ОГЛАВЛЕНИЕ

Введение 8

Глава 1. **Базовые понятия** 11

§ 1.1. Пространство Хемминга 11
1.1.1. Метрика Хемминга (11). 1.1.2. Линейный код (12). 1.1.3. Двойственный код (13). 1.1.4. Пространство, образованное равновесными двоичными векторами (15).

§ 1.2. Сфера в n-мерном евклидовом пространстве 15
1.2.1. Метрика на сфере (15). 1.2.2. Ортогональные и унитарные преобразования (17). 1.2.3. Орбитный код (18).

§ 1.3. Изометрическое вложение орбитного кода на унитарной сфере в орбитный код на евклидовой сфере. 19

§ 1.4. Изометрическое расположение кода в пространстве Хемминга на сфере евклидова пространства 23
1.4.1. Вложение двоичного пространства Джонсона в евклидову сферу (33).

Глава 2. **Оценки** 35

§ 2.1. Верхняя оценка числа элементов кода 35
2.1.1. Оценка Хемминга (35). 2.1.2. Оценки сверху для числа элементов равновесных кодов (37). 2.1.3. Оценка Элайса–Бассалыго (38). 2.1.4. Оценка Плоткина и матрицы Адамара (38). 2.1.5. Оценки Синглтона и Грайсмера (43). 2.1.6. Оценка для числа элементов антиподального кода (45).

§ 2.2. Оценки существования кода 47
2.2.1. Оценка Варшамова–Гилберта (47). 2.2.2. Асимптотические границы (48). 2.2.3. Основные задачи теории кодирования (51).

Глава 3. **Центральные функции на линейном пространстве Хемминга** 53

§ 3.1. Специальные функции 53
3.1.1. Характеры (53). 3.1.2. Автоморфизмы группы $\mathfrak{G}$ (54). 3.1.3. Скалярное произведение (55). 3.1.4. Классы сопряженных элементов (56). 3.1.5. Центральные функции относительно подгруппы H группы $\mathrm{Aut}(\mathfrak{G})$ (56).

§ 3.2. Ортогональные многочлены 60

3.2.1. Элементарная абелева группа (60). 3.2.2. Примарная группа порядка p^l (63). 3.2.3. Многочлены Кравчука и мономиальная группа (64). 3.2.4. Симметрическая группа в качестве группы H и полная весовая функция кода (66). 3.2.5. Ортогональные многочлены для примарного кольца вычетов (68). 3.2.6. Многочлены Кравчука как зональные сферические функции (69).

Глава 4. **Оценка линейного программирования** 72
§ 4.1. Положительно определенные функции. 72
§ 4.2. Оценка линейного программирования 75
4.2.1. Оценка Дельсарта (75). 4.2.2. Выбор многочлена в оценке (4.2.6) (77).

Глава 5. **Коды Рида–Соломона и БЧХ-коды** 83
§ 5.1. Коды Рида–Соломона 83
5.1.1. Определение кода Рида–Соломона (83). 5.1.2. Элементарные свойства кодов Рида–Соломона (85).
§ 5.2. Циклические коды 87
5.2.1. Циклические коды $RS_q(n,d)$ типа 1 (89). 5.2.2. Представление вектора циклического кода в виде рекуррентной последовательности (90). 5.2.3. Представление векторов циклического кода в виде значений функции «след» (92). 5.2.4. Представление элементов циклического кода в виде элементов группового кольца циклической группы над конечным полем (94).
§ 5.3. Коды Боуза–Чоудхури–Хоквингема (БЧХ-коды) 101
5.3.1. Группа автоморфизмов БЧХ-кода (101). 5.3.2. Параметры БЧХ-кода (102). 5.3.3. Циклические коды Боуза–Чоудхури–Хоквингема (105). 5.3.4. Точное значение размерности БЧХ-кода при не слишком больших значениях d (106).
§ 5.4. Обобщенные коды Рида–Соломона $RS_q(n,d)$ 108
5.4.1. Обобщенные БЧХ-коды (108). 5.4.2. Циклический обобщенный БЧХ-код длины $n=q+1$ (109). 5.4.3. Коды Гоппы (110).
§ 5.5. Автоморфизмы кода 113
5.5.1. Группа автоморфизмов кода (114). 5.5.2. Подгруппы группы автоморфизмов кодов Рида–Сололомона $RS_q(n,d)$, $n=q-1,q$ (116).
§ 5.6. Группа обобщенных автоморфизмов кода 117
5.6.1. Группа дробно-линейных преобразований (118).
§ 5.7. Число обобщенных кодов Рида–Соломона 120
5.7.1. Число проверочных матриц кода $RS_q(n,d)$ (120). 5.7.2. Число обобщенных кодов Рида–Соломона (120).

Глава 6. **Декодирование кодов Рида–Соломона** 123
§ 6.1. Что такое алгоритм декодирования? 123

6.1.1. Вводные понятия (126).
§ 6.2. Синдромный метод декодирования RM-кодов 128
6.2.1. Предварительные замечания (128). 6.2.2. Вспомогательные утверждения (129). 6.2.3. Многочлен локаторов ошибок (131). 6.2.4. Алгоритм Берлекэмпа (132). 6.2.5. Формула Кристофеля–Дарбу (137). 6.2.6. Как вычислить число u ошибок, поразивших кодовый вектор? (139). 6.2.7. Один несиндромный алгоритм декодирования кода Рида–Соломона (140). 6.2.8. Краткий обзор некоторых результатов по декодированию кодов Рида–Соломона (141).

Глава 7. **Коды Рида–Маллера** 147
§ 7.1. Булевы функции и многочлены Жегалкина 147
7.1.1. Элементарные свойства кода Рида–Маллера (150).
§ 7.2. Декодирование кода Рида–Маллера 153
7.2.1. Алгоритм декодирования RM-кода первого порядка по максимуму правдоподобия и «быстрое» умножение вектора на матрицу Адамара (155). 7.2.2. Полиномиальный алгоритм декодирования RM-кода порядка $r>1$ (157). 7.2.3. Основная идея полиномиального декодирования RM-кода r-го порядка (159). 7.2.4. Декодирование кода $RM_{1,m}$ первого порядка (161). 7.2.5. Декодирование кода $RM_{2,m}$ (162). 7.2.6. Эффективность алгоритма декодирования в случае $r=2$ (165). 7.2.7. Оценка вероятности ошибки декодирования кода по критерию максимального правдоподобия (167).
§ 7.3. Другие способы представления векторов RM-кода. 171

Глава 8. **Некоторые частные классы кодов** 174
§ 8.1. Вспомогательные результаты. Вычисление некоторых тригонометрических сумм 174
§ 8.2. Код Кердока 179
§ 8.3. Код Препарата. 183
§ 8.4. Циклический линейный код, порождаемый булевыми функциями ранга 2. 187
§ 8.5. Авто- и взаимная корреляции последовательностей 188
§ 8.6. Коды с кодовым расстоянием 5 или 6 197
8.6.1. БЧХ-коды с кодовым расстоянием 5 (197). 8.6.2. Троичный БЧХ-код, исправляющий две ошибки (198). 8.6.3. Троичный код работы, исправляющий две ошибки (199). 8.6.4. Коды Геворкяна (201).

Глава 9. **Весовой спектр линейного кода**. 205
§ 9.1. Соотношение МакВильямс 205
§ 9.2. Спектр линейного кода и многочлены Кравчука 208
9.2.1. Соотношение МакВильямс для весовой функции линейного кода (208). 9.2.2. Соотношение МакВильямс для полной

весовой функции линейного кода (209). 9.2.3. Использование соотношения МакВильямс для вычисления спектра кода (211). 9.2.4. Функция типа χ^2 для элементов спектра кода $\mathfrak{K}$ (215). 9.2.5. Выражение функции $\Xi(\mathfrak{K})$ через спектр двойственного кода (215). 9.2.6. Среднее функции $\Xi(\mathfrak{K})$ (218). 9.2.7. Пример вычисления спектра кода $\mathfrak{K}$ с помощью функции $\Xi(\mathfrak{K})$ (218).

§ 9.3. Спектр БЧХ-кодов 220

Глава 10. **Схемы отношений** 225

§ 10.1. Введение 225
10.1.1. Некоторые общие свойства схемы отношений (227).

§ 10.2. Построение схем отношений 228
10.2.1. Схемы отношений $\mathcal{S}_H(\mathfrak{G})$ (229). 10.2.2. Примеры (231).

§ 10.3. Схемы отношений на $\mathfrak{G}^n$ 232

§ 10.4. Алгебра Бозуа–Меснера ассоциативной схемы 235
10.4.1. Некоторые сведения из теории представления конечных групп (235). 10.4.2. Базисы алгебры Бозуа–Меснера (237). 10.4.3. Вычисление коэффициентов $P_k(j)$ для ассоциативной схемы $\mathcal{S}_H(\mathfrak{G})$, у которой $H = Inn(\mathfrak{G})$. Продолжение примера 10.2.2. (241). 10.4.4. $\mathfrak{G}$ — группа $(\mathbb{F}_p, +)$. Продолжение примера 10.2.1 (243). 10.4.5. Схемы отношений Хемминга (245).

§ 10.5. Метрики на схеме отношений $\mathbf{C}_H(\mathfrak{G})$ 245
10.5.1. Скалярное произведение на группе (247). 10.5.2. Продолжение примера 10.2.1. (247). 10.5.3. Продолжение примера 10.2.2 (248). 10.5.4. Метрики на группе $\mathfrak{G}$ (249). 10.5.5. Метрика на группе $\mathfrak{G}^n$ (251). 10.5.6. Краткий обзор результатов по схемам отношений (252).

Глава 11. **Квантовые коды** 255

§ 11.1. Основные понятия 255
11.1.1. Определения (256). 11.1.2. О некоторых конечных группах порядка 8 (258). 11.1.3. Операторы (259).

§ 11.2. Некоторые конструкции квантовых кодов 261
11.2.1. Квантовые коды, образованные собственными векторами коммутативной подгруппы $\mathcal{H}_L$ группы $\mathcal{E}^{\otimes n}$ (261). 11.2.2. Квантовый «код Хэмминга» длины $n = 2^m$ (264). 11.2.3. Квантовый код с кодовым расстоянием 5 (266).

Глава 12. **Открытые системы шифрования на основе кодов, корректирующих ошибки, и как некоторые из них можно расколоть** 269

§ 12.1. Введение 269

§ 12.2. Роль декодирования в кодовых системах открытого шифрования 270

§ 12.3. Системы открытого шифрования на основе кода, корректирующего ошибки. 272

12.3.1. Система открытого шифрования МакЭлиса (272). 12.3.2. Система открытого шифрования Нидеррайтера (274). 12.3.3. Сравнение систем открытого шифрования МакЭлиса и Нидеррайтера (276). 12.3.4. Некоторые свойства систем открытого шифрования МакЭлиса и Нидеррайтера (276).

§ 12.4. Как раскалывается система открытого шифрования Нидеррайтера, построенная с помощью обобщенного кода Рида–Соломона? Общие подходы 277

§ 12.5. Алгоритм определения секретного ключа системы открытого шифрования, использующего обобщенный код Рида–Соломона 279
12.5.1. Как определить первые три элемента ω_j? (279). 12.5.2. Определение элементов ω_j, $j > 3$ (280). 12.5.3. Определение элементов z_j и матрицы h (282). 12.5.4. Заключительные замечания (284).

Глава 13. **Совершенная секретность в полилинейных системах распределения ключей** 286

§ 13.1. Модель системы распределения ключей 286
13.1.1. Введение (286). 13.1.2. Вводные замечания (287). 13.1.3. Математическая модель системы распределения ключей (288).

§ 13.2. Определение полилинейной (t, w)-системы распределения ключей $\mathcal{S}$ 289
13.2.1. Свойства ключевой системы (291).

§ 13.3. Конструкция полилинейной (t, w)-системы распределения ключей 292

§ 13.4. Основной результат 294
13.4.1. Возможные конструкции множеств Q (297).

§ 13.5. Системы распределения ключей Блундо и другие 298

§ 13.6. Нижние оценки числа ключей у пользователей (w, t)-системы распределения ключей 299

Глава 14. **Дизъюнктные и разделяющие коды** 302

§ 14.1. Дизъюнктные коды (superimposed codes) 302
14.1.1. Разделяющие коды (304). 14.1.2. Построение разделяющих $(w, 1)$-кодов (307).

§ 14.2. Каскадная конструкция дизъюнктных кодов 308

§ 14.3. Максимальные дизъюнктные l-коды 311
14.3.1. Максимальный дизъюнктный l-код $\mathcal{Q}_{q,l}$ с q элементами (311).

§ 14.4. Криптографические приложения дизъюнктных кодов 316