ТВиМС - Коллоквиум 1

Цирк Максимус | telegram

Версия от 22.10.2020 14:02

Содержание

1 Вопросы

1. **Дискретное вероятностное пространство. Свойства вероятностной меры на конечных и счётных множествах. Вероятностный алгоритм проверки числа на простоту.**

   Определение. Пусть задано некоторое множество возможных исходов (эксперимента) $\Omega = \{1, 2, \dots, n\}$. Это множество называют множеством элементарных исходов. Всякое подмножество $A \subset \Omega$ называют событием. Функцию $P : 2^{\Omega} \to [0, 1]$, удовлетворяющую следующим свойствам:

   (1) $P(\Omega) = 1$,

   (2) $A \cap B = P(A \cup B) = P(A) + P(B)$ (правило суммы или аддитивность), называют вероятностной мерой, а значение $P(A)$ - вероятностью события A.

   Тест Ферма проверки числа на простоту.

   Пусть дано некоторое натуральное число $N > 1$. Мы хотим проверить является ли это число простым. Можно перебирать все простые делители до $\sqrt{N}$, но это очень долго. Хотелось бы иметь более быстрый способ проверки.

   Если N простое число, то по малой теореме Ферма для всякого натурального числа b такого, что НОД$(b, N) = 1$, число $b^{N-1} - 1$ делится на N. Следовательно, если для некоторого b, удовлетворяющего условию НОД$(b, N) = 1$, число $b^{N-1} - 1$ не делится на N, то N не является простым. В этом случае будем говорить, что N не проходит тест Ферма по основанию b. Это наблюдение используют для построения простейшего алгоритма проверки числа на простоту: выберем случайное число b из промежутка $2, \dots, N-1$; если НОД$(b, N) \neq 1$, то N составное; если НОД$(b, N) = 1$, но $b^{N-1} - 1$ не делится на N, то N составное. В ином случае N - скорее простое.

   Предположим, что существует хотя бы одно число a: НОД$(a, N) = 1$ и $a^{N-1} - 1$ не делится на N. Посмотрим, с какой вероятностью алгоритм выдаст ответ, что N - скорее простое. Пусть Z_N^* - группа всех чисел из промежутка $1, \dots, N-1$, взаимно простых с N. Если N проходит тест для основания $b \in Z_N^*$, то для основания ab число N уже тест не проходит. В противном случае $(ab)^{N-1} \equiv 1 (mod\ N)$ и $(b^{-1})^{N-1} \equiv 1(mod\ N)$. Следовательно, $a^{N-1} \equiv (b^{-1})^{N-1}(ab)^{N-1} \equiv 1$, что противоречит предположению. Таким образом, каждому основанию b, для которого N проходит тест, можно сопоставить основание ab, для которого N тест не проходит. Значит, оснований, для которых N не проходит тест, не меньше, чем оснований, для которых N проходит тест на простоту. Поэтому в данной ситуации вероятность получить ответ, что N скорее простое, не более $\frac{1}{2}$. Если независимым образом повторять описанную процедуру k раз, то вероятность получить неверный ответ не более $\left(\frac{1}{2}\right)^k$. Отметим, что бывают числа, которые проходят тест для всех оснований b. Это числа Кармайкла, например 561. Для них описанный алгоритм по понятным причинам не применим.

2. **Формула включений-исключений. Парадокс распределения подарков. Задача про конференцию.**

3. **Условная вероятность. Формула полной вероятности. Формула Байеса. Независимые события. Отличие попарной независимости от независимости в совокупности. Задача о билетах к экзамену.**

4. **Задача о сумасшедшей старушке. Парадокс Байеса. Парадокс Монти Холла.**

5. **Случайные величины на дискретном вероятностном пространстве, их распределение. Примеры дискретных распределений. Совместное распределение случайных величин. Независимые случайные величины. Эквивалентное определение независимости случайных величин.**

6. **Математическое ожидание случайной величины на дискретном вероятностном пространстве, эквивалентный способ вычисления математического ожидания. Математическое ожидание функции от случайной величины. Свойства математического ожидания: линейность, ожидание неотрицательной случайной величины, неотрицательная случайная величина с нулевым математическим ожиданием, связь модуля ожидания и ожидания модуля случайной величины, математическое ожидание произведения независимых случайных величин. Балансировка векторов.**

7. **Дисперсия, ковариация и коэффициент корреляции. Их связь и основные свойства: билинейность ковариации, случайная величина с нулевой дисперсией, дисперсия линейного образа случайной величины, дисперсия суммы независимых случайных величин. Неравенство Коши-Буняковского и геометрическая интерпретация ковариации, дисперсии и коэффициент корреляции. Вычисление ожидания и дисперсии у биномиального распределения.**

8. **Неравенство Чебышёва. Закон больших чисел в слабой форме.**

9. **Теорема Муавра-Лапласа (формулировка локальной и интегральной теорем, доказательство локальной теоремы в симметричном случае, идея доказательства интегральной теоремы).**