Механико-математический факультет МГУ

Программа годового или полугодового спецкурса
по выбору студента «Комбинаторные дизайны»,
лектор — доцент Ю. В. Таранников, 2017/2018 уч. год.

Звездочками помечены вопросы для сдачи курса в качестве полугодового.

1. Конечные поля.
2. Символы Лежандра. Их свойства.
3. Кронекерово произведение матриц. Его свойства.
4. Матрицы Адамара. Проблема существования матриц Адамара заданного порядка.
5. Кронекерово произведение матриц Адамара. Матрицы Адамара–Сильвестра.
6. Методы построения матриц Адамара с помощью символов Лежандра. Матрицы Адамара симметрические и кососимметрического типа.
7. Построение матриц Адамара методом Вильямсона.
8. Кодовые множества. Кодовые расстояния. Эквидистантные коды.
9. Неравенство Плоткина.
10. Максимальная мощность кодовых множеств в случае больших кодовых расстояний. Связь с матрицами Адамара.
*11. Блок-дизайны. Основные соотношения, связывающие их параметры.
*12. Соединение блок-дизайнов. Дополнительный блок-дизайн.
*13. Разрешимые блок-дизайны.
*14. Матрица инцидентности блок-дизайна. Неравенство Фишера.
*15. Симметрические блок-дизайны. Свойства их матриц инцидентности.
*16. Неравенства, связывающие параметры симметрических блок-дизайнов.
*17. Связь между адамаровыми блок-дизайнами и матрицами Адамара.
*18. Теорема Лагранжа о представлении в виде суммы четырех квадратов.
*19. Теорема Брука–Райзера–Човлы.
*20. Аффинная плоскость. Разрешимость аффинной плоскости. Существование аффинных плоскостей порядка, равного степени простого числа.
*21. Проективная плоскость. Связь с аффинной плоскостью.
*22. Проективная геометрия.
*23. Латинские квадраты. Ортогональные латинские квадраты. Проблема существования ортогональных латинских квадратов заданного порядка. Существование ортогональных латинских квадраты всех порядков, не сравнимых с 2 по модулю 4.
*24. Опровержение гипотезы Эйлера о несуществовании ортогональных латинских квадратов для порядков, сравнимых с 10 по модулю 12.
* 25. Взаимно ортогональные латинские квадраты.
*26. Связь существования $n-1$ взаимно ортогональных латинских квадратов порядка n с существованием аффинной плоскости порядка n.
27. Ортогональные массивы.
28. Связь взаимно ортогональных латинских квадратов с ортогональными массивами силы 2.
29. Линейные коды. Базис. Дуальный код. Порождающая и проверочная матрицы. Связь кодового расстояния линейного кода с линейной независимостью столбцов его проверочной матрицы.
30. Линейный код как ортогональный массив.
31. Неравенство Варшамова–Гильберта.

32. Некоторые конструкции ортогональных массивов, основанные на линейных кодах.
33. Рекуррентные соотношения для максимального числа столбцов в ортогональных массивах. Неравенства Буша.
34. Конструкция Буша.
35. Неравенство Биербрауера-Фридмана.
36. Неравенство Рао.
*37. Трансверсальные дизайны. Эквивалентность трансверсальных дизайнов и ортогональных массивов силы 2 и индекса 1.
*38. Прямая конструкция ортогонального массива силы 2 и индекса 1 с числом элементов, равным степени простого числа.
*39. Усеченные трансверсальные дизайны. Конструкция Вильсона.
*40. Завершение опровержения гипотезы Эйлера о несуществовании ортогональных латинских квадратов.
*41. t-Дизайны.
*42. Адамаровы дизайны.
*43. Существование нетривиальных t-дизайнов с возможно повторяющимися блоками.
44. Двоичный код Голея и дизайны Витта.
*45. Разностные множества.
*46. Построение симметричных блок-дизайнов с помощью разностных множеств.
*47. Разностные множества, состоящие из квадратичных вычетов.
*48. Теорема Манна.
49. Коэффициенты Уолша булевых функций. Формула обращения и равенство Парсеваля для коэффициентов Уолша.
50. Автокорреляционные коэффициенты булевых функций. Их выражение через квадраты коэффициентов Уолша и наоборот.
51. Нелинейность булевых функций. Бент функции. Характеризация бент функций через коэффициенты Уолша и автокорреляционные коэффициенты. Связь с матрицами Адамара. Пример бент функции.
52. Теорема Титсворта.
*53. Бент функции как характеристические функции разностных множеств.
54. Корреляционно-иммунные и устойчивые булевы функции. Корреляционно-иммунная булева функция как характеристическая функция простого ортогонального массива.
55. Неравенство Зигенталера.
56. Тождество Саркара.
57. Спектральная характеризация корреляционно-иммунных и устойчивых функций.
58. Делимость коэффициентов Уолша корреляционно-иммунных и устойчивых функций.
59. Верхние оценки нелинейности корреляционно-иммунных и устойчивых булевых функций.
60. Ограниченность числа нелинейных переменных в устойчивых функциях высокого порядка.
61. Несуществование неуравновешенных неконстантных корреляционно-иммунных функций больших порядков. Теорема Фон-Дер-Флаасса.

Литература.

*1. Ю. В. Таранников. Комбинаторные свойства дискретных структур и приложения к криптологии. — М.: МЦНМО, 2011.
2. A. S., Sloane N. J. A., Stufken , J. Orthogonal arrays. Theory and applications. — Springer-Verlag, 1999.