ВОПРОСЫ ОСНОВЫ(ЗНАТЬ!)

1)Классическое определение вероятности

Вероятность выполнения события А - это отношение числа всех благоприятных равновероятных исходов к числу всех возможных равновероятных исходов. $P(A) = m/n$, где m число благоприятных исходов, n число всех исходов.

Основные свойства вероятности

1. Вероятность случайного события А есть неотрицательное число, заключенное между нулем и единицей, т. е. $0 \leq P(A) \leq 1$.

2. Вероятность достоверного события равна единице $P(\Omega) = 1$.

Случайное событие называется **достоверным** если оно обязательно происходит при данном случайном эксперименте.

3. Вероятность невозможного события равна нулю $P(\emptyset) = 0$.

Случайное событие считается **невозможным** если при данном эксперименте оно не может произойти.

Дополнительно:Теория вероятности изучает неслучайные закономерности массовых случайных явлений. Причем, рассматривает те явления, которые могут быть неоднократно повторены в одинаковых условиях.

Набор условий называется **случайным экспериментом.**

Результаты случайного эксперимента называют **случайным событием или событием** (обозн.: A, B, C).

Случайное событие – это то что может произойти или не произойти в результате ряда экспериментов.

2)Формула полной вероятности

Пусть событие А происходит при происхождении одного из событий: H_1, H_2, …, H_n, которые попарно несовместны и образуют полную группу.

Событие H_k называется гипотезой, тогда и только тогда, когда вероятность события А равно сумме произведения вероятностей гипотез на условную вероятность событий А, при условии выполнения гипотезы.

Тогда формула полной вероятности события А имеет вид: $\mathbf{P(A)}= \sum_{i=0}^{n} \mathbf{P(H}_i\mathbf{)} \cdot \mathbf{P(A|H}_i\mathbf{)}$

Где P-вероятность, A-любое событие

3)Формула Бернулли

Пусть производится n независимых испытаний, в каждом из которых событие A может появиться с вероятностью p или не появиться с вероятностью q =1 – p. В этом случае говорят, что имеет место *схема испытаний Бернулли*.

Вероятность того, что в описанных n испытаниях событие A появиться ровно k раз $(0 \le k \le n)$, вычисляется по формуле Бернули:

$$P_n(k) = C_n^k p^k q^{n-k}$$

Где q-вероятность противоположного события

Вероятность того, что событие A в схеме Бернулли появится не менее m_1 раз и не более m_2 раз, равна $P_n(m_1 \le m \le m_2) = \sum_{k=m_1}^{m_2} C_n^k p^k q^{n-k}$.

Если после независимых испытаний проводимых достаточно большое число раз, то в формуле Бернули появляются большие числа и требуется больший обьем вычислений в этом случае используются **предельные теоремы**

4)Математическое ожидание, дисперсия, отклонение

Математическим ожиданием *дискретной* случайной величины ξ называют сумму произведений всех ее возможных значений на их вероятности:

$$M_\xi = \sum_{i=1}^{n} x_i p_i$$

Математическим ожиданием *непрерывной* случайной величины ξ, возможные значения которой принадлежат отрезку [a; b], называют определенный интеграл

$$M_\xi = \int_a^b x\,p(x)\,dx.$$

Для *дискретной* случайной величины **дисперсия(среднеквадратическое отклонение)** вычисляется по формуле

$$D_\xi = \sum_{i=1}^{n} \left(x_i - M_\xi\right)^2 p_i$$

Для *непрерывной* случайной величины **дисперсия** равна, если возможные значения принадлежат отрезку [a; b]

$$D_\xi = \int_a^b \left(x - M_\xi\right)^2 p(x)\,dx.$$

Среднее квадратическое отклонение (стандартное отклонение)

$$\sigma = \sqrt{D}$$

Дисперсия и стандартное отклонение показывают рассеивание эмпирических данных вокруг среднего арифметического

Дополнительно знать: Случайной величиной называют величину, которая в результате испытания принимает одно и только одно возможное значение, наперед неизвестное и зависящее от случайных причин, которые заранее не могут быть учтены.

Случайные величины обычно обозначают греческими буквами ξ, η, ζ,… или заглавными буквами X, Y, Z,… латинского алфавита, а их возможные значения – строчными латинскими буквами x, y, z,….

Случайные величины делятся на *дискретные* и *непрерывные*.

Дискретной называют случайную величину, если ее возможные значения можно пронумеровать. Дискретная случайная величина принимает изолированные значения.

Непрерывной называют случайную величину, которая может принимать все значения из некоторого конечного или бесконечного промежутка.

Законом распределения случайной величины называется любое соответствие между возможными значениями случайной величины и их вероятностями. Это соответствие можно задать таблицей, графически и аналитически

5)Законы распределения дискретных и непрерывных случайных величин

Законы распределения **дискретных** случайных величин:

-Биноминальный закон

Если вероятности возможных значений дискретной случайной величины ξ вычисляются по формуле Бернулли $p(\xi = k) = C_n^k p^k q^{n-k}$, то распределение называется биноминальным. Числовые характеристики биноминального распределения:

$$M_\xi = np; \quad D_\xi = npq; \quad \sigma_\xi = \sqrt{npq}.$$

-Пуассоновский закон

Распределение Пуассона – это распределение числа появления редких случайных событий, которые могут принимать только два противоположных значения. Это распределение возникает, когда вероятность наступления одного из признаков мала, а число испытаний **n** большое. Если известна вероятность успеха **p** в каждом испытании, то вероятность того, что в **n** независимых испытаниях событие наступит **k** раз. Т.е. это распределение вероятностей случайной величины X с целочисленными неотрицательными значениями k=0,1,2,.., заданное формулой

$$p_k(\lambda) = \frac{\lambda^k}{k!} e^{-\lambda}$$

Его числовые характеристики:

$$M_\xi = D_\xi = np = \lambda; \quad \sigma_\xi = \sqrt{np}.$$

, где

λ – параметр распределения

ξ – вероятность возможных значений дискретной случайной величины

M_ξ – математическое ожидание

σ_ξ – стандартное отклонение

-Геометрический закон

Дискретная случайная величина имеет ***геометрическое распределение*** с параметром , если она принимает значения 0,1,2, ..., m, … (бесконечное, но счетное множество значений) с вероятностями:

$$P_m = q^m p, \qquad \text{где } m = 0,1,2,\dots, \qquad \text{где } 0 < p < 1$$

Вероятности P_m для последовательности значений m образуют геометрическую прогрессию с первым членом p и знаменателем q.

На практике геометрическое распределение появляется при независимых испытаниях с целью получения положительного результата – наступления события *A,* вероятность появления которого =*p.* СВ X – число неудачных попыток – имеет геометрическое распределение. В этом случае имеем:

P{X=0}=P{первая попытка успешная}=p;

$$P\{X=1\}\left\{\begin{matrix}\text{первая попытка безуспешная,} \\ \text{вторая успешная}\end{matrix}\right\} = qp;$$

…

$$P\{X=m\}\left\{\begin{matrix}\text{первые } m \text{ попыток безуспешная,} \\ (m+1) \text{ успешная}\end{matrix}\right\} = q^m p;$$

Ряд геометрического распределения случайной величины имеет вид:

x_i	1	2	3	…	m	…
p_i	p	pq	pq^2	…	pq^{m-1}	…

Дисперсию и среднее квадратичное отклонение случайной величины X вычисляем по формулам:

$$D_X = \alpha_2 - m_X^2 = \frac{2q^2}{p^2} + \frac{q}{p} - \frac{q^2}{p^2} = \frac{q}{p^2}\,;\ \sigma_X = \sqrt{D_X} = \frac{\sqrt{q}}{p}.$$

Законы распределения **непрерывных** случайных величин:

-Равномерные распределение

Равномерным распределением непрерывной случайной величины называется распределение, в котором значения случайной величины с двух сторон ограничены и в границах интервала имеют одинаковую вероятность. Это означает, что в данном интервале плотность вероятности постоянна. Т.е. СВ называется *равномерно распределенной* на [a,b], если её плотность вероятности на этом интервале постоянна, а вне [a,b] равна 0.

1. НСВ ξ имеет ***равномерное распределение*** на отрезке $[a, b]$, если ее плотность распределения постоянна на этом отрезке, а вне его равна нулю:

$$p(x) = \begin{cases} \dfrac{1}{b-a} & \text{при } x \in [a,b], \\ 0 & \text{при } x \notin [a,b]. \end{cases}$$

Функция распределения равномерно распределенной на $[a, b]$ СВ имеет следующий вид:

$$F(x)=\begin{cases}0 & \text{при } x<a,\\ \dfrac{x-a}{b-a} & \text{при } a\le x\le b,\\ 1 & \text{при } x>b,\end{cases}$$

а вероятность попадания этой СВ в некоторый интервал, лежащий внутри отрезка $[a, b]$, зависит только от длины этого интервала и не зависит от его положения:

$$P(x_1<\xi<x_2)=\int_{x_1}^{x_2} p(x)dx=\frac{x_2-x_1}{b-a}, \quad \text{если } a\le x_1<x_2\le b.$$

Числовые характеристики равномерного распределения:

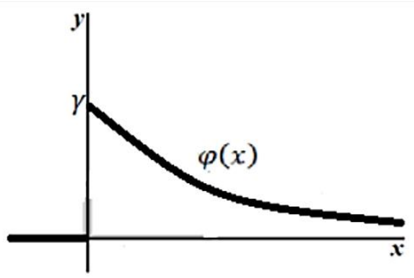
$$M\xi=\frac{a+b}{2},\ D\xi=\frac{(b-a)^2}{12},\quad \sigma_\xi=\frac{b-a}{2\sqrt{3}}.$$

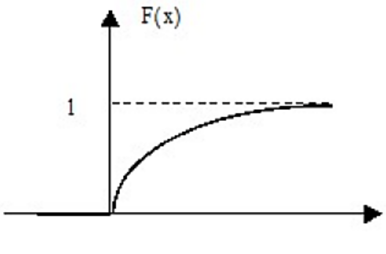
-Показательное распределение

Показательным или экспоненциальным распределением, называется распределение вероятностей непрерывной случайной величины x, которое описывается плотностью с параметром $\lambda > 0$(единственным), в этом и есть его преимущество.

$$p(x)=\begin{cases}\lambda e^{-\lambda x} & \text{при } x\ge 0,\\ 0 & \text{при } x<0.\end{cases}$$

График плотности показательного распределения имеет вид





Функция показательного распределения:

$$F(x)=\begin{cases}1-e^{-\lambda x} & \text{при } x\ge 0,\\ 0 & \text{при } x<0\end{cases}$$

Числовые характеристики показательного распределения:

$$M\xi = \frac{1}{\lambda}, \quad D\xi = \frac{1}{\lambda^2}, \quad \sigma_\xi = \frac{1}{\lambda}.$$

Показательное распределение является одним из основных в теории массового обслуживания и теории надежности. Примером СВ, имеющей показательное распределение, является время ожидания редких явлений: время между двумя вызовами на АТС, продолжительность безотказной работы приборов и т. д.

-Нормальное распределение

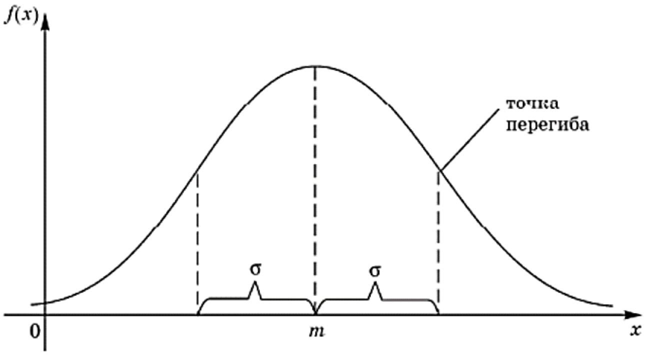
Нормальный закон распределения имеет плотность вероятности

$$p(x)=\frac{1}{\sigma_\xi\sqrt{2\pi}}e^{-\frac{(x-a)^2}{2\sigma_\xi^2}} \quad \text{где } M_\xi=a;\ D_\xi=\sigma_\xi^2$$

$$x\in(-\infty,+\infty)$$

График функции плотности вероятности имеет максимум в точке x=m а точки перегиба отстоят от точки m на расстояние δ.

При $x\to\pm\infty$ функция асимптотически приближается к нулю.



Помимо геометрического смысла, параметры нормального закона распределения имеют и вероятностный смысл. Параметр m равен математическому ожиданию нормально распределенной случайной величины, а дисперсия $D_\xi=\sigma_\xi^2$.

Вероятность попадания случайной величины в заданный интервал $(\alpha;\beta)$ вычисляется по формуле:

$$p(\alpha<\xi<\beta)=\Phi\left(\frac{\beta-a}{\sigma_\xi}\right)-\Phi\left(\frac{\alpha-a}{\sigma_\xi}\right)$$

Вероятность отклонения СВ от математического ожидания на величину δ равна:

$$p\left(\left|\xi-M_\xi\right|<\delta\right)=2\Phi\left(\frac{\delta}{\sigma_\xi}\right)$$

Используя табличные значения ф-ии Лапласа, найдем вероятность

$P(|X-a|\le 3\delta)=\Phi\left(\frac{3\delta}{\delta}\right)=\Phi(3)=0{,}9973$. Эту особенность нормального распределения называют “***правилом трех сигм***”:

Правило трех сигм: Если СВ имеет нормальный закон распределения с параметрами a и δ, то практически достоверно, что её значение заключены в интервале $(a-3\delta, a+3\delta)$

Практическое применение правила 3δ:

1. для оценки нормального распределения

2. для выявления ошибочно полученных результатов

3. для грубого определения δ

6)Эмпирическая функция распределения

Эмпирической функцией распределения (функцией распределения выборки) называется функция $F^*(x)$, которая определяет для каждого значения x относительную частоту события $X < x$:

$F^*(x) = \frac{n_x}{n}$, где n_x – число выборочных значений, меньших x; n – объем выборки.

Основное значение эмпирической функции распределения в том, что она используется в качестве оценки теоретической функции распределения $F(x) = P(\xi < x)$ наблюдаемой случайной величины ξ и обладает всеми свойствами функции распределения дискретной случайной величины:

1) $0 \le F^*(x) \le 1$;

2) $F^*(x)$ – неубывающая непрерывная слева кусочно-постоянная функция;

3) если x_1 – наименьшее, а x_n – наибольшее значения статистического ряда, то $F^*(x) = 0$ при $x \le x_1$ и $F^*(x) = 1$ при $x > x_n$.

Эмпирическая функция распределения $F^*(x)$ является случайной: для разных выборок она получается разной. Если график $F^*(x)$ строится по группированным данным, то скачки происходят в точках, соответствующих серединам интервалов группировки.

1)**Алгоритм Евклида и соотношение Безу*

НОК и НОД, алгоритм Евклида

Наибольшим общим делителем чисел *a* и *b* называется наибольшее число, на которое *a* и *b* делятся без остатка. Обозначается (a,b). Наименьшее общее кратное (НОК) чисел *a* и *b* — это наименьшее число, которое кратно *a* и *b*. Другими словами, это такое маленькое число, которое делится без остатка на число *a* и число *b*.

Для любых чисел A и B, B≠0 существуют такие q, r, что A=B*q+r, причем 0≤r<|B|. q называется полным частным, а r называется остатком от деления, они единственны. **Алгоритм Евклида** – это алгоритм нахождения наибольшего общего делителя (НОД) пары целых чисел.

Алгоритм Евклида заключается в построении ряда чисел следующего вида (|a|>|b|):
$a = b*q_1 + r_1$;

$b = r_1*q_2 + r_2$;

$r_1 = r_2*q_3 + r_3$;

…

$r_{n-1} = r_n*q_{n+1} + 0$

Для нахождения наибольшего общего делителя двух чисел a и b (a и b – целые положительные числа, причем a больше или равно b) последовательно выполняется деление с остатком, которое дает ряд равенств вида

$$a = b \cdot q_1 + r_1, \quad 0 < r_1 < b$$
$$b = r_1 \cdot q_2 + r_2, \quad 0 < r_2 < r_1$$
$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 < r_3 < r_2$$
$$r_2 = r_3 \cdot q_4 + r_4, \quad 0 < r_4 < r_3$$
$$\vdots$$
$$r_{k-2} = r_{k-1} \cdot q_k + r_k, \quad 0 < r_k < r_{k-1}$$
$$r_{k-1} = r_k \cdot q_{k+1}$$

Деление заканчивается, когда $r_{k+1}=0$, при этом r_k=НОД(a, b).

Соотношение Безу — соотношение между парой целых чисел и их наибольшим общим делителем. Это следует из алгоритма Евклида. НОД (a,b) = xa + yb, x, y – коэффициенты Безу. Числа a и b называются взаимно простыми, если их НОД = 1. Из соотношения Безу следует, что для взаимно простых чисел существуют числа au + bV = 1. Для взаимно простых чисел можем записать следующее свойство: 1) Если НОД (a_1, a_2, …, a_k) = d, то $(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_k}{d}) = 1$ – взаимно простые числа. 2) Если число c делит произведение ab, и число c взаимно просто a, то c делит b, записывается c | a*b и (c,a)=1, то c | b. 3) Если a и b1 взаимно простые, a и b2 тоже взаимно простые, то a взаимно просто b1*b2, записывается (a,b1)=1, (a,b2)=1, то (a,b1*b2)=1.

Пусть a, b — целые числа, хотя бы одно из которых не ноль. Тогда существуют такие целые числа x, y, что выполняется соотношение

$$\text{НОД}(a, b) = x \cdot a + y \cdot b$$

$\text{НОД}(12, 30) = 6$. Соотношение Безу имеет вид:

$$6 = 3 \cdot 12 + (-1) \cdot 30$$

- Возможны и другие варианты разложения НОД, например:

$$6 = (-2) \cdot 12 + 1 \cdot 30.$$

Следствие:

Если числа a, b взаимно простые, то уравнение:

$$ax + by = 1$$

имеет целочисленные решения[4]. Этот важный факт облегчает решение диофантовых уравнений первого порядка.

$\text{НОД}(a, b)$ является наименьшим натуральным числом, которое может быть представлено в виде линейной комбинации чисел a и b с целыми коэффициентами[5].

Нахождение коэффициентов Безу эквивалентно решению диофантового уравнения первого порядка с двумя неизвестными:

$$ax + by = d, \text{ где } d = \text{НОД}(a, b).$$

Или, что то же самое:

$$\frac{a}{d}\,x + \frac{b}{d}\,y = 1$$

Отсюда следует, что коэффициенты Безу x, y определены неоднозначно — если какие-то их значения $x_0.y_0$ известны, то всё множество коэффициентов даётся формулой[7]:

$$\left\{ \left(x_0 + \frac{kb}{d},\ y_0 - \frac{ka}{d} \right) \mid k = 0, \pm 1, \pm 2, \pm 3 \ldots \right\}$$

Ниже будет показано, что существуют коэффициенты Безу, удовлетворяющие неравенствам $|x| < \left|\frac{b}{d}\right|$ и $|y| < \left|\frac{a}{d}\right|$.

2)*Решение линейного сравнения

5.1. Решение линейного сравнения. Сравнение степени $n = 1$ имеет вид $a_0 + a_1 x \equiv 0 \pmod{m}$, $a_1 \not\equiv 0 \pmod{m}$, поэтому его можно записать в виде

$$ax \equiv b \pmod{m}, \quad a \not\equiv 0 \pmod{m}. \tag{5.1}$$

Предложение 5.2 (критерий совместности линейного сравнения). *Сравнение 5.1 совместно тогда и только тогда, когда $(a, m) \mid b$.*

Теорема 5.1. *Пусть $ax = b \pmod{m}$ — совместное сравнение первой степени, $d = (a, m)$. Тогда множество X всех решений этого сравнения состоит из одного класса вычетов по модулю m/d:*

$$X = \bar{x}_0 \in \mathbb{Z}_{m/d}, \quad x_0 \text{ — частное решение.}$$

Решить сравнение — значит найти все удовлетворяющие ему x. Если x - решение сравнения, то решением является весь класс вычетов, содержащий x. Сравнения с одинаковым множеством решений называются равносильными. Пусть НОД(a,m)=d. Сравнение ax≡b(mod m) невозможно, если b не делится на d. При b, кратном d, сравнение имеет d решений.

ax≡b(mod m), (a,b)=d. Составим новое сравнение $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, обозначим его $a_d x \equiv b_d \pmod{m_d}$ Пусть его решением будет x0, тогда остальные решения найдутся по следующей формуле: $x_n = x_{n-1} - m_d$ (следует понимать, что x_i вычет по модулю, поэтому в этой формуле можно сменить знак, для удобства), всего решений будет d.

Пример 1.

$12x \equiv 6 (mod\ 18)$

Найдем НОД $(12, 18) = 6$

Перейдем к новому сравнению $2x \equiv 1(3)$

Легко находится $x_0 = 2$

Тогда ответом будет $x_0 = 2, x_1 = x_0 - \frac{m}{(a,m)} = -1, x_2 = -4$

3)Определение и примеры группы, кольца и поля