

Механико-математический факультет МГУ

Программа полугодового спецкурса по выбору студента

«Комбинаторные дизайны (введение)»,

лектор — доцент Ю. В. Таранников, 2019/2020 уч. год.

1. Блок-дизайны. Основные соотношения, связывающие их параметры.
2. Соединение блок-дизайнов. Дополнительный блок-дизайн.
3. Матрица инцидентности блок-дизайна. Неравенство Фишера.
4. Симметричные блок-дизайны. Свойства их матриц инцидентности. Блок-дизайн, дополнительный к симметричному.
5. Неравенства, связывающие параметры симметричных блок-дизайнов. Симметричные блок-дизайны, на которых достигается верхняя оценка.
6. Матрицы Адамара, их свойства. Делимость порядка матрицы Адамара, большего чем 2, на 4. Связь между адямаровыми блок-дизайнами и матрицами Адамара.
7. Необходимое условие существования симметричного блок-дизайна с четным числом элементов.
8. Теорема Лагранжа о представлении в виде суммы четырех квадратов.
9. Теорема Брука–Райзера–Човлы.
10. Примеры применения теоремы Брука–Райзера–Човлы.
11. Аффинная плоскость. Разрешимость аффинной плоскости. Существование аффинных плоскостей порядка, равного степени простого числа.
12. Проективная плоскость. Связь с аффинной плоскостью.
13. Проективная геометрия.
14. Латинские квадраты. Ортогональные латинские квадраты. Проблема существования ортогональных латинских квадратов заданного порядка. Существование ортогональных латинских квадратов всех порядков, не сравнимых с 2 по модулю 4.
15. Опровержение гипотезы Эйлера о несуществовании ортогональных латинских квадратов для порядков, сравнимых с 10 по модулю 12.
16. Взаимно ортогональные латинские квадраты. Верхняя оценка их числа.
17. Связь существования $n - 1$ взаимно ортогональных латинских квадратов порядка n с существованием аффинной плоскости порядка n .
18. Ортогональные массивы.
19. Связь ортогональных массивов силы 2 индекса 1 со взаимно ортогональными латинскими квадратами.
20. Трансверсальные дизайны. Эквивалентность трансверсальных дизайнов и ортогональных массивов силы 2 и индекса 1.
21. Усеченные трансверсальные дизайны. Конструкция Вильсона.
22. Завершение опровержения гипотезы Эйлера о несуществовании ортогональных латинских квадратов.
23. t -Дизайны.
24. Адамаровы дизайны.
25. Существование нетривиальных t -дизайнов с возможно повторяющимися блоками.
26. Расширенный и совершенный двоичные коды Голея.
27. Число наборов веса 8 в расширенном двоичном коде Голея.
28. Дизайны Витта.
29. Разностные множества.
30. Построение симметричных блок-дизайнов с помощью разностных множеств.
31. Разностные множества, состоящие из квадратичных вычетов.
32. Теорема Манна.
33. Коэффициенты Уолша булевых функций. Формула обращения для коэффициентов Уолша.
34. Автокорреляционные коэффициенты булевых функций. Их выражение через квадраты коэффициентов Уолша и наоборот. Равенство Парсевала.
35. Нелинейность булевых функций. Бент-функции. Характеризация бент-функций через коэффициенты Уолша и автокорреляционные коэффициенты.
36. Бент-функции как характеристические функции нетривиальных разностных множеств в \mathbf{Z}_2^n .

Литература.

1. Ю. В. Таранников. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.: МЦНМО, 2011.