, 3;$$

$$A, 1, 11; \quad 0, 11, 3; \quad 10, 11, 12; \quad 11, 2, 13. \quad (15.2.8)$$

$$A, 2, 12; \quad 0, 12, 13; \quad 10, 2, 3;$$

$$A, 3, 13;$$

Аналогично по блоку  $B'_6 = \{2, 4, 8\}$  строится множество  $E'_6 = \{A, 0, 2, 4, 8, 12, 14, 18\}$  и на нем схема  $B'_{63}[3, 1, 7]$ . Подходящая подстановка в (15.2.4) дает следующие блоки схемы  $B'_{63}[3, 1, 7]$ :

$$A, 2, 12; \quad 2, 4, 8; \quad 12, 4, 18; \quad (15.2.9)$$

$$A, 4, 14; \quad 2, 14, 18; \quad 12, 14, 8.$$

$$A, 8, 18;$$

Таким путем, использовав все 12 блоков из (15.2.3), мы построим три системы  $B_3[3, 1, 9]$  и девять систем  $B_3[3, 1, 7]$  и, взяв совокупность всех блоков, исключая выделенные блоки  $\{A, i, 1i\}$ , получим систему  $B_3[3, 1, 21]$ , которая является уравновешенной неполной блок-схемой с параметрами  $v = 21$ ,  $b = 70$ ,  $r = 10$ ,  $k = 3$ ,  $\lambda = 1$ . Читатель без труда сможет построить все 70 блоков, следуя данному выше образцу. Это не самый легкий путь построения схемы с  $v = 21$ ,  $k = 3$ ,  $\lambda = 1$ , но этот пример иллюстрирует способ, при котором уравновешенная относительно пар схема из (15.2.3) может быть использована для построения схемы, в которой  $K$  состоит из одного числа  $k$ .

Следующая теорема по своей природе весьма сходна с теоремой 13.3.5.

**Теорема 15.2.5.** Пусть  $s$ ,  $s+1 \in B(K, \lambda)$ ,  $t \in T_q(s)$ , и либо  $q \in B(K, \lambda)$ , либо  $q = 0$  или 1; тогда  $v = st + q \in B(K, \lambda)$ .

**Доказательство.** В качестве элементов множества  $E$  возьмем точки  $(x, y)$  с  $0 \leq x \leq t-1$ ,  $0 \leq y \leq s-1$ , а также  $(x, s)$  с  $0 \leq x \leq q-1$ . Рассмотрим  $T_q(s, t)$  как  $t^2$  трансверсалей к множествам  $w_0, \dots, w_{s-1}$ , где множе-

ство  $w_i$  состоит из точек  $(x, i)$ ,  $0 \leq x \leq t - 1$ . Система  $T_q(s, t)$  содержит  $q$  параллельных множеств трансверсалей. К каждой трансверсали  $Y_h$  из  $j$ -го параллельного множества добавим точку  $(j, s)$ ,  $j = 0, \dots, q - 1$ . Тогда получим  $qt$  блоков  $Y_h^*$ , каждый из  $s + 1$  точек, а остальные  $(t - q)t$  трансверсалей  $Y_h$  рассмотрим как блоки с  $s$  точками каждый. Если  $q > 1$ , то образуем множество

$$Z = \{(x, s)\}, x = 0, \dots, q - 1.$$

Образуем теперь систему  $B[K, \lambda, v]$ , взяв блоки из  $qt$  систем  $B[K, \lambda, s + 1]$  на элементах из множеств  $Y_h^*$  и  $t^2 - qt$  систем  $B[K, \lambda, s]$  на элементах из множеств  $Y_h$ . Образуем также  $s$  систем  $B[K, \lambda, t]$  на элементах из множеств  $w_0, \dots, w_{s-1}$ . Наконец, если  $q > 1$ , то образуем систему  $B[K, \lambda, q]$  на элементах  $Z$ . Все эти блоки вместе образуют систему  $B[K, \lambda, v]$ . Действительно, множества  $w_i$ ,  $Y_h^*$ ,  $Y_h$ ,  $Z$ , взятые как блоки, образуют уравновешенную относительно пар схему с  $\lambda = 1$ . Следовательно, построение  $B[K, \lambda, r]$  с  $r = t, s + 1, s, q$  на этих множествах в свою очередь дает  $B[K, \lambda, v]$ . Следующие две теоремы тривиальны, но полезны.

**Теорема 15.2.6.** *Если  $v \in B(K', \lambda_1)$  и  $k' \in B(K, \lambda_2)$  для всякого  $k'$  из  $K'$ , то  $v \in B(K, \lambda_1\lambda_2)$ .*

**Доказательство.** Дано  $B = B[K', \lambda_1, v]$ . Возьмем элементы некоторого блока из  $B$ , содержащего  $k'$  элементов, и на этом множестве построим систему  $B[K, \lambda_2, k']$ . Все блоки всех таких систем, взятые вместе, образуют систему  $B[K, \lambda_1\lambda_2, v]$ .

**Теорема 15.2.7.** *Если  $v \in B(K, \lambda_1)$  и  $v \in B(K, \lambda_2)$ , то  $v \in B(K, \lambda_1 + \lambda_2)$ .*

**Доказательство.** Пусть  $B[K, \lambda_1, v]$  и  $B[K, \lambda_2, v]$  представлены на одном и том же множестве  $E$  из  $v$  элементов. Тогда совокупность всех блоков этих двух систем образует систему  $B[K, \lambda_1 + \lambda_2, v]$ .

**Следствие.** *Если  $v \in B(K, \lambda)$ , то  $v \in B(K, \lambda n)$  для произвольного натурального числа  $n$ .*

Нам понадобится еще одна теорема о трансверсальных системах.

**Теорема 15.2.8.** Если  $t \in T_s(m)$  и  $s \in T_0(m)$ , то  $st \in T_{s^2}(m)$ .

**Доказательство.** Нам даны системы  $T_s(m, t)$  и  $T_0(m, s)$ . Пусть  $w_0, w_1, \dots, w_{m-1}$  — множества  $w$  системы  $T_s(m, t)$ , где  $w_x = \{b_{x1}, \dots, b_{xt}\}$ , а множества  $w$  системы  $T_0(m, s)$  — это  $w'_0, \dots, w'_{m-1}$ , где  $w'_x = \{c_{x1}, \dots, c_{xs}\}$ . Мы будем (в случае надобности) отождествлять элементы  $c_{xj}$  из  $w'_x$ ,  $x = 0, \dots, m-1$ , с вычетами по модулю  $s$ , взятыми в некотором произвольном, но фиксированном порядке. Удобно рассматривать трансверсаль  $Y$  как некоторую функцию  $Y(x)$ , где  $x = 0, \dots, m-1$ , и  $Y(x)$  есть элемент, принадлежащий  $Y$  в множестве  $w_x$ . Следовательно, нам даны трансверсальные функции для  $T_s(m, t)$ :

$$\begin{aligned} Y_{1,1}(x), \dots, Y_{1,t}(x), Y_{2,1}(x), \dots, Y_{2,t}(x), \dots \\ \dots, Y_{s,1}(x), \dots, Y_{s,t}(x), Y_{st+1}(x), \dots, Y_{t^2}(x), \quad (15.2.10) \\ x = 0, \dots, m-1, \end{aligned}$$

где  $Y_{i1}, \dots, Y_{it}$  — трансверсали из  $i$ -го параллельного множества,  $i = 1, \dots, s$ , а  $Y_j$ ,  $j = st + 1, \dots, t^2$ , — остальные трансверсали. Трансверсальные функции для  $T_0(m, s)$  обозначим через

$$Y'_1(x), \dots, Y'_{s^2}(x), \quad x = 0, \dots, m-1. \quad (15.2.11)$$

Определим теперь новые множества  $w$  упорядоченных пар:

$$w''_x = \{(b_{xi}, c_{xj})\},$$

$$i = 1, \dots, t; \quad j = 1, \dots, s; \quad x = 0, \dots, m-1. \quad (15.2.12)$$

Каждое из них содержит  $st$  упорядоченных пар  $(b, c)$ . На этих множествах  $w$  определим трансверсальные функции  $Y''(x)$  равенствами

$$\begin{aligned} Y''_{e,f,g}(x) &= (Y_{e,f}(x), Y'_{g}(x) + e), \\ e &= 1, \dots, s; \quad f = 1, \dots, t; \quad g = 1, \dots, s^2; \quad (15.2.13) \\ Y''_{h,g}(x) &= (Y_h(x), Y'_{g}(x)), \\ h &= st + 1, \dots, t^2; \quad g = 1, \dots, s^2. \end{aligned}$$

Это дает нам  $s^2t^2$  трансверсальных функций  $Y''(x)$ . Требуется лишь проверить, что для различных функций  $Y''_i$  и  $Y''_j$  и  $x_1 \neq x_2$  равенства

$$Y''_i(x_1) = Y''_j(x_1) \quad \text{и} \quad Y''_i(x_2) = Y''_j(x_2)$$

невозможны. Это следует непосредственно из соответствующего факта для  $Y$  и  $Y'$ . Следовательно, функции  $Y''$  образуют трансверсальную систему  $T_0(m, st)$  для множеств  $w$  из (15.2.12). При фиксированном  $g$  функции  $Y''_{e, f, g}(x)$ ,  $e = 1, \dots, s$ ;  $f = 1, \dots, t$ , содержат  $st$  трансверсалей. Если бы при некотором  $x_1$

$$Y''_{e_1, f_1, g}(x_1) = Y''_{e_2, f_2, g}(x_1),$$

то

$$Y_{e_1, f_1}(x_1) = Y_{e_2, f_2}(x_1) \quad \text{и} \quad Y'_g(x_1) + e_1 = Y'_g(x_1) + e_2.$$

Из второго соотношения имеем  $e_2 = e_1$ . Но при фиксированном  $e$  функции  $Y_{e, f}(x)$  образуют параллельное множество, и потому  $Y_{e_1, f_1}(x_1) = Y_{e_1, f_2}(x_1)$  возможно лишь при  $f_1 = f_2$ , и трансверсали совпадают. Следовательно, при фиксированном  $g$  трансверсали  $Y''_{e, f, g}(x)$  образуют параллельное множество. Поэтому наша система есть система  $T_{s^2}(m, st)$ , и теорема доказана.

### 15.3. Прямые методы построения

В своей ранней работе, опубликованной в 1939 г., Боуз [1] развел несколько прямых методов построения блок-схем, первый из которых он назвал методом симметрично повторенных разностей (method of symmetrically repeated differences). Мы будем называть его просто методом смешанных разностей (method of mixed differences).

Предположим, что блок-схема  $D(b, v, r, k, \lambda)$  имеет некоторую абелеву группу  $A$  порядка  $m$  в качестве группы автоморфизмов. Будем записывать операцию в  $A$  аддитивно. Если  $A$  циклическая, то ее можно пред-

ставить вычетами по модулю  $m$ . Скажем, что два элемента  $c, d$  из  $D$  находятся на одной и той же орбите, если существует такой автоморфизм  $a \in A$ , что  $(c)a = d$ . Аналогично блоки  $B_1$  и  $B_2$  находятся на одной и той же орбите, если существует такой автоморфизм  $a \in A$ , что  $(B_1)a = B_2$ .

Свойство находиться на одной и той же орбите есть отношение эквивалентности, поэтому группа автоморфизмов  $A$  разделяет элементы и блоки на непересекающиеся орбиты. Представим некоторый произвольный, но фиксированный элемент  $i$ -й орбиты через  $(0)_i$ , где  $0$  — нуль группы  $A$ . При  $y \in A$  обозначим  $((0)_i)y = (y)_i$ . Может случиться, что  $(y)_i = (z)_i$ , даже если  $y \neq z$ ; в этом случае  $(0)_i$  инвариантен относительно некоторой подгруппы группы  $A$ . Однако нам не придется рассматривать эту ситуацию в полной общности. Мы ограничимся крайними случаями, в которых либо  $(y)_i \neq (z)_i$ , если  $y \neq z$ , либо  $(y)_i = (z)_i$  для всех  $y, z \in A$ . В последнем случае единственный элемент в орбите мы обозначим через  $(\infty)_i$ . Орбиты блоков мы будем использовать как промежуточные конструкции, учитывая, что число блоков в орбите равно некоторому делителю числа  $m$ . Если выбрать по одному блоку из каждой орбиты, то тем самым определяется вся схема  $D$ . Такой набор блоков называется *базой*. Если имеется только одна орбита элементов и одна орбита блоков, то база состоит из единственного блока, который является разностным множеством. Этот случай довольно подробно рассмотрен в гл. 11.

Мы дадим два примера схем с циклическими группами автоморфизмов и параметрами  $v = 15$ ,  $b = 35$ ,  $r = 7$ ,  $k = 3$ ,  $\lambda = 1$ . В первом случае (см. (15.3.1))  $A$  — аддитивная группа классов вычетов по модулю 5, во втором (см. (15.3.2)) — по модулю 15.

|                   |                   |
|-------------------|-------------------|
| $(0_1, 1_2, 4_2)$ | $(0_1, 2_2, 3_2)$ |
| $(1_1, 2_2, 0_2)$ | $(1_1, 3_2, 4_2)$ |
| $(2_1, 3_2, 1_2)$ | $(2_1, 4_2, 0_2)$ |
| $(3_1, 4_2, 2_2)$ | $(3_1, 0_2, 1_2)$ |
| $(4_1, 0_2, 3_2)$ | $(4_1, 1_2, 2_2)$ |

|                   |                   |                   |
|-------------------|-------------------|-------------------|
| $(0_2, 1_3, 4_3)$ | $(0_2, 2_3, 3_3)$ | $(0_1, 0_2, 0_3)$ |
| $(1_2, 2_3, 0_3)$ | $(1_2, 3_3, 4_3)$ | $(1_1, 1_2, 1_3)$ |
| $(2_2, 3_3, 1_3)$ | $(2_2, 4_3, 0_3)$ | $(2_1, 2_2, 2_3)$ |
| $(3_2, 4_3, 2_3)$ | $(3_2, 0_3, 1_3)$ | $(3_1, 3_2, 3_3)$ |
| $(4_2, 0_3, 3_3)$ | $(4_2, 1_3, 2_3)$ | $(4_1, 4_2, 4_3)$ |

|                   |                   |
|-------------------|-------------------|
| $(0_3, 1_1, 4_1)$ | $(0_3, 2_1, 3_1)$ |
| $(1_3, 2_1, 0_1)$ | $(1_3, 3_1, 4_1)$ |
| $(2_3, 3_1, 1_1)$ | $(2_3, 4_1, 0_1)$ |
| $(3_3, 4_1, 2_1)$ | $(3_3, 0_1, 1_1)$ |
| $(4_3, 0_1, 3_1)$ | $(4_3, 1_1, 2_1)$ |

|                |               |              |
|----------------|---------------|--------------|
| $(0, 1, 4)$    | $(0, 7, 13)$  | $(0, 5, 10)$ |
| $(1, 2, 5)$    | $(1, 8, 14)$  | $(1, 6, 11)$ |
| $(2, 3, 6)$    | $(2, 9, 0)$   | $(2, 7, 12)$ |
| $(3, 4, 7)$    | $(3, 10, 1)$  | $(3, 8, 13)$ |
| $(4, 5, 8)$    | $(4, 11, 2)$  | $(4, 9, 14)$ |
| $(5, 6, 9)$    | $(5, 12, 3)$  |              |
| $(6, 7, 10)$   | $(6, 13, 4)$  |              |
| $(7, 8, 11)$   | $(7, 14, 5)$  |              |
| $(8, 9, 12)$   | $(8, 0, 6)$   |              |
| $(9, 10, 13)$  | $(9, 1, 7)$   |              |
| $(10, 11, 14)$ | $(10, 2, 8)$  |              |
| $(11, 12, 0)$  | $(11, 3, 9)$  |              |
| $(12, 13, 1)$  | $(12, 4, 10)$ |              |
| $(13, 14, 2)$  | $(13, 5, 11)$ |              |
| $(14, 0, 3)$   | $(14, 6, 12)$ |              |

Заметим, что в (15.3.1) имеются три орбиты элементов и семь орбит блоков, в то время как в (15.3.2) имеется только одна орбита элементов и три орбиты блоков, причем третья орбита содержит только пять блоков, где блок в третьей орбите инвариантен относительно подгруппы порядка 3.

Нам потребуется теорема, устанавливающая условия, при которых, если даны группа  $A$  и множество

блоков  $\{B\}$ , мы можем образовать базу для схемы  $D(v, b, r, k, \lambda)$ . Если мы имеем блок  $B = [(a_1)_{j_1}, (a_2)_{j_2}, \dots, (a_k)_{j_k}]$ ,  $a_i \in A$ , то разность  $a_i - a_t$  называется *разностью класса*  $j_i, j_t$ <sup>1</sup>); при этом  $a_i - a_t$  называется *чистой* разностью, если  $j_i = j_t$ , и *смешанной* разностью, если  $j_i \neq j_t$ . Условия, о которых шла речь, можно описать в терминах чистых и смешанных разностей.

**Теорема 15.3.1.** Пусть даны аддитивная абелева группа  $A$  порядка  $m$  и множество  $\{B\}$  блоков из элементов группы  $A$ , снабженных индексами

$$B = [(a_1)_{j_1}, (a_2)_{j_2}, \dots, (a_k)_{j_k}], \quad a_i \in A.$$

Множество  $\{B\}$  будет базой для схемы  $D(v, b, r, k, \lambda)$ , имеющей  $A$  в качестве группы автоморфизмов, если:  
 1) каждый блок из  $\{B\}$  содержит  $k$  элементов; 2) при действии элементами из  $A$  получается  $b$  блоков; 3) при действии элементами из  $A$  каждый элемент  $(y)_1$  появляется  $r$  раз; 4) в блоках множества  $\{B\}$ , взятых вместе, каждая ненулевая чистая и каждая смешанная разности появляются  $\lambda$  раз. При этом если какой-либо из блоков множества  $\{B\}$  инвариантен относительно подгруппы порядка  $w$  группы  $A$ , то общее число разностей, получающихся из него, следует разделить на  $w$ .

**Доказательство.** Пусть  $y \in A$ . Если  $(a_i)_{j_i}$  и  $(a_t)_{j_t}$  принадлежат  $B$ , то  $(a_i + y)_{j_t}$  и  $(a_t + y)_{j_t}$  принадлежат  $(B)y$ . Следовательно,  $(x)_{j_i}$  и  $(z)_{j_t}$  принадлежат блоку  $(B)y$  тогда и только тогда, когда  $x - z = a_i - a_t$ , где  $y$  определено равенством  $x = a_i + y$  или  $z = a_t + y$  и  $(a_i)_{j_i}$  и  $(a_t)_{j_t}$  принадлежат  $B = (B)0$ . Если  $B$  фиксирован подгруппой порядка  $w$ , то, когда  $y$  пробегает  $A$ , блоки  $(B)y$  проходят одно и то же множество из  $m/w$  блоков, каждый блок  $w$  раз, и потому для подсчета пар элементов, встречающихся в этих  $m/w$  блоках, число разностей, получаемых из  $B$ , нужно разделить на  $w$ . Эту последнюю ситуацию можно проиллюстрировать на примере

<sup>1</sup>) Классы  $j_i, j_t$  и  $j_t, j_i$  не различаются. — Прим. ред.

в (15.3.2), где блок  $(0, 5, 10)$  третьей орбиты можно отнести к базе; мы имеем  $w = 3$ , и любая из разностей  $5, 10$  появляется как разность элементов из  $B = (0, 5, 10)$  три раза. Для фиксированного элемента  $(\infty)_i$  следует считать, что пара  $(\infty)_i$  и  $(u)_j$  дает каждую смешанную разность класса  $i, j$  один раз.

**Теорема 15.3.2.** *Если  $A$  – аддитивная группа классов вычетов по модулю  $m = 2t + 1$ , то блоки*

$$\begin{aligned} & [1_1, 2t_1, 0_2], \dots, [i_1, (2t+1-i)_1, 0_2], \dots, [t_1, (t+1)_1, 0_2], \\ & [1_2, 2t_2, 0_3], \dots, [i_2, (2t+1-i)_2, 0_3], \dots, [t_2, (t+1)_2, 0_3], \\ & [1_3, 2t_3, 0_1], \dots, [i_3, (2t+1-i)_3, 0_1], \dots, [t_3, (t+1)_3, 0_1], \\ & \quad [0_1, 0_2, 0_3] \end{aligned} \tag{15.3.3}$$

образуют базу для схемы с параметрами  $v = 6t + 3$ ,  $b = (3t+1)(2t+1)$ ,  $r = 3t+1$ ,  $k = 3$ ,  $\lambda = 1$ .

**Доказательство.** Условия (1) – (3) теоремы 15.3.1 выполняются тривиально. Все нулевые смешанные разности появляются в блоке  $[0_1, 0_2, 0_3]$ . Общий вид блока в первых трех строках (15.3.3):  $[x_j, y_j, 0_{j+1}]$ , где  $x+y = 2t+1$  и  $j \equiv 1, 2, 3 \pmod{3}$ . Чтобы получить чистую разность  $d \not\equiv 0 \pmod{2t+1}$  класса  $j$ , нам необходимо иметь  $x-y \equiv d \pmod{2t+1}$ . Поскольку  $x+y \equiv 0 \pmod{2t+1}$ , это дает  $2x \equiv d \pmod{2t+1}$ . Поэтому  $x$  и  $y$  определяются однозначно. Первая строка дает каждую ненулевую смешанную разность класса 1, 2 точно один раз. Аналогично другие две строки дают каждую ненулевую смешанную разность классов 2, 3 и 1, 3. Таким образом, все условия теоремы 15.3.1 удовлетворяются, и блоки (15.3.3) образуют базу схемы, что и требовалось доказать. Схема из (15.3.1) дает пример доказанной теоремы с  $2t+1 = 5$ .

**Теорема 15.3.3.** *Пусть  $v = 6t + 3 = 3m$ , где  $m = 2t + 1 \not\equiv 0 \pmod{3}$ . Определим неупорядоченные пары  $(r, s)$  по модулю  $3m$  условиями  $r \equiv s \equiv 1 \pmod{3}$ ,  $r+s \equiv 0 \pmod{m}$ ,  $r, s \not\equiv 0 \pmod{m}$ . Тогда блоки*

$$[0, r, s] \pmod{3m} \tag{15.3.4}$$

вместе с блоком  $[0, m, 2m]$  периода  $m$  образуют базу схемы с параметрами  $v = 6t + 3$ ,  $b = (2t + 1)(3t + 1)$ ,  $r = 3t + 1$ ,  $k = 3$ ,  $\lambda = 1$ .

**Доказательство.** Так как  $v = 3m$ , все элементы находятся на одной орбите, и поэтому все разности являются чистыми. Рассмотрим сначала представление в виде разности для  $d \equiv 0 \pmod{3}$ ,  $d \not\equiv 0 \pmod{m}$ . Тогда из сравнений  $r - s \equiv d \pmod{3m}$ ,  $r + s \equiv 0 \pmod{m}$ ,  $r = s \equiv 1 \pmod{3}$  следует, что  $2r \equiv d \pmod{m}$ ,  $r \equiv 1 \pmod{3}$ ; тем самым  $r$ , а затем и  $s$  определяются по модулю  $3m$  однозначно. Если  $d \equiv 1 \pmod{3}$ ,  $d \not\equiv 0 \pmod{m}$ , то сравнение  $r - 0 \equiv d \pmod{3m}$  определяет  $r$  однозначно; тогда  $s$  также однозначно определяется сравнениями  $s \equiv 1 \pmod{3}$ ,  $r + s \equiv 0 \pmod{m}$ . Если  $d \equiv -1 \pmod{3}$ ,  $d \equiv 0 \pmod{m}$ , то  $0 - r \equiv d \pmod{3m}$  однозначно определяет  $r$ , а тем самым и  $s$ :

$$s \equiv 1 \pmod{3}, \quad r + s \equiv 0 \pmod{m}.$$

Остаются вычеты  $m$  и  $2m$ , каждый из которых появляется трижды как разность элементов блока  $[0, m, 2m]$ ; поскольку этот блок фиксирован подгруппой порядка 3, порожденной  $i \rightarrow i + m \pmod{3m}$ , число разностей для этого блока следует разделить на три, что и доказывает теорему. Пример (15.3.2) — частный случай этой теоремы при  $3m = 15$ .

В следующей теореме мы потребуем, чтобы  $v = p^n$ , где  $p$  — простое число. В качестве группы автоморфизмов  $A$  возьмем аддитивную группу конечного поля  $GF(p^n)$ .

**Теорема 15.3.4.** Пусть  $v = 6t + 1 = p^n$ , где  $p$  — простое число, и  $x$  — примитивный корень поля  $GF(p^n)$ . Тогда блоки

$$(x^0, x^{2t}, x^{4t}), \dots, (x^i, x^{2t+i}, x^{4t+i}), \dots, (x^{t-1}, x^{3t-1}, x^{5t-1}) \tag{15.3.5}$$

образуют базу схемы  $D$  с параметрами  $v = 6t + 1$ ,  $b = 6t^2 + t$ ,  $r = 3t$ ,  $k = 3$ ,  $\lambda = 1$  и группой автоморфизмов  $A$  — аддитивной группой поля  $GF(p^n)$ .

**Доказательство.** Имеем  $x^{6t} = 1$ ,

$$(x^{3t} - 1)(x^{3t} + 1) = 0.$$

Так как  $x$  — примитивный корень  $\text{GF}(p^n)$ ,  $x^{3t} \neq 1$  и  $x^{3t} + 1 = 0$ . Поскольку  $x^{2t} - 1 \neq 0$ , определим  $s$  равенством  $x^{2t} - 1 = x^s$ . Далее, образуем шесть разностей для элементов блока  $(x^0, x^{2t}, x^{4t})$ ;  $\pm(x^{2t} - 1)$ ,  $\pm(x^{4t} - 1)$ ,  $\pm(x^{4t} - x^{2t})$ . Поскольку  $-1 = x^{3t}$ , имеем

$$\begin{aligned} -(x^{2t} - 1) &= x^{s+3t}, \\ x^{s+4t} &= x^{4t}(x^{2t} - 1) = 1 - x^{4t} = -(x^{4t} - 1). \end{aligned}$$

Следовательно, эти шесть разностей будут  $x^s$ ,  $x^{s+4t}$ ,  $x^{s+2t}$ ,  $x^{s+3t}$ ,  $x^{s+4t}$ ,  $x^{s+5t}$ . Тогда разности элементов любых блоков базы — это

$$\begin{aligned} x^{s+i}, \quad x^{s+i+t}, \quad x^{s+i+2t}, \quad x^{s+i+3t}, \quad x^{s+i+4t}, \quad x^{s+i+5t}, \\ i = 0, 1, \dots, t-1, \end{aligned} \quad (15.3.6)$$

т. е. все  $x^j$ ,  $j = 0, \dots, 6t-1$ . Таким образом, каждый ненулевой элемент аддитивной группы  $A$  поля  $\text{GF}(p^n)$  представляется как разность двух элементов какого-либо из блоков базы, и теорема доказана.

**Теорема 15.3.5.** Если  $v = p^n = 12t + 1$ , где  $p$  — простое число, и если  $x$  — примитивный корень поля  $\text{GF}(p^n)$ , такой, что  $x^{4t} - 1 = x^q$  с нечетным  $q$ , то блоки

$$\begin{aligned} (0, x^0, x^{4t}, x^{8t}), \dots, (0, x^{2i}, x^{2i+4t}, x^{2i+8t}), \dots \\ \dots, (0, x^{2t-2}, x^{6t-2}, x^{10t-2}) \end{aligned} \quad (15.3.7)$$

образуют базу относительно группы  $A$ , аддитивной группы поля  $\text{GF}(p^n)$ , для схемы  $D$  с параметрами

$$v = 12t + 1, \quad b = t(12t + 1), \quad r = 4t, \quad k = 4, \quad \lambda = 1.$$

**Доказательство.** Замечая, что

$$x^{6t} = -1, \quad x^{4t} - 1 = x^q \quad \text{и} \quad x^{8t+q} = x^{8t}(x^{4t} - 1) = 1 - x^{8t},$$

имеем двенадцать разностей элементов первого блока

$$\begin{aligned} x^0, \quad x^{6t}, \quad x^{4t}, \quad x^{10t}, \quad x^{8t}, \quad x^{2t}, \quad x^q, \quad x^{q+6t}, \\ x^{q+2t}, \quad x^{q+8t}, \quad x^{q+4t}, \quad x^{q+10t}. \end{aligned} \quad (15.3.8)$$

Разности элементов других блоков получаются умножением этих разностей на  $x^{2i}$ ,  $i = 1, \dots, t - 1$ . Если  $q$  нечетно, то мы получаем каждую ненулевую разность в  $\text{GF}(p^n)$  точно один раз, и теорема доказана.

**Теорема 15.3.6.** Пусть  $4t + 1 = p^n$ , где  $p$  — простое число, и  $x$  — примитивный корень поля  $\text{GF}(p^n)$ . Тогда существует пара нечетных целых чисел  $c, d$ , таких, что  $(x^c + 1)/(x^c - 1) = x^d$ . Для этих  $c$  и  $d$  блоки

$$\begin{aligned} & (x_1^{2t}, x_1^{2t+2t}, x_2^{2t+c}, x_2^{2t+2t+c}), \\ & (x_2^{2t}, x_2^{2t+2t}, x_3^{2t+c}, x_3^{2t+2t+c}), \\ & (x_3^{2t}, x_3^{2t+2t}, x_1^{2t+c}, x_1^{2t+2t+c}), \quad i = 0, \dots, t - 1, \\ & (\infty, 0_1, 0_2, 0_3) \end{aligned} \quad (15.3.9)$$

образуют базу относительно группы  $A$ , аддитивной группы поля  $\text{GF}(p^n)$ , для схемы с параметрами

$$v = 12t + 4, \quad b = (3t + 1)(4t + 1), \quad r = 4t + 1, \quad k = 4, \quad \lambda = 1.$$

**Доказательство.** Так как  $x$  — примитивный корень поля  $\text{GF}(p^n)$ , то  $x^{2t} = -1$ . Следовательно, при  $c \neq 0$ ,  $2t, 0 < c \leq 4t - 1$ , имеем  $x^c + 1 \neq 0$  и  $x^c - 1 \neq 0$ , поэтому  $(x^c + 1)/(x^c - 1) = x^d$  при некотором  $d$ , которое определяется однозначно через  $c$ . Среди  $4t - 2$  значений  $c$ :  $1, \dots, 2t - 1, 2t + 1, \dots, 4t - 1$  имеется  $2t - 2$  четных и  $2t$  нечетных. Далее,  $x^d \neq \pm 1$ , так как в противном случае  $x^c + 1 = \pm(x^c - 1)$ , откуда либо  $2 = 0$ , либо  $2x^c = 0$ , что противоречит нечетности  $p$ . Следовательно,  $d \neq 0, 2t$ ,

$$0 < d \leq 4t - 1,$$

и  $d$  принимает  $2t - 2$  четных и  $2t$  нечетных значений. Следовательно, по меньшей мере для двух нечетных значений  $c$  имеем  $d$  также нечетное.

Последний блок дает все смешанные разности фиксированного элемента  $\infty$  с элементами других трех классов, а также нулевые смешанные разности для трех возможных пар. Так как  $x^{2t} = -1$ , чистые разности первого класса, которые даются первой и третьей строками, равны  $\pm 2x^{2i}$  и  $\pm 2x^{2t+c}$ ,  $i = 0, \dots, t$ , или  $2x^{2i}, 2x^{2t+2i}, 2x^{2t+c}, 2x^{2t+c+2t}$ . Поскольку  $c$  нечетно, тем

самым получаются все ненулевые чистые разности первого класса. Совершенно аналогично получаем ненулевые чистые разности второго и третьего классов. Для смешанных разностей класса 2,1 (принимая во внимание, что  $x^{2t} = -1$ ) имеем

$$\begin{aligned} x^{2i}(x^c - 1), \quad x^{2i}(x^c + 1), \quad x^{2i+2t}(x^c + 1), \\ x^{2i+2t}(x^c - 1). \end{aligned} \quad (15.3.10)$$

Так как  $x^c + 1 = x^d(x^c - 1)$ , эти разности принимают вид  $(x^c - 1)x^{2i}$ ,  $(x^c - 1)x^{2i+d}$ ,  $(x^c - 1)x^{2i+d+2t}$ ,

$$(x^c - 1)x^{2i+2t}, \quad i = 0, \dots, t-1. \quad (15.3.11)$$

Но так как  $d$  нечетно, эти разности пробегают все ненулевые элементы поля  $GF(p^n)$ , каждый точно по одному разу. Эти же аргументы применимы к другим смешанным разностям, и теорема доказана.

Мы перечислим еще некоторые базы для схем, основанных на конечных полях  $GF(p^n)$ . В каждом случае  $x$  — примитивный корень, и, если нужно, указываются дополнительные условия. Доказательство в каждом случае по существу то же самое, что и в предыдущих теоремах:

$$v = 20t + 1 = p^n, \quad b = t(20t + 1), \quad r = 5t, \quad k = 5, \quad \lambda = 1, \\ x^{4t} + 1 = x^q, \quad q \text{ нечетно}, \quad (15.3.12)$$

$$(x^{2i}, \quad x^{4t+2i}, \quad x^{8t+2i}, \quad x^{12t+2i}, \quad x^{16t+2i}), \quad i = 0, \dots, t-1.$$

$$v = 20t + 5, \quad b = (5t + 1)(4t + 1), \quad r = 5t + 1, \quad k = 5, \quad \lambda = 1,$$

$$4t + 1 = p^n, \quad \frac{x^c + 1}{x^c - 1} = x^d, \quad c, d \text{ оба нечетны},$$

$$\begin{aligned} & (x_1^{2i}, \quad x_1^{2i+2t}, \quad x_3^{2i+c}, \quad x_3^{2i+c+2t}, \quad 0_2), \\ & (x_2^{2i}, \quad x_2^{2i+2t}, \quad x_4^{2i+c}, \quad x_4^{2i+c+2t}, \quad 0_3), \\ & (x_3^{2i}, \quad x_3^{2i+2t}, \quad x_5^{2i+c}, \quad x_5^{2i+c+2t}, \quad 0_4), \end{aligned} \quad (15.3.13)$$

$$\cdots (x_4^{2i}, \quad x_4^{2i+2t}, \quad x_1^{2i+c}, \quad x_1^{2i+c+2t}, \quad 0_5),$$

$$(x_5^{2i}, \quad x_5^{2i+2t}, \quad x_2^{2i+c}, \quad x_2^{2i+c+2t}, \quad 0_1),$$

$$(0_1, \quad 0_2, \quad 0_3, \quad 0_4, \quad 0_5),$$

$$i = 0, 1, \dots, t-1.$$

$$v = 6t + 1 = p^n, \quad b = t(6t + 1), \quad r = 4t, \quad k = 4, \quad \lambda = 2, \\ (0, \quad x^i, \quad x^{2t+i}, \quad x^{4t+i}), \quad i = 0, \dots, t-1. \quad (15.3.14)$$

$$v = 4t + 1 = p^n, \quad b = t(4t + 1), \quad r = 4t, \quad k = 4, \quad \lambda = 3, \\ (x^i, \quad x^{t+i}, \quad x^{2t+i}, \quad x^{3t+i}), \quad i = 0, \dots, t-1. \quad (15.3.15)$$

$$v = p^n > k, \quad b = (p^n - 1)p^n, \quad r = k(p^n - 1), \\ k = k, \quad \lambda = k(k-1), \quad (15.3.16) \\ (x^i, \quad x^{i+1}, \dots, \quad x^{i+k-1}), \quad i = 0, \dots, p^n - 2.$$

$$v = 6t + 6, \quad b = 2(t+1)(6t+5), \quad r = 6t + 5, \quad k = 3, \quad \lambda = 2, \\ A - \text{аддитивная группа классов} \quad \text{вычетов по модулю } 6t + 5,$$

$$(\infty, \quad 0, \quad 3t + 2), \\ (0, \quad i, \quad 2t + 3 - i), \quad i = 1, \dots, t+1, \quad (15.3.17) \\ (0, \quad 2i, \quad 3t + 3 + i), \quad i = 1, \dots, t.$$

$$v = 6t + 4, \quad b = 2(2t+1)(3t+2), \quad r = 6t + 3, \quad k = 3, \quad \lambda = 2, \\ A - \text{аддитивная группа классов} \quad \text{вычетов по модулю } 6t + 3,$$

$$(\infty, \quad 0, \quad 3t + 1), \\ (0, \quad i, \quad 2t + 1 - i), \quad i = 1, \dots, t, \\ (0, \quad 2i, \quad 3t + 1 + i), \quad i = 1, \dots, t, \quad (15.3.18) \\ (0, \quad 2t + 1, \quad 4t + 2) \text{ периода } 2t + 1.$$

## 15.4. Системы троек

Блок-схема с  $k = 3$  вполне естественно называется системой троек. Параметры схемы  $D(v, b, r, 3, \lambda)$  должны удовлетворять условиям

$$3b = rv, \quad 2r = \lambda(v - 1). \quad (15.4.1)$$

Выразим отсюда  $r$  и  $b$  через остальные параметры:

$$r = \frac{\lambda(v-1)}{2}, \quad b = \frac{\lambda v(v-1)}{6}. \quad (15.4.2)$$

Для целочисленности  $r$  и  $b$  необходимо, чтобы выполнялись следующие сравнения:

$$\lambda(v - 1) \equiv 0 \pmod{2}, \quad \lambda v(v - 1) \equiv 0 \pmod{6}. \quad (15.4.3)$$

Основным результатом этого раздела будет доказательство того, что эти необходимые условия на параметры являются также достаточными для существования таких схем. Это будет доказано при помощи рекурсивных методов Ханани.

Система троек с  $\lambda = 1$  называется *системой троек Штейнера*. Условие  $v \equiv 1, 3 \pmod{6}$  необходимо для существования штейнеровой системы троек. Штейнер [1] в 1853 г. поставил задачу: являются ли эти необходимые условия также и достаточными для ее существования. Положительный ответ был дан Райссом [1] в 1859 г. Обе работы появились в журнале Крелля<sup>1)</sup>. Эти авторы не знали, что эта проблема была поставлена и решена Киркманом [1] в 1847 г. в статье, помещенной в Кембриджском и Дублинском математическом журнале (Cambridge and Dublin Mathematical Journal); более того, до недавнего времени о работе Киркмана, по-видимому, не знал никто.

Системы троек Штейнера порядков  $v = 3, 7, 9$  единственны с точностью до эквивалентности (при этом две системы считаются эквивалентными, если одна из них может быть получена из другой подстановкой на элементах и перестановкой блоков):

| $v = 3$ | $v = 7$ | $v = 9$         |          |
|---------|---------|-----------------|----------|
| 1 2 3   | 123 246 | 123             | (15.4.4) |
|         | 145 257 | 145 249 348     |          |
|         | 167 347 | 168 256 357 467 |          |
|         | 356     | 179 278 369 589 |          |

Для  $v = 13$  существует точно две неизоморфных штейнеровых системы троек. В обе системы мы можем вклю-

<sup>1)</sup> J. reine u. angew. Math. См. библиографию в конце книги.—  
Прим. перев.

чить тройки

$$\begin{aligned}
 & 1, 2, 3, 2, 4, 6 \\
 & 1, 4, 5, 2, 5, 7, 4, 3, 8, 7, 3, 11, \\
 & 1, 6, 7, 2, 8, 10, 4, 7, 9, 7, 8, 13, 8, 5, 11, 6, 9, 11, \\
 & 1, 8, 9, 2, 9, 12, 4, 10, 13, 7, 10, 12, 8, 6, 12, 3, 5, 12, \\
 & 1, 10, 11, 2, 11, 13, 4, 11, 12, \\
 & 1, 12, 13,
 \end{aligned} \tag{15.4.5}$$

В первом случае мы добавим к этим следующие тройки:

$$\begin{aligned}
 & 3, 6, 10, 5, 6, 13, \\
 & 3, 9, 13, 5, 9, 10.
 \end{aligned} \tag{15.4.6}$$

Во втором:

$$\begin{aligned}
 & 3, 6, 13, 5, 6, 10, \\
 & 3, 9, 10, 5, 9, 13.
 \end{aligned} \tag{15.4.7}$$

Коул, Уайт и Каммингс [1] нашли 80 различных систем троек Штейнера для  $v = 15$ . Фишер [1] перечислил системы из 15 букв, найдя 79 систем и пропустив одну из списка Коула. Автор этой книги и Свифт (Холл, Свифт [1]) провели систематическое исследование и подтвердили правильность перечня Коула.

*Теорема 15.4.1. Если существуют системы троек Штейнера порядков  $v_1$  и  $v_2$ , то существует система троек Штейнера порядка  $v = v_1 v_2$ , содержащая подсистемы, изоморфные системам порядков  $v_1$  и  $v_2$ .*

*Доказательство.* Пусть  $A = S(v_1)$  и  $B = S(v_2)$  — системы троек Штейнера порядков  $v_1$  и  $v_2$  соответственно, и пусть  $(a_i, a_j, a_k)$  — произвольная тройка из  $A$ , а  $(b_r, b_s, b_u)$  — произвольная тройка из  $B$ . Образуем новую систему  $C$  с элементами  $c_{ij}$ ,  $i = 1, \dots, v_1$ ,  $j = 1, \dots, v_2$ . Тройка  $(c_{ir}, c_{js}, c_{ku})$  принадлежит системе  $C$  в том и только том случае, когда выполнено одно из следующих трех условий: 1)  $r = s = u$  и  $(a_i, a_j, a_k)$  — тройка из  $A$ ; 2)  $i = j = k$  и  $(b_r, b_s, b_u)$  — тройка из  $B$ ; 3)  $(a_i, a_j, a_k)$  — тройка из  $A$  и  $(b_r, b_s, b_u)$  — тройка из  $B$ . Легко убедиться, что  $C$  есть система троек Штейнера.

Тройки с  $r = s = u = 1$  образуют подсистему в  $C$ , изоморфную системе  $A$ , а тройки с  $i = j = k = 1$  образуют подсистему, изоморфную системе  $B$ . Таким образом, теорема доказана.

Существует и другое доказательство.

Из системы троек Штейнера  $S$  образуем квазигруппу  $S^*$  следующим образом. За элементы  $S^*$  возьмем элементы  $S$ . Произведение  $xy$  определим правилами:

1)  $xx = x$  для всех  $x \in S^*$ , 2)  $xy = z$ , если  $x \neq y$  и  $(x, y, z)$  — тройка из  $S$ . Квазигруппу  $S^*$  можно охарактеризовать следующими свойствами: а)  $x^2 = x$  (идемпотентность), б)  $yx = xy$  (коммутативность) и в) из  $xy = z$  следует, что  $yz = x$ . Такая квазигруппа определяет систему троек Штейнера. Если теперь  $S_1^*$  и  $S_2^*$  — штейнеровы квазигруппы с  $v_1$  и  $v_2$  элементами соответственно, то можно определить новую систему  $S^*$ , элементы которой — упорядоченные пары  $(x_1, x_2)$ ,  $x_1 \in S_1^*$ ,  $x_2 \in S_2^*$ , а правило умножения таково:  $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$ . Тогда  $S^*$  имеет те же свойства, что  $S_1^*$  и  $S_2^*$ , и определяет систему троек Штейнера  $S$  на  $v_1v_2$  элементах.

Рекурсивный метод построения систем троек Штейнера, принадлежащий Муру [1], состоит в следующем.

**Теорема 15.4.2.** *Если существует система троек Штейнера порядка  $v_2$ , содержащая подсистему порядка  $v_3$  (или если  $v_3 = 1$ ), то мы можем построить систему порядка  $v = v_3 + v_1(v_2 - v_3)$ , содержащую  $v_1$  подсистем порядка  $v_2$  и по одной подсистеме порядков  $v_1$  и  $v_3$  соответственно.*

**Доказательство.** Построим таблицу из  $v = v_3 + v_1(v_2 - v_3)$  элементов, принадлежащих следующим  $v_1 + 1$  множествам:

$$\begin{aligned}
 S_0: & a_1 \quad a_2 \quad \dots \quad a_{v_3}, \\
 S_1: & b_{11} \quad \dots \quad \dots \quad b_{1s}, \\
 S_2: & b_{21} \quad \dots \quad \dots \quad b_{2s}, \quad s = v_2 - v_3. \quad (15.4.8) \\
 & \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
 S_{v_1}: & b_{v_11} \quad \dots \quad \dots \quad b_{v_1s},
 \end{aligned}$$

Образуем на этих  $v$  элементах систему троек  $S$  по следующим правилам:

1. Пусть на элементах множества  $S_0$  задана система порядка  $v_3$ ; полагаем  $(a_i, a_j, a_k) \in S$ , если  $a_i, a_j, a_k$  образуют тройку в указанной системе.

2. Пусть для каждого  $i$  на множествах  $S_0$  и  $S_i$  ( $i = 1, \dots, v_1$ ), взятых вместе, построена система порядка  $v_2$ , причем подсистема  $S_0$  определена, как в правиле 1. Тройки, не принадлежащие  $S_0$ , содержат не более одного  $a_i$  и имеют вид  $(a_m, b_{ij}, b_{ik})$ ,  $(b_{ij}, b_{ik}, b_{ir})$ ; отнесем к  $S$  все такие тройки.

3. Определим систему порядка  $v_1$  на числах  $1, \dots, v_1$ ; если  $(j, k, r)$  — тройка этой системы, то отнесем к  $S$  все тройки  $(b_{jx}, b_{ky}, b_{rz})$  для индексов  $x, y, z$ , удовлетворяющих сравнению  $x + y + z \equiv 0 \pmod{s}$ .

По первому правилу получаем тройки из  $S_0$ ; замечаем, что тройка, содержащая элементы  $a_i, a_{l_1}$ , в качестве третьего элемента содержит также элемент из  $S_0$ . По второму правилу получаем тройки, содержащие некоторое  $a_m$  и некоторое  $b_{ij}$ , а третьим элементом  $b_{ik}$  — другой элемент в той же самой строке, а также все тройки, содержащие два элемента  $b_{ij}, b_{ik}$  из одной строки; третьим элементом они будут иметь либо некоторое  $a_m$ , либо элемент из той же самой строки. Для элементов  $b_{jx}, b_{ky}$  из разных строк мы определяем  $r$  из тройки  $(j, k, r)$  в системе с  $v_1$  элементами, а  $z$  из сравнения  $x + y + z \equiv 0 \pmod{s}$ . Таким образом, любая пара из  $v = v_3 + v_1(v_2 - v_3)$  элементов определяет в  $S$  единственную тройку, содержащую ее. Тройки из  $S_0$  образуют подсистему порядка  $v_3$ , тройки из  $S_0 \cup S_i$  образуют подсистемы порядка  $v_2$ ,  $i = 1, \dots, v_1$ , а тройки из элементов  $b_{1s}, b_{2s}, \dots, b_{v_1 s}$  — подсистему порядка  $v_1$ . В каждом случае подсистемы изоморфны заданным подсистемам. Доказательство теоремы завершено.

Мы можем использовать эту рекурсивную теорему для построения систем троек Штейнера всех порядков  $v$  вида  $v = 6t + 1$ ,  $v = 6t + 3$ . Тем самым будет показано, что необходимое условие существования штейнеровых систем троек будет также достаточным.

**Теорема 15.4.3.** Если  $v = 6t + 1$  или  $v = 6t + 3$ , то существует система троек Штейнера порядка  $v$ .

**Доказательство.** Мы используем несколько частных случаев теоремы 15.4.2. Приведем их в виде рекурсивных правил:

- (A)  $v_1 = v'$ ,  $v_2 = 3$ ,  $v_3 = 1$ ,  $v = 2v' + 1$ ,  $v' \geq 3$ .
- (B)  $v_1 = 3$ ,  $v_2 = v'$ ,  $v_3 = 1$ ,  $v = 3v' - 2$ ,  $v' \geq 3$ .
- (C)  $v_1 = 3$ ,  $v_2 = v'$ ,  $v_3 = 3$ ,  $v = 3v' - 6$ ,  $v' \geq 7$ .
- (D)  $v_1 = v'$ ,  $v_2 = 9$ ,  $v_3 = 3$ ,  $v = 6v' + 3$ ,  $v' \geq 3$ .
- (E)  $v_1 = 3$ ,  $v_2 = v'$ ,  $v_3 = 7$ ,  $v = 3v' - 14$ ,  $v' \geq 15$ .
- (F)  $v_1 = v'$ ,  $v_2 = 7$ ,  $v_3 = 1$ ,  $v = 6v' + 1$ ,  $v' \geq 3$ .

Заметим, что всякий раз, когда мы имеем систему порядка  $v'$ , мы можем использовать любое из приведенных правил, за исключением правила Е, где система порядка  $v'$  должна иметь подсистему порядка 7. Так как система порядка  $v = v_3 + v_1(v_2 - v_3)$  имеет подсистемы порядков  $v_1$ ,  $v_2$ ,  $v_3$ , изоморфные подсистемам, используемым при ее построении, свойство иметь подсистему порядка 7 переносится при построении на системы большего порядка. Мы будем строить системы рекурсивно, используя то или иное из перечисленных выше правил в зависимости от значения  $v$  по модулю 36, как показано в табл. 15.1.

В некоторых случаях можно пользоваться и другими правилами, и мы всегда будем предпочитать правило, которое гарантирует существование подсистемы порядка 7. Построение с помощью правила F всегда дает систему с подсистемой порядка 7. Мы можем, конечно, использовать также теорему 15.4.1; в частности, при  $v = 3v'$  систему троек порядка 3 можно применить для построения систем с параметрами

$$\begin{aligned} 36t + 3 &= 3(12t + 1), \\ 36t + 9 &= 3(12t + 3), \\ 36t + 21 &= 3(12t + 7), \\ 36t + 27 &= 3(12t + 9). \end{aligned} \tag{15.4.9}$$

**Таблица 15.1**  
**Подсистемы систем порядка  $v$**

| Вид $v$    | Правило | Значение $v'$ |
|------------|---------|---------------|
| $36t + 1$  | (B)     | $12t + 1$     |
| $36t + 3$  | (A)     | $18t + 1$     |
| $36t + 7$  | (F)     | $6t + 1$      |
| $36t + 9$  | (D)     | $6t + 1$      |
| $36t + 13$ | (E)     | $12t + 9$     |
| $36t + 15$ | (A)     | $18t + 7$     |
| $36t + 19$ | (F)     | $6t + 3$      |
| $36t + 21$ | (D)     | $6t + 3$      |
| $36t + 25$ | (B)     | $12t + 9$     |
| $36t + 27$ | (A)     | $18t + 13$    |
| $36t + 31$ | (A)     | $18t + 15$    |
| $36t + 33$ | (C)     | $12t + 13$    |

Используя эти и некоторые другие следствия теорем 15.4.1 и 15.4.2, мы можем найти системы троек Штейнера для всех порядков  $v$  вида  $v = 6t + 1$  или  $6t + 3$ , причем всегда найдется система порядка  $v$ , содержащая подсистему порядка 7, за исключением значений  $v = 1, 3, 9, 13, 25, 27, 33, 37, 67, 69, 75, 81, 97, 109, 201, 289, 321$ . Может случиться, что другое представление числа  $v$ , а не то, что дается табл. 15.1, позволяет построить системы порядка  $v$  с подсистемой порядка 7. Поэтому полезна следующая таблица:

**Таблица 15.2**  
**Подсистемы порядка 7**

| Вид $v$    | Правило | Значение $v'$ |
|------------|---------|---------------|
| $36t + 3$  | (C)     | $12t + 3$     |
| $36t + 15$ | (C)     | $12t + 7$     |
| $36t + 21$ | (C)     | $12t + 9$     |
| $36t + 25$ | (E)     | $12t + 13$    |
| $36t + 31$ | (E)     | $12t + 15$    |

Необходимо также дополнить общие правила таблиц 15.1, 15.2 и (15.4.9) следующими частными случаями порядков вида  $v = v_1v_2$  или  $v = v_3 + v_1(v_2 - v_3)$ , где соответственно применяются теоремы 15.4.1 или 15.4.2:

$$\begin{aligned}
 49 &= 7^2, & 229 &= 1 + 19(13 - 1), \\
 73 &= 3 + 7(13 - 3), & 285 &= 15 \cdot 19, \\
 85 &= 1 + 7(13 - 1), & 325 &= 3 + 7(49 - 3), \\
 103 &= 3 + 25(7 - 3), & 589 &= 19 \cdot 31, \\
 105 &= 7 \cdot 15, & 861 &= 7 \cdot 123 \\
 193 &= 3 + 19(13 - 3), & 865 &= 7 + 13(73 - 7), \\
 195 &= 13 \cdot 15, & 949 &= 13 \cdot 73, \\
 225 &= 15^2, & 961 &= 31^2.
 \end{aligned} \tag{15.4.10}$$

Если исходим из начальных систем троек Штейнера  $S(v)$  порядка  $v$ , где  $v = 3, 7, 9, 13$ , приведенных в (15.4.4)–(15.4.7), то по правилам табл. 15.1 мы получаем из них индуктивно системы для всех значений  $v$  вида  $6t + 1$  или  $6t + 3$ , если только в каждом случае, когда применяется правило Е, мы исходим из  $S(v')$ , содержащей  $S(7)$ . Характер наших построений в теоремах 15.4.1 и 15.4.2 таков, что свойство содержать  $S(7)$  является наследственным, т. е. если  $S(v_1)$ ,  $S(v_2)$  или  $S(v_3)$  содержат  $S(7)$ , то и  $S(v)$ , где  $v = v_1v_2$  или  $v = v_3 + v_1(v_2 - v_3)$ , содержит  $S(7)$ . Применение правила F всегда дает  $S(v)$ , содержащую  $S(7)$ . Скажем, что значение  $v$  обладает „здоровой наследственностью“, если существует  $S(v)$ , содержащая  $S(7)$ , и „незддоровой наследственностью“, если не существует  $S(v)$ , содержащей  $S(7)$ . Наша теорема будет доказана, если мы сможем показать, что  $v$  с „незддоровой наследственностью“ исчерпываются значениями 1, 3, 9, 13, 25, 27, 33, 37, 67, 69, 75, 81, 97, 109, 201, 289, 321<sup>1)</sup>, а все другие числа вида  $6t + 1$  или  $6t + 3$  обладают „здоровой наследственностью“. Очевидно, значение  $v$  с „незддоровой наследственностью“ можно получить лишь в случае применения одного из правил А, ..., Е к  $v'$  с тем же свойством. Но для всех чисел  $v$ , не принадлежащих приведенному выше списку, суще-

<sup>1)</sup> Очевидно, для всех этих чисел  $v$  системы троек Штейнера порядка  $v$  существуют. — Прим. ред.

ствуют другие представления, которые получаются либо из табл. 15.2, либо из равенств (15.4.9) или (15.4.10). Например, если  $v' = 321$ , то мы имеем:

- (A)  $2 \cdot 321 + 1 = 643 = 3 \cdot 219 - 14$ ,
  - (B)  $3 \cdot 321 - 2 = 961 = 31^2$ ,
  - (C)  $3 \cdot 321 - 6 = 957 = 3 \cdot 319$ ,
  - (D)  $6 \cdot 321 + 3 = 1929 = 3 \cdot 643$ ,
  - (E)  $3 \cdot 321 - 14 = 949 = 13 \cdot 73$ ,
- (15.4.11)

и ввиду существования представлений, написанных справа, все „преемники“ числа 321 обладают „здоровой наследственностью“. Тем самым теорема доказана.

Эту теорему можно было бы доказать непосредственным построением систем троек Штейнера порядков 25, 27, 33 и 37, содержащих  $S(7)$ .

Киркман поставил следующую задачу о системах троек, общее решение которой неизвестно, во всяком случае, автору книги. Это так называемая „задача Киркмана о школьницах“. В первоначальной задаче требовалось составить расписание прогулок для 15 школьниц. Девушки ежедневно должны гулять пятью группами, по три в каждой группе. Задача состоит в том, чтобы построить расписание прогулок так, чтобы каждая девушка смогла в течение семи дней точно один раз попасть в одну группу с каждой из остальных. Это равнозначно задаче нахождения системы троек Штейнера с параметрами  $v = 15$ ,  $b = 35$ ,  $r = 7$ ,  $k = 3$ ,  $\lambda = 1$ , представляющей собой разрешимую схему с семью дубликатами, т. е. все тройки должны быть разбиты на семь множеств, по пять троек в каждом множестве, так что каждый элемент содержится точно один раз в каждой такой системе из пяти троек. Дадим решение этой задачи с аддитивной группой классов вычетов по модулю 7 в качестве группы автоморфизмов  $A$  и базовыми блоками:

$$\begin{aligned}
 & (\infty, 0_1, 0_2), \\
 & (1_1, 2_1, 4_1), \\
 & (5_1, 1_2, 6_2), \\
 & (3_1, 2_2, 5_2), \\
 & (6_1, 3_2, 4_2).
 \end{aligned} \tag{15.4.12}$$

Здесь базовые блоки образуют полный дубликат, а прибавление  $1, 2, \dots, 6 \pmod{7}$  к элементам в блоках из (15.4.12) дает еще шесть дубликатов.

Общая задача Киркмана о школьницах состоит в том, чтобы найти систему троек, в которой тройки могут быть разделены на  $r$  полных дубликатов. Если это возможно, то число элементов  $v$ , будучи числом элементов в дубликате из троек, должно быть кратно 3, т. е.  $v$  должно быть вида  $v = 6t + 3$ . Для  $v = 9$  задача решается легко, и решением служит совокупность прямых аффинной плоскости порядка 3, разбитая на четыре подмножества параллельных прямых. Для  $v = 15$  решение дано в предыдущем абзаце. Для  $v = 21$  мы имеем следующее решение с аддитивной группой классов вычетов по модулю 7 в качестве группы автоморфизмов  $A$ . Параметры схемы:

$$v = 21, b = 70, r = 10, k = 3, \lambda = 1.$$

Базовые блоки:

$$\begin{aligned} & (0_1, 1_1, 3_1), \\ & (0_2, 1_2, 3_2), \quad (0_1, 1_3, 3_2), \\ & (0_3, 1_3, 3_3), \quad (0_2, 1_1, 3_3), \\ & (2_1, 4_2, 5_3), \quad (0_3, 1_2, 3_1), \\ & (2_2, 4_3, 5_1), \\ & (2_3, 4_1, 5_2), \\ & (6_1, 6_2, 6_3). \end{aligned} \tag{15.4.13}$$

Первые семь из этих блоков составляют полный дубликат, и применение  $A$  дает нам еще шесть полных дубликатов. Каждый из последних трех базовых блоков при действии  $A$  дает полный дубликат. Таким образом, (15.4.13) приводит к требуемой системе на 21 элементе, которая разрешима и состоит из 10 полных дубликатов. Решения задачи о школьницах известны для нескольких частных значений  $v = 6t + 3$ , но решение в общем случае автору не известно.

Для системы троек с  $\lambda = 2$  необходимые условия (15.4.3) относительно  $v$  сводятся к  $v \equiv 0 \pmod{3}$  или  $v \equiv 1 \pmod{3}$ . Мы можем теперь легко доказать и достаточность этих условий.

**Теорема 15.4.4 (Бхаттачария).** *Если число  $v \geq 3$  имеет вид  $v = 3t$  или  $v = 3t + 1$ , то существует система троек с  $v$  элементами и  $\lambda = 2$ .*

**Доказательство.** Если  $v$  имеет вид  $v = 6t + 1$  или  $v = 6t + 3$ , то существует система троек Штейнера порядка  $v$ . Взяв каждый ее блок дважды, мы получим систему троек порядка  $v$  с  $\lambda = 2$ . Остается рассмотреть значения  $v$  вида  $v = 6t + 6$  или  $v = 6t + 4$ . Схемы, определяемые базовыми блоками (15.3.17) и (15.3.18) и найденные Бхаттачария [1], показывают, что и в этих случаях искомые системы существуют. Теорема доказана.

**Теорема 15.4.5 (Ханани).** *Необходимое и достаточное условие существования уравновешенной неполной блок-схемы с  $k = 3$  и любым  $\lambda$  состоит в том, чтобы*

$$\lambda(v - 1) \equiv 0 \pmod{2} \quad \text{и} \quad \lambda v(v - 1) \equiv 0 \pmod{6}. \quad (15.4.14)$$

**Доказательство.** В блок-схеме  $D(v, b, r, 3, \lambda)$  основные условия (15.2.1) и (15.2.2) дают  $r = \lambda(v - 1)/2$  и  $b = \lambda v(v - 1)/6$ . Чтобы  $r$  и  $b$  были целыми числами, очевидно, необходимы условия (15.4.14). Основная задача, конечно, доказать достаточность этих условий. Это будет показано при помощи рекурсивных теорем Ханани из раздела 15.2. Представим сначала условия (15.4.9) в следующем виде:

- если  $\lambda \equiv 1$  или  $5 \pmod{6}$ , то  $v \equiv 1$  или  $3 \pmod{6}$ ;
- если  $\lambda \equiv 2$  или  $4 \pmod{6}$ , то  $v \equiv 0$  или  $1 \pmod{3}$ ;
- если  $\lambda \equiv 3 \pmod{6}$ , то  $v \equiv 1 \pmod{2}$ ; (15.4.15)
- если  $\lambda \equiv 0 \pmod{6}$ , то на  $v$  не накладывается ограничений.

По следствию теоремы 15.2.7 достаточность (15.4.14) будет установлена, если мы сумеем показать, что при  $v \geq 3$ :

$$v \equiv 1 \text{ или } 3 \pmod{6} \quad \text{влечет} \quad v \in B(3, 1), \quad (15.4.16a)$$

$$v \equiv 0 \text{ или } 1 \pmod{3} \quad \text{влечет} \quad v \in B(3, 2), \quad (15.4.16b)$$

$$v \equiv 1 \pmod{2} \quad \text{влечет} \quad v \in B(3, 3), \quad (15.4.16c)$$

$$\text{Для всякого } v \geq 3 \quad \text{влечет} \quad v \in B(3, 6). \quad (15.4.16d)$$

Здесь (15.4.16a) — это утверждение теоремы 15.4.3, а (15.4.16b) — утверждение теоремы 15.4.4. Но мы будем следовать доказательству Ханани и не воспользуемся ни одной из этих теорем. Будем опираться на рекурсивные теоремы 15.2.4 и 15.2.5 и построения в явном виде для некоторых начальных значений  $v$ . Для удобства ссылок повторим утверждения этих теорем.

**Теорема 15.2.4.** *Если  $v = (m - 1)u + 1$ , где  $u \in B(K', \lambda')$ , и если для каждого  $k' \in K'$  имеем  $(m - 1)k' + 1 \in B_m(K, \lambda'')$ , то  $v \in B_m(K, \lambda)$ , где  $\lambda = \lambda'\lambda''$ .*

**Теорема 15.2.5.** *Пусть  $s, s+1 \in B(K, \lambda)$ ,  $t \in T_q(s)$  и либо  $q \in B(K, \lambda)$ , либо  $q = 0$  или  $1$ ; тогда  $v = st + q \in B(K, \lambda)$ .*

Для доказательства теоремы нам потребуются несколько лемм.

**Лемма 15.4.1.** *Если  $u \equiv 0$  или  $1 \pmod{3}$  и  $u \geq 3$ , то  $u \in B(K_3^1, 1)$ , где  $K_3^1 = \{3, 4, 6\}$ .*

**Доказательство.** По теореме 15.2.3  $t \in T_t(3)$  для  $t \geq 3$  и  $t \equiv 0, 1, 3 \pmod{4}$ . Поскольку  $2 \in T_0(3)$  и  $n \in T_2(3)$  для  $n$  нечетного,  $n > 1$ , по теореме 15.2.8 имеем  $t = 2n \in T_4(3)$ ; следовательно, для  $t \equiv 2 \pmod{4}$ ,  $t \geq 6$ , получаем  $t \in T_4(3)$ . Доказываем лемму индукцией по  $u$ . Тривиальным образом,  $3, 4, 6 \in B(K_3^1, 1)$ . Системы троек Штейнера с  $v = 7, 9$  из (15.4.4) показывают, что  $7, 9 \in B(K_3^1, 1)$ . Для  $u > 9$  применяем теорему 15.2.5 с  $s = 3$  во всех случаях, выбирая  $q$  и  $t$  по следующим правилам в зависимости от класса вычетов, которому принадлежит  $u$  по модулю 9 (при этом учитываем, что  $3 \in T_3(3)$  и  $t \in T_4(3)$  при  $t \geq 4$ ):

$$u \equiv 0 \pmod{9}, \quad q = 0, \quad t = \frac{u}{3},$$

$$u \equiv 1 \pmod{9}, \quad q = 1, \quad t = \frac{u - 1}{3},$$

$$u \equiv 3 \pmod{9}, \quad q = 0, \quad t = \frac{u}{3},$$

$$u \equiv 4 \pmod{9}, \quad q = 1, \quad t = \frac{u - 1}{3},$$

$$\begin{aligned} u \equiv 6 \pmod{9}, \quad q = 3, \quad t = \frac{u-3}{3}, \\ u \equiv 7 \pmod{9}, \quad q = 4, \quad t = \frac{u-4}{3}. \end{aligned} \quad (15.4.17)$$

По индукции лемма 15.4.1 доказана.

**Лемма 15.4.2.** *Если  $u \geq 3$ , то  $u \in B(K_3^2, 1)$ , где  $K_3^2 = \{3, 4, 5, 6, 8, 11, 14\}$ .*

**Доказательство.** Для  $u \equiv 0$  или  $1 \pmod{3}$  эта лемма есть частный случай леммы 15.4.1, так как  $K_3^1$  есть подмножество  $K_3^2$ . Для значений  $u = 8, 11, 14$  утверждение леммы тривиально, поскольку эти  $u$  принадлежат  $K_3^2$ . Следовательно, первым значением, для которого требуется доказательство, является  $u = 17$ . Доказательство проводим индукцией по  $u$ . Выберем  $q, s$  и  $t$  в соответствии со значением  $u$  по следующим правилам:

$$\begin{aligned} u = 17, & \quad q = 1 & s = 4, \quad t = 4, \\ u = 18, 19, 20, & \quad q = u - 15, & s = 3, \quad t = 5, \\ u = 21, 22, & \quad q = u - 21, & s = 3, \quad t = 7, \\ u = 23, & \quad q = 3, & s = 4, \quad t = 5, \\ u = 24, \dots, 28, & \quad q = u - 21, & s = 3, \quad t = 7, \\ u = 29, & \quad q = 1, & s = 4, \quad t = 7, \\ u = 30, \dots, 36, & \quad q = u - 27, & s = 3, \quad t = 9, \\ u = 37, \dots, 44, & \quad q = u - 33, & s = 3, \quad t = 11, \\ u = 45, \dots, 50, & \quad q = u - 39, & s = 3, \quad t = 13, \\ u \geq 51, & \quad q \equiv u \pmod{12}, \quad s = 3, \quad t = \frac{u-q}{3}. & \\ & \quad 3 \leq q \leq 14, \end{aligned} \quad (15.4.18)$$

Здесь, по выбору  $s, t, q$ , в каждом случае  $u = st + q$ . Имеем  $s, s+1 \in B(K_3^2, 1)$ , так как  $s = 3$  или  $4$  в каждом случае. По индукции также  $q \in B(K_3^2, 1)$ . Мы должны теперь в каждом случае проверить, что  $t \in T_q(s)$ . Заметим, что  $t \in T_t(3)$  и  $T_t(4)$  для  $t = 4, 5, 7, 9, 11, 13$ , так как эти числа — степени простых чисел. Для  $u \geq 51$  выбор  $t$  таков, что  $t \equiv 0 \pmod{4}$  и  $t > q$ . Но тогда  $t \in T_t(3)$  по теореме 15.2.3 и, поскольку  $t > q$ ,  $t \in T_q(3)$ . Тем самым лемма доказана.

Мы использовали трансверсальные системы (по существу ортогональные таблицы) и рекурсивные методы теоремы 15.2.5 и построили уравновешенные относительно пар схемы

$B[\{3, 4, 6\}, 1, u]$  с  $u \equiv 0$  или  $1 \pmod{3}$ ,  $u \geq 3$ ,

и

$B[\{3, 4, 5, 6, 8, 11, 14\}, 1, u]$  для всех  $u \geq 3$ .

Доказательство основной теоремы будет завершено теперь обращением к теореме 15.2.4 с  $K'_3$  или  $K''_3$  в роли  $K'$  или к более простой теореме 15.2.6, которую мы повторим здесь для удобства ссылок.

**Теорема 15.2.6.** *Если  $v \in B(K', \lambda_1)$  и для всякого  $k' \in K'$  имеем  $k' \in B(K, \lambda_2)$ , то  $v \in B(K, \lambda_1 \lambda_2)$ .*

Таким образом, на данном этапе доказательство теоремы сводится к конечному числу построений, связанных с конечным множеством чисел  $k'$  из  $K'$ .

**Лемма 15.4.3.** *Если  $v \equiv 1$  или  $3 \pmod{6}$ , то  $v \in B(3, 1)$ .*

**Доказательство.** Если  $v = 6t + 1$ , то возьмем  $u = 3t$ , а если  $v = 6t + 3$ , то возьмем  $u = 3t + 1$ . В обоих случаях  $v = 2u + 1$  и  $u \in B(\{3, 4, 6\}, 1)$  по лемме 15.4.1. В теореме 15.2.4 возьмем  $m = 3$  и  $K = \{3\}$ . Системы троек Штейнера порядков 7, 9 и 13, данные в (15.4.4), (15.4.5), (15.4.6) и (15.4.7), показывают, что  $7, 9, 13 \in B_3(\{3\}, 1)$ , и лемма доказана. Тем самым, доказано утверждение (15.4.16а), эквивалентное теореме 15.4.3.

**Лемма 15.4.4.** *Если  $v \equiv 0$  или  $1 \pmod{3}$ ,  $v \geq 3$ , то  $v \in B(3, 2)$ .*

**Доказательство.** По лемме 15.4.1  $v \in B(\{3, 4, 6\}, 1)$ . Воспользуемся теоремой 15.2.6 с  $\lambda_1 = 1$ ,  $\lambda_2 = 2$ ; лемма будет доказана, если мы установим, что  $3, 4, 6 \in B(3, 2)$ . Для 3 это тривиально. Для 4 мы построим уравновешенную неполную блок-схему  $B[4, 4, 3, 3, 2]$ :

$$\begin{aligned} &1, 2, 3; \\ &1, 2, 4; \\ &1, 3, 4; \\ &2, 3, 4, \end{aligned}$$

(15.4.19)

так что  $4 \in B(3, 2)$ . Для 6 построим уравновешенную неполную блок-схему  $B[6, 10, 5, 3, 2]$ :

$$\begin{array}{ll} 1, 2, 3; & 2, 3, 6; \\ 1, 2, 4; & 2, 4, 5; \\ 1, 3, 5; & 2, 5, 6; \\ 1, 4, 6; & 3, 4, 5; \\ 1, 5, 6; & 3, 4, 6, \end{array} \quad (15.4.20)$$

так что  $6 \in B(3, 2)$ . Эти построения завершают доказательство леммы. Тем самым доказано утверждение (15.4.16b), эквивалентное теореме 15.4.4.

**Лемма 15.4.5.** *Если  $v \equiv 1 \pmod{2}$ , то  $v \in B(3, 3)$ .*

**Доказательство.** Это есть утверждение (15.4.16c). Для  $v \equiv 1$  или  $3 \pmod{6}$ , поскольку  $v \in B(3, 1)$ , мы можем взять схему  $B[3, 1, v]$  трижды, и тогда получим  $v \in B_3(3, 3)$ . В любом случае мы можем применить теорему 15.2.4 с  $m = 3$ ,  $K' = K_3^2$ ,  $\lambda' = 1$ ,  $\lambda'' = 1$ . Так как по лемме 15.4.2  $u \in B(K_3^2, 1)$ , если  $u \geq 3$ , мы заключаем, что  $v = 2u + 1 \in B_3(3, 3)$ , если  $2k' + 1 \in B_3(3, 3)$  для любого  $k' \in K_3^2$ . Здесь  $v = 2u + 1$  может быть любым нечетным числом, не меньшим 7. Следовательно, чтобы доказать лемму, мы должны показать, что  $3, 5 \in B(3, 3)$  и что  $7, 9, 11, 13, 17, 23, 29 \in B_3(3, 3)$  (эти числа — значения  $2k' + 1$  при  $k' \in K_3^2$ ). Поскольку  $3, 7, 9, 13 \in B(3, 1)$ , имеем  $3, 7, 9, 13 \in B_3(3, 3)$ , так как соответствующую схему можно взять трижды. Остальные значения 5, 11, 17, 23, 29 нужно рассмотреть отдельно.

**Подлемма 1.**  $5 \in B_3(3, 3)$ . Базовые блоки по модулю 5:

$$(0, 1, 4); \quad (0, 2, 3).$$

**Подлемма 2.**  $11 \in B_3(3, 3)$ . Применим теорему 15.2.4 с  $m = 3$ ,  $K = \{3\}$ ,  $K' = \{3\}$ ,  $\lambda' = 3$ ,  $\lambda'' = 1$ . Действительно,  $11 = (3 - 1)5 + 1$ , и, так как  $5 \in B(3, 3)$ ,  $7 \in B_3(3, 1)$ , утверждение доказано.

**Подлемма 3.**  $17 \in B_3(3, 3)$ . Покажем сначала, что  $8 \in B(4, 3)$ . За элементы схемы примем пары  $(i, j)$ ,

$i \equiv 0, 1, 2, 3 \pmod{4}$ ,  $j \equiv 0, 1 \pmod{2}$ , и определим блоки

$$\{(0, b_0), (1, b_1), (2, b_2), (3, b_3)\}, \quad \sum b_i \equiv 0 \pmod{2},$$

$$\{(i, 0), (i, 1), (i', 0), (i', 1)\}, \quad i < i'.$$

Теперь применим теорему 15.2.4 с  $m = 3$ ,  $u = 8$ ,  $K' = \{4\}$ ,  $\lambda' = 3$ ,  $K = \{3\}$ ,  $\lambda'' = 1$ . Тогда  $(m - 1)k' + 1 = 9 \in B_3(3, 1)$ , и, поскольку  $8 \in B(4, 3)$ , действительно получаем, что  $17 = (3 - 1)8 + 1 \in B_3(3, 3)$ .

*Подлемма 4.*  $23 \in B_3(3, 3)$ . Воспользуемся теоремой 15.2.4 с  $m = 3$ ,  $u = 11$ ,  $K' = \{3\}$ ,  $\lambda' = 3$ ,  $K = \{3\}$ ,  $\lambda'' = 1$ . Имеем  $(m - 1)k' + 1 = 7 \in B_3(3, 1)$ , и, поскольку  $11 \in B_3(3, 3)$ , в силу подлеммы 2 заключаем, что  $23 = (3 - 1)11 + 1 \in B_3(3, 3)$ .

*Подлемма 5.*  $29 \in B_3(3, 3)$ . Мы сначала покажем, что  $14 \in B(\{3, 4\}, 3)$ , за элементы схемы примем вычеты  $i$  по модулю 13,  $i \equiv 0, \dots, 12 \pmod{13}$ , и  $\infty$ ; базовые блоки по модулю 13 определим следующим образом:  $(1, 2, 6, 12)$ ,  $(2, 4, 12, 11)$ ,  $(\infty, 1, 3, 9)$ ,  $(2, 6, 5)$ . Применим теперь теорему 15.2.4 с  $m = 3$ ,  $u = 14$ ,

$$K' = \{4, 3\}, \quad \lambda' = 3, \quad K = \{3\}, \quad \lambda'' = 1.$$

Так как  $14 \in B(\{3, 4\}, 3)$ , а  $7 \in B_3(3, 1)$ ,  $9 \in B_3(3, 1)$ , имеем

$$29 = (3 - 1)14 + 1 \in B_3(3, 3).$$

Эти пять подлемм охватывают все частные случаи, нужные для доказательства леммы.

**Лемма 15.4.6.** *Если  $v \geq 3$ , то  $v \in B(3, 6)$ .*

**Доказательство.** Это утверждение есть (15.4.16d) — последняя часть основной теоремы 15.4.5. Обратимся к теореме 15.2.6 с  $K' = K_3^2 = \{3, 4, 5, 6, 8, 11, 14\}$ ,  $\lambda_1 = 1$ ,  $K = \{3\}$ ,  $\lambda_2 = 6$ . По лемме 15.4.2 мы знаем, что  $v \in B(K', 1)$ . Таким образом, чтобы доказать нашу лемму, мы должны показать, что  $3, 4, 5, 6, 8, 11, 14 \in B(3, 6)$ . Из следствия теоремы 15.2.7 и лемм 15.4.3, 15.4.4 и 15.4.5 вытекает, что  $3, 4, 5, 6, 11 \in B(3, 6)$ . Остается показать, что  $8 \in B(3, 6)$  и  $14 \in B(3, 6)$ .

*Подлемма 6.*  $8 \in B(3, 6)$ . В  $GF(2^3)$  пусть  $x$  — примитивный корень, удовлетворяющий уравнению  $x^3 = x + 1$ . Примем блоки  $(x^i, x^{i+1}, x^{i+2})$ ,  $i = 0, \dots, 6$ , за блоки базы над аддитивной группой поля  $GF(2^3)$ . Тогда получаем частный случай (15.3.16).

*Подлемма 7.*  $14 \in B(3, 6)$ . Примем за элементы схемы вычеты по модулю 13 и  $\infty$  и определим базовые блоки:

- (1, 3, 9), взятый 5 раз,
- (2, 6, 5), взятый 6 раз,
- $(\infty, 1, 12)$ ,  $(\infty, 3, 10)$ ,  $(\infty, 4, 9)$ .

Этим завершается доказательство леммы и, в свою очередь, доказательство основной теоремы.

## 15.5. Блок-схемы с $k > 3$

В работе [1] Ханани показал, что для  $k = 4$  ситуация в точности такая же, что и при  $k = 3$ , а именно основные необходимые условия являются также достаточными. При  $k = 5$  это неверно, и, может быть, при каждом  $k \geq 5$  существует хотя бы одно множество параметров, удовлетворяющих основным соотношениям  $bk = vr$ ,  $r(k-1) = \lambda(v-1)$  из (10.1.1), для которых не существует никакой блок-схемы. Тем не менее автор склонен придерживаться мнения, что это в некотором смысле относительно необычная ситуация. Неизвестно, кто первый выдвинул следующее предположение.

*Предположение.* Пусть даны  $k$  и  $\lambda$ . Тогда, за конечным числом исключений, существует блок-схема для всякого множества параметров  $v, b, r, k, \lambda$ , удовлетворяющих соотношениям  $bk = vr$ ,  $r(k-1) = \lambda(v-1)$ .

Мы опишем здесь в общих чертах результаты Ханани для  $k=4$ . За подробностями читатель отсылается к оригинальной работе Ханани [1].

*Теорема 15.5.1.* Необходимым и достаточным условием существования уравновешенной неполной блок-схемы с  $v \geq 4$  элементами,  $k = 4$  и любым  $\lambda$  является

*выполнение соотношений*

$$\lambda(v-1) \equiv 0 \pmod{3} \quad \text{и} \quad \lambda v(v-1) \equiv 0 \pmod{12}. \quad (15.5.1)$$

Заметим, что эти условия тривиальным образом необходимы, будучи следствиями из (10.1.1). Они эквивалентны следующим соотношениям:

- если  $\lambda \equiv 1$  или  $5 \pmod{6}$ , то  $v \equiv 1$  или  $4 \pmod{12}$ ;
- если  $\lambda \equiv 2$  или  $4 \pmod{6}$ , то  $v \equiv 1 \pmod{3}$ ;
- если  $\lambda \equiv 3 \pmod{6}$ , то  $v \equiv 0$  или  $1 \pmod{4}$ ;
- если  $\lambda \equiv 0 \pmod{6}$ , то ограничений на  $v$  нет.

В свою очередь условия (15.5.1) будут достаточными, если мы сумеем показать, что при  $v \geq 4$

$$v \equiv 1 \text{ или } 4 \pmod{12} \text{ влечет } v \in B(4, 1); \quad (15.5.3a)$$

$$v \equiv 1 \pmod{3} \quad \text{влечет } v \in B(4, 2); \quad (15.5.3b)$$

$$v \equiv 0 \text{ или } 1 \pmod{4} \quad \text{влечет } v \in B(4, 3); \quad (15.5.3c)$$

$$v \geq 4 \quad \text{влечет } v \in B(4, 6). \quad (15.5.3d)$$

Для доказательства требуются следующие леммы.

**Лемма 15.5.1.** *Если  $u \equiv 0$  или  $1 \pmod{4}$  и  $u \geq 4$ , то*

$$u \in B(K_4^1, 1), \quad \text{где } K_4^1 = \{4, 5, 8, 9, 12\}.$$

**Лемма 15.5.2.** *Если  $u \geq 4$ , то  $u \in B(K_4^2, 1)$ , где*

$$K_4^2 = \{4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 18, 19, 22, 23\}.$$

**Лемма 15.5.3.** *Если  $v \equiv 1$  или  $4 \pmod{12}$ ,  $v \geq 4$ , то  $v \in B(4, 1)$ .*

Эта лемма доказывается путем представления  $v$  в виде  $v = 3u + 1$ ,  $u \equiv 0$  или  $1 \pmod{4}$  и применения теоремы 15.2.4 с  $m = 4$ , так как по лемме 15.5.1  $u \in B(K_4^1, 1)$ . Для этого требуется доказать, что  $v \in B_4(4, 1)$  для частных значений  $v = 4, 13, 16, 25, 28, 37$ . Лемма 15.5.3 – это утверждение (15.5.3a).

**Лемма 15.5.4.** *Если  $v \equiv 1 \pmod{3}$ , то  $v \in B(4, 2)$ .*

Здесь применяется теорема 15.2.4 с  $m = 4$  и  $v = 3u + 1$ , где для  $u \geq 4$  в силу леммы 15.5.2  $u \in B(K_4^2, 1)$ . Для

этого требуется доказать, что  $v \in B_4(4, 2)$  для всех значений  $v = 3u + 1$ ,  $u \in K_4^2$ . Лемма 15.5.4 – это утверждение (15.5.3b).

**Лемма 15.5.5.** *Если  $v \equiv 0$  или  $1 \pmod{4}$ , то  $v \in B(4, 3)$ .*

По лемме 15.5.1  $v \in B(K_4^1, 1)$ . Применяется теорема 15.2.6, и нужно только показать, что  $4, 5, 8, 9, 12 \in B(4, 3)$ . Лемма 15.5.5 – это утверждение (15.5.3c).

**Лемма 15.5.6.** *Если  $v \geq 4$ , то  $v \in B(4, 6)$ .*

По лемме 15.5.2 имеем включение  $v \in B(K_4^2, 1)$ . Лемма доказывается применением теоремы 15.2.6, если показать, что для всех 15 значений  $v \in K_4^2$  мы имеем  $v \in B(4, 6)$ . Лемма 15.5.6 – это утверждение (15.5.3d). Леммы 15.5.1–15.5.6 в совокупности дают теорему 15.5.1.

Для  $k \geq 5$  ситуация иная. Следующая теорема будет доказана в гл. 16.

**Теорема 15.5.2.** *Пусть имеется схема  $D$  с параметрами*

$$v = v_1 - k_1, \quad b = v_1 - 1, \quad r = k_1, \quad k = k_1 - \lambda, \quad \lambda = \lambda,$$

где  $k_1(k_1 - 1) = \lambda(v_1 - 1)$  и  $\lambda = 1$  или 2. Тогда  $D$  может быть вложена в симметричную блок-схему  $D^*$  с параметрами  $v_1, k_1, \lambda$ .  $D$  получается из схемы  $D^*$  как некоторая остаточная схема.

При помощи этой теоремы можно доказать несуществование схемы  $D$ . В частности, если бы существовала схема  $D$  с параметрами  $v = 15$ ,  $b = 21$ ,  $r = 7$ ,  $k = 5$ ,  $\lambda = 2$ , то по теореме 15.5.2 ее можно было бы вложить в симметричную схему  $D^*$  с параметрами  $v_1 = 22$ ,  $k_1 = 7$ ,  $\lambda = 2$ . По теореме 10.3.1 такой схемы  $D^*$  не существует, так как  $v_1$  четно, но  $n = k_1 - \lambda = 5$  не есть квадрат. Следовательно, схемы  $D$  с указанными параметрами не существует. Аналогично, так как по теореме 10.3.1 не существует схемы с параметрами  $v_1 = 43$ ,  $k_1 = 7$ ,  $\lambda = 1$ , мы выводим из теоремы 15.5.2,

что не существует схемы с  $v = 36$ ,  $b = 42$ ,  $r = 7$ ,  $k = 6$ ,  $\lambda = 1$ . Фактически для большинства значений  $k \geq 5$  применением теорем 10.3.1 и 15.5.2 удается показать, что существуют некоторые параметры, удовлетворяющие основным соотношениям (10.1.1), которым не соответствует никакая схема.

Для  $k = 5$  Ханани указывает частные результаты. Ему нужно доказать следующее:

$$\text{если } v \equiv 1 \text{ или } 5 \pmod{20}, \text{ то } v \in B(5,1); \quad (15.5.4a)$$

$$\text{если } v \equiv 1 \text{ или } 5 \pmod{20}, \text{ то } v \in B(5,2); \quad (15.5.4b)$$

$$\text{если } v \equiv 0 \text{ или } 1 \pmod{5}, \text{ то } v \in B(5,4); \quad (15.5.4c)$$

$$\text{если } v \equiv 1 \pmod{4}, \text{ то } v \in B(5,5); \quad (15.5.4d)$$

$$\text{если } v \equiv 1 \pmod{2}, \text{ то } v \in B(5,10); \quad (15.5.4e)$$

$$\text{если } v \geq 5, \text{ то } v \in B(5,20). \quad (15.5.4f)$$

Он использует при этом два основных множества:

$$K_5^1 = \{5, 6, 10, 11, 15, 16, 20, 35, 36, 40, 70, 71, 75, 76\}, \quad (15.5.5)$$

$$K_5^2 = \{5, 6, \dots, 20, 22, 23, 24, 27, 28, 29, 32, 33, 34, 38, 39\}. \quad (15.5.6)$$

Для  $u \geq 5$ , удовлетворяющего условию  $u \equiv 0$  или  $1 \pmod{5}$ , доказывается, что  $u \in B(K_5^1, 1)$ , и этот же результат даже при отбрасывании 35 из  $K_5^1$  доказывается для всех других  $u \equiv 0$  или  $1 \pmod{5}$ . Отсюда он доказывает (15.5.4a) с возможным исключением  $141 = 4 \cdot 35 + 1$ . Устанавливается также, что  $u \in B(K_5^2, 1)$  для  $u \geq 5$ . Отсюда выводятся (15.5.4c) и (15.5.4f). Он замечает также, что (15.5.4d) верно, если  $4u + 1 \in B_5(5, 5)$ , для всякого  $u \in K_5^2$ .

Как мы заметили, схемы с  $v = 15$ ,  $k = 5$ ,  $\lambda = 2$  не существует. Тем не менее существует схема с  $v = 15$ ,  $k = 5$ ,  $\lambda = 4$ :

$$v = 15, \quad b = 42, \quad r = 14, \quad k = 5, \quad \lambda = 4.$$

Элементы:  $(i, j)$ ,  $i \equiv 0, 1, 2, 3, 4 \pmod{5}$ ,  $j \equiv 0, 1, 2 \pmod{3}$ .

Блоки:  $\{(i, j), (i+2, j), (i+3, j), (i, j+1), (i+4, j+2)\}$ ,  
 $\{(i, j), (i+1, j), (i, j+1), (i+2, j+1), (i, j+2)\}$ ,  
 $\{(i, 0), (i+2, 1), (i+3, 1), (i+4, 1), (i+1, 2)\}$ ,  
 $\{(i, 0), (i+1, 0), (i+2, 1), (i+3, 2), (i+4, 2)\}$ ,  
 $\{(0, 0), (1, 0), (2, 0), (3, 0), (4, 0)\}$ ,  
 $\{(0, 2), (1, 2), (2, 2), (3, 2), (4, 2)\}$ .

Построение схемы  $D(15, 63, 21, 5, 6)$  показало бы, что для  $v = 15$ ,  $k = 5$  и  $\lambda \equiv 0 \pmod{2}$  все  $\lambda$ , за исключением  $\lambda = 2$ , возможны, так как всякое четное число  $\geq 4$  может быть записано в виде суммы четверок и шестерок.

Но можно заметить, что множество всех  $\binom{15}{5} = 3003$  сочетаний из 15 элементов по 5 есть схема  $D(15, 3003, 1001, 5, 286)$ , и во всяком случае при  $v = 15$ ,  $k = 5$  и  $\lambda \equiv 0 \pmod{2}$ ,  $\lambda \geq 284$  схема существует.

Если в любой схеме  $D(v, b, r, k, \lambda)$  для каждого блока взять множество из  $v - k$  элементов, не входящих в этот блок, то, как легко заметить, совокупность всех этих дополнительных множеств образует блоки некоторой схемы  $D'$  с параметрами  $v, b, b - r, v - k, b - 2r + \lambda$ . Эта схема  $D'$  называется *дополнением* схемы  $D$ . Каждая схема есть дополнение некоторой другой, и в перечне схем проще приводить лишь одну из этих схем с меньшим объемом блока; поэтому без ограничения общности можно принять  $k \leq v/2$ . Для данного значения  $r$  соотношения  $r \geq k$  и  $r(k-1) = \lambda(v-1)$  показывают, что существует лишь конечное число возможностей для  $k$ ,  $\lambda$  и  $v$ . Если эти  $r$ ,  $k$ ,  $v$  даны, то  $b$  определяется из равенства  $bk = vr$ . В приложении I приведены схемы для  $r = 3, \dots, 15$  с  $k \leq v/2$  и упорядоченные по  $r$ ,  $v$ ,  $k$  соответственно.

# Теоремы о пополнении и вложении

---

## 16.1. Метод Коннора

Пусть  $D(v, b, r, k, \lambda)$  — блок-схема. Как было отмечено в разделе 10.1,  $D$  определяется своей матрицей инцидентности

$$A = (a_{ij}), \quad i = 1, \dots, v, \quad j = 1, \dots, b,$$

соответствующей элементам  $a_1, \dots, a_v$  и блокам  $B_1, \dots, B_b$ , где

$$a_{ij} = \begin{cases} 1, & \text{если } a_i \in B_j, \\ 0, & \text{если } a_i \notin B_j. \end{cases} \quad (16.1.1)$$

Тогда матрица  $A$  удовлетворяет соотношениям

$$\begin{aligned} AA^T &= B = (r - \lambda) I_v + \lambda J_v, \\ w_v A &= k w_b, \quad A w_b^T = r w_v^T. \end{aligned} \quad (16.1.2)$$

Здесь  $J_v$  —  $(v \times v)$ -матрица из единиц, а  $w_v$  и  $w_b$  — вектор-строки из  $v$  и  $b$  единиц соответственно. Сопоставим  $v$  элементам схемы неизвестные  $x_1, \dots, x_v$  и определим линейные формы  $L_j$  равенством

$$L_j = \sum_{i=1}^v a_{ij} x_i, \quad j = 1, \dots, b. \quad (16.1.3)$$

Тогда (16.1.2) эквивалентно соотношению

$$\begin{aligned} L_1^2 + \dots + L_b^2 &= (r - \lambda)(x_1^2 + \dots + x_v^2) + \\ &+ \lambda(x_1 + \dots + x_v)^2 = Q(x_1, \dots, x_v). \end{aligned} \quad (16.1.4)$$

Идея, лежащая в основе метода Коннора [1], состоит в следующем. Для данных параметров  $v, b, r, k, \lambda$  форма  $Q = Q(x_1, \dots, x_v)$  из (16.1.4) известна, и если мы выберем первые  $t$  блоков нашей схемы  $B_1, \dots, B_t$ , то формы  $L_1, \dots, L_t$  также известны. Определим теперь форму  $Q^* = Q^*(x_1, \dots, x_v)$ :

$$Q^* = Q - L_1^2 - \dots - L_t^2 = L_{t+1}^2 + \dots + L_b^2; \quad (16.1.5)$$

если  $v, b, r, k, \lambda$  даны, а  $B_1, \dots, B_t$  выбраны, то  $Q$  и  $L_1, \dots, L_t$  известны, и потому  $Q^*$  также известна. Следовательно, в силу (16.1.5), если  $B_{t+1}, \dots, B_b$  существуют, то  $Q^* = L_{t+1}^2 + \dots + L_b^2$  должна быть положительно полуопределенной формой. Таким образом, необходимое условие существования блок-схемы  $D(v, b, r, k, \lambda)$  с начальными блоками  $B_1, \dots, B_t$  состоит в том, чтобы форма  $Q^*$ , определенная формулой (16.1.5), была положительно полуопределенной. Достоинство метода Коннора заключается в том, что с его помощью можно проверить, является ли форма  $Q^*$  из (16.1.5) положительно полуопределенной, путем вычисления определителя порядка  $t$ .

Начнем со следующей леммы.

**Лемма 16.1.1.** *Если  $|K|$  – определитель, заданный формулой*

$$|K| = \begin{vmatrix} a & b & \dots & b & e_{1, v+1} & \dots & e_{1, v+t} \\ b & a & \dots & b & e_{2, v+1} & \dots & e_{2, v+t} \\ \cdot & \cdot & \ddots & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & & \cdot \\ b & b & \dots & a & e_{v, v+1} & \dots & e_{v, v+t} \\ e_{v+1, 1} & e_{v+1, 2} & \dots & e_{v+1, v} & e_{v+1, v+1} & \dots & e_{v+1, v+t} \\ \cdot & \cdot & \ddots & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & & \cdot \\ e_{v+t, 1} & e_{v+t, 2} & \dots & e_{v+t, v} & e_{v+t, v+1} & \dots & e_{v+t, v+t} \end{vmatrix} \quad (16.1.6)$$

то

$$|K| = (a + (v - 1)b)^{-t+1} (a - b)^{v-t-1} |B_t|, \quad (16.1.7)$$

где  $|B_t|$  — определитель порядка  $t$  с элементами

$$b_{ju} = (a + (v - 1)b)(a - b)e_{v+j, v+u} -$$

$$\begin{aligned} & - (a + (v - 1)b) \sum_{i=1}^v e_{i, v+u} e_{v+j, i} + \\ & + b \sum_{i=1}^v e_{i, v+u} \sum_{i=1}^v e_{v+j, i}. \end{aligned} \quad (16.1.8)$$

**Доказательство.** Проведем следующие операции над  $|K|$ .

1. Умножим последние  $t$  столбцов на  $[a + (v - 1)b] \times [a - b]$ , а чтобы значение определителя не изменилось, перед  $|K|$  напишем соответствующий множитель.

2. Прибавим к  $v$ -й строке 1-ю, 2-ю, ...,  $(v - 1)$ -ю строки.

3. Вынесем множитель  $[a + (v - 1)b]$  из  $v$ -й строки.

4. Умножим  $v$ -ю строку на  $b$  и вычтем полученное произведение из 1-й, 2-й, ...,  $(v - 1)$ -й строк.

5. Вынесем множитель  $(a - b)$  из 1-й, 2-й, ...,  $(v - 1)$ -й строк.

6. Вычтем из  $v$ -й строки 1-ю, 2-ю, ...,  $(v - 1)$ -ю строки.

7. Вычтем из  $(v + 1)$ -го,  $(v + 2)$ -го, ...,  $(v + t)$ -го столбцов умноженные на соответствующие числа 1-й, 2-й, ...,  $v$ -й столбцы, с тем чтобы обратить в нуль все элементы, находящиеся в первых  $v$  строках и последних  $t$  столбцах.

После этого утверждение леммы становится очевидным.

Если  $A = (a_{ij})$ ,  $i = 1, \dots, v$ ,  $j = 1, \dots, b$ , есть матрица инцидентности блок-схемы  $D(v, b, r, k, \lambda)$ , то обозначим через  $A_{11} = (a_{ij})$ ,  $i = 1, \dots, v$ ,  $j = 1, \dots, t$ , матрицу инцидентности для некоторых  $t$  блоков  $B_1, \dots, B_t$ , выбранных в схеме  $D$ . Определим теперь матрицу  $C_t$ :

$$C_t = r(r - \lambda)I_t + \lambda k J_t - r A_{11}^T A_{11}. \quad (16.1.9)$$

Матрицу  $C_t$  назовем *характеристической матрицей  $t$  выбранных блоков  $B_1, \dots, B_t$* .

**Теорема 16.1.1.** *Если  $C_t$  — характеристическая матрица любого множества из  $t$  блоков, выбранных из*

уравновешенной неполной блок-схемы с параметрами  $v$ ,  $b$ ,  $r$ ,  $k$ ,  $\lambda$ , то

- 1)  $|C_t| \geq 0$ , если  $t < b - v$ ;
- 2)  $|C_t| = 0$ , если  $t > b - v$ ;
- 3)  $k(r)^{-b+v+1} (r - \lambda)^{v-(b-v)-1} |C_{b-v}|$  есть квадрат целого числа.

Доказательство. Определим  $[(v+t) \times b]$ -матрицу  $A_1$  формулой

$$A_1 = \begin{bmatrix} A_{11} & A_{12} \\ I_t & 0 \end{bmatrix}, \quad (16.1.10)$$

где

$$\begin{aligned} A &= (A_{11}, A_{12}), \\ A_{11} &= (a_{ij}), \quad i = 1, \dots, v; \quad j = 1, \dots, t, \\ A_{12} &= (a_{ij}), \quad i = 1, \dots, v; \quad j = t + 1, \dots, b. \end{aligned} \quad (16.1.11)$$

Тогда, перемножая матрицы блоками, получаем

$$B_1 = A_1 A_1^T = \begin{bmatrix} A_{11} A_{11}^T + A_{12} A_{12}^T & A_{11} \\ A_{11}^T & I_t \end{bmatrix} = \begin{bmatrix} B & A_{11} \\ A_{11}^T & I_t \end{bmatrix}, \quad (16.1.12)$$

где  $B = (r - \lambda) I_v + \lambda J_v$  [см. (16.1.2)]. Применяя лемму 16.1.1, находим, что

$$|B_1| = |A_1 A_1^T| = k r^{-t+1} (r - \lambda)^{v-t-1} |C_t|. \quad (16.1.13)$$

Из теории квадратичных форм вытекает, что для действительной матрицы  $A_1$  определитель  $|A_1 A_1^T| \geq 0$ , и, так как  $k$ ,  $r$ ,  $r - \lambda$  положительны, это доказывает условие 1 теоремы, т. е.  $|C_t| \geq 0$ . Ранг матрицы  $A_1 A_1^T$  не превосходит ранга матрицы  $A_1$ . Поэтому если  $t > b - v$ , матрица  $A_1 A_1^T$  вырождена, т. е.  $|A_1 A_1^T| = 0$  и  $|C_t| = 0$ . Если  $t = b - v$ , то  $A_1$  — квадратная матрица и  $|A_1 A_1^T| = |A_1|^2$ . Поскольку элементы  $A_1$  — целые числа, то  $|A_1|$  есть целое число, следовательно, часть 3 теоремы также доказана.

Формулировка теоремы 16.1.1 по существу равносильна утверждению о том, что форма  $Q^* = Q - L_1^2 - \dots - L_t^2$  полуопределенна. Матрица  $B_1$  из (16.1.12) — это матрица

квадратичной формы:

$$\begin{aligned} Q_1 &= Q_1(x_1, \dots, x_v, y_1, \dots, y_t) = \\ &= (L_1 + y_1)^2 + \dots + (L_t + y_t)^2 + L_{t+1}^2 + \dots + L_b^2, \end{aligned} \quad (16.1.14)$$

где  $y_1, \dots, y_t$  — дополнительные неизвестные. Для любых действительных значений  $x$  мы можем выбрать  $y_1, \dots, y_t$  так, что  $L_1 + y_1 = \dots = L_t + y_t = 0$ , и  $Q_1$  есть положительно полуопределенная форма тогда и только тогда, когда форма  $L_{t+1}^2 + \dots + L_b^2 = Q - L_1^2 - \dots - L_t^2 = Q$  положительно полуопределена.

Определим структурную матрицу  $S_t$ :

$$S_t = A_{11}^T A_{11} = (s_{ij}), \quad i, j = 1, \dots, t. \quad (16.1.15)$$

Здесь  $s_{ii} = k$ , а  $s_{ij}$ ,  $i \neq j$ , есть число элементов, общих для блоков  $B_i$  и  $B_j$ . По теореме 10.2.2, если  $D$  — симметричная схема, при  $i \neq j$  должно быть  $s_{ij} = \lambda$ . В этом случае матрица  $C_t$  при любом  $t$  равна нулевой матрице, и получить какую-либо дополнительную информацию, изучая  $C_t$ , не удается.

В разделе 10.1 были определены производные и остаточные схемы симметричной схемы. Если  $v_1, k_1, \lambda_1$  — параметры симметричной схемы  $D$ , удовлетворяющие условию

$$k_1(k_1 - 1) = \lambda_1(v_1 - 1), \quad (16.1.16)$$

то остаточная схема  $\bar{D}$ , получаемая вычеркиванием из  $D$  некоторого блока  $B_0$  и всех его элементов, имеет параметры

$$v = v_1 - k_1, \quad b = v_1 - 1, \quad r = k_1, \quad k = k_1 - \lambda_1, \quad \lambda = \lambda_1, \quad (16.1.17)$$

а производная схема  $D'$  имеет параметры

$$v = k_1, \quad b = v_1 - 1, \quad r = k_1 - 1, \quad k = \lambda_1, \quad \lambda = \lambda_1 - 1. \quad (16.1.18)$$

Естественно возникает вопрос: можно ли схему с параметрами остаточной схемы, указанными в (16.1.17) и удовлетворяющими условию (16.1.16), вложить в симметричную схему, добавляя новый блок из  $k_1$  новых элементов и  $\lambda_1$  этих элементов к каждому из  $v_1 - 1$  блоков. Это возможно не всегда, как показывает следую-

щий пример, принадлежащий Бхаттачария [2]:

$$v = 16, \quad b = 24, \quad r = 9, \quad k = 6, \quad \lambda = 3,$$

$(1, 2, 7, 8, 14, 15), (3, 5, 7, 8, 11, 13), (2, 3, 8, 9, 13, 16),$   
 $(3, 5, 8, 9, 12, 14), (1, 6, 7, 9, 12, 13)^*, (2, 5, 7, 10, 13, 15),$   
 $(3, 4, 7, 10, 12, 16), (3, 4, 6, 13, 14, 15), (4, 5, 7, 9, 12, 15),$   
 $(2, 4, 9, 10, 11, 13), (3, 6, 7, 10, 11, 14), (1, 2, 3, 4, 5, 6)$ .

---

$(1, 4, 7, 8, 11, 16), (2, 4, 8, 10, 12, 14), (5, 6, 8, 10, 15, 16),$   
 $(1, 6, 8, 10, 12, 13)^*, (1, 2, 3, 11, 12, 15), (2, 6, 7, 9, 14, 16),$   
 $(1, 4, 5, 13, 14, 15), (2, 5, 6, 11, 12, 16), (1, 3, 9, 10, 15, 16),$   
 $(4, 6, 8, 9, 11, 15), (1, 5, 9, 10, 11, 14), (11, 12, 13, 14, 15, 16).$

---

(16.1.19)

Здесь блоки, помеченные звездочкой, имеют по четыре общих элемента, а два подчеркнутых блока совсем не имеют общих элементов. Если бы можно было добавить новый блок из 9 элементов и по три из этих элементов к каждому из имеющихся 24 блоков, чтобы образовалась симметричная схема  $D$  с  $v_1 = 25$ ,  $k_1 = 9$ ,  $\lambda_1 = 3$ , то любые два блока в  $D$  имели бы точно три общих элемента. Но блоки, отмеченные звездочкой, уже имеют четыре общих элемента, поэтому дополнить схему до симметричной невозможно.

Мы можем сформулировать условия, при которых вложение осуществимо.

**Теорема 16.1.2.** Схема  $D$  с параметрами, удовлетворяющими условиям

$$r = k + \lambda, \quad v\lambda = k(k + \lambda - 1), \quad b\lambda = (k + \lambda)(k + \lambda - 1), \quad (16.1.20)$$

может быть вложена как остаточная схема в некоторую симметричную схему в том и только в том случае, если мы можем найти в  $D$  множества блоков  $S_j$ ,  $j = 1, \dots, k + \lambda$ , такие, что:

- 1) каждое  $S_j$  состоит из  $k + \lambda - 1$  блоков  $D$ ;
- 2) блоки из некоторого  $S_j$  в совокупности содержат каждый элемент  $\lambda$  раз;
- 3) любые два различных множества  $S_i$ ,  $S_j$  содержат в точности  $\lambda - 1$  общих блоков;

4) любой блок схемы  $D$  входит точно в  $\lambda$  множеств  $S_j$ .

**Доказательство.** Присоединим к  $D$  новые элементы  $x_1, \dots, x_{k+\lambda}$  и новый блок  $B_0$ , содержащий эти элементы. Присоединим, кроме того, новый элемент  $x_j$  к каждому блоку из  $S_j$ . Из свойств 1) – 4) в формулировке теоремы вытекает, что блок  $B_0$  и блоки  $B_i^*$ ,  $i=1, \dots, b$ , где  $B_i^*$  есть блок  $B_i$  из  $D$  с добавленными к нему элементами  $x_j$ , образуют симметричную схему с параметрами  $v_1 = v + k + \lambda$ ,  $k_1 = r$ ,  $\lambda_1 = \lambda$ . Обратно, если из симметричной схемы с параметрами  $v_1$ ,  $k_1$ ,  $\lambda_1$  удалить блок  $B_0$  и его элементы, то остается схема  $D$ , параметры которой удовлетворяют (16.1.20). Если  $x_1, \dots, x_{k_1}$  – элементы блока  $B_0$ , то множество тех блоков, из которых удален элемент  $x_j$ , обозначим через  $S_j$ . Множества  $S_1, \dots, S_{k_1}$  обладают свойствами, указанными в формулировке теоремы.

Пример Бхаттачария показывает, что вложение возможно не всегда. Мы докажем теорему о том, что вложение возможно, когда  $\lambda = 1$  или  $\lambda = 2$ .

**Теорема 16.1.3.** Пусть  $v_1$ ,  $k_1$ ,  $\lambda_1$  удовлетворяют соотношению  $k_1(k_1 - 1) = \lambda_1(v_1 - 1)$ , и пусть дана схема  $D$  с параметрами  $v = v_1 - k_1$ ,  $b = v_1 - 1$ ,  $r = k_1$ ,  $k = k_1 - \lambda_1$ ,  $\lambda = \lambda_1$ , причем  $\lambda = 1$  или 2. Тогда  $D$  может быть вложена как остаточная схема в симметричную схему с параметрами  $v_1$ ,  $k_1$ ,  $\lambda_1$ .

**Доказательство.** При  $\lambda = 1$  это есть вложение конечной аффинной плоскости в конечную проективную плоскость, а этот результат уже был доказан в теореме 12.3.3. При  $\lambda = 2$  доказательство значительно усложняется и опирается на применение теоремы 16.1.1. В основе его – установление следующей леммы.

**Лемма 16.1.2.** Каждая блок-схема  $D$  с параметрами, для которых выполнены соотношения

$$v = \frac{k(k+1)}{2}, \quad b = \frac{(k+1)(k+2)}{2}, \quad r = k+2, \quad \lambda = 2, \quad (16.1.21)$$

удовлетворяет условиям теоремы 16.1.2 и потому может быть вложена в симметричную схему. Это вложение единствено с точностью до изоморфизма.

**Доказательство.** Если  $k = 2$ , параметрами схемы будут  $v = 3$ ,  $b = 6$ ,  $r = 4$ ,  $k = 2$ ,  $\lambda = 2$ , и схема тривиальна:

$$\begin{array}{lll} (1, 2) & (1, 3) & (2, 3) \\ (1, 2) & (1, 3) & (2, 3). \end{array} \quad (16.1.22)$$

Пусть  $x_1, x_2, x_3, x_4$  — новые элементы, и мы имеем по существу единственное вложение в симметричную схему с параметрами  $v = b = 7$ ,  $r = k = 4$ ,  $\lambda = 2$ :

$$\begin{array}{ll} (x_1, x_2, x_3, x_4); \\ (x_1, x_2, 1, 2); & (x_2, x_4, 1, 3); \\ (x_3, x_4, 1, 2); & (x_1, x_4, 2, 3); \\ (x_1, x_3, 1, 3); & (x_2, x_3, 2, 3). \end{array} \quad (16.1.23)$$

Эта симметричная схема — дополнение<sup>1)</sup> к проективной плоскости  $\text{PG}(2, 2)$ , параметры которой  $v = 7$ ,  $k = 3$ ,  $\lambda = 1$ . С этого момента мы будем предполагать, что  $k \geq 3$ .

Доказательство начнем с рассмотрения структуры пересечения данного блока  $B_0$  с остальными  $b - 1$  блоками схемы  $D$ . Пусть  $n_i$  — число блоков из  $B_1, \dots, B_{b-1}$ , имеющих в точности  $i$  элементов, общих с  $B_0$ . Тогда выполняются следующие соотношения:

$$\sum_{i=0}^k n_i = b - 1 = \frac{k^2 + 3k}{2}, \quad (16.1.24)$$

$$\sum_{i=0}^k i n_i = (r - 1) k = k^2 + k, \quad (16.1.25)$$

$$\sum_{i=0}^k i(i - 1) n_i = (\lambda - 1)(k^2 - k) = k^2 - k. \quad (16.1.26)$$

<sup>1)</sup> См. конец раздела 15.5. — Прим. ред.

В первом из этих равенств просто подсчитывается число остальных блоков. Пусть

$$B_0 = \{a_1, \dots, a_k\},$$

тогда второе равенство отражает тот факт, что каждый из элементов  $a_1, \dots, a_k$  появляется  $r - 1$  раз в остальных блоках, а в каждом блоке  $B_j$ , имеющем с  $B_0$   $i$  общих элементов, фиксируется  $i$  появлений элементов из  $B_0$ . Если  $B_j$  имеет  $i$  общих с  $B_0$  элементов, то он содержит  $i(i - 1)/2$  неупорядоченных пар  $(a_m, a_n)$  элементов из  $B_0$ ,  $m, n = 1, \dots, k$ ,  $m \neq n$ , каждая из которых должна появляться всего  $\lambda - 1$  раз в остальных блоках. Это обстоятельство учитывается в третьем из равенств. Из этих соотношений получается, что

$$\sum_{i=0}^k [i(i - 1) - 2i + 2] n_i = k^2 - k - 2(k^2 + k) + k^2 + 3k = 0, \quad (16.1.27)$$

или

$$\sum_{i=0}^k (i - 1)(i - 2)n_i = 0. \quad (16.1.28)$$

При  $i = 0$  или  $i > 2$  коэффициент  $(i - 1)(i - 2) > 0$ , поэтому  $n_i = 0$  при  $i \neq 1, 2$ . Соотношения (16.1.24), (16.1.25) показывают, что  $n_1 = 2k$ ,  $n_2 = (k^2 - k)/2$ .

Назовем два блока *связанными*, если они имеют один общий элемент, и *дважды связанными*, если они имеют два общих элемента. Сформулируем полученные результаты в виде леммы.

**Лемма 16.1.3.** *Если в схеме D задан блок  $B_0$ , то среди остальных  $b - 1 = (k^2 + 3k)/2$  блоков  $2k$  блоков связаны с  $B_0$  и  $(k^2 - k)/2$  блоков дважды связаны с  $B_0$ .*

Рассмотрим теперь структуру пересечения двух блоков с остальными  $b - 2$  блоками. Выделим блоки  $B_1$  и  $B_2$ . Пусть

$$\begin{aligned} B_1 &= \{z_1, z_t, a_1, \dots, a_{k-t}\}, \\ B_2 &= \{z_1, z_t, b_1, \dots, b_{k-t}\}. \end{aligned} \quad t = 1 \text{ или } 2, \quad (16.1.29)$$

Здесь  $z_1$  или  $z_1, z_2$  — элементы, общие для  $B_1$  и  $B_2$ , в зависимости от того, являются ли  $B_1$  и  $B_2$  связанными

или дважды связанными. Остальные блоки пересекаются с  $B_1$  и  $B_2$  по одному или двум элементам, но мы заметим, что при  $t = 2$  не может быть других блоков, содержащих одновременно  $z_1$  и  $z_2$ , так как  $\lambda = 2$ . Таким образом, схему пересечений можно задать следующим образом:

$$\begin{array}{ll} x_1: \{z_h, a_i, b_s, \dots\}; & y_1: \{a_i, a_j, b_s, b_u, \dots\}; \\ x_2: \{z_h, a_i, \dots\}; & y_2: \{a_i, a_j, b_s, \dots\}; \\ x_3: \{z_h, b_s, \dots\}; & y_3: \{a_i, b_s, b_u, \dots\}; \\ x_4: \{z_h, \dots\}; & y_4: \{a_i, b_s, \dots\}. \end{array} \quad (16.1.30)$$

Здесь  $x_1, \dots, x_4, y_1, \dots, y_4$  обозначают числа блоков, имеющих в точности указанный характер пересечения с  $B_1$  и  $B_2$ . Эти числа удовлетворяют следующим соотношениям:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= tk, & y_1 + y_2 + y_3 + y_4 &= \frac{k^2 + 3k - 2}{2} - tk, \\ x_1 + x_2 &= t(k-t), & y_1 + y_2 &= \frac{(k-t)(k-t-1)}{2}, \\ x_1 + x_3 &= t(k-t), & y_1 + y_3 &= \frac{(k-t)(k-t-1)}{2}, \\ x_1 + 4y_1 + 2y_2 + 2y_3 + y_4 &= 2(k-t)^2. & & \end{aligned} \quad (16.1.31)$$

Здесь  $x_1 + x_2 + x_3 + x_4$  дает число появлений  $z_1$  и  $z_t$  в остальных блоках;  $y_1 + y_2 + y_3 + y_4$  дает число блоков, не содержащих ни  $z_1$ , ни  $z_t$ . Далее  $x_1 + x_2$  дает число появлений в остальных блоках всевозможных пар  $z_h, a_i$ ,  $h = 1, t$ ;  $x_1 + x_3$  — соответствующее число для пар вида  $z_h, b_s$ ,  $h = 1, t$ ;  $y_1 + y_2$  — для пар вида  $a_i, a_j$ ;  $y_1 + y_3$  — для пар вида  $b_s, b_u$ ; в последнем равенстве дается число пар  $a_i, b_s$ ,  $i, s = 1, \dots, k-t$ ; так как  $\lambda = 2$ , каждая такая пара появляется дважды в остальных блоках. Решения этой системы уравнений таковы:

$$t = 1$$

$$\begin{aligned} x_1 &= k - 2 + x_4, & y_1 &= \frac{k^2 - 5k + 6}{2} - x_4, \\ x_2 &= 1 - x_4, & y_2 &= k - 2 + x_4, \\ x_3 &= 1 - x_4, & y_3 &= k - 2 + x_4, \\ x_4 &= x_4, & y_4 &= k - x_4. \end{aligned} \quad (16.1.32)$$

$$t = 2$$

$$\begin{aligned} x_1 &= 2k - 8 + x_4, & y_1 &= \frac{k^2 - 9k + 22}{2} - x_4, \\ x_2 &= 4 - x_4, & y_2 &= 2k - 8 + x_4, \\ x_3 &= 4 - x_4, & y_3 &= 2k - 8 + x_4, \\ x_4 &= x_4, & y_4 &= 4 - x_4. \end{aligned} \quad (16.1.32)$$

Заметим, что хотя значение  $x_4$  не определено, мы знаем, чему равна сумма  $x_4 + y_4$ , — это число остальных блоков, которые связаны как с  $B_1$ , так и с  $B_2$ . Аналогично  $x_3 + y_3$ ,  $x_2 + y_2$  и  $x_1 + y_1$  также известны и дают точное число остальных блоков с предписанным типом связи с блоками  $B_1$  и  $B_2$ . Сформулируем полученные результаты.

**Лемма 16.1.4.** *Если  $B_1$  и  $B_2$  — связанные блоки, то существует  $k$  блоков, которые связаны как с  $B_1$ , так и с  $B_2$ ,  $k-1$  блоков, связанных с  $B_1$  и дважды связанных с  $B_2$ ,  $k-1$  блоков, дважды связанных с  $B_1$  и связанных с  $B_2$ , и  $(k^2 - 3k + 2)/2$  блоков, дважды связанных как с  $B_1$ , так и с  $B_2$ . Если  $B_1$  и  $B_2$  дважды связаны, то эти числа принимают соответственно значения*

$$4, \quad 2k - 4, \quad 2k - 4 \quad \text{и} \quad (k^2 - 5k + 6)/2.$$

В матрице  $C_t$  из (16.1.9) элементы равны

$$c_{jj} = r(r - \lambda) + \lambda k - rk = (r - k)(r - \lambda), \quad j = 1, \dots, t; \quad (16.1.33)$$

$$c_{ju} = \lambda k - rs_{ju}, \quad j \neq u, \quad j, u = 1, \dots, t,$$

где  $s_{ju}$  — соответствующий элемент в  $S_t$ . В нашем случае  $r = k + 2$ ,  $\lambda = 2$  и в силу леммы 16.1.3  $s_{ju} = 1$  или 2. Следовательно,  $c_{jj} = 2k$  и  $c_{ju} = k - 2$ , если  $s_{ju} = 1$ , и  $c_{ju} = -4$ , если  $s_{ju} = 2$ .

Применим теорему 16.1.1 в трех частных случаях:

$$S_5^{(1)} = \begin{bmatrix} k & 1 & 1 & 2 & 2 \\ 1 & k & 1 & 1 & 1 \\ 1 & 1 & k & 1 & 1 \\ 2 & 1 & 1 & k & s_{45} \\ 2 & 1 & 1 & s_{45} & k \end{bmatrix}, \quad S_5^{(2)} = \begin{bmatrix} k & 1 & 1 & 1 & 2 \\ 1 & k & 1 & 2 & 1 \\ 1 & 1 & k & 2 & 1 \\ 1 & 2 & 2 & k & s_{45} \\ 2 & 1 & 1 & s_{45} & k \end{bmatrix},$$

$$S_6 = \begin{bmatrix} k & 1 & 1 & 1 & 1 & 2 \\ 1 & k & 1 & 2 & 2 & 1 \\ 1 & 1 & k & 2 & 2 & 1 \\ 1 & 2 & 2 & k & s_{45} & 2 \\ 1 & 2 & 2 & s_{45} & k & 2 \\ 2 & 1 & 1 & 2 & 2 & k \end{bmatrix}. \quad (16.1.34)$$

Лемма 16.1.5. В  $S_5^{(1)}$  должно быть  $s_{45} = 1$ ; в  $S_5^{(2)}$  должно быть  $s_{45} = 2$  и в  $S_6$  должно быть  $s_{45} = 1$ .

Доказательство. Вычислим определители  $|C_t|$ , соответствующие этим структурным матрицам; используя (16.1.33), находим, что

$$\begin{aligned} |C_5^{(1)}| &= 4(k+2)^2(2k - c_{45})[(k-1)c_{45} + 2(k-4)], \\ |C_5^{(2)}| &= 4(k+2)^2[-(k-1)c_{45}^2 - \\ &\quad -(k-2)(k+8)c_{45} + (k-2)(k^2 - k - 18)], \\ |C_6| &= 4(k+2)^3(2k - c_{45})[(k-2)c_{45} + 2(k-6)]. \end{aligned} \quad (16.1.35)$$

Замечаем, что если  $c_{45} = -4$  в  $|C_5^{(1)}|$  или  $|C_6|$  либо  $c_{45} = k-2$  в  $|C_5^{(2)}|$ , то определитель отрицателен. По теореме 16.1.1 получаем утверждение леммы.

Пусть  $B_1$  — некоторый блок, а  $B_2$  — блок, связанный с  $B_1$ . Тогда по лемме 16.1.4 первые две строки структурной матрицы всей схемы могут быть представлены в форме

$$\begin{array}{c|cccccc|cccccc|ccccc} k & 1 & 1 & 1 & \dots & 1 & 1 & \dots & 1 & 2 & \dots & 2 & 2 & \dots & 2 \\ 1 & k & 1 & 1 & \dots & 1 & 2 & \dots & 2 & 1 & \dots & 1 & 2 & \dots & 2, \end{array} \quad (16.1.36)$$

где столбцы слева направо соответствуют блокам  $B_1, B_2, \dots, B_b$ ; мы упорядочили множество столбцов и подразделили его на подмножества из 2,  $k$ ,  $k-1$ ,  $k-1$ ,  $(k^2 - 3k + 2)/2$  столбцов в соответствии с типами связи блоков с фиксированными блоками  $B_1$  и  $B_2$ . Если  $B_3$  — произвольный блок, связанный с  $B_1$  и  $B_2$  одновременно, то схема первых трех строк имеет вид

$$\begin{array}{c|c|c|c|c|c|c|c|c|c}
 k & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 \\
 k & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 2 & 2 \\
 1 & k & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 2 \\
 1 & 1 & k & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 2 \\
 \end{array} \quad (16.1.37)$$

К этой схеме, учитывая, что  $B_3$  связан и с  $B_1$ , и с  $B_2$ , применим лемму 16.1.4. Пусть число столбцов вида

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \text{ в (16.1.37) равно } j. \text{ Тогда разбиение в (16.1.37)}$$

происходит на  $3, j, k - 1 - j, k - 1 - j, j, k - 1 - j, j, j$  и  $(k^2 - 3k + 2)/2 - j$  столбцов соответственно. Рассмотрим следующие блоки:  $B_1, B_2, B_3, j$  блоков с тремя первыми

строками  $\begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}$  в (16.1.37) и  $k - 1 - j$  блоков с тремя

первыми строками  $\begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$  в (16.1.37). Образуем для них структурную матрицу

$$S_{k+2} = \left[ \begin{array}{c|c|c}
 k & 1 & 1 & 1 \dots 1 & 2 \dots 2 \\
 1 & k & 1 & 2 \dots 2 & 1 \dots 1 \\
 1 & 1 & k & 2 \dots 2 & 1 \dots 1 \\
 \hline
 1 & 2 & 2 & & \\
 \dots & & & F & G \\
 1 & 2 & 2 & & \\
 \hline
 2 & 1 & 1 & & \\
 \dots & & & G^T & H \\
 2 & 1 & 1 & &
 \end{array} \right] \quad (16.1.38)$$

Рассматривая  $B_1, B_2, B_3$  и любые два блока с  $\begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$ , мы получаем матрицу вида  $S_5^{(1)}$  из леммы 16.1.5; таким

образом, каждый недиагональный элемент в  $H$  равен 1. Аналогично можно получить матрицу вида  $S_5^{(2)}$ , и лемма 16.1.5 показывает, что каждый элемент в  $G$  и  $G^T$  равен 2. Точно так же, если  $k - 1 - j > 0$ , образуем матрицу вида  $S_6$  и получим, что всякий недиагональный элемент в  $F$  равен 1. Поскольку  $0 \leq j \leq k - 1$ , исключен лишь случай  $j = k - 1$ . Вычислим детерминант  $|C_{k+2}|$ :

$$|C_{k+2}| = (k-6)j(j-k+2)(k+2)^{k+1}. \quad (16.1.39)$$

Так как  $k+2 > b-v$ , по теореме 16.1.1  $|C_{k+2}| = 0$ . Отсюда заключаем, что если  $k \neq 6$ , то

$$j = 0, k-2 \text{ или } k-1. \quad (16.1.40)$$

Последнее значение,  $j = k-1$ , соответствует случаю, в котором нельзя получить матрицу  $S_6$ . Исключим  $k=6$  из дальнейшего рассмотрения. Специальное доказательство для этого случая дано в первой работе Коннора [1].

Рассмотрим часть структурной матрицы нашей схемы  $D$ , состоящую из блоков, связанных с  $B_1$ :

| $B_1$    | $B_2$    | $B_3$    | $B_4$    | $\dots$  | $B_{k+2}$ | $B_{k+3}$ | $\dots$  | $B_{2k+1}$ |
|----------|----------|----------|----------|----------|-----------|-----------|----------|------------|
| $k$      | $1$      | $1$      | $1$      | $\dots$  | $1$       | $1$       | $1$      | $\dots$    |
| $1$      | $k$      | $1$      | $1$      | $\dots$  | $1$       | $2$       | $2$      | $\dots$    |
| $1$      | $1$      |          |          |          |           |           |          |            |
| $1$      | $1$      |          |          |          |           |           |          |            |
| $\ddots$ |          |          |          |          |           |           |          |            |
| $\ddots$ |          |          |          |          |           |           |          |            |
| $1$      | $1$      |          |          |          |           |           |          |            |
| $\hline$ | $\hline$ | $\hline$ | $\hline$ | $\hline$ | $\hline$  | $\hline$  | $\hline$ | $\hline$   |
| $1$      | $2$      |          |          |          |           |           |          |            |
| $1$      | $2$      |          |          |          |           |           |          |            |
| $\ddots$ |          |          |          |          |           |           |          |            |
| $\ddots$ |          |          |          |          |           |           |          |            |
| $1$      | $2$      |          |          |          |           |           |          |            |
| $\hline$ | $\hline$ | $\hline$ | $\hline$ | $\hline$ | $\hline$  | $\hline$  | $\hline$ | $\hline$   |
|          |          |          |          |          | $A$       | $B$       |          |            |
|          |          |          |          |          |           |           |          |            |
|          |          |          |          |          | $B^T$     | $C$       |          |            |
|          |          |          |          |          |           |           |          |            |

(16.1.41)

Здесь  $B$  имеет  $k$  строк и  $k-1$  столбцов. Так как  $B_{k+3}, \dots, B_{2k+1}$  связаны с  $B_1$ , каждый из столбцов

$k+3, \dots, 2k+1$  в (16.1.41) содержит, помимо 1 и 2 в первой и второй строках, в точности  $k$  единиц и  $k-2$  двоек. Поэтому каждый столбец подматрицы  $B$  содержит не менее двух единиц, и поскольку  $2(k-1) > k$ , в  $B$  должна существовать хотя бы одна строка, содержащая не менее двух единиц. Пусть блоки перенумерованы так, что такая строка является третьей и соответствует блоку  $B_3$ . В обозначениях (16.1.37) при таком выборе  $B_3$

мы имеем  $k-1-j$  столбцов  $\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$ , причем  $k-1-j \geq 2$ ,

или  $j \leq k-3$ . В силу (16.1.40) это возможно только при  $j=0$ . Поэтому (16.1.41) принимает следующий вид:

|            | $B_1$ | $B_2$ | $B_3$ | $B_4 \dots B_{k+2}$ | $B_{k+3} \dots B_{2k+1}$ |
|------------|-------|-------|-------|---------------------|--------------------------|
| $B_1$      | $k$   | 1     | 1     | 1 ... 1             | 1 ... 1                  |
| $B_2$      | 1     | $k$   | 1     | 1 ... 1             | 2 ... 2                  |
| $B_3$      | 1     | 1     | $k$   | 2 ... 2             | 1 ... 1                  |
| $B_4$      | 1     | 1     | 2     |                     |                          |
|            | ⋮     | ⋮     | ⋮     | $A$                 |                          |
|            | ⋮     | ⋮     | ⋮     | $B$                 |                          |
| $B_{k+2}$  | 1     | 1     | 2     |                     |                          |
| $B_{k+3}$  | 1     | 2     | 1     |                     |                          |
|            | ⋮     | ⋮     | ⋮     | $B^T$               |                          |
| $B_{2k+1}$ | 1     | 2     | 1     |                     |                          |

(16.1.42)

Рассмотрим структурную матрицу для блоков  $B_3, B_1, B_2, B_i, B_j$  при любых  $i, j, 4 \leq i, j \leq k+2$ . Это матрица вида  $S_5^{(1)}$  [см. (16.1.34)] и по лемме 16.1.5  $s_{ij} = 1, i \neq j$ . Следовательно, все недиагональные элементы в  $A$  — единицы. Каждая строка, соответствующая блокам  $B_4, \dots, B_{k+2}$ , содержит в точности  $k+1$  единиц, поэтому каждая строка в  $B$  содержит одну единицу, а все остальные ее элементы — двойки. Это показывает, что наш выбор блока  $B_3$  со строкой, содержащей не менее двух

единиц в столбцах  $k+3, \dots, 2k+1$ , был фактически единственным возможным. Если взять блоки

$$B_2, B_1, B_3, B_i, B_1 \text{ с } k+3 \leq i, j \leq 2k+1,$$

то для них структурная матрица имеет вид  $S_5^{(1)}$  и по лемме 16.1.5 каждый недиагональный элемент в  $C$  равен 1. Отсюда также следует, что в каждом столбце подматрицы  $B$  найдется в точности одна единица. Можно так перенумеровать  $B_{k+3}, \dots, B_{2k+1}$ , что все единицы в  $B$  лежат на главной диагонали, так как в каждой строке и в каждом столбце матрицы  $B$  имеется в точности одна единица.

Предыдущие рассмотрения показывают, что блоки множества

$$S_1 = \{B_1, B_2, B_4, B_5, \dots, B_{k+2}\}$$

связаны друг с другом, и то же самое верно для блоков множества

$$S_2 = \{B_1, B_3, B_{k+3}, B_{k+4}, \dots, B_{2k+1}\}.$$

Полученные результаты можно сформулировать следующим образом.

**Лемма 16.1.6.** *Любой блок  $B_1$  и  $2k$  связанных с ним блоков единственным способом распределяются по двум множествам  $S_1$  и  $S_2$ , имеющим только один общий блок  $B_1$ , каждое из которых состоит из  $k+1$  попарно связанных блоков.*

**Доказательство.** Все, что требуется для доказательства леммы, — это установить единственность подразделения блоков  $B_1, B_2, \dots, B_{2k+1}$  на множества  $S_1$  и  $S_2$ . Если нумерация блоков  $B_{k+3}, \dots, B_{2k+1}$  такова, что единицы в матрице  $B$  из (16.1.42) лежат на главной диагонали, то  $B_i$  и  $B_{i+k-1}$  при  $i=4, \dots, k+2$  связаны, так же как  $B_2$  и  $B_3$ . С другой стороны, любые  $B_i \neq B_1$  из  $S_1$  и  $B_j \neq B_1$  из  $S_2$  дважды связаны. Поэтому множество из  $k+1$  попарно связанных блоков единственным образом определяется блоком  $B_1$  и любым связанным с ним блоком; при этом получается либо множество  $S_1$ , либо множество  $S_2$ .

Мы можем теперь продолжить доказательство теоремы 16.1.3. Для доказательства этой теоремы достаточно найти множества  $S_i$ , со свойствами 1) – 4), указанными в теореме 16.1.2. Для каждого блока мы определили множества  $S_1$  и  $S_2$ , обладающие по лемме 16.1.6 свойствами 1) и 4). Пусть  $n$  – общее число таких множеств. Так как имеется всего  $b = (k+1)(k+2)/2$  блоков и каждый из этих блоков находится точно в двух множествах, содержащих по  $k+1$  блоков, число  $n$  должно удовлетворять соотношению  $2b = n(k+1)$ , следовательно,  $n = k+2$ , как и требуется в теореме 16.1.2. Далее, любой блок является единственным общим блоком для двух множеств  $S$ , содержащих его. Поскольку  $n = k+2$ , отсюда следует, что совокупность  $n(n-1)/2 = b$  пересечений множеств  $S$  включает каждый блок в точности один раз. Это есть свойство 3) теоремы 16.1.2.

Докажем теперь свойство 2) теоремы 16.1.2. Пусть  $m_i$  – число элементов, появляющихся  $i$  раз в каком-либо множестве  $S_i$ . Тогда справедливы следующие соотношения:

$$\sum_{i=0}^{k+1} m_i = v = \frac{k(k+1)}{2},$$

$$\sum_{i=0}^{k+1} i m_i = k(k+1), \quad (16.1.43)$$

$$\sum_{i=0}^{k+1} i(i-1)m_i = k(k+1).$$

Первое соотношение означает, что каждый элемент схемы учитывается точно один раз при некотором  $m_i$ ; второе соотношение получается путем подсчета общего числа элементов в  $k+1$  блоках множества  $S_i$ ; третье получается путем подсчета общего числа элементов в пересечениях  $k+1$  блоков из  $S_i$ , если при этом иметь в виду, что любые два блока из  $S_i$  связаны. Эти соотношения приводят к равенству

$$\sum_{i=0}^{k+1} (i-2)^2 m_i = 0. \quad (16.1.44)$$

Так как, конечно,  $m_i \geq 0$  при любом  $i$ , отсюда следует, что  $m_j = 0$  при  $j \neq 2$  и  $m_2 = v$ . Это есть свойство 2), и доказательство теоремы завершено. В силу единственности построения множеств  $S_i$  вложение в теореме 16.1.3 также единственно.

## 16.2. Коположительные и вполне положительные квадратичные формы

Метод Коннора не использует в полной мере информацию, содержащуюся в неявном виде в уравнении (16.1.5), которое мы перепишем здесь снова:

$$Q^* = Q - L_1^2 - \dots - L_t^2 = L_{t+1}^2 + \dots + L_b^2, \quad (16.2.1)$$

где  $Q$  и  $L_1, \dots, L_t$  известны, а  $L_{t+1}, \dots, L_b$  неизвестны. Коннор использует тот факт, что форма  $Q^*$  должна быть положительно полуопределенной. Методы Брука — Райзера — Човла основываются на рациональности форм  $L_{t+1}, \dots, L_b$ . Но в нашем распоряжении также информация другого рода, а именно  $L_{t+1}, \dots, L_b$  — линейные формы с неотрицательными коэффициентами (точнее, с коэффициентами 0 или 1). При этом естественно возникает вопрос, насколько ограничивающей является эта информация. Конечно,  $Q^*$  — положительно полуопределенная форма, имеющая неотрицательные коэффициенты. Но для квадратичных форм пяти или более переменных этих двух свойств недостаточно, чтобы гарантировать возможность представления  $Q^*$  в виде суммы квадратов линейных форм, имеющих неотрицательные коэффициенты.

В качестве примера рассмотрим следующую форму:

$$\begin{aligned} Q(x_1, \dots, x_5) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_1x_2 + \\ &\quad + x_1x_5 + x_2x_3 + \frac{3}{2}x_3x_4 + x_4x_5 = \\ &= \left(x_2 + \frac{1}{2}x_1 + \frac{1}{2}x_3\right)^2 + \left(x_5 + \frac{1}{2}x_1 + \frac{1}{2}x_4\right)^2 + \\ &\quad + \frac{1}{2}\left(x_1 - \frac{1}{2}x_3 - \frac{1}{2}x_4\right)^2 + \frac{5}{8}(x_3 + x_4)^2. \end{aligned} \quad (16.2.2)$$

Из первого представления  $Q$  видно, что она имеет положительные коэффициенты, а из второго — что  $Q$

полуопределена. Но мы покажем непосредственно, что  $Q$  не может быть представлена в виде суммы квадратов неотрицательных линейных форм. Предположим от противного, что

$$Q = L_1^2 + \dots + L_r^2 + L_{r+1}^2 + \dots + L_n^2, \quad (16.2.3)$$

где линейные формы  $L$  имеют неотрицательные коэффициенты и перенумерованы так, что  $L_1, \dots, L_r$  — формы, в которых как  $x_3$ , так и  $x_4$  имеют положительные коэффициенты. Так как в  $Q$  нет членов с  $x_1x_3$ ,  $x_2x_4$  и  $x_3x_5$ , формы  $L_1, \dots, L_r$  должны иметь нулевые коэффициенты при  $x_1, x_2$  и  $x_5$ , т. е.  $L_i = u_{i3}x_3 + u_{i4}x_4$ ,  $u_{i3} > 0$ ,  $u_{i4} > 0$ ,  $i = 1, \dots, r$ . Следовательно,

$$L_1^2 + \dots + L_r^2 = Ax_3^2 + \frac{3}{2}x_3x_4 + Bx_4^2. \quad (16.2.4)$$

Если обозначить

$$Q_1 = Q_1(x_1, \dots, x_5) = L_{r+1}^2 + \dots + L_n^2, \quad (16.2.5)$$

то (16.2.3) принимает вид

$$Q(x_1, \dots, x_5) = Ax_3^2 + \frac{3}{2}x_3x_4 + Bx_4^2 + Q_1(x_1, \dots, x_5). \quad (16.2.6)$$

Полагаем

$$x_1 = \frac{x_3 + x_4}{2}, \quad x_2 = \frac{-(3x_3 + x_4)}{4}, \quad x_5 = -\frac{x_3 + 3x_4}{4}. \quad (16.2.7)$$

Эта подстановка не изменяет (16.2.4), а  $Q$  сводится к  $\frac{5}{8}(x_3 + x_4)^2$  [см. (16.2.2)]. Следовательно, (16.2.6) принимает вид

$$\frac{5}{8}(x_3 + x_4)^2 = Ax_3^2 + \frac{3}{2}x_3x_4 + Bx_4^2 + Q_1. \quad (16.2.8)$$

При этой подстановке свойство полуопределенности формы  $Q_1$  сохраняется, так что  $0 \leq A \leq \frac{5}{8}$ ,  $0 \leq B \leq \frac{5}{8}$ . Теперь, полагая в (16.2.4)  $x_3 = 1$ ,  $x_4 = -1$ , получаем

$$(u_{13} - u_{14})^2 + \dots + (u_{r3} - u_{r4})^2 = A - \frac{3}{2} + B \leq \frac{5}{8} - \frac{3}{2} + \frac{5}{8} = -\frac{1}{4}, \quad (16.2.9)$$

что невозможно. Следовательно, предположение (16.2.3), что  $Q$  можно записать в виде суммы квадратов неотрицательных линейных форм, неверно. Поэтому свойство формы  $Q^*$  в (16.2.1) быть представимой в виде суммы квадратов неотрицательных линейных форм является, вообще говоря, более сильным, чем свойство быть положительно полуопределенной формой, имеющей неотрицательные коэффициенты.

Чтобы продолжить рассмотрение общей задачи, введем следующие обозначения:

$$Q = Q(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij}x_i x_j, \quad a_{ii} = a_{ji}, \quad (16.2.10)$$

и, если не возникает двусмысленности, можно (16.2.10) записывать сокращенно  $Q = \sum a_{ij}x_i x_j$ . Условие  $L_i \geq 0$  означает, что

$$L_i = u_{1i}x_1 + \dots + u_{ni}x_n, \quad u_{si} \geq 0, \quad s = 1, \dots, n, \quad (16.2.11)$$

и  $x = (x_1, \dots, x_n) \geq 0$  означает, что

$$x_i \geq 0, \quad i = 1, \dots, n. \quad (16.2.12)$$

**Определение.** Квадратичная форма  $Q = Q(x_1, \dots, x_n)$  называется *вполне положительной*, если  $Q$  можно представить в виде

$$Q = \sum_{i=1}^N L_i^2, \quad L_i \geq 0, \quad i = 1, \dots, N. \quad (16.2.13)$$

**Определение.** Квадратичная форма  $Q = Q(x_1, \dots, x_n)$  называется *коположительной*, если  $Q(x_1, \dots, x_n) \geq 0$ , как только  $(x_1, \dots, x_n) \geq 0$ .

Квадратичной форме  $Q(x_1, \dots, x_n) = \sum a_{ij}x_i x_j$  можно поставить в соответствие точку евклидова пространства  $E_m$ , где  $m = (n^2 + n)/2$ , следующим образом:

$$\begin{aligned} Q &= \sum_{i,j=1}^n a_{ij}x_i x_j \Leftrightarrow \\ &\Leftrightarrow (a_{11}, a_{22}, \dots, a_{nn}, \sqrt{2}a_{12}, \dots, \sqrt{2}a_{1n}, \dots, \sqrt{2}a_{n-1,n}). \end{aligned} \quad (16.2.14)$$

При этом соответствии каждой квадратичной форме от  $n$  переменных соответствует единственная точка в  $E_m$ , и обратно. Будем применять терминологию выпуклых пространств и теоремы о них (см. гл. 8).

**Теорема 16.2.1.** *Пространства коположительных квадратичных форм от  $n$  переменных и вполне положительных квадратичных форм от  $n$  переменных — замкнутые выпуклые конусы. Каждое из них является двойственным конусом другого.*

**Доказательство.** Если  $Q_1$  и  $Q_2$  — коположительные квадратичные формы, то непосредственно из определения следует, что  $Q_1 + Q_2$  и  $bQ_1$ ,  $b \geq 0$ , также коположительны. Поэтому коположительные квадратичные формы образуют выпуклый конус. Пусть квадратичная форма  $Q$  есть предел последовательности коположительных форм  $Q_k$ ,  $k = 1, 2, \dots$  (где предел определяется в терминах евклидовой метрики в  $E_m$ ). Тогда для точки  $x = (x_1, \dots, x_n) \geq 0$  в  $E_n$  каждое  $Q_k(x_1, \dots, x_n) \geq 0$ , и поскольку квадратичные формы — непрерывные функции своих коэффициентов, отсюда следует, что  $Q(x_1, \dots, x_n) \geq 0$ . Следовательно,  $Q$  коположительна, и пространство коположительных квадратичных форм замкнуто.

Аналогично если  $Q_1$  и  $Q_2$  вполне положительны, то по определению  $Q_1 + Q_2$  также вполне положительна. Если  $Q_1 = L_1^2 + \dots + L_N^2$ ,  $L_i \geq 0$  и  $b \geq 0$ , то при  $c \geq 0$ , таком, что  $c^2 = b$ ,  $bQ_1 = (cL_1)^2 + \dots + (cL_N)^2$ , где  $cL_i \geq 0$ . Следовательно, вполне положительные квадратичные формы образуют выпуклый конус. Замкнутость этого конуса уже несколько менее очевидна. Для доказательства замкнутости нам нужна следующая лемма.

**Лемма 16.2.1.** *Если  $Q = Q(x_1, \dots, x_n) = L_1^2 + \dots + L_N^2$ , где  $L_i \geq 0$ ,  $i = 1, \dots, N$ , то  $Q$  имеет также представление этого же вида с  $N < 2^n$ .*

**Доказательство.** Пусть две из форм  $L_i$  имеют положительные коэффициенты в точности при одних и тех же переменных  $x_j$ . Перенумеруем индексы таким образом, чтобы эти формы были  $L_1$  и  $L_2$ , а перемен-

ные —  $x_1, \dots, x_s$ . Тогда имеем

$$\begin{aligned} L_1 &= c_1 x_1 + \dots + c_s x_s, \quad c_i > 0, \quad i = 1, \dots, s, \\ L_2 &= d_1 x_1 + \dots + d_s x_s, \quad d_i > 0, \quad i = 1, \dots, s. \end{aligned} \quad (16.2.15)$$

Если теперь,  $\theta$  — некоторый угол, то имеет место тождество

$$\begin{aligned} L_1^2 + L_2^2 &= (L_1 \cos \theta + L_2 \sin \theta)^2 + (-L_1 \sin \theta + L_2 \cos \theta)^2 = \\ &= L'_1^2 + L'_2^2. \end{aligned} \quad (16.2.16)$$

При любом  $\theta$  из первого квадранта  $L'_1$  имеет положительные коэффициенты, а при достаточно малом  $\theta$  это верно и для  $L'_2$ , хотя при  $\theta = \pi/2$  у формы  $L'_2 = -L_1$  все коэффициенты отрицательны. Поэтому, когда  $\theta$  возрастает от 0 до  $\pi/2$ , найдется значение  $\theta$ , при котором по крайней мере один коэффициент в  $L'_2$  обращается в нуль, а ненулевые коэффициенты в  $L'_2$  остаются положительными. При этом значении  $\theta$  форма  $L'_1$  имеет положительные коэффициенты при тех же самых переменных, что и  $L_1$ , а  $L'_2$  — для меньшего числа переменных. Таким образом, в выражении  $Q = L_1^2 + \dots + L_N^2$  с  $L_i \geq 0$  мы можем предположить, что ни одно из  $L_i$  не есть тождественный нуль и что никакие две линейные формы не могут иметь положительные коэффициенты в точности при одних и тех же переменных. Следовательно,  $N$  не больше числа различных непустых подмножеств множества из  $n$  элементов, т. е.  $N < 2^n$ . По одной общей теореме о выпуклых конусах, здесь не приведенной, получается следующая граница для  $N$ :  $N \leq m = (n^2 + n)/2$  — размерности пространства, но граница  $N < 2^n$  достаточна для наших целей.

Если теперь  $Q = Q(x_1, \dots, x_n)$  есть предел последовательности  $Q_k$  ( $k = 1, 2, \dots$ ) вполне положительных квадратичных форм, то каждое  $Q_k$  можно представить в виде суммы квадратов  $N$  неотрицательных линейных форм, где  $N < 2^n$ . Если коэффициенты форм  $Q_k$  при  $k \geq k_0$  отличаются от коэффициентов формы  $Q$  менее чем на  $1/2$ , то коэффициенты этих  $N$  линейных форм равномерно ограничены, и для последовательности  $Q_k$

формы  $L_1, \dots, L_n$  имеют пределы, являющиеся неотрицательными линейными формами, сумма квадратов которых равна  $Q$ . Таким образом,  $Q$  вполне положительна, и конус вполне положительных форм — замкнутый конус.

Если  $(c_1, \dots, c_n) \geqslant 0$ , то по определению

$$Q_2 = (c_1 x_1 + \dots + c_n x_n)^2 = \sum c_i c_j x_i x_j = \sum b_{ij} x_i x_j \quad (16.2.17)$$

— вполне положительная форма.

Пусть  $Q_1 = \sum a_{ij} x_i x_j$  — квадратичная форма. Если  $q_1, q_2$  — точки в  $E_m$ , соответствующие  $Q_1$  и  $Q_2$ , то скалярное произведение  $(q_1, q_2)$ , согласно (16.2.14), равно

$$(q_1, q_2) = a_{11} b_{11} + \dots + a_{nn} b_{nn} + 2a_{12} b_{12} + \dots$$

$$\dots + 2a_{n-1, n} b_{n-1, n} = \sum_{i,j} a_{ij} b_{ij}, \quad i, j = 1, \dots, n. \quad (16.2.18)$$

Если  $b_{ij} = c_i c_j$ , как в (16.2.17), то

$$(q_1, q_2) = \sum a_{ij} c_i c_j. \quad (16.2.19)$$

Предположим теперь, что  $Q_1$  обладает тем свойством, что  $(q_1, q_2) \geqslant 0$  при всяком  $Q_2$  вида

$$Q_2 = L^2 = (c_1 x_1 + \dots + c_n x_n)^2, \quad (c_1, \dots, c_n) \geqslant 0.$$

Тогда из (16.2.19) следует, что

$$\sum a_{ij} c_i c_j \geqslant 0 \text{ при } (c_1, \dots, c_n) \geqslant 0. \quad (16.2.20)$$

Это равносильно утверждению, что  $Q_1$  коположительна. С другой стороны, если

$$Q_2 = L_1^2 + \dots + L_t^2 = Q_2^{(1)} + \dots + Q_2^{(t)},$$

$$L_i \geqslant 0, \quad i = 1, \dots, t,$$

то из  $(q_1, q_2^{(i)}) \geqslant 0, i = 1, \dots, t$ , и билинейности скалярного произведения следует, что  $(q_1, q_2) \geqslant 0$ . Это показывает, что если  $H$  — конус вполне положительных квадратичных форм, то  $H^*$  есть конус коположительных форм. Поскольку  $H$  — замкнутый выпуклый конус, отсюда по теореме 8.1.5 следует, что  $(H^*)^* = H$ . Это доказывает, что конусы коположительных и вполне положительных форм двойственны один другому. Теорема 16.2.1 полностью доказана.

Заметим, что для множеств  $A$  и  $B$  в  $E_m$

$$A \equiv B \text{ влечет за собой } A^* \subseteq B^*. \quad (16.2.21)$$

Это утверждение следует непосредственно из определения двойственности, так как если  $(x, y) \geqslant 0$  для данного  $x$  и всех  $y \in A$ , то, разумеется,  $(x, y) \geqslant 0$  для всех  $y \in B$ . Таким образом,  $x \in A^*$  влечет за собой  $x \in B^*$ .

Для любых двух множеств  $A$  и  $B$  в  $E_n$  пусть  $A \cap B$  есть множество точек, общих для  $A$  и  $B$ , а  $A + B$  — множество всех точек  $a + b$ ,  $a \in A$ ,  $b \in B$ .

**Лемма 16.2.2.** *Если  $C_1$  и  $C_2$  — два замкнутых выпуклых конуса, то  $C_1 \cap C_2$  и  $C_1 + C_2$  — также замкнутые выпуклые конусы и  $(C_1 + C_2)^* = C_1^* \cap C_2^*$ ,  $(C_1 \cap C_2)^* = C_1^* + C_2^*$ .*

**Доказательство.** Проверка того факта, что  $C_1 \cap C_2$  и  $C_1 + C_2$  — замкнутые выпуклые конусы, тривиальна. Рассмотрим  $(C_1 + C_2)^*$ . Так как  $C_1 \subseteq C_1 + C_2$  и  $C_2 \subseteq C_1 + C_2$ , из (16.2.21) следует, что  $(C_1 + C_2)^* \subseteq C_1^*$  и  $(C_1 + C_2)^* \subseteq C_2^*$ . Поэтому  $(C_1 + C_2)^* \subseteq C_1^* \cap C_2^*$ . Пусть теперь  $y \in C_1^* \cap C_2^*$ . Любая точка  $x \in C_1 + C_2$  может быть представлена в виде  $x = x_1 + x_2$ ,  $x_1 \in C_1$ ,  $x_2 \in C_2$ . Поэтому  $(x, y) = (x_1 + x_2, y) = (x_1, y) + (x_2, y)$ . Так как  $(x_1, y) \geqslant 0$  и  $(x_2, y) \geqslant 0$ , то  $(x, y) \geqslant 0$  и  $y \in (C_1 + C_2)^*$ . Таким образом,  $C_1^* \cap C_2^* \subseteq (C_1 + C_2)^*$ , и из двух противоположных включений получаем, что  $(C_1 + C_2)^* = C_1^* \cap C_2^*$ . Используя это равенство, по теореме 8.1.5 находим, что

$$(C_1^* + C_2^*)^* = (C_1^*)^* \cap (C_2^*)^* = C_1 \cap C_2.$$

Отсюда

$$(C_1 \cap C_2)^* = C_1^* + C_2^*,$$

т. е. установлено и второе соотношение леммы.

Обозначим класс вполне положительных квадратичных форм через  $B$ ; мы используем это обозначение ввиду связи этого класса с блок-схемами. Класс коположительных форм обозначим через  $C$ . Еще два класса связаны с этими классами — класс  $P$  форм с положительными коэффициентами и класс  $S$  полуопределеных квадратичных форм.

**Лемма 16.2.3.** *Каждый из классов  $P$  и  $S$  двойствен самому себе.*

**Доказательство.** Класс  $P$ , очевидно, — замкнутый конус. В  $P$  возьмем формы  $Q_{rs}$  с  $b_{rs} = 1$ ,  $b_{ij} = 0$  в остальных случаях. Если теперь  $Q = \sum a_{ij}x_i x_j$  и  $Q \in P^*$ , то

$$(q, q_{rs}) = a_{rs} \text{ или } 2a_{rs}$$

и  $a_{rs} \geq 0$ . Следовательно,  $Q \in P$  и  $P = P^*$ . Класс  $S$  также, очевидно, замкнут. Пусть

$$Q_0 = (c_1 x_1 + \dots + c_n x_n)^2$$

— произвольная форма ранга 1 в  $S$ . Если  $Q = \sum a_{ij}x_i x_j$  и  $Q \in S^*$ , то

$$(q, q_0) = \sum a_{ij}c_i c_j \geq 0.$$

Это означает, что  $Q$  неотрицательна для всех действительных значений  $x_1, \dots, x_n$ . Следовательно,  $Q \in S$  и  $S = S^*$ .

Так как каждая положительная форма и каждая полуопределенная форма коположительны, мы имеем

$$C \equiv P + S. \quad (16.2.22)$$

По теореме 16.2.1  $C^* = B$  и  $B^* = C$ , а леммы 16.2.2 и 16.2.3 дают

$$B = C^* \subseteq (P + S)^* = P^* \cap S^* = P \cap S. \quad (16.2.23)$$

Равенство в соотношении (16.2.22) влечет за собой равенство в соотношении (16.2.23), и наоборот. Диананда [1] доказал, что  $C = P + S$  для форм с числом переменных не больше четырех, но пример (16.2.2) показывает, что для пяти переменных классы  $B$  и  $P \cap S$  не совпадают.

Легко определить экстремальные точки (экстремальные формы) для классов  $P$ ,  $S$  и  $B$ .

**Теорема 16.2.2.** *Экстремальные формы для класса  $P$  положительных форм, класса  $S$  положительно полуопределенных форм и класса  $B$  вполне положительных форм следующие:*

1. Для класса  $P$ 

$$ax_i^2, \quad a > 0; \quad bx_i x_j, \quad b > 0, \quad i \neq j,$$

$$i, j = 1, \dots, n.$$

2. Для класса  $S$  — формы ранга 1

$$(c_1 x_1 + \dots + c_n x_n)^2;$$

где  $c_i$  — действительные числа, не равные одновременно нулю.

3. Для класса  $B$  — формы ранга 1

$$(c_1 x_1 + \dots + c_n x_n)^2, \quad c_i \geq 0, \quad i = 1, \dots, n,$$

где  $c_i$  — действительные числа, не равные одновременно нулю.

**Доказательство.** Для класса  $P$  справедливость утверждения получается непосредственно. Для класса  $S$  каждая форма может быть записана в виде

$$Q = L_1^2 + \dots + L_t^2.$$

Пусть  $Q = (c_1 x_1 + \dots + c_n x_n)^2 \neq 0$ . Если не каждая  $L_i$  есть скалярное кратное формы  $L_0 = c_1 x_1 + \dots + c_n x_n$ , то мы можем найти числа  $x_1, \dots, x_n$ , не равные одновременно нулю, такие, что  $L_0 = 0$ , а некоторое  $L_i \neq 0$ . Но так как  $L_0^2 = L_1^2 + \dots + L_t^2$ , получаем противоречие. То же рассуждение годится и для класса  $B$ . Так как формы для классов  $P, S, B$  могут быть выражены в виде суммы конечного числа перечисленных экстремальных форм, отсюда следует, что этими последними исчерпываются все экстремальные формы соответствующих классов.

Экстремальные формы класса  $C$  до сих пор не описаны. В следующей теореме указываются некоторые из них.

**Теорема 16.2.3.** Совокупность экстремальных форм класса  $C$  коположительных форм от  $x_1, \dots, x_n$  включает следующие формы:  $ax_i^2, a > 0, i = 1, \dots, n$ ,  $bx_i x_j, b > 0, i \neq j, i, j = 1, \dots, n$ , и  $(U - V)^2$ , где

$$U = \sum_{i=1}^r a_i u_i, \quad V = \sum_{i=1}^s b_i v_i, \quad a_i > 0, \quad b_i > 0, \quad r \geq 1, \quad s \geq 1$$

и  $\{u_1, u_2, \dots, u_r\}$  и  $\{v_1, v_2, \dots, v_s\}$  — непересекающиеся подмножества множества  $\{x_1, \dots, x_n\}$ . Эти формы — экстремальные точки в  $P + S$ .

**Доказательство.** Если  $Q = \sum a_{ij}x_i x_j$  коположительна, то при  $x_i = 1, x_j = 0, j \neq i$ , имеем  $Q = a_{ii} \geq 0$ . Далее, если в форме

$$Q = a_{ii}x_i^2 + 2a_{ij}x_i x_j = x_i(a_{ii}x_i + 2a_{ij}x_j)$$

с  $a_{ii} \geq 0$  и  $a_{ij} < 0$  взять  $x_j = 1$  и  $x_i = \epsilon > 0$  достаточно малым, то  $Q < 0$ . Следовательно, если в коположительной форме  $a_{ii} = 0$  или  $a_{jj} = 0$ , то  $a_{ii} \geq 0$ .

Допустим теперь, что  $a_{rr}x_r^2 = Q_1 + Q_2$ , где  $Q_1$  и  $Q_2$  коположительны и

$$Q_1 = \sum b_{ij}x_i x_j, \quad Q_2 = \sum c_{ij}x_i x_j.$$

Тогда при  $j \neq r$

$$b_{jj} \geq 0, \quad c_{jj} \geq 0 \text{ и } b_{jj} + c_{jj} = 0,$$

следовательно,  $b_{jj} = c_{jj} = 0$ . Точно так же  $b_{ij} \geq 0, c_{ij} \geq 0, b_{ij} + c_{ij} = 0$  во всех случаях с  $i \neq j$ , поэтому  $b_{ij} = c_{ij} = 0$ . Таким образом,

$$Q_1 = b_{rr}x_r^2, \quad Q_2 = c_{rr}x_r^2, \quad b_{rr}, c_{rr} \geq 0,$$

т. е. форма  $Q = a_{rr}x_r^2$  экстремальна. Аналогично пусть  $Q = a_{rs}x_r x_s, r \neq s$ , и  $Q = Q_1 + Q_2, Q_1 = \sum b_{ij}x_i x_j, Q_2 = \sum c_{ij}x_i x_j$ , где  $Q_1$  и  $Q_2$  — коположительны. Для любого  $i$   $b_{ii} \geq 0, c_{ii} \geq 0$  и  $b_{ii} + c_{ii} = 0$ , следовательно,  $b_{ii} = c_{ii} = 0$ . Сделанное выше замечание показывает, что  $b_{ij} \geq 0, c_{ij} \geq 0$  для всех  $i \neq j$ . Тогда, исключая случай  $i = r, j = s$ , имеем  $b_{ij} = c_{ij} = 0$ . Следовательно,  $Q_1 = 2b_{rs}x_r x_s, Q_2 = 2c_{rs}x_r x_s$  и форма  $a_{rs}x_r x_s$  экстремальна.

Чтобы показать экстремальность формы  $(U - V)^2$ , где

$$U = a_1u_1 + \dots + a_ru_r, \quad V = b_1v_1 + \dots + b_sv_s,$$

$$a_i > 0, \quad b_i > 0, \quad r \geq 1, \quad s \geq 1,$$

и  $\{u_1, u_2, \dots, u_r\}, \{v_1, v_2, \dots, v_s\}$  — непересекающиеся подмножества множества  $\{x_1, \dots, x_n\}$ , достаточно заме-

нить  $a_i u_i$  на  $y_i$  и  $b_j v_j$  на  $z_j$  и показать, что

$$(y_1 + \dots + y_r - z_1 - \dots - z_s)^2, \quad r \geq 1, \quad s \geq 1,$$

является экстремальной формой относительно переменных  $y_i, z_j$ . Рассмотрим сначала форму  $(y_1 - z_1)^2$  и ее представление в виде  $(y_1 - z_1)^2 = Q_1 + Q_2$ , где  $Q_1$  и  $Q_2$  — коположительные формы от  $y_1$  и  $z_1$ . При  $y_1 = z_1$  имеем  $Q_1 = Q_2 = 0$ . Следовательно,

$$\begin{aligned} Q_1 &= (y_1 - z_1)(ay_1 - bz_1), \\ Q_2 &= (y_1 - z_1)(cy_1 - dz_1), \end{aligned} \quad (16.2.24)$$

где  $a, b, c, d$  неотрицательны и  $a + c = 1, b + d = 1$ . Если  $a > b$ , то, полагая  $z_1 = y_1 + e$ , при положительных  $y_1, z_1$  и достаточно малом  $e > 0$  имеем  $Q_1 < 0$ , что невозможно. Аналогично при  $a < b$ , взяв  $z_1 = y_1 - e$ , для достаточно малого  $e > 0$  получим  $Q_1 < 0$ , т. е. снова приходим к противоречию. Следовательно,  $a = b$ ,

$$Q_1 = a(y_1 - z_1)^2, \quad Q_2 = (1 - a)(y_1 - z_1)^2$$

и  $Q$  экстремальна. Пусть теперь

$$Q = (y_1 + y_2 - z_1)^2 = Q_1 + Q_2.$$

Полагая поочередно  $y_1$  и  $y_2$  равными нулю, получаем, согласно предыдущему случаю, что

$$Q_1 = a(y_1^2 + y_2^2 + z_1^2 - 2y_1 z_1 - 2y_2 z_1) + ky_1 y_2, \quad (16.2.25)$$

$$Q_2 = (1 - a)(y_1^2 + y_2^2 + z_1^2 - 2y_1 z_1 - 2y_2 z_1) + ty_1 y_2,$$

где  $0 \leq a \leq 1$  и, конечно,  $k + t = 2$ . Отсюда

$$Q_1 = a(y_1 + y_2 - z_1)^2 + (k - 2a)y_1 y_2, \quad (16.2.26)$$

$$Q_2 = (1 - a)(y_1 + y_2 - z_1)^2 + (t + 2a - 2)y_1 y_2.$$

Если  $k - 2a < 0$ , то полагаем  $y_1 = y_2 = 1, z_1 = 2$  и тогда  $Q_1 < 0$ . Следовательно, должно быть  $k - 2a \geq 0$ . Аналогично  $t + 2a - 2 \geq 0$ . Поскольку  $k + t = 2$ ,

$$0 = (k - 2a) + (t + 2a - 2). \quad (16.2.27)$$

Значит,  $k = 2a, t = 2 - 2a$ ,

$$Q_1 = a(y_1 + y_2 - z_1)^2, \quad Q_2 = (1 - a)(y_1 + y_2 - z_1)^2,$$

и  $Q = (y_1 + y_2 - z_1)^2$  экстремальна. То же рассуждение показывает, что

$$(y_1 - z_1 - z_2)^2$$

— экстремальная форма.

В общем случае предположим, что

$$Q = (y_1 + \dots + y_r - z_1 - \dots - z_s)^2 = Q_1 + Q_2,$$

где  $Q_1$  и  $Q_2$  коположительны. Пусть

$$Q_1 = ay_1^2 + \dots \text{ и } Q_2 = (1-a)y_1^2 + \dots$$

Полагая соответствующие  $y_i$  и  $z_j$  равными нулю, мы можем воспользоваться уже рассмотренными случаями, чтобы определить все коэффициенты у  $Q_1$  и  $Q_2$  и убедиться, что  $Q_1 = aQ$ ,  $Q_2 = (1-a)Q$ , где  $0 \leq a \leq 1$ . Следовательно,  $Q$  экстремальна. Заметим, что форма

$$(U + V)^2 = (U - V)^2 + 4UV$$

не может быть экстремальной. Так как каждая форма в  $P + S$  есть сумма конечного числа рассмотренных форм, то найдены все экстремальные формы класса  $P + S$ .

В  $C$  имеются другие экстремальные формы, не содержащиеся в  $P + S$ . Следующая форма, открытая А. Хорном, носит название „формы Хорна“:

$$Q = (x_1 + x_2 + x_3 + x_4 + x_5)^2 - 4x_1x_2 - 4x_2x_3 - 4x_3x_4 - 4x_4x_5 - 4x_5x_1. \quad (16.2.28)$$

Мы можем выразить  $Q$  следующими двумя способами:

$$Q = \begin{cases} (x_1 - x_2 + x_3 + x_4 - x_5)^2 + 4x_2x_4 + 4x_3(x_5 - x_4), \\ (x_1 - x_2 + x_3 - x_4 + x_5)^2 + 4x_2x_5 + 4x_1(x_4 - x_5). \end{cases} \quad (16.2.29)$$

При  $x_5 \geq x_4$  первое выражение показывает, что  $Q \geq 0$ , тогда как второе выражение дает, что  $Q \geq 0$ , если  $x_4 \geq x_5$ . Следовательно,  $Q$  коположительна. Кроме того,  $Q$  — экстремальная форма, ибо если  $Q = Q_1 + Q_2$ , где  $Q_1$  и  $Q_2$  коположительны, то при  $x_4 = x_5 = 0$  форма  $Q$  сводится к экстремальной форме  $(x_1 - x_2 + x_3)^2$ . Следова-

тельно,

$$\begin{aligned} Q_1 &= a(x_1 - x_2 + x_3)^2 + x_4L + x_5M, \\ Q_2 &= (1-a)(x_1 - x_2 + x_3)^2 + x_4U + x_5V. \end{aligned} \quad (16.2.30)$$

Точно так же, полагая поочередно  $x_i = x_{i+1} = 0$  для  $i = 1, 2, 3$  и  $x_5 = x_1 = 0$ , мы каждый раз получаем экстремальную форму. Сравнение всех этих случаев дает соотношения  $Q_1 = aQ$  и  $Q_2 = (1-a)Q$ . Следовательно,  $Q$  экстремальна. Очевидно,  $Q \notin P$  и  $Q \notin S$ , и, поскольку  $Q$  экстремальна,  $Q \notin P + S$ .

Если мы в качестве  $Q_1$  возьмем квадратичную форму (16.2.2), а в качестве  $Q_2$  — форму Хорна (16.2.28), то для соответствующих точек  $q_1$  и  $q_2$  из  $E_{15}$  будет

$$(q_1, q_2) = -\frac{1}{2}. \quad (16.2.31)$$

Так как  $Q_2 \in C$ , это означает, что  $Q_1 \notin B$ , как было показано непосредственно [см. (16.2.3)–(16.2.9)]. Так как  $Q_1 \in P \cap S$ , это показывает, как коположительные формы, не принадлежащие  $P + S$ , можно использовать для доказательства того, что какая-либо форма из  $P \cap S$  не принадлежит  $B$ .

Недавно Бомер показал существование других экстремальных коположительных форм  $Q$  от пяти переменных. Если  $Q = \sum a_{ij}x_i x_j$  нормализована, так что  $a_{11} = a_{22} = \dots = a_{55} = 1$ , то  $Q$  имеет нули вида

$$\begin{aligned} u &= (u_1, u_2, 1, 0, 0), \\ v &= (0, v_2, v_3, 1, 0), \\ w &= (0, 0, w_3, w_4, 1), \\ y &= (1, 0, 0, y_4, y_5), \\ z &= (z_1, 1, 0, 0, z_5), \end{aligned} \quad (16.2.32)$$

где ни одно из чисел  $u_1, \dots, z_5$  не равно нулю. Эти числа определяют коэффициенты  $a_{ij}$ . Один такой набор нулей следующий:

$$\begin{aligned} u &= \left( \frac{1}{8}, \frac{\sqrt{8^4 - 15}}{64}, 1, 0, 0 \right) = (0, 125; 1, 1075+; 1; 0; 0), \\ v &= \left( 0, \frac{1}{8}, \frac{\sqrt{8^4 - 15} + \sqrt{8^6 - 15}}{512}, 1, 0 \right) = \\ &\quad = (0; 0, 125; 1, 1247+; 1; 0), \end{aligned}$$

$$\begin{aligned}
 w &= \left( 0, 0, \frac{1}{8}, \frac{\sqrt{8^6 - 15} + \sqrt{8^8 - 15}}{4096}, 1 \right) = \\
 &\quad = (0; 0; 0,125; 1,1249+; 1), \\
 y &= \left( 1, 0, 0, \frac{1}{8}, \frac{\sqrt{8^8 - 15} + \sqrt{8^{10} - 15}}{8^5} \right) = \\
 &\quad = (1; 0; 0; 0,125; 1,1249+), \\
 z &= \left( \frac{7 + \sqrt{8^{10} - 15}}{8}, 1, 0, 0, 8^4 \right) = (4096,874+; 1; 0; 0; 4096).
 \end{aligned} \tag{16.2.33}$$

Хотя экстремальные формы для класса С неизвестны, имеется тест для проверки, является ли данная форма коположительной или нет. Приводимая здесь формулировка принадлежит Гарсиа.

**Тест для коположительных квадратичных форм.** Пусть  $Q = Q(x_1, \dots, x_n) = \sum a_{ij}x_i x_j$  — квадратичная форма от  $n$  переменных, и пусть приравнивание любой из переменных  $x_i$ ,  $i = 1, \dots, n$ , нулю дает коположительную форму от  $n - 1$  переменных. Если  $A = [a_{ij}]$ , то пусть  $A(\varepsilon) = A + \varepsilon I$ ,  $D(\varepsilon)$  обозначает определитель матрицы  $A(\varepsilon)$  и  $E_1(\varepsilon), \dots, E_n(\varepsilon)$  — алгебраические дополнения элементов последней строки матрицы  $A(\varepsilon)$ . Тогда  $Q$  не коположительна в том и только том случае, когда для достаточно малых положительных значений  $\varepsilon$  все величины  $E_1(\varepsilon) D(\varepsilon), \dots, E_n(\varepsilon) D(\varepsilon)$  положительны. Это можно проверить путем представления определителей в виде полиномов от  $\varepsilon$  и исследования членов с наименьшей степенью в каждом случае. В случае  $E_n(0) \neq 0$  имеет место более сильный результат:  $Q$  не коположительна в том и только том случае, когда все величины  $E_1(0) D(0), \dots, E_n(0) D(0)$  положительны.

### 16.3. Рациональные пополнения матриц инцидентности

В разд. 16.1 было отмечено, что для симметричной схемы  $D(v, k, \lambda)$  из условия Коннора вытекает требование  $s_{ij} = \lambda$ ,  $i \neq j$ , в (16.1.15), необходимость которого была показана в теореме 10.2.2. При этом возникает

естественный вопрос: является ли требование рациональности, а также действительности форм  $L_{t+1}, \dots, L_b$  в (16.1.5) дополнительным ограничением, и если да, то как это ограничивает выбор начальных блоков для симметричных схем. Несколько неожиданным оказывается, что для любой рациональной  $(v \times v)$ -матрицы  $A$ , удовлетворяющей соотношению

$$AA^T = (k - \lambda) I + \lambda J, \quad (16.3.1)$$

существует рациональное пополнение и даже рациональное нормальное (см. ниже) пополнение, для которого в действительности  $s_{ij} = \lambda$ . Этот результат принадлежит автору и Райзеру [2].

Рассмотрим параметры  $v, k, \lambda$ , для которых выполнено равенство

$$k(k-1) = \lambda(v-1). \quad (16.3.2)$$

В доказательстве теоремы 10.3.1 устанавливается несколько большее, чем сказано в ее формулировке. Приведем условия Брука — Райзера — Човла:

- 1) если  $v$  четно, то  $k - \lambda$  есть квадрат;
- 2) если  $v$  нечетно, то уравнение  $z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$  имеет решение в целых  $x, y, z$ , не равных одновременно нулю.

Было доказано, что из существования рациональных линейных форм

$$L_j = \sum_i a_{ij}x_i, \quad j = 1, \dots, v,$$

удовлетворяющих соотношению (10.3.1), вытекают условия Брука — Райзера — Човла. Но (10.3.1) эквивалентно утверждению, что матрица  $A = (a_{ij})$  удовлетворяет (16.3.1). В разд. 10.4, посредством глубокой теории Хассе — Минковского, было показано обратное, т. е. что условия 1 и 2 влекут существование рациональных форм  $L_j$ , удовлетворяющих (10.3.1), и, значит, рациональной матрицы  $A$ , удовлетворяющей (16.3.1). В теореме 10.2.3 было доказано, что если дополнительно выполнено одно из условий

$$AJ = kJ, \quad JA = kJ, \quad (16.3.3)$$

то выполнено и другое и матрица  $A$  нормальна, т. е.  $AA^T = A^TA$ , а значит,

$$AA^T = A^TA = (k - \lambda)I + \lambda J. \quad (16.3.4)$$

Следующая теорема — основная в этом разделе.

**Теорема 16.3.1.** Пусть даны положительные целые числа  $v, k, \lambda$ , удовлетворяющие соотношению  $k(k-1) = \lambda(v-1)$ , и выполняется соответствующее условие 1 или 2. Пусть, кроме того, имеется рациональная  $(t \times v)$ -матрица  $A_1$  ( $0 \leq t \leq v$ ), такая, что

$$A_1 A_1^T = (k - \lambda)I_t + \lambda J_t \text{ и } A_1 J_v = k J_{t,v}. \quad (16.3.5)$$

Тогда существует рациональная  $(v \times v)$ -матрица  $A$ , в которой  $A_1$  составляет первые  $t$  строк, такая, что

$$AA^T = A^TA = (k - \lambda)I_v + \lambda J_v, \quad AJ_v = J_v A = k J_v. \quad (16.3.6)$$

Здесь  $J_t, J_v$  — квадратные матрицы из единиц, а  $J_{t,v}$  —  $(t \times v)$ -матрица из единиц.

**Замечание.** С очевидными изменениями в формулировке мы могли бы предположить, что даны первые  $t$  столбцов. Если нам даны  $t$  начальных блоков из  $k$  элементов, таких, что  $s_{ij} = \lambda$ ,  $i \neq j$ , в их структурной матрице, то это приводит к условию (16.3.5), записанному для  $t$  начальных столбцов. Но теорема формулируется всецело в терминах рациональных матриц и не содержит в явном виде никаких ссылок на блок-схемы. Тем не менее заключение теоремы резко контрастирует с выводами Коннора относительно блок-схем. В самом деле, теорема означает, что при выполнении основных условий 1 и 2 любой набор  $t$  начальных блоков, подчиненных условию  $s_{ij} = \lambda$ , может быть пополнен не только в поле действительных, но даже в поле рациональных чисел до рациональной матрицы  $A$ , удовлетворяющей не только соотношению (16.3.1), но также и другим соотношениям (16.3.6). В некотором смысле это является отрицательной информацией, так как получается, что никакие  $t$  начальных блоков из  $k$  элементов с  $s_{ij} = \lambda$  не могут быть исключены. Рациональное пополнение будет существовать даже для некоторых начальных наборов блоков, которые заведомо невозможны, ибо некоторая

пара элементов может появиться более чем в  $\lambda$  из начального множества  $t$  блоков, не нарушая условия  $s_{ij} = \lambda$ , относящегося лишь к пересечениям блоков.

Доказательство теоремы 16.3.1 опирается на некоторые предварительные результаты, которые назовем теоремами, а не леммами ввиду их самостоятельного значения.

Мы будем следовать некоторым стандартным обозначениям, относящимся к квадратичным формам и симметрическим матрицам, которые даны, например, в книге Джонса [1]. Пусть

$$Q_1 = \sum_{i,j=1}^n a_{ij}x_i x_j, \quad Q_2 = \sum_{i,j=1}^n b_{ij}y_i y_j, \quad a_{ii} = a_{II}, \quad b_{ii} = b_{II}. \quad (16.3.7)$$

Тогда  $Q_1$  и  $Q_2$  соответствуют симметрическим матрицам  $A$  и  $B$ :

$$A = (a_{ij}), \quad a_{II} = a_{ii}, \quad B = (b_{ij}), \quad b_{II} = b_{ii}. \quad (16.3.8)$$

Если

$$x_i = \sum_{j=1}^n c_{ij}y_j, \quad i = 1, \dots, n, \quad (16.3.9)$$

таковы, что при подстановке значений  $x_i$  в  $Q_1$  мы получаем  $Q_2$ , то, положив

$$C = (c_{ij}), \quad (16.3.10)$$

находим

$$C^T A C = B. \quad (16.3.11)$$

В этом случае скажем, что  $Q_1$  представляет  $Q_2$ . Если  $C$  невырождена, то  $Q_2$  также представляет  $Q_1$ . Мы скажем тогда, что  $Q_1$  и  $Q_2$  *конгруэнтны* и что симметрические матрицы  $A$  и  $B$  конгруэнтны. Отношение конгруэнтности обозначаем символом  $A \stackrel{c}{=} B$ . В силу формулы (16.3.11) если  $A$  и  $B$  невырождены, то и  $C$  невырождена.

Теорема 16.3.2 (Витт [1]). Пусть  $Q_1$  и  $Q_2$  — квадратичные формы от  $x_1, \dots, x_n$ , заданные над полем  $F$  характеристики, отличной от 2. Если  $a x_0^2 + Q_1$  представляет  $a x_0^2 + Q_2$  для какого-либо  $a$  из  $F$ , то  $Q_1$  представляет  $Q_2$ .

**Доказательство.** Пусть  $Q_1 = \sum a_{ij}x_i x_j$  и  $Q_2 = \sum b_{ij}x_i x_j$ ,  $A = (a_{ij})$ ,  $B = (b_{ij})$ . Нам дано, что существует матрица

$$C = \begin{bmatrix} c_0 & c_1 \\ c_2 & C_0 \end{bmatrix}, \quad (16.3.12)$$

такая, что

$$\begin{bmatrix} c_0 & c_2^T \\ c_1^T & C_0^T \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} c_0 & c_1 \\ c_2 & C_0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & B \end{bmatrix}. \quad (16.3.13)$$

Это уравнение эквивалентно следующим трем:

$$\begin{aligned} c_0^2 a + c_2^T A c_2 &= a, \\ c_0 a c_1 + c_2^T A C_0 &= 0, \\ c_1^T a c_1 + C_0^T A C_0 &= B. \end{aligned} \quad (16.3.14)$$

Выберем знак в выражении  $c_0 \pm 1$  так, чтобы эта величина не равнялась нулю, и введем обозначение  $u = (c_0 \pm 1)^{-1}$ .

Далее определим

$$S = C_0 - u c_2 c_1. \quad (16.3.15)$$

Тогда

$$\begin{aligned} S^T A S &= (C_0^T - u c_1^T c_2^T) A (C_0 - u c_2 c_1) = \\ &= C_0^T A C_0 - u c_1^T c_2^T A C_0 - u C_0^T A c_2 c_1 + u^2 c_1^T c_2^T A c_2 c_1. \end{aligned} \quad (16.3.16)$$

Используя формулы (16.3.14), приходим к соотношениям

$$\begin{aligned} S^T A S &= C_0^T A C_0 + u c_1^T c_0 a c_1 + u c_1^T a c_0 c_1 + u^2 c_1^T (a - c_0^2 a) c_1 = \\ &= C_0^T A C_0 + u c_1^T c_1 a \{c_0 + c_0 + u(1 - c_0^2)\} = \\ &= C_0^T A C_0 + a c_1^T c_1 = B. \end{aligned} \quad (16.3.17)$$

Теорема доказана.

Так как квадратичная форма  $Q(x_1, \dots, x_r)$  над полем  $F$  характеристики, отличной от 2, конгруэнтна диагональной форме  $d_1 x_1^2 + \dots + d_r x_r^2$ , мы получаем важное

**Следствие.** Если  $Q_1(x_1, \dots, x_r) + Q_2(x_{r+1}, \dots, x_n)$  представляет

$$Q_1(x_1, \dots, x_r) + Q_3(x_{r+1}, \dots, x_n),$$

то  $Q_2(x_{r+1}, \dots, x_n)$  представляет  $Q_3(x_{r+1}, \dots, x_n)$ .

Обозначим через  $A \oplus B$  прямую сумму матриц  $A$  и  $B$ , т. е. матрицу, определяемую следующим образом:

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}, \quad (16.3.18)$$

где  $0$  обозначает матрицу из нулей.

**Теорема 16.3.3.** Пусть  $AA^T = D_1 \oplus D_2$ , где  $D_1$  – невырожденная матрица порядка  $r$ ,  $D_2$  – невырожденная матрица порядка  $s$  и  $r+s=n$ . Пусть  $X$  – произвольная  $(r \times n)$ -матрица, для которой  $XX^T = D_1$ . Тогда существует  $(n \times n)$ -матрица  $Z$ , содержащая  $X$  в качестве своих первых  $r$  строк и такая, что  $ZZ^T = D_1 \oplus D_2$ .

**Доказательство.** Матрица  $X$  имеет ранг  $r$ , так как  $D_1$  невырождена. Следовательно, векторы  $w = (w_1, \dots, w_n)$ , такие, что скалярное произведение  $(x_i, w) = 0$  для всякой строки  $x_i$  из  $X$ ,  $i = 1, \dots, r$ , образуют пространство размерности  $s = n - r$ . Пусть  $W$  –  $(s \times n)$ -матрица, строки которой образуют базис этого пространства. Тогда для матрицы

$$Y = \begin{bmatrix} X \\ W \end{bmatrix} \quad (16.3.19)$$

получаем

$$YY^T = D_1 \oplus D_3. \quad (16.3.20)$$

Мы утверждаем, что  $Y$  невырождена. Поскольку  $D_1$  невырождена, существует такая невырожденная матрица  $C$ , что

$$C^T D_1 C = D, \quad D = \text{диаг. } [d_1, \dots, d_r], \quad d_i \neq 0. \quad (16.3.21)$$

Тогда

$$\begin{bmatrix} C^T X \\ W \end{bmatrix} [X^T C, \quad W^T] = \begin{bmatrix} D & 0 \\ 0 & D_3 \end{bmatrix}. \quad (16.3.22)$$

Обозначим вектор-строки матрицы

$$K = \begin{bmatrix} C^T X \\ W \end{bmatrix}$$

через  $a_1, \dots, a_r, \beta_1, \dots, \beta_s$ . Здесь  $a_1, \dots, a_r$  — линейные комбинации строк матрицы  $X$ , поэтому

$$(a_i, \beta_k) = 0, \quad i = 1, \dots, r, \quad k = 1, \dots, s.$$

Кроме того, так как  $D$  диагональна,

$$(a_i, a_j) = 0, \quad i \neq j, \quad \text{и} \quad (a_i, a_i) = d_i \neq 0.$$

Если имеем соотношение

$$a_1 a_1 + \dots + a_r a_r + b_1 \beta_1 + \dots + b_s \beta_s = 0, \quad (16.3.23)$$

то, умножая левую часть скалярно на  $a_i$ , получаем

$$a_i d_i = 0, \quad i = 1, \dots, r, \quad (16.3.24)$$

и так как  $d_i \neq 0, i = 1, \dots, r$ , отсюда следует

$$a_1 = a_2 = \dots = a_r = 0. \quad (16.3.25)$$

Поскольку  $\beta_j$  были выбраны независимыми, то отсюда, кроме того, следует, что

$$b_1 = \dots = b_s = 0. \quad (16.3.26)$$

Значит, строки матрицы  $K$  независимы, и, поскольку  $C$  невырождена, строки матрицы  $Y$  также независимы, т. е.  $Y$  невырождена. Поэтому имеем

$$\begin{aligned} (AY^{-1})(D_1 \oplus D_3)(AY^{-1})^T &= AY^{-1}(YY^T)(Y^T)^{-1}A^T = \\ &= AA^T = D_1 \oplus D_2. \end{aligned} \quad (16.3.27)$$

Следовательно, по теореме Витта существует невырожденная матрица  $E$ , для которой  $E^T D_3 E = D_2$ , и если

$$Z = \begin{bmatrix} X \\ E^T W \end{bmatrix}, \quad (16.3.28)$$

то мы получаем

$$ZZ^T = \begin{bmatrix} D_1 & 0 \\ 0 & E^T D_3 E \end{bmatrix} = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix}. \quad (16.3.29)$$

Теорема доказана.

**Теорема 16.3.4.** Пусть  $x = (x_1, \dots, x_n)$  и  $y = (y_1, \dots, y_n)$  — векторы, обладающие свойством:

$$x_1^2 + \dots + x_n^2 = y_1^2 + \dots + y_n^2 = c \neq 0. \quad (16.3.30)$$

Тогда существует ортогональная матрица  $O$ , такая, что  $xO = y$ . Это утверждение справедливо в любом поле  $F$  характеристики  $\neq 2$ .

**Доказательство.** Существует  $[(n-1) \times n]$ -матрица  $W$  ранга  $n-1$ , такая, что

$$X = \begin{bmatrix} x \\ W \end{bmatrix}, \quad XX^T = \begin{bmatrix} c & 0 \\ 0 & D_2 \end{bmatrix}. \quad (16.3.31)$$

По теореме 16.3.3 существует матрица  $Y$ ,

$$Y = \begin{bmatrix} y \\ R \end{bmatrix}, \quad YY^T = \begin{bmatrix} c & 0 \\ 0 & D_2 \end{bmatrix}. \quad (16.3.32)$$

Тогда  $X$  и  $Y$  невырождены, и  $O = X^{-1}Y$  ортогональна. Так как

$$(1, 0, \dots, 0) XO = (1, 0, \dots, 0) Y, \quad (16.3.33)$$

получаем

$$XO = y, \quad (16.3.34)$$

что и требовалось доказать.

Теорема 16.3.4 утверждает, что существует вращение, переводящее вектор данной длины в любой другой вектор той же длины. Это, конечно, хорошо известно, когда  $F$  — поле действительных чисел, но нас интересует случай поля рациональных чисел, в котором этот результат очевиден.

**Теорема 16.3.5.** Пусть  $k(k-1) = \lambda(v-1)$  и  $A$  — рациональная невырожденная матрица, такая, что  $AA^T = B = (k-\lambda)I + \lambda J$ . Тогда существует такая рациональная матрица  $C$ , что

$$CC^T = C^TC = B, \quad CJ = JC = kJ.$$

**Доказательство.** Как было показано в разделе 10.4, рациональная матрица  $A$  существует, если выполняются условия Брука — Райзера — Човла из теоремы 10.3.1. Если  $s_i$  есть сумма элементов  $i$ -го столбца матрицы  $A$ , то

$$\begin{aligned} JAATJ &= (s_1^2 + \dots + s_v^2)J = \\ &= JBJ = (kv - \lambda v + \lambda v^2)J = k^2vJ. \quad (16.3.35) \end{aligned}$$

Отсюда, сравнивая коэффициенты при  $J$ , получаем

$$s_1^2 + \dots + s_v^2 = k^2 v. \quad (16.3.36)$$

Поэтому по теореме 16.3.4 существует рациональная ортогональная матрица  $O$ , такая, что

$$(s_1, \dots, s_v) O = (k, \dots, k). \quad (16.3.37)$$

Следовательно,

$$JAO = \begin{bmatrix} s_1 & s_2 & \dots & s_v \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ s_1 & s_2 & \dots & s_v \end{bmatrix} O = kJ. \quad (16.3.38)$$

Если мы теперь возьмем  $C = AO$ , то ввиду того, что  $OO^T = I$ , получаем

$$CC^T = AOO^TA^T = AA^T = B = (k - \lambda)I + \lambda J, \quad (16.3.39)$$

а также, согласно (16.3.38),

$$JC = JAO = kJ. \quad (16.3.40)$$

По теореме 10.2.3 из условий (16.3.39) и (16.3.40) вытекает, что также

$$C^TC = B, \quad CJ = kJ. \quad (16.3.41)$$

Доказательство теоремы завершено.

Теперь мы можем доказать основную теорему.

**Доказательство теоремы 16.3.1.** Нам дана  $(t \times v)$ -матрица  $A_1$ , такая, что

$$A_1 A_1^T = B_1 = (k - \lambda)I_t + \lambda J_t, \quad A_1 J_v = k J_{t,v}. \quad (16.3.42)$$

Поскольку мы предположили также справедливость условий 1 и 2 Брука — Райзера — Човла теоремы 10.3.1, по теореме 16.3.5 существует рациональная  $(v \times v)$ -матрица  $C$ , такая, что

$$\begin{aligned} CC^T &= C^TC = B = (k - \lambda)I_v + \lambda J_v, \\ CJ_v &= J_v C = k J_v. \end{aligned} \quad (16.3.43)$$

Рассмотрим  $(t \times v)$ -матрицу  $A_1 C^{-1}$ . Для нее имеем:

$$\begin{aligned} (A_1 C^{-1})(A_1 C^{-1})^T &= A_1 C^{-1} (C^{-1})^T A_1^T = \\ &= A_1 B^{-1} A_1^T = \\ &= A_1 [(k - \lambda)^{-1} (I_v - \lambda k^{-2} J_v)] A_1^T = \\ &= (k - \lambda)^{-1} B_1 - \lambda (k - \lambda)^{-1} J_t. \end{aligned} \quad (16.3.44)$$

Легко проверить, что  $B^{-1}$  совпадает с использованным здесь выражением. Мы воспользовались обоими свойствами  $A_1$ , выраженнымми формулами (16.3.42). Так как  $B_1 = (k - \lambda) I_t + \lambda J_t$ , (16.3.44) упрощается:

$$(A_1 C^{-1})(A_1 C^{-1})^T = I_t. \quad (16.3.45)$$

Следовательно, по теореме 16.3.3 существует рациональная  $[(v-t) \times v]$ -матрица  $Q$ , такая, что

$$Y = \begin{bmatrix} A_1 C^{-1} \\ Q \end{bmatrix}, \quad YY^T = I_v. \quad (16.3.46)$$

Отсюда

$$I_v = Y^T Y = [(C^{-1})^T A_1^T, Q^T] \begin{bmatrix} A_1 C^{-1} \\ Q \end{bmatrix}. \quad (16.3.47)$$

Это дает

$$C^T I_v C = [A_1^T, C^T Q^T] \begin{bmatrix} A_1 \\ QC \end{bmatrix} = C^T C = B. \quad (16.3.48)$$

Пусть  $r_i$  обозначает сумму элементов в  $i$ -й строке матрицы  $QC$ . Мы утверждаем, что

$$r_1^2 + \dots + r_s^2 = k^2 s, \quad s = v - t. \quad (16.3.49)$$

Действительно, формула (16.3.48) дает

$$A_1^T A_1 + (QC)^T QC = B, \quad (16.3.50)$$

следовательно,

$$J_v A_1^T A_1 J_v + J_v ((QC)^T QC) J_v = J_v B J_v = k^2 v J_v. \quad (16.3.51)$$

Используя (16.3.35) и (16.3.42), находим, что

$$J_v ((QC)^T QC) J_v = k^2 (v - t) J_v. \quad (16.3.52)$$

Но это приводит к соотношению (16.3.49). По теореме 16.3.4 существует рациональная ортогональная матрица  $O_s^T$  порядка  $s$  со свойством

$$(r_1, \dots, r_s) O_s^T = (k, \dots, k). \quad (16.3.53)$$

Определим теперь матрицу

$$A = \begin{bmatrix} A_1 \\ O_s Q C \end{bmatrix}. \quad (16.3.54)$$

Из (16.3.50) получаем, что

$$A^T A = B. \quad (16.3.55)$$

Находим также, что

$$AJ_v = kJ_v, \quad (16.3.56)$$

так как по (16.3.5) сумма элементов в каждой строке матрицы  $A_1$  равна  $k$ , а по (16.3.53) суммы элементов в строках матрицы  $O_s Q C$  также равны  $k$ . В силу теоремы 10.2.3 из (16.3.55) и (16.3.56) вытекает, что, кроме того,

$$AA^T = B, \quad J_v A = kJ_v. \quad (16.3.57)$$

Таким образом, теорема 16.3.1 доказана.

Эта теорема была обобщена Йонсеном [1]. Доказательство аналогично приведенному выше, но несколько более сложно.

**Теорема 16.3.6 (Йонсен [1]).** Предположим, что для  $v, k, \lambda$  выполняются условия 1 и 2 теоремы 10.3.1 и  $k(k-1) = \lambda(v-1)$ . Пусть заданы первые  $r$  строк и первые  $s$  столбцов некоторой  $(v \times v)$ -матрицы, причем  $A_r$  есть  $(r \times v)$ -матрица из первых  $r$  строк, а  $A_s$  есть  $(v \times s)$ -матрица из первых  $s$  столбцов. Пусть, далее,  $A_r$  и  $A_s$  удовлетворяют соотношениям

$$\begin{aligned} A_r A_r^T &= (k - \lambda) I_r + \lambda J_r, & A_r J_v &= k J_{r, v}, \\ A_s^T A_s &= (k - \lambda) I_s + \lambda J_s, & J_v A_s &= k J_{v, s}. \end{aligned} \quad (16.3.58)$$

Тогда существует рациональная  $(v \times v)$ -матрица  $A$  со следующими свойствами: первые  $r$  строк  $A$  составляют  $A_r$ ; первые  $s$  столбцов  $A$  составляют  $A_s$ ;  $A$  удовлетворяет уравнениям (16.3.6).

## 16.4. Целые решения уравнений инцидентности

Пусть  $A = (a_{ij})$  есть  $(v \times v)$ -матрица, где  $a_{ij}$  — рациональные целые числа, и пусть выполняется уравнение инцидентности

$$AA^T = B = (k - \lambda)I + \lambda J, \quad k(k-1) = \lambda(v-1). \quad (16.4.1)$$

В этом разделе мы коснемся вопроса, существуют ли такие матрицы  $A$ , и если существуют, то при каких условиях  $A$  является матрицей инцидентности некоторой симметричной блок-схемы с параметрами  $v, k, \lambda$ . Первая теорема проста, но не совсем тривиальна.

**Теорема 16.4.1.** *Если всякий элемент  $a_{ij}$  в матрице  $A$ , удовлетворяющей уравнению (16.4.1), равен нулю или единице, то  $A$  является матрицей инцидентности симметричной блок-схемы с параметрами  $v, k, \lambda$ .*

**Доказательство**<sup>1)</sup>. Пусть столбцы  $A$  соответствуют блокам  $B_1, \dots, B_v$ , а строки — элементам  $a_1, \dots, a_v$ . Определим систему инцидентности  $S$ . Пусть  $a_i \in B_j$ , если  $a_{ij} = 1$ , и  $a_i \notin B_j$ , если  $a_{ij} = 0$ . Условие (16.4.1) означает, что скалярное произведение некоторой строки на себя равно  $k$ , а скалярное произведение двух различных строк матрицы  $A$  равно  $\lambda$ . Для системы инцидентности  $S$  это означает, что каждый элемент появляется точно в  $k$  блоках, а каждая пара различных элементов появляется вместе в  $\lambda$  различных блоках. Но пока неясно, сколько элементов содержится в каждом блоке. Пусть  $b_i$  — число элементов в блоке  $B_i$ ,  $i = 1, \dots, v$ . Тогда имеем

$$b_1 + b_2 + \dots + b_v = kv, \quad (16.4.2)$$

$$\frac{b_1(b_1-1)}{2} + \dots + \frac{b_v(b_v-1)}{2} = \frac{\lambda v(v-1)}{2}. \quad (16.4.3)$$

<sup>1)</sup> Теорема 16.4.1 — прямое следствие теоремы 10.2.3 из гл. 10. Действительно,  $|A|^2 = |B| = (k - \lambda)^{v-1} (\lambda v - \lambda + k)$  [см. (10.2.2)]  $= (k - \lambda)^{v-1} k^2 \neq 0$ , и  $A$  невырождена. Из (16.4.1) следует, что  $AJ = kJ$ , так как  $A$  состоит из нулей и единиц. Таким образом,  $A$  невырождена и удовлетворяет уравнениям (10.2.5) и (10.2.7); по теореме 10.2.3 тогда получается, что  $A^T A = (k - \lambda)I + \lambda J$  и  $JA = kJ$ , т. е.  $A$  — действительно матрица инцидентности симметричной блок-схемы. — Прим. ред.

В первом равенстве (двумя способами) подсчитывается общее число вхождений элементов в блоки, которое должно равняться  $kv$ , так как каждый из  $v$  элементов содержится в  $k$  блоках. Во втором — подсчитываются пары элементов: блок  $B_i$  содержит  $b_i(b_i - 1)/2$  неупорядоченных пар, а элементы каждой из  $v(v - 1)/2$  неупорядоченных пар элементов появляются вместе  $\lambda$  раз. Эти равенства приводят к соотношению

$$(b_1 - k)^2 + \dots + (b_v - k)^2 = \lambda v(v - 1) - \\ -(2k - 1)kv + vk^2 = vk(k - 1) - (2k - 1)kv + vk^2 = 0, \quad (16.4.4)$$

где  $\lambda(v - 1)$  заменяется на  $k(k - 1)$  по (16.4.1). Но формула (16.4.4) влечет за собой  $b_1 = b_2 = \dots = b_v = k$ . Таким образом, каждый блок содержит  $k$  элементов, т. е. система инцидентности  $S$  является симметричной блок-схемой с параметрами  $v, k, \lambda$ . Теорема доказана.

Следующие теоремы, принадлежащие Райзеру [1], значительно более глубокие.

**Теорема 16.4.2.** Пусть  $A = (a_{ij})$  есть  $(v \times v)$ -матрица целых чисел,  $k(k - 1) = \lambda(v - 1)$  и  $AA^T = A^TA = (k - \lambda)I + \lambda J$ . Тогда либо  $A$ , либо  $-A$  состоит целиком из нулей и единиц и является матрицей инцидентности блок-схемы.

**Доказательство.** Пусть  $s_j$  — сумма элементов в  $j$ -м столбце  $A$ :

$$s_j = \sum_{t=1}^v a_{tj}. \quad (16.4.5)$$

Из выражения для  $AA^T$  имеем

$$\sum_{i=1}^v a_{ti}a_{ii} = \begin{cases} k, & \text{если } i = t, \\ \lambda, & \text{если } i \neq t. \end{cases} \quad (16.4.6)$$

Следовательно,

$$\sum_{t, j=1}^v a_{tj}a_{ij} = k + (v - 1)\lambda = k^2, \quad (16.4.7)$$

откуда в силу (16.4.5)

$$\sum_{i=1}^v a_{ti}s_j = k^2, \quad i = 1, \dots, v. \quad (16.4.8)$$

Суммируя (16.4.8) по  $i$  от 1 до  $v$ , получаем

$$\sum_{j=1}^v s_j^2 = vk^2. \quad (16.4.9)$$

Из условий теоремы для диагональных элементов  $A^T A$  имеем

$$\sum_{i=1}^v a_{ii}^2 = k. \quad (16.4.10)$$

Но теперь, поскольку  $|x| \leq x^2$  для любого целого числа  $x$ ,

$$|s_j| = \left| \sum_{i=1}^v a_{ij} \right| \leq \sum_{i=1}^v |a_{ij}| \leq \sum_{i=1}^v a_{ii}^2 = k. \quad (16.4.11)$$

Это неравенство вместе с (16.4.9) дает

$$s_j^2 = k^2, \quad j = 1, \dots, v. \quad (16.4.12)$$

Таким образом, в (16.4.11) все знаки  $\leq$  нужно заменить на равенства. Тогда в  $j$ -м столбце все ненулевые элементы имеют один и тот же знак, а также  $|a_{ij}| = a_{ii}^2$ , откуда следует, что  $a_{ij} = 0, +1$  или  $-1$ . Следовательно, каждый столбец содержит либо  $k$  положительных единиц и  $v - k$  нулей, либо  $k$  отрицательных единиц и  $v - k$  нулей. Так как скалярное произведение любых двух различных столбцов равно положительному целому числу  $\lambda$ , ненулевые элементы во всех столбцах имеют один и тот же знак, т. е. либо  $A$ , либо  $-A$  состоит целиком из нулей и единиц и, по предыдущей теореме, является матрицей инцидентности симметричной блок-схемы.

В силу теоремы 10.2.3 получаем такое

**Следствие.** Если  $A$  — матрица целых чисел, удовлетворяющая (16.4.1), и либо  $AJ = kJ$ , либо  $JA = kJ$ , то  $A$  есть матрица инцидентности симметричной блок-схемы.

Следующая теорема носит более арифметический характер.

**Теорема 16.4.3.** Пусть  $A$  — матрица целых чисел, удовлетворяющая (16.4.1). Предположим, что  $k - \lambda$  нечетно и что  $k$  и  $k - \lambda$  взаимно просты. Тогда, умножая, если нужно, некоторые столбцы на  $-1$ , можно из

матрицы  $A$  получить матрицу инцидентности симметричной блок-схемы.

**Доказательство.** Обозначим через  $|A|$  определитель матрицы  $A$ , а через  $A_{rs}$  — алгебраическое дополнение элемента  $a_{rs}$  матрицы  $A$ . Тогда, как хорошо известно, матрица  $A^{-1}$  строится так:

$$A^{-1} = [a_{rs}^*], \quad r, s = 1, \dots, v; \quad a_{rs}^* = \frac{A_{sr}}{|A|}. \quad (16.4.13)$$

В силу (10.2.2)

$$|B| = (k - \lambda)^{v-1} (k + (v-1)\lambda) = k^2 (k - \lambda)^{v-1},$$

поэтому

$$|A| = \pm k (k - \lambda)^{\frac{v-1}{2}}. \quad (16.4.14)$$

Из соотношения  $AA^T = B$  и того факта, что  $A$  невырождена, имеем

$$A^T A = A^{-1} B A = (k - \lambda) I + \lambda A^{-1} J A. \quad (16.4.15)$$

Для  $i, j = 1, \dots, v$  определим

$$s_j = \sum_{w=1}^v a_{wj}, \quad t_{ij} = \sum_{w=1}^v a_{wi} a_{wj}. \quad (16.4.16)$$

Если мы применим (16.4.13) и приравняем элементы, стоящие на одном и том же месте  $(m, n)$  в матрицах слева и справа в (16.4.15), то

$$|A| t_{mn} = (k - \lambda) |A| \delta_{mn} + \lambda \sum_{i,j} A_{im} a_{jn}, \quad (16.4.17)$$

где  $\delta_{rs}$  — дельта Кронекера. Равенства (16.4.8) и (16.4.9) в нашем случае выполняются, так как они были выведены лишь в предположении, что  $AA^T$  удовлетворяет (16.4.1). Умножая (16.4.8) на  $A_{im}$  и суммируя по  $i$ , получаем

$$\sum_{i,j} A_{im} a_{ij} s_j = k^2 \sum_i A_{im}. \quad (16.4.18)$$

Но

$$\sum_i A_{im} a_{ij} = \delta_{mj} |A|, \quad (16.4.19)$$

и (16.4.18) упрощается:

$$|A| \sum_i \delta_{mi} s_i = k^2 \sum_i A_{im}, \quad (16.4.20)$$

или

$$|A| s_m = k^2 \sum_i A_{im}. \quad (16.4.21)$$

Отсюда, умножая (16.4.17) на  $k^2$  и деля на  $|A|$ , получаем

$$k^2 t_{mn} = k^2 (k - \lambda) \delta_{mn} + \lambda s_m s_n, \quad (16.4.22)$$

так как  $\sum_j a_{jn} = s_n$ .

Подстановка в (16.4.21) значения  $|A|$  из (16.4.14) дает

$$\pm k(k - \lambda)^{\frac{v-1}{2}} s_m = k^2 \sum_i A_{im}, \quad m = 1, \dots, v. \quad (16.4.23)$$

Так как по предположению  $k$  и  $k - \lambda$  взаимно просты, из (16.4.23) следует, что

$$s_m \equiv 0 \pmod{k}, \quad m = 1, \dots, v. \quad (16.4.24)$$

Любой столбец  $A$  можно умножить на  $-1$ , не нарушая справедливости (16.4.1), поэтому можно считать, что  $s_m \geq 0$ ,  $m = 1, 2, \dots, v$ . Из (16.4.24) имеем  $s_m = k u_m$ ,  $m = 1, \dots, v$ , где  $u_m \geq 1$  — некоторое целое число. Подстановка в (16.4.22) дает

$$t_{mn} = (k - \lambda) \delta_{mn} + \lambda u_m u_n. \quad (16.4.25)$$

Пусть теперь  $u_i = 0$  для некоторого  $i$ . Тогда

$$t_{ii} = k - \lambda + \lambda u_i^2 = k - \lambda. \quad (16.4.26)$$

В этом случае  $s_i = 0$  и

$$0 = s_i^2 \equiv a_{1i}^2 + \dots + a_{vi}^2 \equiv (k - \lambda) \pmod{2}. \quad (16.4.27)$$

Это противоречит предположению о нечетности  $k - \lambda$ . Следовательно, ни одно  $u_i$  не равно нулю. Из (16.4.9) имеем

$$s_1^2 + s_2^2 + \dots + s_v^2 = v k^2 \quad (16.4.28)$$

и, подставляя  $s_i = k u_i$ , находим

$$u_1^2 + u_2^2 + \dots + u_v^2 = v. \quad (16.4.29)$$

Но если ни одно  $u_i$  не равно нулю и  $u_i \geq 0$ , то отсюда следует, что

$$u_1 = u_2 = \dots = u_v = 1 \quad (16.4.30)$$

и

$$s_i = k, \quad i = 1, \dots, v. \quad (16.4.31)$$

Поскольку (16.4.25) также дает  $t_{ii} = k$ , то каждое  $a_{ij}$  есть нуль или единица, и  $A$  является матрицей инцидентности симметричной блок-схемы. Теорема доказана.

При четном  $k - \lambda$  теорема неверна. При  $\lambda = 1$  существует много контрпримеров.

**Теорема 16.4.4.** Пусть  $v = n^2 + n + 1$ ,  $k = n + 1$ ,  $\lambda = 1$  и  $A = (a_{ij})$  есть  $(v \times v)$ -матрица целых чисел, такая, что

$$AA^T = nI + J. \quad (16.4.32)$$

Умножив соответствующие столбцы каждой такой матрицы на  $-1$  так, что суммы элементов в них становятся неотрицательными, можно прийти к матрице  $A$  одного из следующих двух типов:

**Тип I.**  $A$  есть матрица инцидентности конечной проективной плоскости.

**Тип II.**  $n$  четно, один из столбцов состоит из нуля и  $n^2 + n$  единиц,  $n + 1$  столбцов состоят из  $n + 1$  единиц и  $n^2$  нулей, а сумма элементов в каждом из остальных столбцов равна нулю.

Матрица  $A$  типа II существует для всякого  $n$ , являющегося порядком матрицы Адамара, а также для  $n = 10$ .

**Доказательство.** Большая часть доказательства теоремы 16.4.3 проходит и здесь, поскольку  $k = n + 1$  и  $k - \lambda = n$  взаимно просты. Если  $n$  нечетно, доказательство повторяется полностью, и  $A$  является матрицей инцидентности конечной проективной плоскости. Точно так же, если  $n$  четно и никакое  $u_i$  не равно нулю, то  $A$  дает конечную плоскость. В условиях нашей теоремы (16.4.29) принимает вид

$$u_1^2 + \dots + u_v^2 = v = n^2 + n + 1. \quad (16.4.33)$$

Поскольку  $x \leqslant x^2$  для любого целого  $x$ ,

$$(n+1)u_j = s_j = a_{1j} + a_{2j} + \dots + a_{vj} \leqslant a_{1j}^2 + \dots + a_{vj}^2 = t_{jj}, \quad (16.4.34)$$

Согласно формуле (16.4.25),

$$t_{jj} = n + u_j^2 \quad (16.4.35)$$

и неравенство (16.4.34) принимает вид

$$0 \leq n - (n+1)u_j + u_j^2 = (1-u_j)(n-u_j). \quad (16.4.36)$$

Умножим теперь, если нужно,  $j$ -й столбец на  $-1$ , чтобы выполнялось  $u_j \geq 0$ . Если  $u_j \leq 1$  при всяком  $j$ , то по (16.4.33)  $u_j = 1$  при всяком  $j$ , и, как в теореме 16.4.3,  $A$  является матрицей инцидентности конечной проективной плоскости. Если  $u_j > 1$  для некоторого  $j$ , то в силу (16.4.36) мы должны иметь  $u_j \geq n$ . Но ясно, что не может быть  $u_j \geq n+1$ , так как  $(n+1)^2 > n^2 + n + 1$ , и мы получаем противоречие с (16.4.33). Следовательно, если  $u_j > 1$  для некоторого  $j$ , то  $u_j = n$ . В (16.4.33) не может быть более одного  $u_j$ , равного  $n$ . Переставим столбцы  $A$  так, чтобы единственный столбец с  $u_j = n$  был первым столбцом, т. е.  $u_1 = n$ . Теперь из (16.4.33) имеем

$$u_1^2 + \dots + u_v^2 = n + 1. \quad (16.4.37)$$

Следовательно, должно быть еще  $n+1$  чисел  $u_i$ , равных 1, а остальные должны равняться нулю. Тогда

$$\begin{aligned} s_1 &= (n+1)u_1 = n^2 + n, \\ s_j &= n+1 \text{ для } n+1 \text{ значений } j \end{aligned}$$

и

$$s_j = 0 \text{ для } n^2 - 1 \text{ значений } j.$$

Для  $t_{mn}$  из (16.4.25)

$$s_1 = t_{11} = n + n^2 \quad (16.4.38a)$$

и

$$\begin{aligned} \text{если } s_j = n+1, \text{ то } t_{1j} &= n, \quad t_{jj} = n+1, \\ \text{если } s_j = 0, \text{ то } t_{ij} &= 0, \quad i \neq j, \quad t_{jj} = n. \end{aligned} \quad (16.4.38b)$$

Всякий раз, когда  $s_j = t_{jj}$ ,  $j$ -й столбец состоит из  $s_j$  положительных единиц и  $v - s_j$  нулей.

Тем самым, чтобы полностью доказать теорему, остается лишь построить целочисленные матрицы типа II. Так как первый столбец содержит  $n^2 + n$  единиц и один нуль, мы можем без ограничения общности поместить

этот нуль на место  $(1, 1)$ . Для столбцов с  $s_j = n + 1$  мы имеем  $t_{1j} = n$ , и поэтому одна из единиц в таком столбце должна находиться в первой строке. Это дает нам  $n + 1$  единиц в первой строке, и, поскольку скалярное произведение этой строки на себя равно  $n + 1$ , то остальные элементы ее суть нули.

Пусть  $n$  четно и  $X - (n \times n)$ -матрица целых чисел, такая, что первый столбец  $X$  содержит  $n$  положительных единиц и

$$XX^T = nI_n. \quad (16.4.39)$$

Очевидно, этим требованиям удовлетворяет матрица Адамара, у которой первый столбец нормализован, т. е. состоит из +1. Построим  $A$  следующим образом:

$$A = \begin{array}{|c|c|c|c|c|} \hline & 0 & 1 & 0 & \dots & 0 \\ \hline & 1 & & & & \\ & 1 & & & & \\ & \cdot & X & & 0 & \\ & \cdot & & & 0 & \dots \\ & 1 & & & & 0 \\ \hline & 1 & & & & \\ & 1 & & & & \\ & \cdot & 0 & & X & \\ & \cdot & & & 0 & \dots \\ & 1 & & & & 0 \\ \hline & & & & \cdot & \\ & & & & \cdot & \\ & & & & & 0 \\ \hline & \cdot & 0 & \dots & 0 & \dots \\ & \cdot & & & \vdots & \\ & \cdot & & & \vdots & \\ & 1 & & & & X \\ & 1 & & 0 & \dots & 0 & \dots \\ \hline \end{array}$$

Здесь  $A$ , если удалить первую строку и первый столбец, представляет собой прямую сумму  $n+1$  экземпляров матрицы  $X$ . Единицы в первой строке матрицы  $A$  находятся над первыми столбцами матриц  $X$ . Исходя из свойств  $X$ , непосредственно проверяется, что

$$AA^T = nI + J. \quad (16.4.41)$$

Для  $n=10$ , чтобы получить матрицу  $A$  порядка 111, в качестве  $X$  можно взять следующую матрицу:

$$K = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 2 & -1 & -1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & -1 & 2 & -1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & -1 & -1 & 2 & 0 & 0 & 0 & 1 \\ 1 & -1 & 1 & 0 & 0 & 0 & 2 & -1 & -1 & -1 \\ 1 & -1 & 0 & 1 & 0 & 0 & -1 & -2 & 1 & 1 \\ 1 & -1 & 0 & 0 & 1 & 0 & -1 & 1 & -2 & 1 \\ 1 & -1 & 0 & 0 & 0 & 1 & -1 & 1 & 1 & -2 \end{bmatrix} \quad (16.4.42)$$

Ионсен нашел бесконечно много решений типа II как для  $n \equiv 2 \pmod{4}$ , так и для  $n \equiv 0 \pmod{4}$ .

## Уравновешенные неполные блок-схемы с числом повторений каждого элемента от 3 до 15

В следующей таблице дается одна или несколько блок-схем  $D(v, b, r, k, \lambda)$  с  $3 \leq r \leq 15$  и при  $k \leq v/2$ , причем приводится по крайней мере одна блок-схема в каждом случае, когда блок-схемы с указанными параметрами известны. Исключены лишь параметры таких схем, как, например,  $D(7, 14, 6, 3, 2)$ , которые строятся тривиальным образом как кратные известных схем, в данном случае как  $D(7, 7, 3, 3, 1)$ , взятая дважды. Взятие  $D(v, b, r, k, \lambda) t$  раз дает  $D(v, tb, tr, k, t\lambda)$ . Приведенные схемы взяты большей частью из книги Фишера и Йетса „Статистические таблицы для биологических, сельскохозяйственных и медицинских исследований“, Эдинбург, 1957 (для  $3 \leq r \leq 10$ ) и из работы Rao [1] (для  $11 \leq r \leq 15$ ). Эти авторы не указывали значений параметров для схем, заданных подпространствами конечных евклидовых или проективных геометрий над конечными полями. Здесь EG(2, 3) — евклидова геометрия размерности 2 над GF(3), а PG(2, 4) — проективная геометрия размерности 2 над GF(4).

В общем виде эти параметры даны в (12.2.2) и (12.2.3). Под номерами 13 и 31 схемы даны полностью. В остальных случаях даны базисные блоки относительно некоторой абелевой группы автоморфизмов. В некоторых случаях используются обозначения, введенные Боузом\* для метода смешанных разностей (см. разд. 15.3). Блок-схема номер 88 — хороший пример на обозначения Rao, когда  $(x, y) \text{ mod } (5, 7)$  означает, что все вычеты по модулю 5 прибавляются к  $x$ , а все вычеты по модулю 7 прибавляются к  $y$ ; но  $(x, y) \text{ mod } (-, 7)$  означает, что  $x$  фиксирован, а все вычеты по модулю 7 надо прибавить

к  $y$ . В каждом случае  $\infty$  обозначает элемент, фиксируемый группой автоморфизмов.

Если схемы не существует, то делается ссылка на соответствующие теоремы. В ряде случаев схемы описаны как остаточные для других схем. Построение остаточной схемы — процесс, описанный в разд. 10.1, при котором мы удаляем из симметричной схемы один блок, а из всех остальных блоков — элементы, входящие в него.

Таблица 1

| Номер схемы | $v$ | $b$ | $r$ | $k$ | $\lambda$ | Номер схемы по Фишеру и Яетсу [1] 1) | Решение<br>(блок-схема с указанными параметрами)  |
|-------------|-----|-----|-----|-----|-----------|--------------------------------------|---|
| 1           | 7   | 7   | 3   | 3   | 1         |                                      | 1, 2, 4 (mod 7). PG (2,2).  |
| 2           | 9   | 12  | 4   | 3   | 1         |                                      | Остаточная для схемы 3. EG (2,3).   |
| 3           | 13  | 13  | 4   | 4   | 1         |                                      | 0, 1, 3, 9 (mod 13). PG (2,3).  |
| 4           | 6   | 10  | 5   | 3   | 2         | 1                                    | Остаточная для схемы 5.   |
| 5           | 11  | 11  | 5   | 5   | 2         | 2                                    | 1, 3, 4, 6, 9 (mod 11). Тип Q (разд. 11.6).   |
| 6           | 16  | 20  | 5   | 4   | 1         |                                      | Остаточная для схемы 7. EG (2,4).   |
| 7           | 21  | 21  | 5   | 5   | 1         |                                      | 3, 6, 7, 12, 14 (mod 21). PG (2,4).   |
| 8           | 10  | 15  | 6   | 4   | 2         | 3                                    | Остаточная для схемы 10.  |
| 9           | 13  | 26  | 6   | 3   | 1         | 4                                    | [1, 3, 9]; [2, 5, 6] (mod 13). (Теорема 15.3.4.)  |
| 10          | 16  | 16  | 6   | 6   | 2         | 5                                    | [(1, 0, 0, 0); (0, 1, 0, 0); (0, 0, 1, 0);<br>(0, 0, 0, 1); (1, 1, 0, 0); (0, 0, 1, 1)] (mod (2, 2, 2, 2)).   |
| 11          | 25  | 30  | 6   | 5   | 1         |                                      | Остаточная для схемы 12. EG (2,5).  |
| 12          | 31  | 31  | 6   | 6   | 1         |                                      | 1, 5, 11, 24, 25, 27 (mod 31). PG (2,5).  |
| 13          | 8   | 14  | 7   | 4   | 3         | 6                                    | 1, 2, 3, 4; 1, 2, 7, 8; 1, 3, 6, 8; 5, 6, 7, 8; 3, 4, 5, 6;<br>2, 4, 5, 7; 1, 4, 6, 7; 1, 2, 5, 6; 1, 3, 5, 7; 2, 3, 5, 8;<br>3, 4, 7, 8; 2, 4, 6, 8; 1, 4, 5, 8; 2, 3, 6, 7.   |
| 14          | 15  | 35  | 7   | 3   | 1         | 7                                    | [1 <sub>1</sub> , 4 <sub>1</sub> , 0 <sub>2</sub> ]; [2 <sub>1</sub> , 3 <sub>1</sub> , 0 <sub>2</sub> ]; [1 <sub>2</sub> , 4 <sub>2</sub> , 0 <sub>3</sub> ]; [2 <sub>2</sub> , 3 <sub>2</sub> , 0 <sub>3</sub> ];<br>[0 <sub>1</sub> , 0 <sub>2</sub> , 0 <sub>3</sub> ]; [1 <sub>3</sub> , 4 <sub>3</sub> , 0 <sub>1</sub> ]; [2 <sub>3</sub> , 3 <sub>3</sub> , 0 <sub>1</sub> ] (mod 5). |
| 15          | 15  | 21  | 7   | 5   | 2         | 8                                    | Не существует. Была бы остаточной для схемы 17. (Теорема 16.1.3.).  |
| 16          | 15  | 15  | 7   | 7   | 3         | 9                                    | 0, 1, 2, 4, 5, 8, 10 (mod 15). Тип T (разд. 11.6).  |
| 17          | 22  | 22  | 7   | 7   | 2         | 10                                   | Не существует. (Теорема 10.3.1.)  |
| 18          | 36  | 42  | 7   | 6   | 1         |                                      | Не существует. Была бы остаточной для схемы 19. (Теорема 12.3.3.)   |
| 19          | 43  | 43  | 7   | 7   | 1         |                                      | Не существует. (Теорема 10.3.1.)  |
| 20          | 9   | 18  | 8   | 4   | 3         | 11                                   | [0, 1, 2, 4]; [0, 1, 4, 6] (mod 9).   |
| 21          | 21  | 28  | 8   | 6   | 2         | 12                                   | Не существует. Была бы остаточной для схемы 23. (Теорема 16.1.3.)   |
| 22          | 25  | 50  | 8   | 4   | 1         | 13                                   | [ (0, 0), (1, 0), (0, 1), (4, 4) ] (mod (5, 5));<br>[ (0, 0), (2, 0), (0, 2), (1, 1) ] (mod (5, 5)).  |
| 23          | 29  | 29  | 8   | 8   | 2         | 14                                   | Не существует. (Теорема 10.3.1.)  |
| 24          | 49  | 56  | 8   | 7   | 1         |                                      | Остаточная для схемы 25. EG (2,7).  |
| 25          | 57  | 57  | 8   | 8   | 1         |                                      | 1, 6, 7, 9, 19, 38, 42, 49 (mod 57). PG (2,7).  |
| 26          | 10  | 30  | 9   | 3   | 2         | 15                                   | [∞, 0, 5]; [0, 1, 4]; [0, 2, 3]; [0, 2, 7] (mod 9).<br>B (15.3.17).   |
| 27          | 10  | 18  | 9   | 5   | 4         | 16                                   | Остаточная для схемы 30.  |
| 28          | 16  | 24  | 9   | 6   | 3         | 17                                   | Остаточная для схемы 31. Неостаточное решение — в (16.1.19).  |
| 29          | 19  | 57  | 9   | 3   | 1         | 18                                   | [1, 7, 11]; [2, 14, 3]; [4, 9, 6] (mod 19).<br>(Теорема 15.3.4.)  |
| 30          | 19  | 19  | 9   | 9   | 4         | 19                                   | 1, 4, 5, 6, 7, 9, 11, 16, 17 (mod 19).<br>Тип Q (разд. 11.6).   |

1) Эта часть таблицы 1 взята из книги Фишера и Яетса: Fisher and Yates, Statistical Tables for Biological, Agricultural and Medical Research, Edinburgh, 1957.

Таблица 1 (продолжение)

| Номер схемы | $v$ | $k$ | $b$ | $r$ | $k$ | $\lambda$ | Номер схемы по Фишеру и Йетсу [1] | Решение   |
|-------------|-----|-----|-----|-----|-----|-----------|-----------------------------------|---|
| 31          | 25  | 25  | 9   | 9   | 3   |           | 20                                | $a b c d e f g h i$<br>$b h j e s p n l u$<br>$c g o m j e v p y$<br>$d m x c h j u w r$<br>$e d y u w q s o f$<br>$f q t j n m i c s$<br>$g r m l d a q s p$<br>$h t r k q b m e o$<br>$i y p w b n k d m$<br>$j l w y g r t f b$<br>$k s u x m g f b v$<br>$l v q b x o d i j$<br>$m o f n y l h a x$   |
| 32          | 28  | 63  | 9   | 4   | 1   |           | 21                                | <p>Элементы <math>-\infty</math> и <math>(x, y, z) \pmod{(3, 3, 3)}</math>.<br/>     База: <math>[(0, 2, 1); (0, 0, 1); (1, 1, 2); (1, 1, 0)]</math><br/> <math>[(0, 2, 0); (1, 2, 2); (0, 0, 2); (1, 0, 0)]</math><br/> <math>[\infty; (0, 1, 1); (1, 1, 1); (2, 1, 1)]</math></p> <p>Все по <math>\pmod{(3, 3, 3)}</math>. Прибавление <math>(0, 0, 0), (1, 0, 0)</math> и <math>(2, 0, 0)</math> к блокам базы дает полный дубликат (множество блоков, содержащих в совокупности все элементы схемы, каждый точно по одному разу); при этом последний блок не изменяется (см. также теорему 15.3.6).</p> |
| 33          | 28  | 36  | 9   | 7   | 2   |           | 22                                | Остаточная для схемы 34.  |
| 34          | 37  | 37  | 9   | 9   | 2   |           | 23                                | $1, 7, 9, 10, 12, 16, 26, 33, 34 \pmod{37}$ .<br>Тип В (Теорема 11.6.5.)  |
| 35          | 46  | 69  | 9   | 6   | 1   |           | 24                                | Решение неизвестно.   |
| 36          | 64  | 72  | 9   | 8   | 1   |           |                                   | Остаточная для схемы 37. EG (2,8).  |
| 37          | 73  | 73  | 9   | 9   | 1   |           |                                   | $1, 2, 4, 8, 16, 32, 37, 55, 64 \pmod{73}$ .<br>PG (2,8)  |
| 38          | 21  | 70  | 10  | 3   | 1   |           | 25                                | $[0, 1, 13]; [0, 4, 10]; [0, 16, 19] \pmod{21}$ и $[0, 7, 14] \pmod{21}$ периода 7. Теорема 15.3.3, а также (15.4.16).  |
| 39          | 21  | 30  | 10  | 7   | 3   |           | 26                                | Остаточная для схемы 40.  |
| 40          | 31  | 31  | 10  | 10  | 3   |           | 27                                | $[1_1, 6_1, 2_2, 5_2, 3_3, 4_3, 3_4, 5_4, 6_4, \infty_1] \pmod{7}$ ,<br>$[2_1, 5_1, 3_2, 4_2, 1_3, 6_3, 3_4, 5_4, 6_4, \infty_2] \pmod{7}$ ,<br>$[3_1, 4_1, 1_2, 6_2, 2_3, 5_3, 3_4, 5_4, 6_4, \infty_3] \pmod{7}$ ,<br>$[1_1, 2_1, 4_1, 1_2, 2_2, 4_2, 1_3, 2_3, 4_3, 0_4] \pmod{7}$ ,<br>$[0_1, 1_1, 2_1, 3_1, 4_1, 5_1, 6_1, \infty_1, \infty_2, \infty_3]$ ,<br>$[0_2, 1_2, 2_2, 3_2, 4_2, 5_2, 6_2, \infty_1, \infty_2, \infty_3]$ ,<br>$[0_3, 1_3, 2_3, 3_3, 4_3, 5_3, 6_3, \infty_1, \infty_2, \infty_3]$ .  |
| 41          | 36  | 45  | 10  | 8   | 2   |           | 28                                | Не существует. Была бы остаточной для схемы 43. (Теорема 16.1.3.)   |
| 42          | 41  | 82  | 10  | 5   | 1   |           | 29                                | $[1, 37, 16, 18, 10]; [8, 9, 5, 21, 39] \pmod{41}$ .<br>В (15.3.12).  |
| 43          | 46  | 46  | 10  | 10  | 2   |           | 30                                | Не существует. (Теорема 10.3.1.)  |
| 44          | 51  | 85  | 10  | 6   | 1   |           | 31                                | Решение неизвестно.   |
| 45          | 81  | 90  | 10  | 9   | 1   |           |                                   | Остаточная для схемы 46. EG (2,9).  |
| 46          | 91  | 91  | 10  | 10  | 1   |           |                                   | $0, 1, 3, 9, 27, 49, 56, 61, 77, 81 \pmod{91}$ . PG (2,9).  |

Таблица 1 (продолжение)

| Номер схемы | $a$ | $b$ | $r$ | $k$ | $\lambda$ | Номер схемы по Rao [1] <sup>1)</sup> | Решение   |
|-------------|-----|-----|-----|-----|-----------|--------------------------------------|---|
| 47          | 12  | 44  | 11  | 3   | 2         | 32                                   | [0, 1, 3]; [4, 5, 9]; [2, 8, 6]; [ $\infty$ , 7, 10] (mod 11). Второе решение: [0, 1, 3]; [0, 1, 4]; [0, 2, 6]; [ $\infty$ , 0, 5] (mod 11). См. также (15.3.17).   |
| 48          | 12  | 33  | 11  | 4   | 3         | 33                                   | [0, 1, 3, 7]; [2, 4, 9, 10]; [ $\infty$ , 5, 6, 8] (mod 11).  |
| 49          | 12  | 22  | 11  | 6   | 5         | 34                                   | [0, 1, 3, 7, 8, 10]; [ $\infty$ , 0, 5, 6, 8, 10] (mod 11).   |
| 50          | 23  | 23  | 11  | 11  | 5         | 35                                   | 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 (mod 23). Тип Q (разд. 11.6).   |
| 51          | 45  | 99  | 11  | 5   | 1         | 36                                   | Элементы — $(x, y, z)$ (mod (3, 3, 5)).<br>[(0, 1, 0), (0, 2, 0), (1, 0, 2), (2, 0, 2), (0, 0, 1)] (mod (3, 3, 5)),<br>[(2, 1, 0), (1, 2, 0), (2, 2, 2), (1, 1, 2), (0, 0, 1)] (mod (3, 3, 5)),<br>[(0, 0, 0), (0, 0, 1), (0, 0, 2), (0, 0, 3), (0, 0, 4)] (mod (3, 3, —)).   |
| 52          | 45  | 55  | 11  | 9   | 2         | 37                                   | Решение неизвестно. Остаточная для схемы 53.  |
| 53          | 56  | 56  | 11  | 11  | 2         | 38                                   | Решение неизвестно.   |
| 54          | 100 | 110 | 11  | 10  | 1         | 39                                   | Решение неизвестно. Остаточная для схемы 55.<br>EG (2, 10.)   |
| 55          | 111 | 111 | 11  | 11  | 1         | 40                                   | Решение неизвестно. PG (2, 10).   |
| 56          | 13  | 26  | 12  | 6   | 5         | 41                                   | [0, 1, 3, 6, 7, 11]; [0, 1, 2, 3, 7, 11] (mod 13).  |
| 57          | 19  | 57  | 12  | 4   | 2         | 42                                   | [0, 1, 3, 12]; [0, 1, 5, 13]; [0, 4, 6, 9] (mod 19).  |
| 58          | 21  | 42  | 12  | 6   | 3         | 43                                   | [0, 2, 10, 15, 19, 20]; [0, 3, 7, 9, 10, 16] (mod 21).  |
| 59          | 22  | 33  | 12  | 8   | 4         | 44                                   | Решение неизвестно.   |
| 60          | 25  | 100 | 12  | 3   | 1         | 45                                   | [0, 1, 3]; [0, 4, 13]; [0, 5, 11]; [0, 7, 17] (mod 25). Второе решение:   |
|             |     |     |     |     |           |                                      | [ (0, 1), (4, 1), [1, 3] ]; [ (1, 0), (3, 3), (1, 2) ];<br>[ (3, 2), (2, 1), (0, 2) ]; [(1, 1), (2, 4), (2, 0)] (mod (5, 5)).   |
| 61          | 33  | 44  | 12  | 9   | 3         | 46                                   | Решение неизвестно.   |
| 62          | 34  | 34  | 12  | 12  | 4         | 47                                   | Не существует. (Теорема 10.3.1.)  |
| 63          | 37  | 111 | 12  | 4   | 1         | 48                                   | Элементы: $(x, y)$ , $x=0, 1, 2$ (mod 3), $y=0, \dots, 10$ (mod 11), а также $y=\infty$ и $(x, y)=(\infty, \infty)$ ,<br>[(0, 0), (0, 1), (1, 2), (1, 5)]; [(0, 1), (0, 3), (0, 8), (1, 0)],<br>[(0, $\infty$ ), (0, 7), (1, 5), (2, 1)] (mod (3, 11)),<br>[( $\infty$ , $\infty$ ), (0, 0), (1, 0), (2, 0)] (mod (-, 11)),<br>[(0, $\infty$ ), (1, $\infty$ ), (2, $\infty$ ), ( $\infty$ , $\infty$ )]. |
| 64          | 45  | 45  | 12  | 12  | 3         | 49                                   | Решение неизвестно.   |
| 65          | 55  | 66  | 12  | 10  | 2         | 50                                   | Не существует. Была бы остаточной для схемы 67. (Теорема 16.1.3.)   |
| 66          | 61  | 122 | 12  | 6   | 1         | 51                                   | Решение неизвестно.   |
| 67          | 67  | 67  | 12  | 12  | 2         | 52                                   | Не существует. (Теорема 10.3.1.)  |
| 68          | 121 | 132 | 12  | 11  | 1         |                                      | Остаточная для схемы 69. EG (2, 11).  |
| 69          | 133 | 133 | 12  | 12  | 1         |                                      | 1, 8, 9, 11, 25, 37, 69, 88, 94, 99, 103, 121 (mod 133).<br>PG (2, 11).   |
| 70          | 27  | 117 | 13  | 3   | 1         |                                      | [0, 1, 22]; [0, 2, 8]; [0, 3, 14]; [0, 7, 17] (mod 26).   |
| 71          | 27  | 39  | 13  | 9   | 4         |                                      | [ $\infty$ , 0, 13] (mod 26) периода 13. Прямые в EG (3, 3).<br>Остаточная для схемы 75. Плоскости в EG (3, 3).   |

1) Эта часть таблицы 1 взята из работы Rao: Rao C. R., A Study of BIB Designs with Replications 11 to 15, Sankhya, 23 (1961), 117–127.

Таблица 1 (продолжение)

| Номер схемы | $v_k$ | $b$ | $r$ | $k$ | $\lambda$ | Номер схемы по Rao [1] | Решение  |
|-------------|-------|-----|-----|-----|-----------|------------------------|--|
| 72          | 27    | 27  | 13  | 13  | 6         | 53                     | [ (0, 0, 1), (1, 0, 0), (1, 2, 0), (1, 1, 1), (2, 0, 2) (1, 1, 0), (1, 0, 2), (0, 2, 0), (0, 2, 1), (1, 2, 1), (2, 1, 1), (0, 2, 2), (2, 2, 1) ] (mod (3, 3, 3)).<br>Тип Q (разд. 11.6).   |
| 73          | 40    | 130 | 13  | 4   | 1         |                        | [0, 1, 26, 32]; [0, 7, 19, 36]; [0, 3, 16, 38] (mod 40).<br>[0, 10, 20, 30] (mod 40) периода 10.   |
| 74          | 40    | 52  | 13  | 10  | 3         | 54                     | Прямые в PG (3, 3).<br>Решение неизвестно.   |
| 75          | 40    | 40  | 13  | 13  | 4         |                        | 1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35 (mod 40).<br>Плоскости в PG (3, 3).   |
| 76          | 53    | 53  | 13  | 13  | 3         | 55                     | Не существует. (Теорема 10.3.1.)   |
| 77          | 66    | 143 | 13  | 6   | 1         | 56                     | Решение неизвестно.  |
| 78          | 66    | 78  | 13  | 11  | 2         | 57                     | Решение неизвестно. Остаточная для схемы 79.   |
| 79          | 79    | 79  | 13  | 13  | 2         | 58                     | Решение неизвестно.  |
| 80          | 144   | 156 | 13  | 12  | 1         | 59                     | Решение неизвестно. Остаточная для схемы 81.<br>EG (2, 12).  |
| 81          | 157   | 157 | 13  | 13  | 1         | 60                     | Решение неизвестно. PG (2, 12)   |
| 82          | 15    | 42  | 14  | 5   | 4         | 61                     | [0, 1, 4, 9, 11]; [0, 1, 4, 10, 12]; [ $\infty$ , 0, 1, 2, 7] (mod 14).<br>Удвоение неразрешимого случая 15.   |
| 83          | 15    | 35  | 14  | 6   | 5         | 62                     | [ $\infty$ , 0 <sub>0</sub> , 0 <sub>1</sub> , 1 <sub>1</sub> , 2 <sub>1</sub> , 4 <sub>1</sub> ]; [ $\infty$ , 0 <sub>1</sub> , 0 <sub>0</sub> , 6 <sub>0</sub> , 5 <sub>0</sub> , 3 <sub>0</sub> ]; [1 <sub>0</sub> , 2 <sub>0</sub> , 4 <sub>0</sub> , 0 <sub>1</sub> , 1 <sub>1</sub> , 3 <sub>1</sub> ]; [2 <sub>0</sub> , 3 <sub>0</sub> , 5 <sub>0</sub> , 0 <sub>1</sub> , 1 <sub>1</sub> , 3 <sub>1</sub> ]; [0 <sub>0</sub> , 4 <sub>0</sub> , 5 <sub>0</sub> , 0 <sub>1</sub> , 1 <sub>1</sub> , 3 <sub>1</sub> ] (mod 7).  |
| 84          | 22    | 77  | 14  | 4   | 2         | 63                     | [0 <sub>0</sub> , 3 <sub>0</sub> , 9 <sub>0</sub> , 10 <sub>0</sub> ]; [0 <sub>0</sub> , 0 <sub>1</sub> , 2 <sub>1</sub> , 7 <sub>1</sub> ]; [0 <sub>0</sub> , 0 <sub>1</sub> , 9 <sub>1</sub> , 10 <sub>1</sub> ];<br>[0 <sub>0</sub> , 2 <sub>0</sub> , 5 <sub>1</sub> , 8 <sub>1</sub> ]; [0 <sub>0</sub> , 3 <sub>0</sub> , 4 <sub>1</sub> , 7 <sub>1</sub> ]; [0 <sub>0</sub> , 4 <sub>0</sub> , 3 <sub>1</sub> , 9 <sub>1</sub> ];<br>[0 <sub>0</sub> , 5 <sub>0</sub> , 2 <sub>1</sub> , 6 <sub>1</sub> ] (mod 11).   |
| 85          | 22    | 44  | 14  | 7   | 4         | 64                     | Решение неизвестно. Удвоение неразрешимого случая 17.  |
| 86          | 29    | 58  | 14  | 7   | 3         | 65                     | [1, 7, 16, 20, 23, 24, 25]; [2, 3, 11, 14, 17, 19, 21] (mod 29).   |
| 87          | 36    | 84  | 14  | 6   | 2         | 66                     | [0, 1, 3, 5, 11, 23]; [0, 5, 8, 9, 18, 24] (mod 35) и<br>[ $\infty$ , 0, 7, 14, 21, 28] (mod 35) периода 7, взятый дважды. Удвоение неразрешимого случая 18.   |
| 88          | 43    | 86  | 14  | 7   | 2         | 67                     | Элементы: ( $x, y$ ), $x \equiv 0, \dots, 4 \pmod{5}$ и $x = \infty$ ,<br>$y \equiv 0, \dots, 6 \pmod{7}$ , а также $(\infty, \infty)$ [ $\{\infty, 0\}$ ,<br>$(0, 1)$ , $(0, 6)$ , $(1, 5)$ , $(1, 2)$ , $(2, 3)$ , $(2, 4)$ ] (mod (5, 7)).<br>[ $(\infty, 0)$ , $(0, 1)$ , $(0, 6)$ , $(3, 5)$ , $(3, 2)$ , $(1, 3)$ , $(1, 4)$ ] (mod (5, 7));<br>[ $(\infty, 0)$ , $(\infty, \infty)$ $(0, 0)$ , $(1, 0)$ , $(2, 0)$ , $(3, 0)$ , $(4, 0)$ ] (mod (-, 7)), взятый дважды.<br>[ $(\infty, 0)$ , $(\infty, 1)$ , $(\infty, 2)$ , $(\infty, 3)$ , $(\infty, 4)$ , $(\infty, 5)$ ,<br>$(\infty, 6)$ ], взятый дважды. Удвоение неразрешимого случая 19. |
| 89          | 78    | 91  | 14  | 12  | 2         | 68                     | Не существует. Была бы остаточной для схемы 91. (Теорема 16.1.3.)  |
| 90          | 85    | 170 | 14  | 7   | 1         | 69                     | Решение неизвестно.  |
| 91          | 92    | 92  | 14  | 14  | 2         | 70                     | Не существует. (Теорема 10.3.1.)   |
| 92          | 11    | 55  | 15  | 3   | 3         | 71                     | [0, 1, 3]; [0, 1, 5]; [0, 2, 7]; [0, 1, 8]; [0, 3, 5] (mod 11).  |
| 93          | 13    | 39  | 15  | 5   | 5         | 72                     | [0, 1, 2, 4, 8]; [0, 1, 3, 6, 12]; [0, 2, 5, 6, 10] (mod 13).  |

Таблица 1 (продолжение)

| Номер схемы | $v$ | $b$ | $r$ | $k$ | $\lambda$ | Номер схемы по Рао [1] | Решение  |
|-------------|-----|-----|-----|-----|-----------|------------------------|--|
| 94          | 16  | 80  | 15  | 3   | 2         | 73                     | $[0, 1, 3]; [0, 3, 8]; [0, 2, 12]; [0, 1, 7]; [0, 4, 9] \pmod{16}$ . Второе решение: $[0_1, 1_1, 2_1]; [0_1, 2_1, 5_1]; [0_0, 7_0, 0_1]; [1_0, 6_0, 0_1]; [2_0, 5_0, 0_1]; [3_0, 4_0, 0_1]; [1_0, 7_0, 0_1]; [2_0, 6_0, 0_1]; [3_0, 5_0, 0_1]; [0_0, 0_1, 4_1] \pmod{8}$ . |
| 95          | 16  | 48  | 15  | 5   | 4         | 74                     | $[0, 1, 2, 4, 7]; [0, 1, 8, 5, 10]; [0, 1, 3, 7, 11] \pmod{16}$ .  |
| 96          | 16  | 40  | 15  | 6   | 5         | 75                     | $[0, 1, 3, 5, 9, 12]; [0, 1, 2, 3, 6, 12] \pmod{16}$ ,   |
| 97          | 16  | 30  | 15  | 8   | 7         |                        | $[0, 8, 1, 9, 2, 10] \pmod{16}$ периода 8.   |
| 98          | 21  | 35  | 15  | 9   | 6         | 76                     | $[\infty, 0, 1, 2, 7, 9, 12, 13]; [3, 4, 5, 6, 8, 10, 11, 14] \pmod{16}$ .   |
| 99          | 26  | 65  | 15  | 6   | 3         | 77                     | $[0_0, 1_0, 2_0, 4_0, 0_1, 1_1, 2_1, 4_1, 2_2]; [0_0, 6_0, 5_0, 3_0, 6_2, 4_2, 3_2, 2_2, 0_1]; [1_0, 6_1, 5_1, 3_1, 6_2, 4_2, 3_2, 2_2, 0_0]; [4_0, 1_0, 3_0, 0_1, 2_1, 6_1, 4_2, 1_2, 2_2]; [0_0, 2_0, 6_0, 4_1, 1_1, 3_1, 4_2, 1_2, 2_2] \pmod{7}$ .                     |
| 100         | 28  | 42  | 15  | 10  | 5         | 78                     | Решение неизвестно.  |
| 101         | 31  | 155 | 15  | 3   | 1         |                        | $[0, 1, 18]; [0, 2, 5]; [0, 4, 10]; [0, 8, 20]; [0, 9, 16] \pmod{31}$ . Прямые в PG (4, 2). Система троек Штейнера.  |
| 102         | 31  | 93  | 15  | 5   | 2         | 79                     | $[1, 2, 4, 8, 16]; [3, 6, 12, 24, 17]; [9, 18, 5, 10, 20] \pmod{31}$ .   |
| 103         | 31  | 31  | 15  | 15  | 7         |                        | $1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28 \pmod{31}$ . Тип Q (разд. 11.6). 1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30 (mod 31). Тип H <sub>6</sub> (разд. 11.6).  |
| 104         | 36  | 36  | 15  | 15  | 6         | 80                     | Решение неизвестно.  |
| 105         | 43  | 43  | 15  | 15  | 5         | 81                     | Решение неизвестно.  |
| 106         | 46  | 69  | 15  | 10  | 3         | 82                     | Решение неизвестно.  |
| 107         | 56  | 70  | 15  | 12  | 3         | 83                     | Решение неизвестно.  |
| 108         | 61  | 183 | 15  | 5   | 1         | 84                     | $[1, 9, 20, 58, 34]; [4, 36, 19, 49, 14]; [16, 22, 15, 13, 56] \pmod{61}$ .  |
| 109         | 71  | 71  | 15  | 15  | 3         | 85                     | Решение неизвестно.  |
| 110         | 76  | 190 | 15  | 6   | 1         | 86                     | Решение неизвестно.  |
| 111         | 91  | 195 | 15  | 7   | 1         | 87                     | $[0, 10, 27, 28, 31, 43, 50]; [0, 11, 20, 25, 49, 55, 57] \pmod{91}$ . $[0, 13, 26, 39, 52, 65, 78] \pmod{91}$ периода 13.   |
| 112         | 91  | 105 | 15  | 13  | 2         | 88                     | Не существует. Была бы остаточной для схемы 113. (Теорема 16.1.3.)   |
| 113         | 106 | 106 | 15  | 15  | 2         | 89                     | Не существует. (Теорема 10.3.1.)   |
| 114         | 136 | 204 | 15  | 10  | 1         | 90                     | Решение неизвестно.  |
| 115         | 196 | 210 | 15  | 14  | 1         | 91                     | Не существует. Была бы остаточной для схемы 116. (Теорема 12.3.3.)   |
| 116         | 211 | 211 | 15  | 15  | 1         | 92                     | Не существует. (Теорема 10.3.1.)   |

Матрицы Адамара типа Уильямсона

| <i>t</i> | <i>n</i> | $W_1^2 + W_2^2 + W_3^2 + W_4^2$ | $W_1$   | $W_2$   | $W_3$  | $W_4$   |
|----------|----------|---------------------------------|---|---|--|---|
| 3        | 12       | $1^2 + 1^2 + 1^3 + 3^2$         | 1   | 1   | 1  | $1 - 2\omega_1$   |
| 5        | 20       | $1^2 + 1^2 + 3^2 + 3^2$         | 1   | 1   | $1 - 2\omega_1$  | $1 - 2\omega_2$   |
| 7        | 28       | $1^2 + 3^2 + 3^2 + 3^2$         | 1   | $1 - 2\omega_1$   | $1 - 2\omega_2$  | $1 - 2\omega_3$   |
| 7        | 28       | $1^2 + 1^2 + 1^2 + 5^2$         | 1   | 1   | $1 + 2\omega_1 - 2\omega_2$                                | $1 + 2\omega_3$   |
| 9        | 36       | $3^2 + 3^2 + 3^2 + 3^2$         | $1 - 2\omega_1$   | $1 - 2\omega_2$   | $1 - 2\omega_3$  | $1 - 2\omega_4$   |
| 9        | 36       | $1^2 + 1^2 + 3^2 + 5^2$         | 1   | $1 - 2\omega_2 + 2\omega_1$   | $1 - 2\omega_4$  | $1 + 2\omega_3$   |
|          |          |                                 | 1   | 1   | $1 - 2\omega_2$  | $1 + 2\omega_1 + 2\omega_3 + 2\omega_4$   |
| 11       | 44       | $1^2 + 3^2 + 3^2 + 5^2$         | $1 + 2\omega_1 - 2\omega_2$                                   | $1 - 2\omega_4$   | $1 - 2\omega_5$  | $1 + 2\omega_3$   |
| 13       | 52       | $1^2 + 1^2 + 1^2 + 7^2$         | 1   | 1   | $1 + 2\omega_1 - 2\omega_4 +$<br>$+ 2\omega_5 - 2\omega_6$ | $1 - 2\omega_2 - 2\omega_3$   |
|          |          |                                 | 1   | $1 + 2\omega_4 - 2\omega_5$   | $1 + 2\omega_6 - 2\omega_1$                                | $1 - 2\omega_2 - 2\omega_3$   |
| 13       | 52       | $3^2 + 3^2 + 3^2 + 5^2$         | $1 - 2\omega_2$   | $1 - 2\omega_4$   | $1 - 2\omega_1 - 2\omega_3 + 2\omega_5$                    | $1 + 2\omega_6$   |
| 13       | 52       | $1^2 + 1^2 + 5^2 + 5^2$         | $1 + 2\omega_4 - 2\omega_3$                                   | $1 + 2\omega_6 - 2\omega_2$   | $1 + 2\omega_1$  | $1 + 2\omega_5$   |
| 15       | 60       | $1^2 + 3^2 + 5^2 + 5^2$         | 1   | $1 - 2\omega_5$   | $1 + 2\omega_6$  | $1 + 2\omega_1 - 2\omega_2 + 2\omega_3 +$<br>$+ 2\omega_4 - 2\omega_7$                |
|          |          |                                 | $1 - 2\omega_1 + 2\omega_7$                                   | $1 - 2\omega_3$   | $1 + 2\omega_2$  | $1 + 2\omega_4 + 2\omega_5 - 2\omega_6$   |
|          |          |                                 | $1 + 2\omega_6 - 2\omega_4$                                   | $1 + 2\omega_5 - 2\omega_1 - 2\omega_3$                                   | $1 + 2\omega_7$  | $1 + 2\omega_2$   |
| 15       | 60       | $1^2 + 1^2 + 3^2 + 7^2$         | 1   | 1   | $1 - 2\omega_1 - 2\omega_5 + 2\omega_7$                    | $1 - 2\omega_3 - 2\omega_6 + 2\omega_2 - 2\omega_4$                                   |
| 17       | 68       | $3^2 + 3^2 + 5^2 + 5^2$         | $1 - 2\omega_2$   | $1 - 2\omega_8$   | $1 - 2\omega_1 + 2\omega_5 + 2\omega_6$                    | $1 - 2\omega_4 + 2\omega_3 + 2\omega_7$   |
|          |          |                                 | $1 + 2\omega_6 + 2\omega_7 - 2\omega_5 - 2\omega_3$           | $1 - 2\omega_2$   | $1 - 2\omega_8$  | $1 - 2\omega_1 - 2\omega_4$   |
| 17       | 68       | $1^2 + 3^2 + 3^2 + 7^2$         | 1   | $1 + 2\omega_6 - 2\omega_5 - 2\omega_4$                                   | $1 + 2\omega_7 - 2\omega_1 - 2\omega_3$                    | $1 - 2\omega_8 - 2\omega_2$   |
| 19       | 76       | $1^2 + 5^2 + 5^2 + 5^2$         | 1   | $1 + 2\omega_5 - 2\omega_4 - 2\omega_2$                                   | $1 + 2\omega_3 - 2\omega_1 - 2\omega_8$                    | $1 - 2\omega_7 - 2\omega_6$   |
|          |          |                                 | $1 + 2\omega_9 + 2\omega_5 - 2\omega_4 - 2\omega_3$           | $1 + 2\omega_1 + 2\omega_4 - 2\omega_2$                                   | $1 + 2\omega_8 + 2\omega_6 - 2\omega_3$                    | $1 + 2\omega_7 + 2\omega_9 - 2\omega_5$   |
| 19       | 76       | $3^2 + 3^2 + 3^2 + 7^2$         | 1   | $1 + 2\omega_8 + 2\omega_2 - 2\omega_7$                                   | $1 + 2\omega_6$  | $1 + 2\omega_1$   |
| 19       | 76       | Hет                             |   | $1 + 2\omega_9 + 2\omega_8 - 2\omega_3$                                   | $1 + 2\omega_7 + 2\omega_4 - 2\omega_5$                    | $1 + 2\omega_1 + 2\omega_6 - 2\omega_2$   |
|          |          |                                 | $1 + 2\omega_1 + 2\omega_5 + 2\omega_7$                       | 1   | $1 + 2\omega_1 + 2\omega_8 - 2\omega_3$                    | $1 + 2\omega_2 + 2\omega_6 - 2\omega_9 -$<br>$- 2\omega_7 - 2\omega_5 - 2\omega_4$    |
| 21       | 84       | $3^2 + 5^2 + 5^2 + 5^2$         | $1 - 2\omega_7$   | $1 + 2\omega_7 - 2\omega_4$   | $1 + 2\omega_6 + 2\omega_3 - 2\omega_9$                    | $1 - 2\omega_1 - 2\omega_5$   |
| 21       | 84       | $1^2 + 1^2 + 1^2 + 9^2$         | $1 - 2\omega_3 + 2\omega_2$                                   | $1 + 2\omega_2 - 2\omega_5$   | $1 + 2\omega_1$  | $1 + 2\omega_7 - 2\omega_9 - 2\omega_8 - 2\omega_3$                                   |
|          |          |                                 | 1   | $1 + 2\omega_3 + 2\omega_5 - 2\omega_7$                                   | $1 + 2\omega_6 + 2\omega_4 - 2\omega_2$                    | $1 + 2\omega_9 + 2\omega_1 - 2\omega_{10}$  |
| 21       | 84       | $1^2 + 3^2 + 5^2 + 7^2$         | $1 + 2\omega_9 - 2\omega_3$                                   | $1 + 2\omega_8 - 2\omega_{10}$  | $1 - 2\omega_9 + 2\omega_8$                                | $1 + 2\omega_1 + 2\omega_5 + 2\omega_4 - 2\omega_7$                                   |
|          |          |                                 | $1 + 2\omega_5 - 2\omega_4$                                   | $1 + 2\omega_{10} + 2\omega_2 -$<br>$- 2\omega_9 - 2\omega_8 - 2\omega_6$ | $1 + 2\omega_9 + 2\omega_7 -$<br>$- 2\omega_6 - 2\omega_5$ | $1 + 2\omega_7 + 2\omega_8 + 2\omega_4 +$<br>$+ 2\omega_2 - 2\omega_{10} - 2\omega_3$ |
| 21       | 84       | $1^2 + 3^2 + 5^2 + 7^2$         | $1 + 2\omega_9 - 2\omega_5$                                   | $1 + 2\omega_2 - 2\omega_{10} -$<br>$- 2\omega_4$                         | $1 + 2\omega_7 + 2\omega_6 - 2\omega_8$                    | $1 - 2\omega_1 - 2\omega_3$   |
|          |          |                                 | $1 + 2\omega_8 - 2\omega_6$                                   | $1 + 2\omega_2 - 2\omega_{10} -$<br>$- 2\omega_4$                         | $1 + 2\omega_7 + 2\omega_5 - 2\omega_9$                    | $1 - 2\omega_1 - 2\omega_3$   |
| 23       | 92       | $1^2 + 1^2 + 3^2 + 9^2$         | $1 + 2\omega_{11} + 2\omega_9 -$<br>$- 2\omega_8 - 2\omega_4$ | $1 + 2\omega_5 - 2\omega_7$   | $1 - 2\omega_3 + 2\omega_1 -$<br>$- 2\omega_{10}$          | $1 + 2\omega_2 + 2\omega_6$   |
| 23       | 92       | $3^2 + 3^2 + 5^2 + 7^2$         | Hет   |   |  |   |

## Приложение II (окончание)

| $t$              | $n$ | $W_1^2 + W_2^2 + W_3^2 + W_4^2$ | $W_1$   | $W_2$  | $W_3$  | $W_4$  |
|------------------|-----|---------------------------------|---|--|--|--|
|                  |     | ?                               |   |  |  |  |
| 25               | 100 | $1^2 + 3^2 + 3^2 + 9^2$         | $1 + 2\omega_6 - 2\omega_{11}$  | $1 - 2\omega_1 + 2\omega_3 - 2\omega_{12}$                         | $1 - 2\omega_7 + 2\omega_4 - 2\omega_9$  | $1 + 2\omega_5 + 2\omega_{10} + 2\omega_2 - 2\omega_8$   |
| 25               | 100 | $5^2 + 5^2 + 5^2 + 5^2$         | $1 + 2\omega_1 + 2\omega_9 - 2\omega_6$   | $1 + 2\omega_7 + 2\omega_{12} - 2\omega_8$                         | $1 + 2\omega_5 + 2\omega_2 - 2\omega_4$  | $1 + 2\omega_{10} + 2\omega_{11} - 2\omega_3$  |
| 25               | 100 | $1^2 + 1^2 + 7^2 + 7^2$         | $1$   | $1$  | $1 + 2\omega_{12} + 2\omega_6 - 2\omega_7 - 2\omega_5 - 2\omega_3 - 2\omega_2$ | $1 + 2\omega_9 + 2\omega_8 - 2\omega_1 - 2\omega_{11} - 2\omega_{10} - 2\omega_4$                |
|                  |     |                                 | $1 + 2\omega_3 - 2\omega_7$   | $1 + 2\omega_4 - 2\omega_1$  | $1 + 2\omega_8 - 2\omega_{11} - 2\omega_{10} - 2\omega_9$                      | $1 + 2\omega_6 - 2\omega_{12} - 2\omega_5 - 2\omega_2$   |
| 27               | 108 | $1^2 + 1^2 + 9^2 + 5^2$         | $1$   | $1$  | $1 + 2\omega_{12} + 2\omega_7 + 2\omega_5 - 2\omega_9 - 2\omega_3 + 2\omega_4$ | $1 + 2\omega_{13} + 2\omega_{10} + 2\omega_8 + 2\omega_6 - 2\omega_1 - 2\omega_{11} - 2\omega_2$ |
| 29               | 116 | $1^2 + 3^2 + 5^2 + 9^2$         | $1 + 2\omega_{12} + 2\omega_6 + 2\omega_2 - 2\omega_{11} - 2\omega_9 - 2\omega_4$ | $1 + 2\omega_{10} + 2\omega_7 - 2\omega_8 - 2\omega_3 - 2\omega_5$ | $1 + 2\omega_1$  | $1 + 2\omega_{13} + 2\omega_{14}$  |
| 37 <sup>1)</sup> | 148 | $1^2 + 7^2 + 7^2 + 7^2$         | $1$   | $1 + 2\alpha_5 - 2\alpha_0 - 2\alpha_1$                            | $1 + 2\alpha_8 - 2\alpha_3 - 2\alpha_4$  | $1 + 2\alpha_2 - 2\alpha_6 - 2\alpha_7$  |
| 43 <sup>2)</sup> | 172 | $1^2 + 1^2 + 1^2 + 13^2$        | $1 + 2\alpha_0 - 2\alpha_2$   | $1 + 2\alpha_3 - 2\alpha_1$  | $1 + 2\alpha_4 - 2\alpha_6$  | $1 + 2\alpha_5$  |

<sup>1)</sup>  $\alpha_j = \omega_{2j} + \omega_{29+j}$ .

<sup>2)</sup>  $\alpha_j = \omega_{3j} + \omega_{37+j} + \omega_{314+j}$ .

## Библиография

---

Алберт (Albert A. A.)

- [1] On non-associative division algebras, *Trans. Amer. Math. Soc.*, **72** (1952), 296—309.  
[2] Fundamental Concepts of Modern Algebra, Chicago, 1956.

Блюменталь (Blumenthal L. M.)

- [1] A Modern View of Geometry, San Francisco, 1961.

Боумер (Baumert L. D.)

- [1] Hadamard matrices of Williamson type, *Math. of Comp.*, **19** (1965), 442—447.

Боумер, Голомб, Холл М. (Baumert L. D., Golomb S. W., Hall M., Jr.)

- [1] Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.*, **68** (1962), 237—238.

Боумер, Холл М. (Baumert L. D., Hall M., Jr.)

- [1] A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.*, **71** (1965), 169—170.

Боуз (Bose R. C.)

- [1] On the construction of balanced incomplete block designs, *Ann. Eugenics*, **9** (1939), 353—399.

Боуз, Паркер, Шрикханде (Bose R. C., Parker E. T., Shrikhande S.)

- [1] Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.*, **12** (1960), 189—203.

Боуз, Шрикханде (Bose R. C., Shrikhande S.)

- [1] On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Trans. Amer. Math. Soc.*, **95** (1960), 191—209.

Брук (Bruck R. H.)

- [1] Difference sets in a finite group, *Trans. Amer. Math. Soc.*, **78** (1955), 464—481.

Брук, Райзер (Bruck R. H., Ryser H. J.)

- [1] The nonexistence of certain finite projective planes, *Canad. J. Math.*, **1** (1949), 88—93.

**Бхаттачария** (Bhattacharya K. N.)

- [1] A note on two-fold triple systems, *Sankhyā*, **6** (1943), 313—314.
- [2] A new balanced incomplete block design, *Sci. Cult.*, **9** (1944), 508.

**Веблен, Веддербёрн** (Veblen O., Wedderburn J. H. M.)

- [1] Non-Desarguesian and non-Pascalian Geometries, *Trans. Amer. Math. Soc.*, **8** (1907), 379—388.

**Веблен, Юнг** (Veblen O., Young J. W.)

- [1] Projective Geometry, vol. 1, Boston, 1910.

**Вейснер** (Weisner L.)

- [1] Abstract theory of inversion of finite series, *Trans. Amer. Math. Soc.*, **38** (1935), 474—484.

**Витт** (Witt E.)

- [1] Theorie der quadratischen Formen in beliebigen Körpern, *J. für die reine u. angew. Math.*, **176** (1937), 31—44.

**Гейл, Кун, Текер** (Gale D., Kuhn H. W., Tucker A. W., Jr.)

- [1] Linear programming and the theory of games, Activity Analysis of Production and Allocation, New York, 1951, 317—329.

**Гуд** (Good I. J.)

- [1] Normal recurring decimals, *J. Lond. Math. Soc.*, **21** (1946), 167—169.

**Данциг** (Dantzig G.)

- [1] Maximization of a linear function of variables subject to linear inequalities, Chap. XXI, Activity Analysis of Production and Allocation, New York, 1951.

**Де Брёйн** (De Bruijn N. G.)

- [1] A combinatorial problem, *Nederl. Akad. Wetensch. Proc.*, **49**, 758—764; *Indagationes Math.*, **8** (1946), 461—467.

**Джонс** (Jones B. W.)

- [1] The Arithmetic Theory of Quadratic Forms, Carus Mathematical Monograph No. 10, Mathematical Association of America, 1950.

**Диананд** (Diananda P. H.)

- [1] On non-negative forms in real variables some or all of which are non-negative, *Proc. Cambr. Philos. Soc.*, **58** (1962), 17—25.

**Диксон** (Dickson L. E.)

- [1] Cyclotomy, higher congruences, and Waring's problem, *Amer. J. Math.*, **57** (1935), 391—424.

**Дилворт** (Dilworth R. P.)

- [1] A decomposition theorem for partially ordered sets, *Ann. Math.*, (2) **51** (1950), 161—166.

**Дин** (Dean R.)

- [1] Elements of Abstract Algebra, New York, 1966.

- Дюльмаж, Джонсон, Мендельсон (Dulmage A. L., Johnson D. M., Mendelsohn N. S.)**  
 [1] Orthomorphisms of groups and orthogonal Latin squares, I, *Canad. J. Math.*, 13 (1961), 356—372.
- Зингер (Singer J.)**  
 [1] A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, 43 (1938), 377—385.
- Йонсен (Johnsen E.)**  
 [1] Matrix rational completions satisfying generalized incidence equations, *Canad. J. Math.*, 17 (1965), 1—12.
- Кёниг (König D.)**  
 [1] Theorie der endlichen und unendlichen Graphen, New York, 1950.
- Киркман (Kirkman Rev. Thomas)**  
 [1] On a problem in combinations, *Cambr. and Dublin Math. J.*, 2 (1847), 191—204.
- Коннор (Connor W. S.)**  
 [1] On the structure of balanced incomplete block designs, *Ann. Math. Stat.*, 23 (1952), 57—71.
- Коул, Уайт, Каммингс (Cole F. N., White A. S., Cummings L. D., Jr.)**  
 [1] Complete classification of triad systems on fifteen elements, *Mem. Nat. Acad. Sci.*, 14 (1925), Second Memoir, 89.
- Лемер (Lehmer D. H.)**  
 [1] On the Hardy-Ramanujan series for the partition function, *J. Lond. Math. Soc.*, 12 (1937), 171—176.
- Макнейш (MacNeish H. F.)**  
 [1] Euler squares, *Ann. Math.*, 23 (1922), 221—227.
- Манн (Mann H. B.)**  
 [1] The construction of orthogonal Latin squares, *Ann. Math. Stat.*, 13 (1942), 418—423.
- Митчелл (Mitchell H. H.)**  
 [1] On the generalized Jacobi-Kummer cyclotomic function, *Trans. Amer. Math. Soc.*, 17 (1916), 165—177.
- Мур (Moore E. H.)**  
 [1] Concerning triple systems, *Math. Ann.*, 43 (1893), 271—285.
- Оре (Ore Oystein)**  
 [1] On coset representatives in groups, *Proc. Amer. Math. Soc.*, 9 (1958), 665—670.
- Паркер (Parker E.)**  
 [1] On collineations of symmetric designs, *Proc. Amer. Math. Soc.*, 8 (1957), 350—351.  
 [2] Construction of some sets of mutually orthogonal Latin squares, *Proc. Amer. Math. Soc.*, 10 (1959), 946—949.

**Пэли** (Paley R. E. A. C.)

- [1] On orthogonal matrices, *J. Math. Phys.*, **12** (1933), 311—320.

**Радемахер** (Rademacher H.)

- [1] A convergent series for the partition function  $p(n)$ , *Proc. Nat. Acad. Sci.*, **23** (1937), 78—84.

**Райзер** (Ryser H. J.)

- [1] Matrices with integer elements in combinatorial investigations, *Amer. J. Math.*, **74** (1952), 769—773.

**Райсс** (Reiss M.)

- [1] Über eine Steinersche kombinatorische Aufgabe welche in 45sten Bande dieses Journals, Seite 181, gestellt worden ist, *J. reine u. angew. Math.*, **56** (1859), 326—344.

**Рамсей** (Ramsey F. P.)

- [1] On a problem of formal logic, *Proc. Lond. Math. Soc.*, 2nd series, **30** (1930), 264—286.

**Рао** (Rao C. Radhakrishna)

- [1] A study of BIB designs with replications 11 to 15, *Sankhyā*, **23** (1961), 117—127.

**Рота** (Rota G. C.)

- [1] On the foundations of combinatorial theory, I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, **2** (1964), 340—368.

**Скарпис** (Scarpis V.)

- [1] Sui determinanti di valore massimo, *Rend. R. Ist. Lombardo Sci. e Lett.*, (2) **31** (1898), 1441—1446.

**Такер** (Tucker A.)

- [1] Combinatorial theory underlying linear programs, Recent Advances in Mathematical Programming, New York, 1963, 1—16.

**Тэрри** (Tarry G.)

- [1] Le problème des 36 officiers, *C. R. Assoc. Fr. Av. Sci.*, **1** (1900), 122—123; **2** (1901), 170—203.

**Тьюки** (Tukey J.)

- [1] Convergence and uniformity in topology, *Ann. of Math. Studies*, No. 2, Princeton University Press, 1940.

**Уитмен** (Whiteman A. L.)

- [1] A family of difference sets, *Ill. J. Math.*, **6** (1962), 107—121.

**Уильямсон** (Williamson J.)

- [1] Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.*, **11** (1944), 65—81.

- [2] Note on Hadamard's determinant theorem, *Bull. Amer. Math. Soc.*, **53** (1947), 608—613.

**Фаркаш** (Farkas J.)

- [1] Über die Theorie der einfachen Ungleichungen. I, *reine u. angew. Math.*, **124** (1902), 1—24.

**Фишер (Fisher R. A.)**

- [1] An examination of the different possible solutions of a problem in incomplete blocks, *Ann. Eugenics*, **10** (1940), 52—75.

**Фишер, Яетс (Fisher R. A., Yates F.)**

- [1] Statistical Tables for Biological, Agricultural and Medical Research, 2nd ed., London, 1943.

**Флуд (Flood M.)**

- [1] On the Hitchcock distribution problem, *Pacific J. Math.*, **3** (1953), 369—386.

**Франклайн (Franklin J.)**

- [1] Sur le développement du produit infini  $(1-x)(1-x^2)\dots$ , *C. R. Acad. Fr.*, **92** (1881), 448—450.

**Ханани (Hanani H.)**

- [1] The existence and construction of balanced incomplete block designs, *Ann. Math. Stat.*, **32** (1961), 361—386.

**Харди, Райт (Hardy G. H., Wright E. M.)**

- [1] An Introduction to the Theory of Numbers, Oxford, 1938.

**Харди, Рамануджан (Hardy G. H., Ramanujan S.)**

- [1] Asymptotic formulae in combinatorial analysis, *Proc. Lond. Math. Soc.*, (2), **17** (1918), 75—115.

**Холл М. (Hall Marshall, Jr.)**

- [1] A survey of difference sets, *Proc. Amer. Math. Soc.*, **7** (1956), 975—986.

- [2] Characters and cyclotomy, *Proc. Symposia in Pure Math., Amer. Math. Soc.*, **8** (1965), 31—43.

**Холл М., Райзер (Hall M. Jr., Ryser H. J.)**

- [1] Cyclic incidence matrices, *Canad. J. Math.*, **3** (1951), 495—502.

- [2] Normal completions of incidence matrices, *Amer. J. Math.*, **76** (1954), 581—589.

**Холл М., Свифт (Hall M. Jr., Swift J. D.)**

- [1] Determination of Steiner triple systems of order 15, *Math. Tables Aids Comput.*, **9** (1955), 146—156.

**Холл Ф. (Hall Ph.)**

- [1] On representatives of subsets, *J. Lond. Math. Soc.*, **10** (1935), 26—30.

- [2] The Eulerian functions of a group, *Quart. J. Math., Ox. Series*, **7** (1936), 134—151.

**Хьюз (Hughes D. R.)**

- [1] A class of non-Desarguesian projective planes, *Canad. J. Math.*, **9** (1957), 378—388.

**Цассенгауз (Zassenhaus H.)**

- [1] Über endliche Fastkörper, *Abh. Math. Sem. Hamburg*, **11** (1936), 187—220.

Чо вла, Райзер (Chowla S., Ryser H. J.)

[1] Combinatorial problems, *Canad. J. Math.*, **2** (1950), 93—99.

Чо вла, Эрдёш, Страус (Chowla S., Erdős P., Straus F. G.)

[1] On the maximal number of pairwise orthogonal Latin squares of a given order, *Canad. J. Math.*, **12** (1960), 204—208.

Шрикханде (Shrikhande S. S.)

[1] The impossibility of certain symmetrical balanced incomplete block designs, *Ann. Math. Stat.*, **21** (1950), 106—111.

Штейнер (Steiner J.)

[1] Combinatorische Aufgabe, *J. reine u. angew. Math.*, **45** (1853), 181—182.

Элих (Ehlich H.)

[1] Neue Hadamard-Matrizen, *Arch. Math.*, **16** (1965), 34—36.

Эрдёш, Капланский (Erdős P., Kaplansky I.)

[1] The asymptotic number of Latin rectangles, *Amer. J. Math.*, **68** (1946), 230—236.

Эрдёш, Секереш (Erdős P., Szekeres G.)

[1] A combinatorial problem in geometry, *Compositio Math.*, **2** (1935), 463—470.

Автоморфизм блок-схемы 167  
Адамара матрица 283  
Аксиомы проективной геометрии 230  
— — плоскости 238  
Аффинное пространство 235

База 319  
Базисная точка 169  
Биномиальный коэффициент 10, 12  
Блок 65  
— критический 66  
Блок-схема 140, 309  
— дополнительная 347  
— остаточная 144  
— производная 143  
— разрешимая 274  
— с делимостью на группы 275  
— связь с ортогональными таблицами 275, 276  
— симметричная 143  
— уравновешенная относительно пар элементов 271  
— — неполная 140  
— центрально разрешимая 312  
— циклическая 168  
де Брёйна последовательности 128  
де Брёйна теорема 136  
Брука теорема 190  
Брука — Райзера теорема 241  
Брука — Райзера — Човла теорема 149  
Бхаттачария теорема 337

Веблена — Веддербёрна система 250  
Веддербёрна теорема 234  
Ведущий главный минор 159  
*m*-вершина 131  
Витта теорема 381  
Включения и исключения принцип (метод) 18, 19  
Вполне положительная квадратичная форма 367  
Выделенные блоки 312  
Выпуклая оболочка множества 81

Выпуклое множество 95  
— пространство 95  
— тело 81, 95  
Выпуклый конус 97

Галуа поле 175  
Гаусса — Якоби тождество 53  
Гиперплоскость 96, 179, 234  
Голоморф группы 198  
Границная гиперплоскость 96  
Граф 129  
2-граф 135  
Групповое кольцо 191  
— разностное множество 170  
Гуда теорема 134

Дважды связанные блоки 356  
Двойственное пространство 101  
Двойственности теорема 105  
Двойственные задачи линейного программирования 105, 110, 111  
Двойственный граф 135  
Дезаргà теорема 231  
Дезаргова плоскость 233  
Диаграммы разбиения 48, 50  
Дилуорса теорема 90  
Дирихле производящая функция 43  
Дзета-функция 29  
Дополнение блок-схемы 347  
Допустимость задачи линейного программирования 105, 111

Евклидово пространство 95

Задача о беспорядках 19  
— — встречах 20  
— — гостях 24  
— — кёнигсбергских мостах 133  
— — назначениях 85, 108—109  
— — супружеских парах 24  
— — школьницах 335  
Замыкание множества 96  
Зингера теорема 179  
Зингеровы разностные множества 196

- Изоморфные блок-схемы** 167  
**Инцидентности матрица** 141  
 — отношение 230  
 — система 140  
**Йонсена теорема** 388  
**Квадратичный вычет** 155  
 — закон взаимности 156  
 — невычет 155  
**Кёнига теорема** 72  
**Киркмана задача** 335, 336  
**Класс разности** 321  
**Конгруэнтность** 381  
**Конечная геометрия** 230  
**Конечное поле** 172  
**Коннора метод** 349  
**Конфигурация** 231  
**Коположительная квадратичная форма** 367  
 — — — тест для проверки 378  
**Кососимметрического типа матрица** 290  
**Лангранжа теорема** 151  
**Латинский квадрат** 74  
 — прямоугольник 73, 74  
**Лежандра символ** 156  
**Линейное программирование** 104, 105  
**Линейно упорядоченное множество** 27  
**Линия в матрице** 72  
**Локально конечное частично упорядоченное множество** 27  
**Макнейша теорема** 263  
**Манна теорема** 267  
**Матрица инцидентности** 141  
 — кососимметрического типа 290  
**H-матрица** см. Адамара матрица  
**Мёбиуса функция** 21  
**Множитель разностного множества** 183, 184, 190  
**Модулярность** 231  
**Недезаргова плоскость** 233  
**Независимые элементы** 91  
**Неприводимый полином** 175  
**Несравнимые элементы** 90  
**Нормализованная матрица Адамара** 283  
**Норма точки** 95  
**Общих представителей системы**  
 75  
**Опорная гиперплоскость** 96  
**Опорное решение** 119  
**Оптимальное назначение** 85  
**Орбита** 319  
**Ориентированный граф** 129  
**Ортогональная таблица** 262  
**Ортогональные векторы** 262  
 — латинские квадраты 244  
 — матрицы 261  
**Осевое преобразование** 115, 116  
**Оси правило выбора** 120  
**Основное матричное соотношение** 144  
**Остаточная блок-схема** 144  
**Отделяющая гиперплоскость** 96  
  
**Паппа теорема** 231  
**Параллельное множество трансверсалей** 310  
**Параллельные блоки** 243  
**Первообразный элемент** 177  
**Перестановка** 9, 10  
**Петля** 129  
**Поле** 172  
**Полиномиальный коэффициент**  
 13  
**Полный цикл** 128  
**Полуполе** 254  
**Порядок конечной проективной**  
 плоскости 241  
**Почти-поле** 253  
**Представление квадратичной**  
 формы 381  
**Примитивный корень (первообразный элемент)** 177  
**«Принцип ящиков»** 174  
**Проективная геометрия** 178, 230  
**Производная блок-схема** 143  
**Производящая функция** 33  
 — — экспоненциальная 34  
**Прямая сумма матриц** 383  
 — — полей Галуа 227  
**Прямое произведение матриц** 288  
**Путь** 129  
  
**Равноблочная компонента** 271  
**Разбиения целого числа** 45, 48, 50  
 — — — арифметические свойства 56

- Разбиения целого числа произвоящая функция 49  
 Различных представителей системы 64, 65  
 — алгоритм нахождения 70, 71  
 Размерность проективного пространства 230  
 $(v, k, \lambda)$ -разностное множество 168  
 Разностных множеств типы 196, 197  
 Разрешимая блок-схема 274  
 Райзера теорема 146  
 Рамсей теорема 79  
 Свободное множество блоков 271  
 Свойство «здоровой наследственности» 334  
 — «незддоровой наследственности» 334  
 Связанные блоки 356  
 Связный граф 129  
 Символ норменного вычета Гильберта 158  
 — Хассе 159  
 Симметричная блок-схема 143  
 Симплексный метод 110, 119  
 Т-система (трансверсальная система) 309  
 Система троек 327  
 Скалярное произведение 100  
 Смешанная разность 321  
 Сопряженные разбиения 48  
 Сочетание 9, 11  
 Сравнимые элементы 90  
 Стирлиинга числа второго рода 42  
 — первого рода 42  
 Строго зависимое подмножество 93  
 Структурная матрица  $S_i$  352  
 Тактическая конфигурация 140  
 Тернар 249  
 Тернарная операция 249  
 Трансверсальная система 309  
 Уильямсона метод 299  
 Уравновешенная неполная блок-схема 140  
 Условие С 65, 69  
 Фаркаша теорема 102  
 Ферма теорема о классах вычетов 174  
 Фибоначчи числа 42  
 Фишера неравенство 144  
 Формула обращения Мёбиуса 22  
 Ханани теорема 337  
 Характер 289  
 Характеристическая матрица блоков 350  
 Характеристический полином рекуррентного соотношения 35, 37  
 Хассе символ 159  
 Хассе—Минковского теорема 160  
 Холла системы 251  
 Холла Ф. теорема 65  
 Хорна форма 376  
 Центр блок-схемы 312  
 Центральная разрешимость блок-схем 312  
 Цепь 26  
 Цикл 128, 129  
 Циклическая блок-схема 168  
 Циклические последовательности 22  
 Циклическое разностное множество 168  
 Частично упорядоченное множество 26  
 Чистая разность 321  
 Штейнера система троек 328  
 — — — метод построения Мура 330  
 Эйлера предположение 265, 277  
 Эйлера теорема 131  
 — — обобщение см. Гуда теорема  
 Эйлера тождество 50  
 Эквивалентность матриц Адамара 283  
 — ортогональных таблиц 263  
 Экстремальная точка 96  
 — — выпуклого конуса 97  
 Якоби тождество 55

# ОГЛАВЛЕНИЕ

|   |           |
|---|-----------|
| Предисловие редактора перевода . . . . .                                  | 5         |
| Предисловие . . . . .   | 7         |
| <b>Глава 1. Перестановки и сочетания . . . . .</b>                        | <b>9</b>  |
| 1.1. Определения . . . . .  | 9         |
| 1.2. Приложения к теории вероятностей . . . . .                           | 13        |
| Задачи . . . . .  | 16        |
| <b>Глава 2. Формулы обращения . . . . .</b>                               | <b>18</b> |
| 2.1. Принцип включения и исключения. Обращение Мёбиуса . . . . .          | 18        |
| 2.2. Частично упорядоченные множества и их функции Мёбиуса . . . . .      | 26        |
| Задачи . . . . .  | 32        |
| <b>Глава 3. Производящие функции и рекуррентные соотношения . . . . .</b> | <b>33</b> |
| 3.1. Правила и свойства . . . . .   | 33        |
| 3.2. Комбинаторные задачи . . . . .                                       | 37        |
| Задачи . . . . .  | 42        |
| <b>Глава 4. Разбиения . . . . .</b>                                       | <b>45</b> |
| 4.1. Разбиения. Тождества и арифметические свойства . . . . .             | 45        |
| 4.2. Асимптотические свойства $p(n)$ . . . . .                            | 59        |
| Задачи . . . . .  | 63        |
| <b>Глава 5. Системы различных представителей . . . . .</b>                | <b>64</b> |
| 5.1. Теоремы Ф. Холла и Д. Кёнига . . . . .                               | 64        |
| Задачи . . . . .  | 78        |
| <b>Глава 6. Теорема Рамсея . . . . .</b>                                  | <b>79</b> |
| 6.1. Формулировка и доказательство теоремы . . . . .                      | 79        |
| 6.2. Одно приложение теоремы Рамсея . . . . .                             | 81        |
| Задачи . . . . .  | 83        |
| <b>Глава 7. Некоторые экстремальные задачи . . . . .</b>                  | <b>85</b> |
| 7.1. Задача о назначениях . . . . .                                       | 85        |
| 7.2. Теорема Дилуорса . . . . .   | 90        |
| Задачи . . . . .  | 94        |

|   |                        |           |
|---|------------------------|-----------|
| <b>Глава 8. Выпуклые пространства и линейное программиро-</b>                             | <b>вание . . . . .</b> | <b>95</b> |
| 8.1. Выпуклые пространства. Выпуклые конусы и двой-<br>ственные им пространства . . . . . | 95                     |           |
| 8.2. Линейные неравенства . . . . .   | 102                    |           |
| 8.3. Линейное программирование. Симплексный метод . .                                     | 110                    |           |
| <b>Глава 9. Графические методы. Последовательности де Брёйна</b>                          | <b>128</b>             |           |
| 9.1. Полные циклы . . . . .   | 128                    |           |
| 9.2. Теоремы о графах . . . . .   | 130                    |           |
| 9.3. Доказательство теоремы де Брёйна . . . . .   | 134                    |           |
| <b>Глава 10. Блок-схемы . . . . .</b>   | <b>140</b>             |           |
| 10.1. Предварительное обсуждение . . . . .  | 140                    |           |
| 10.2. Элементарные теоремы о блок-схемах . . . . .  | 144                    |           |
| 10.3. Теорема Брука — Райзера — Човла . . . . .   | 149                    |           |
| 10.4. Формулировка теоремы Хассе — Минковского. При-<br>ложения . . . . .                 | 155                    |           |
| <b>Глава 11. Разностные множества . . . . .</b>   | <b>167</b>             |           |
| 11.1. Примеры и определения . . . . .   | 167                    |           |
| 11.2. Конечные поля . . . . .   | 172                    |           |
| 11.3. Теорема Зингера . . . . .   | 178                    |           |
| 11.4. Теорема о множителе . . . . .   | 183                    |           |
| 11.5. Разностные множества в группах общего вида . .                                      | 189                    |           |
| 11.6. Некоторые семейства разностных множеств . . . .                                     | 196                    |           |
| <b>Глава 12. Конечные геометрии . . . . .</b>   | <b>230</b>             |           |
| 12.1. Основания . . . . .   | 230                    |           |
| 12.2. Конечные геометрии как блок-схемы . . . . .   | 235                    |           |
| 12.3. Конечные плоскости . . . . .  | 238                    |           |
| 12.4. Некоторые типы конечных плоскостей . . . . .  | 248                    |           |
| <b>Глава 13. Ортогональные латинские квадраты . . . . .</b>                               | <b>261</b>             |           |
| 13.1. Ортогональность и ортогональные таблицы . . . .                                     | 261                    |           |
| 13.2. Основные теоремы . . . . .  | 263                    |           |
| 13.3. Построение ортогональных квадратов . . . . .  | 269                    |           |
| 13.4. Опровержение предположения Эйлера . . . . .   | 277                    |           |

|   |     |
|---|-----|
| <b>Глава 14. Матрицы Адамара</b>  | 283 |
| 14.1. Конструкции Пэли  | 283 |
| 14.2. Метод Уильямсона  | 299 |
| 14.3. Три новых метода  | 305 |
| <b>Глава 15. Общие методы построения блок-схем</b>  | 308 |
| 15.1. Методы построения   | 308 |
| 15.2. Основные определения. Теоремы Ханани  | 308 |
| 15.3. Прямые методы построения  | 318 |
| 15.4. Системы троек   | 327 |
| 15.5. Блок-схемы с $k > 3$  | 343 |
| <b>Глава 16. Теоремы о пополнении и вложении</b>  | 348 |
| 16.1. Метод Коннора   | 348 |
| 16.2. Коположительные и вполне положительные квадратичные формы   | 365 |
| 16.3. Рациональные пополнения матриц инцидентности  | 378 |
| 16.4. Целые решения уравнений инцидентности   | 389 |
| <b>Приложение I. Уравновешенные неполные блок-схемы с числом повторений каждого элемента от 3 до 15</b> | 398 |
| <b>Приложение II. Матрицы Адамара типа Уильямсона</b>   | 410 |
| <b>Библиография</b>   | 413 |
| <b>Предметный указатель</b>   | 419 |

Маршалл Холл

КОМБИНАТОРИКА