ТВиМС - Коллоквиум 1

Цирк Максимус | telegram

Версия от 23.10.2020 12:15

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) $\Omega = \{1, 2, \ldots, n\}$. 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 $2, \ldots, N - 1$; 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 $1, \ldots, N - 1$, 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.

Предложение. Формула включений и исключений. Для произвольных событий $A_1, A_2, A_3, \ldots, A_n$ верно равенство $P(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum\limits_{k=1}^{n}(-1)^{k-1} \sum\limits_{i_1 < \cdots < i_k} P(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k})$.

Доказательство. Докажем утверждение по индукции. База: $P(A_1 \cup A_2) = P((A_1\ A_2) \cup (A_2\ A_1) \cup (A_1 \cap A_2)) = P(A_1\ A_2) + P(A_2\ A_1) + P(A_1 \cap A_2) = P(A_1) + P(A_2) - P(A_1 \cap A_2)$.

Предположим, что утверждение выполняется для n множеств. Проверим, что оно выполнено и для $n + 1$.

$P(A_1 \cup \cdots \cup A_{n+1}) = P(A_1 \cup \cdots \cup A_n) + P(A_{n+1}) - P((A_1 \cap A_{n+1}) \cup \cdots \cup (A_n \cap A_{n+1})) =$

$\sum\limits_{k=1}^{n}(-1)^{k-1} \sum\limits_{i_1 < \cdots < i_k} P(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}) + P(A_{n+1}) - \sum\limits_{k=1}^{n}(-1)^{k-1} \sum\limits_{i_1 < \cdots < i_k} P(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k} \cap A_{n+1}) =$

$\sum\limits_{k=1}^{n+1}(-1)^{k-1} \sum\limits_{i_1 < \cdots < i_k} P(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k})$. ■

Парадокс распределения подарков

Пусть n человек принесли подарки друг для друга. Затем эти подарки сложили в мешок и каждый наугад вынул из мешка себе подарок. Какова вероятность того, что конкретный человек вынул подарок, который он принёс? Какова вероятность того, что никто не вытащил подарок, который сам принёс?

Пространство исходов состоит из всех возможных перестановок чисел $1, 2, \ldots, n$, причём все перестановки являются равновозможными. Значит вероятность конкретной перестановки равна $\frac{1}{n!}$. Событие, состоящее в том, что конкретный человек вытащил подарок, который сам принёс, состоит из $(n-1)!$ исходов. Следовательно, вероятность такого события равна $\frac{1}{n}$. При больших n эта вероятность стремится к нулю. Можно было бы думать, что

вероятность события: ни один человек не вытащил подарок, который сам принёс, стремится к единице, но это ошибочное мнение.

Пусть A_k - событие состоящее в том, что k-й человек вытащил свой подарок. Тогда $A_1 \cup \cdots \cup A_n$ - это событие, состоящее в том, что хотя бы один вытащил свой подарок. По формуле включения и исключения:

$$P(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{k=1}^{n} (-1)^{k-1} C_n^k \frac{(n-k)!}{n!} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!}.$$

Таким образом, вероятность того, что ни один человек не вытащил подарок, который сам принёс, равна $1 - P(A_1 \cup \cdots \cup A_n) = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \ldots$ и стремится к $\frac{1}{e}$.

Задача про конференцию. В научном центре работают специалисты по 60 различным разделам компьютерных наук. Известно, что по каждому разделу в центре работает ровно 7 учёных, причём вполне может быть, что один учёный является специалистом сразу по нескольким направлениям. Все учёные должны принять участие в одной (и только одной) из двух конференций, одна из которых проходит в Канаде, а другая в Австралии. Оказывается, что всегда можно так распределить учёных по этим конференциям, что на каждой конференции будут присутствовать специалисты по всем 60 направлениям компьютерных наук.

Будем для каждого учёного выбирать конференцию простым подбрасыванием правильной монеты. Для k-го направления рассмотрим событие A_k, состоящее в том, что среди учёных этого направления окажутся и те, которые поехали в Канаду, и те, которые поехали в Австралию. Вероятность этого события равна $1 - 2^{-6}$ (нас устроят все исходы кроме двух, когда все отправились на конференцию в одну страну). Остаётся заметить, что количество событий A_k равно 60 и вероятность каждого события больше $1 - \frac{1}{60}$.

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).**