ДИСКРЕТНАЯ МАТЕМАТИКА

проф. С. Б. Гашков

1/2 года, 3 курс, экономический поток

1. Правило сложения и правило умножения в комбинаторике. Декартово произведение множеств. Множество всех подмножеств данного множества. Алгебра множеств. Характеристические функции.

2. Формула включения–исключения и ее применения.

3. Множество всех отображений из одного множества в другое. Множество инъективных отображений. Число размещений. Множество всех перестановок.

4. Выборки и сочетания. Число подмножеств данной мощности. Биномиальные коэффициенты и треугольник Паскаля. Полиномиальные коэффициенты и полиномиальная теорема.

5. Мультимножества и число мультимножеств данной мощности. Сочетания с повторениями. Упорядоченные разбиения на натуральные слагаемые.

6. Множество сюръективных отображений из одного множества в другое. Числа Стирлинга и их выражение через биномиальные коэффициенты.

7. Производящие функции. Тождества с биномиальными коэффициентами. Задача Эйлера о размене монет.

8. Производящие функции. Вычисление с их помощью числа Каталана. Задача Эйлера о числе триангуляций.

9. Решение линейных рекуррентных соотношений. Формула Бине для чисел Фибоначчи.

10. Графы, орграфы и мультиграфы. Элементы графа, способы задания графов. Цепи и циклы в графах. Реализация графов в трехмерном пространстве. Связность и связные компоненты. Метрическое пространство, связанное с графом.

11. Деревья и их свойства. Оценка числа попарно неизоморфных плоских укладок корневых деревьев. Теорема Кэли о числе деревьев с занумерованными вершинами. Кодирование деревьев методом Прюфера.

12. Потоки в сетях. Теорема Форда–Фалкерсона о максимальном потоке и минимальном разрезе. Теорема о целочисленности максимального потока.

13. Алгоритм Форда–Фалкерсона нахождения максимального потока и минимального разреза.

14. Двудольные графы. Паросочетания и вершиные покрытия ребер. Теорема Кенига–Эгервари и реберная форма теоремы Менгера как следствия теоремы о максимальном потоке и минимальном разрезе.

15. Матричная форма теоремы Кенига–Эгервари. Паросочетания и системы различных представителей. Теорема Холла.

16. Булевы функции. Формулы. Полиномы Жегалкина. Разложение булевых функций по переменным. Дизъюнктивные и конъюнктивные нормальные формы.

17. Бинарный многомерный куб. Геометрическая интепретация ДНФ. Максимальные интервалы. Сокращенная, минимальная и кратчайшие ДНФ. Тупиковые ДНФ.

18. Схемы из функциональных элементов. Сложность схемы и сложность функции. Метод каскадов и бинарные разрешающие диаграммы. Верхняя оценка сложности произвольной булевой функции, полученная методом каскадов.

19. Алфавитное кодирование. Разделимые коды. Префиксные коды. Неравенство Крафта–Макмиллана. Существование префиксного кода с заданными динами слов.

20. Графовый алгоритм распознавания разделимости кода.

21. Коды с минимальной избыточностью и их построение алгоритмом Хаффмана.

22. Самокорректирующиеся двоичные коды. Минимальное расстояние кода. Неравенства Хемминга для мощности максимального кода с заданным расстоянием.

23. Коды Хемминга и их порождающие и проверочные матрицы. Коды Хемминга как совершенные (плотно упакованные) коды. Задача поиска фальшивой монеты.

24. Простейшие понятия криптологии. Криптосистемы с открытым (асимметричным) ключом. Кольца вычетов, конечные поля, примитивные элементы и дискретное логарифмирование.

25.Криптосистема RSA и алгоритм генерации общего секретного ключа Диффри и Хеллмана. Электронная подпись и электронные деньги.

26. Детерминированные и недетерминированные машины Тьюринга. Временная сложность вычисления на машинах Тьюринга. Языки и проблема распознавания принадлежности слова данному языку. Классы P и NP. Полиномиальная сводимость. NP-полные задачи.

27. NP полнота задачи выполнимости КНФ и ее интерпретация в виде “карточного пасьянса”.

28. NP-полнота задач о вершинном покрытии ребер графа, клике, независимом множестве и изоморфизме подграфу.

29. NP-полнота задачи о 3-выполнимости.