

Ю. В. ТАРАННИКОВ

**Комбинаторные свойства
дискретных структур
и приложения к криптологии**

Ю. В. Таранников

КОМБИНАТОРНЫЕ СВОЙСТВА ДИСКРЕТНЫХ СТРУКТУР И ПРИЛОЖЕНИЯ К КРИПТОЛОГИИ

Москва

Издательство МЦНМО

2011

Тверской государственный университет



Научная библиотека 00294088

03

ОГЛАВЛЕНИЕ

Введение	6
Глава 1. Теоремы Дилуорса, Кёнига, Холла и Шпернера	8
§ 1.1. Теорема Дилуорса	8
§ 1.2. Теорема Кёнига	10
§ 1.3. Теорема Холла	11
§ 1.4. Теорема Шпернера	12
Глава 2. Теорема Рамсея	15
§ 2.1. Теорема Рамсея	15
§ 2.2. Следствия из теоремы Рамсея	16
§ 2.3. Числа Рамсея	21
Глава 3. Теоремы Грэхема–Ротшильда и ван дер Вардена	26
§ 3.1. Теорема Грэхема–Ротшильда	26
§ 3.2. Теорема ван дер Вардена	29
Глава 4. Теорема Симона–Вегенера	30
§ 4.1. Теорема Симона–Вегенера	30
§ 4.2. Следствия из теоремы Симона–Вегенера	34
Глава 5. Матрицы Адамара	37
§ 5.1. Символы Лежандра	37
§ 5.2. Кронекерово произведение матриц	39
§ 5.3. Определение матриц Адамара	39
§ 5.4. Методы построения матриц Адамара	40
§ 5.5. Построение матриц Адамара методом Вильямсона	43
Глава 6. Кодовые множества с большими кодовыми расстояниями	47
§ 6.1. Коды, кодовое расстояние и исправление ошибок	47
§ 6.2. Некоторые оценки мощности кода	50
§ 6.3. Построение кодов с большими кодовыми расстояниями при помощи матриц Адамара	52

Глава 7. Блок-дизайны	56
§ 7.1. Блок-дизайны и условия на их параметры	56
§ 7.2. Симметричные блок-дизайны и условия на их параметры	59
Глава 8. Теорема Брука–Райзера–Човлы	63
§ 8.1. Теорема Лагранжа о четырех квадратах	63
§ 8.2. Теорема Брука–Райзера–Човлы	65
Глава 9. Конечные геометрии	69
§ 9.1. Аффинная плоскость	69
§ 9.2. Проективная плоскость	71
§ 9.3. Проективная геометрия	73
Глава 10. Взаимно ортогональные латинские квадраты	76
§ 10.1. Ортогональные латинские квадраты и их простейшие конструкции	76
§ 10.2. Опровержение гипотезы Эйлера для одного из случаев .	79
§ 10.3. Взаимно ортогональные латинские квадраты	81
Глава 11. Ортогональные массивы	85
§ 11.1. Ортогональные массивы	85
§ 11.2. Соотношения на параметры ортогональных массивов . .	88
§ 11.3. Применение ортогональных массивов	89
Глава 12. Линейные коды	92
§ 12.1. Линейные коды	92
§ 12.2. Линейный код как ортогональный массив	98
Глава 13. Неравенство Бирбрауэра–Фридмана	99
§ 13.1. Неравенство Бирбрауэра–Фридмана	99
§ 13.2. Неравенство Рао	103
Глава 14. Трансверсальные дизайны	105
§ 14.1. Трансверсальные дизайны. Эквивалентность трансвер- сальных дизайнов и ортогональных массивов силы 2 и индекса 1	105
§ 14.2. Прямая конструкция ортогонального массива силы 2 и индекса 1 с числом элементов, равным степени просто- го числа	107
§ 14.3. Усеченные ортогональные дизайны. Конструкция Виль- сона	108

§ 14.4. Завершение опровержения гипотезы Эйлера о несуществовании ортогональных латинских квадратов	112
Глава 15. Комбинаторные t-дизайны	115
§ 15.1. Условия существования t -дизайнов	115
§ 15.2. Адамаровы дизайны	116
§ 15.3. Существование нетривиальных t -дизайнов с возможно повторяющимися блоками	117
Глава 16. Код Голея и дизайны Витта	120
§ 16.1. Код Голея	120
§ 16.2. Дизайны Витта	122
Глава 17. Разностные множества	125
§ 17.1. Разностные множества	125
§ 17.2. Теорема Манна	127
Глава 18. Булевы функции. Бент-функции	129
§ 18.1. Булевы функции и коэффициенты Уолша	129
§ 18.2. Бент-функции	132
§ 18.3. Связь между бент-функциями и разностными множествами	136
Глава 19. Корреляционно-иммунные и устойчивые булевы функции	140
§ 19.1. Корреляционно-иммунные и устойчивые функции	140
§ 19.2. Спектральная характеристика корреляционно-иммунных функций	143
§ 19.3. Верхние оценки нелинейности корреляционно-иммунных и устойчивых булевых функций	146
§ 19.4. Теорема Фон-Дер-Флаасса	148
Литература	150